



Payment Card Security

12-Steps to meeting PCI-DSS Compliance with SafeNet

INTRODUCTION

With the rising incidence of threats to consumer data, and increasing requirements to protect that data, merchants must focus on their security infrastructure. Regulations have been implemented not only by the state and federal governments, but by the credit card industry as well.

Companies are compelled to prove their compliance with these regulations and will be held liable for their failure to do so. While these rules focus on protecting the consumer, they also serve as protection for the merchant, as security breaches can have a far-reaching impact to both a company's finances and reputation.

In 2004, through collaboration of the major credit card companies, the Payment Card Industry (PCI) Data Security Standard was developed to create common industry security requirements. These requirements have also been endorsed by other payment card companies operating in the United States.

SafeNet, a global leader in information security, provides the industry's most comprehensive range of solutions to help companies achieve compliance with the PCI Data Security Standard. Through its own proven set of products, along with an extensive partner network, SafeNet can provide merchants with the assurance that sensitive and valuable cardholder information is protected from all types of threats, and that regulatory compliance is not only being met, but exceeded.

Between January 2005 and June 2007 over 155 million individual records in the U.S. were reported compromised through unauthorized access to data systems, insider wrongdoing, administrative incompetence or theft of computers and other storage media.

WHAT IS THE PCI DATA SECURITY STANDARD?

The PCI Data Security Standard (DSS) was developed through joint effort by the major credit card companies (Visa, MasterCard, American Express, Discover, JCB) in order to establish a standard set of regulations for all members, merchants, and vendors who transmit, process, or store cardholder data. The PCI DSS consists of twelve requirements, which are organized around six basic elements:



Build and Maintain a Secure Network

Protect Cardholder Data

Maintain a Vulnerability Management Program

Implement Strong Access Control Measures

Regularly Monitor and Test Networks

Maintain an Information Security Policy

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

By complying with the PCI Data Security Standard, merchants and service providers not only meet their obligations to the payment system, but also gain the ability to promote their business as adhering to the highest security standards established for handling sensitive cardholder data. Customers demand complete assurance that their account information is safeguarded from all possible threats, and where they put their trust, and their money, will be based on a merchant's reputation for providing a safe and secure place to do business.

SAFENET OFFERINGS FOR THE PCI DATA SECURITY STANDARD

To ensure their compliance with the PCI Data Security Standard, many businesses have turned to SafeNet technology for a solution. To meet these demands, SafeNet offers a range of products, proprietary and through partner alliance.

Here's how SafeNet solutions can help companies achieve compliance with the PCI DSS requirements:

▪ **Requirement 1: Install and maintain a firewall configuration to protect data.**

Although SafeNet does not offer its own firewall product, the majority of firewall vendors embed SafeNet technology into their solutions.

- **Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.**

- **Part 2.3 Encrypt all non-console administrative access.**

This section requires that SSH (Secure Shell), VPN (Virtual Private Network), or SSL/TLS (Secure Socket Layer/Transport Layer Security) is used for Web-based management and other non-console administrative access, including access to Web and databases servers.

SafeNet has a number of VPN or SSL-based solutions that fit this requirement:

- **IPSec Gateways:** HighAssurance 500, HighAssurance 1000, HighAssurance 2000, HighAssurance 4000
- **IPSec/SSL Gateway:** Borderless Access Server
- **VPN Clients:** HighAssurance Remote, SoftRemote, SoftRemote Lite

In addition, SafeNet's two-factor authentication solutions can be used with certificates to further strengthen the process and provide flexibility.

- **Requirement 3: Protect Stored Data**

SafeNet can provide an end-to-end solution with partners, or support specific aspects of this requirement as follows:

- **Part 3.4 Render sensitive cardholder data unreadable anywhere it is stored.**


SafeNet DataSecure® platforms deliver sophisticated capabilities for encrypting sensitive data in databases and applications. These products feature granular encryption, seamless integration, and centralized security management—enabling organizations to eliminate an array of critical security threats, with unprecedented ease and cost-effectiveness. With DataSecure, enterprises can secure the critical data that matters most to their business, including credit card numbers, social security numbers, and other sensitive, personally-identifiable records.

SafeNet offers a family of Hardware Security Modules (HSMs), each designed to protect critical cryptographic keys and accelerate sensitive cryptographic operations across a wide range of security applications. All of SafeNet's HSM devices provide strong cryptography aligned with best practice key management processes and procedures.

- **Part 3.4.1 If disk encryption is used (rather than file or column level database encryption), logical access must be managed independently of native operating system access controls.**

SafeNet's ProtectDrive software encrypts the hard drives of laptops, workstations, and servers—including operating system files—to ensure ultimate protection against unauthorized access of sensitive data. As an added security advantage, integration with SafeNet's iKey® USB token allows enforcement of user access to systems only

At DSW Retail Ventures, hackers compromised 1.3 million cardholder records.



after successful two-factor authentication.

Logical access can also be managed independently through any of SafeNet's two-factor authentication solutions, including USB tokens and smart cards.

- **Part 3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuses**

SafeNet's family of HSMs ensure that all encryption keys are stored in tamper-proof environments and that access to the devices is highly controlled.

- **Part 3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data.**

The architecture of the SafeNet HSMs enforces best practice procedures as described in Part 3.6 for the generation of keys, secure key distribution and storage, changing of keys, dual control of keys, prevention of unauthorized substitution of keys, and revocation of old or invalid keys.

- **Requirement 4: Encrypt transmission of cardholder data across open public networks**

This is similar to requirement 2.3 in that transmitted cardholder data needs to be encrypted using established security protocols, such as SSL, TLS, and IPSec. SafeNet can meet the technology requirements in full through a number of VPN and SSL-based solutions, specifically;

- **IPSec Gateways:** HighAssurance 500, HighAssurance 1000, HighAssurance 2000, HighAssurance 4000
- **IPSec/SSL Gateway:** Borderless Access Server
- **VPN Clients:** HighAssurance Remote, SoftRemote, SoftRemote Lite


In addition, to protect data that is being sent within the organization across private Wide Area Networks (WANs), SafeNet offers several WAN encryptors for a range of circuits, including digital, frame, ATM, SONET/SDH, and Ethernet. Data sent across these networks, unless specifically encrypted on premises, is not encrypted and can be intercepted. SafeNet can demonstrate how unencrypted data can be captured over a SONET fiber circuit.

- **Requirement 5: Use and regularly update anti-virus software or programs**

SafeNet has no offerings for this requirement.

- **Requirement 6: Develop and maintain secure systems and applications**

- **Part 6.3 Develop software applications based on industry best practices and include information security throughout the software development lifecycle**



SafeNet's Sentinel Security Products have protected over 35 million software applications worldwide since 1984 and offer the world's leading range of anti-piracy solutions. Sentinel® RMS is a comprehensive system that dramatically reduces or eliminates many of the costs normally associated with software license management, allowing software vendors to optimize the entire licensing lifecycle.

Sentinel Hardware Keys allow you to carefully control and regulate your distribution channels through the use of Distributor Keys. You can assign and securely imbed encryption keys during the manufacturing process in order to control the creation of licenses through your channels.

In addition, SafeNet HSMs protects the critical cryptographic keys and accelerate sensitive cryptographic operations across a wide range of security applications.

▪ **Requirement 7: Restrict access to cardholder data by business need-to-know**

This requirement mandates that critical data can only be accessed by authorized personnel. SafeNet smart cards and iKey® USB tokens are secure devices that can hold users credentials, such as passwords, keys, certificates, or biometrics. The devices have an open, flexible operating system that can enable other capabilities, such as storing personal information or physical access credentials securely to the device.

SafeNet smart cards and tokens require users to authenticate themselves before initiating any security functions, ensuring that only authorized users can perform the cryptographic functions.

▪ **Requirement 8: Assign a unique ID to each person with computer access**

Not only does this requirement mandate that a unique ID be issued to each person, but that either passwords, token devices, or biometrics be used for authentication. If remote access is necessary, then the requirement further specifies that two-factor authentication must be used.

Storing "digital identities" on a secured device, such as a *smart card* or *token*, is emerging as a preferred method for positive employee identification. SafeNet smart cards and iKey® USB tokens are secure devices that enable positive user identification. Private information never leaves the card and is protected by two-factor security—something that is owned (the smart card) and something that is known (the smart card passphrase).

SafeNet CMS (Card Management System) is a Web-based smart card/token and digital credential management solution for enterprises that is used to issue, manage, and support SafeNet cryptographic smart cards and SafeNet iKey USB tokens for identity-based applications throughout the organization. SafeNet CMS gives enterprise customers a powerful, interoperable, and secure system that reduces the cost of deploying and supporting smart cards and iKeys.

Thieves replaced credit card scanners and downloaded 5 days of account numbers at Albertson's grocery stores. The thieves stole a total of \$100,000 from unsuspecting customers.

- **Requirement 9: Restrict physical access to cardholder data.**
 - **Part 9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies a visitor as non-employees**

SafeNet smart cards can be integrated with various building access technologies in order to function as both an employee's physical and digital ID. The same smart card that is used for network and computer security can be personalized and printed with ID pictures to function as an employee's ID badge. Fitted with a magnetic stripe or RF proximity technology, the card can also be used for door access systems. Smart ID badges can be issued using the same technology that issues standard ID badges today; existing badge printers would simply need to be upgraded to accept the smart card chip.

Further, SafeNet delivers comprehensive capabilities for managing user access, authentication, and access control between application servers and the DataSecure platform. SafeNet offers effective capabilities for addressing these access requirements. The only way to access the DataSecure platform is at the administrator level via a secure Web-management console, a command line interface over SSH, or a direct console connection. The platform can be configured so that individual administrators are granted access only to areas for which they are responsible.

- **Requirement 10: Track and monitor all access to network resources and cardholder information**

SafeNet has no offerings for this requirement.

- **Requirement 11: Regularly test security systems and processes**

SafeNet has no offerings for this requirement.


- **Requirement 12: Maintain a policy that addresses information security for employees and contractors**

In support of this requirement, SafeNet's Professional Services organization can provide a range of *Best Practice* training courses related to Network Security, Identity Management, Key Management, and PKI to assist an enterprise in developing a comprehensive and compliant security policy.

STRONG PRODUCT OFFERING

Strong Authentication

SafeNet smart cards provide some of the most powerful cryptographic PKI token technology available today. SafeNet smart card-based information security products continue to support industry standards, such as PKCS #11 and Microsoft CryptoAPI, allowing for seamless integration with applications and products from leading PKI vendors. SafeNet smart cards perform all sensitive cryptographic functions directly on the card, including public/private key generation, digital signature creation, and cryptographic session key



unwrapping. Unauthorized users have no means of accessing a user's digital credentials without stealing the smart card and guessing the passphrase.

The **SafeNet iKey® USB Token** is a USB-based portable PKI authentication token that generates and stores private key and digital certificate credentials on a device small enough to fit on a key chain. An extension of smart card technology, the iKey simply plugs into any USB port and provides strong user authentication without the need for costly reader devices. The iKey is designed to support a wide range of desktop applications and portable systems. Its low-cost, compact design and standard USB interface make it easier to deploy than smart cards or one-time PIN tokens. Its FIPS Level 2-validated hardware and on-board key generation, key storage, encryption, and digital signing capabilities add high assurance security to client applications.

Card Management System

Deploying and managing smart cards or iKeys and issuing digital identities can be a huge task without the proper tools. **SafeNet CMS** (Card Management System) removes the complexities associated with deploying smart cards/tokens and digital identities, enabling enterprises to quickly leverage the benefits offered by these technologies. Through innovative, policy-based enrolment features, SafeNet CMS significantly reduces the time an enterprise spends issuing and managing smart cards/tokens for geographically distributed users.

Hardware Security Modules


SafeNet's family of HSM products feature true hardware key management to maintain the integrity of encryption keys. Sensitive keys are created, stored, and used exclusively within the secure confines of the HSM to prevent compromise. SafeNet HSMs provide advanced features such as direct hardware-to-hardware backup, split user role administration, multi-person authentication, and trusted path authentication, coupled with proven security and operational deployment experience in some of the largest PKI's in the world.

Virtual Private Networks

IPSec VPN Gateways

SafeNet HighAssurance 500 Gateway is built to meet the scalable demands of today's branch office networks. It provides key security and data management features, including IPSec VPN tunneling, Network Address Translation, and a firewall, while operating at 1.5 Mbps full-duplex. The HighAssurance 500 Gateway supports up to 500 VPN tunnels and a maximum of 1,000 simultaneous secure connections with DES, Triple DES, or AES encryption.

SafeNet HighAssurance 1000 Gateway offers performance and manageability features that drive down the total cost of ownership for network security. Built to meet the scalable demands of today's mid-size office networks, its key security and data management features include IPSec VPN tunnelling, Network Address Translation, and a firewall, while operating at 10



Mbps full-duplex. The HighAssurance 1000 Gateway supports up to 1,000 VPN tunnels and a maximum of 2,000 simultaneous secure connections with DES, Triple DES, or AES encryption.

SafeNet HighAssurance 2000 Gateway is built to meet the scalable demands of today's medium to large office networks. It provides key security and data management features, including IPSec VPN tunneling and Network Address Translation, while operating at 100 Mbps full-duplex. The HighAssurance 2000 Gateway supports up to 10,000 IPSec tunnels and a maximum of 100,000 simultaneous secure connections using DES or Triple DES encryption.

The SafeNet HighAssurance 4000 Gateway is scaleable to meet the demands of today's headquarter and enterprise-class networks. It provides key security and data management features, including IPSec VPN tunnelling. FIPS-certified and operating at GigaBit full-duplex rates, with support for TDES and AES, the SafeNet HighAssurance 4000 Gateway is ideal for regulatory-controlled environments, and provides better performance-to-cost ratios than integrated VPN/Routing solutions. It maximizes cost and time savings by optimizing security, performance, interoperability, and manageability. By enabling companies to move their business communications to the Internet, it helps further reduce costs, increase business opportunities, and provides for secure communication and transactions with employees, business partners, and customers.

IPSec/SSL VPN Gateways

SafeNet Borderless Security Access Server has been designed and built specifically to satisfy the demanding requirements of enterprises that have a need to quickly implement a secure access control solution. Built on a high performance 1U appliance with a hardened OS, the SafeNet Borderless Security Access Server provides secure remote access by integrating IPSec and SSL VPN technology, strong user authentication, multi-dimensional authorization, endpoint security compliance checking, and extensive auditing functionality into a single, easily manageable appliance.

VPN Clients

SafeNet SoftRemote is the next generation of remote access client software and offers unparalleled extended features to remote access users connecting to the corporate VPN. Features include Windows XP compatibility, NAT-T support, personal firewall capabilities, and support for strong two-factor authentication through industry-standard smart cards. The combination of several industry-standard technologies provides corporations with an unmatched solution to complete and secure remote access. SoftRemote protects the corporate network from malicious activity by creating a secure tunnel over the Internet, while providing solid protection against Internet thieves and vandals through endpoint security.

HighAssurance Remote is similar to SoftRemote, but is a FIPS-approved solution that provides secure client-to-client or client-to-gateway communications over wireless LANs, TCP/IP networks, and dial-up connections.



Data Protection

SafeNet ProtectDrive is a Common Criteria (CC) EAL2-certified complete drive encryption solution that protects all data (including operating system files) stored on the hard drive of laptops, workstations, or servers. It is commonly employed to protect against disclosure of sensitive information in the case of theft or accidental loss of the hardware device. Additionally, the core encryption modules in ProtectDrive Enterprise Version are FIPS 140-2, Level 2-certified.

Database Encryption

SafeNet DataSecure allows enterprise and government organizations to ensure compliance and limit liabilities by protecting any sensitive data accessed by employees, customers, or third-parties. With SafeNet DataSecure, organizations can protect critical data from both internal and external threats, ensure compliance with regulatory and legislative mandates for security, and mitigate the risk of data theft.

SafeNet DataSecure offers the highest level of database and application security available in a commercial solution, featuring breakthrough performance, high availability, and streamlined implementation.

SafeNet EdgeSecure enables organizations to encrypt sensitive data in hundreds or even thousands of remote locations, and to do so with unprecedented efficiency and cost-effectiveness. EdgeSecure appliances are combined with DataSecure appliances to offer a streamlined, centralized management model for deploying encryption across geographically-distributed locations.

SafeNet KeySecure appliances offer organizations a way to leverage any number of disparate encryption solutions, while enjoying the efficiency and security of a dedicated, centralized appliance for key management. KeySecure offers robust capabilities for managing cryptographic keys throughout their entire lifecycle, including key generation, key import and export, policy management, key rotation, and much more.

Software Protection

SafeNet Unified Software Protection is the world's first fully comprehensive solution for protecting software products throughout the entire product lifecycle. Unified Software Protection is comprised of a suite of products and services that work together to protect and manage the assets of software vendors.

Software vendors no longer need to purchase software protection in individual components from different vendors. Only SafeNet offers an all-inclusive solution, providing complete protection that can be measured and managed as a part of your business operations. Components of SafeNet Unified Software Protection can be purchased individually, or complete protection can be purchased in a single package, providing a comprehensive, cost-effective alternative.



SAFENET OVERVIEW

SafeNet is a global leader in information security. Founded more than 25 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products, including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.