

Addressing PCI Encryption and Key Management End User Challenges

Introduction

The Payment Card Industry (PCI) Data Security Standard was introduced by Visa, MasterCard, American Express and Discover to establish a common set of security requirements for both online and “brick and mortar” merchants and credit card processors. Most burdened by these requirements are Level 1 merchants, those processing over 6 million credit card transactions a year or who meet specific risk qualifications, such as suffering a security breach. Level 1 merchants must be actively audited on a yearly basis by a PCI-approved services organization.

The PCI Standard is one of the most detailed and stringent regulations affecting businesses today. As opposed to broad regulations such as HIPAA and Sarbanes-Oxley, which leave much room for interpretation, PCI is divided into twelve major requirements with specific subsections that state exactly what form businesses’ security programs must take. While this granularity helps organizations better understand their compliance status, the lack of flexibility presents its own set of challenges.

One major challenge for retailers and other businesses in meeting PCI compliance is securing their end-user bases. While other PCI requirements can be centrally managed through IT policy, well-trained administrators and granular auditing, ensuring end-user security requires a well-thought-out, multifaceted approach. With a large employee base, distributed environment, multiple lines of communication, mobile devices and a business that depends on credit card numbers to transact daily business, merchants must take measures to ensure that all sensitive information is encrypted based on PCI requirements with a key management structure to match.

This paper will focus specifically on meeting end-user based key management and encryption requirements for PCI compliance. Specifically, we detail how a comprehensive, easy-to-administer key management structure, backed by automated policy-based encryption for emails and mobile devices, can empower end-users to execute their responsibilities, while at the same time deliver the ability to meet PCI security requirements and provide a stronger level of security.. Specific topics covered include:

- ▶ Overview of end–eser-related requirements and challenges for PCI key management and encryption
- ▶ How to meet PCI challenges cost effectively.
- ▶ Point-by-point table describing how Voltage Security directly addresses Sections 3 and 4 of the PCI Standard.

End-User-Related PCI Encryption and Key Management Requirements

PCI Encryption and key-management requirements primarily fall under sections 3 and 4 of the PCI Standard. Requirement 3: **Protect Stored Data**, sets forth requirements for the secure storage of credit card numbers. Also included in this section of the standard are extensive key-management requirements. Requirement Four, **Encrypt transmission of cardholder and sensitive information over public networks**, sets forth encryption requirements for the types of communications that are considered to be “public networks” including email, remote access and wireless communications.

While the standard provides firm direction for what kinds of communication must be protected and how to protect it, many merchants and credit card processors struggle with meeting these requirements due to the following:

- ▶ Key management is perceived to be expensive and complex.
- ▶ The lack of integrated support for content monitoring and encryption.
- ▶ The perceived lack of usability in email encryption products.
- ▶ The difficulty of creating a centralized management infrastructure for disk encryption at a reasonable cost.

Given these difficulties, organizations determined to successfully manage PCI compliance efforts must:

- ▶ Understand how security affects the organization beyond PCI
- ▶ Make manageability a priority for key management
- ▶ Understand how email encryption fits in to the organization’s security strategy
- ▶ Develop a comprehensive disk encryption management strategy
- ▶ Cost Effectively Meeting PCI Challenges

Addressing PCI Challenges:

Understanding how security affects the organization beyond PCI

Every successful IT security initiative begins with an understanding of what business processes leverage sensitive information or important services, the determination of risk and protection requirements, and the identification of technology to support company requirements. Complying with PCI is no different. Gaining the proper support and funding for your PCI-based end-user security program includes creating a clear picture of how these security measures can benefit your organization beyond PCI.

A strong example for how encryption helps organizations beyond PCI is data breach laws. Consider the case of Card Systems, one of the top providers of payment processing solutions, and how data breach laws directly affected the organization, even through it had passed their PCI audit.

With the PCI standard, the ramifications of a security breach can be incredibly dire as demonstrated by the CardSystems security breach that resulted in the theft of 40 million customer records by cyber criminals. As a result of this event, Visa revoked CardSystems' ability to process credit card transactions; the lifeblood of the firm's business, even though CardSystems had passed its last PCI audit. The final outcome left CardSystems out of business, leaving a strong message that "check-box" PCI compliance is not enough. In addition, this example highlights the importance of how security is now mission critical to the success of a business.

Understanding "security beyond your business" will help you to evaluate and implement the best possible technologies to streamline the PCI compliance process and fulfill your security mission to be a trusted custodian of sensitive data.

Addressing PCI Challenges:

Make Manageability a Priority For Key Management

When it comes to the dynamic world of end users, setting up a PCI-compliant key-management system to support disk and email encryption can seem daunting. Hierarchical public key infrastructures have proven costly and difficult to manage in this environment because key storage, key revocation, changes and auditing require rigorous policy administration and manual processes. Fortunately, rapid advances in key management, such as Identity Based Encryption (IBE), are providing for a secure key-management structure that automates administrative processes, is transparent to end users, and enables easy key revocation and update. But how should merchants evaluate encryption solutions on the market? Critical requirements for selecting a key management system include:

1. The Key Management system must support the dynamic nature of the business. Evaluate the key management system to determine how easily keys can be mapped to your organization's ever-changing user base. While many implementations of complex key management systems have failed due to the inability to cost-effectively support required certificate revocation and changes, many organizations have succeeded through implementing identity-based key-management systems that dynamically perform key generation via a time-based policy that automatically expires and re-generates keys on a regular basis.
2. Evaluate Auditability of the Solution. Segregation of duties is critical to ensure that key management administrators are operating according to policy. An effective key management system will provide logging of issues related to key management.

Addressing PCI Challenges:

Understand how email encryption fits in to the organization's security strategy

The PCI standard requires encryption of emails containing credit card data and sensitive information when transmitted over public networks. Due to past problems of poor usability of email encryption and associated key-management technologies, email encryption can be perceived as difficult to use and difficult to implement. But this is hardly the case today. New usability and management advances in email encryption products have enabled easy-to-implement, policy-based encrypted communications across a diverse user base. To determine the need and architecture for secure email in a merchant environment, organizations must address the following issues:

Understand the current state of email encryption solutions and how it relates to your business processes

In the past, organizations have avoided implementation of secure mail because of the complexity and high management costs of legacy solutions. The advances that make key management more automated, also have solved encrypted email end-user usability issues, subsequently making email encryption available to a diverse user base at a minimal training and support cost.

Without the ability to easily and securely send sensitive email to partners and to customers, organizations have been forced to institute more complex processes to address the need to transfer data. So what does this mean to your business? Without secure email as an option, there is a great chance that your business had to implement a number of manual, complex and/or expensive point processes to enable secure communication within the organization and with business partners and customers. With secure email, however, your business can eliminate these processes and realize solid cost savings through a required compliance investment.

Identifying these processes and implementing a secure mail solution can not only secure the business, but enable stronger and more accessible communication at a drastically lower cost than traditional methods.

Accept that transmission of sensitive email is a reality, regardless of policy

Although policies may state that sensitive data is not to be sent via email, often employees will take the path of least resistance, disregard policy and send credit card numbers and other sensitive data in email. Enabling secure communications in a merchant or business-partner environment will enable workers to expediently achieve their daily tasks while providing an appropriate level of security through automated, policy-based encryption.

Ensure that encryption is automated

To meet PCI requirements, email encryption should not be at the discretion of a large untrained user base. While selective encryption is acceptable for smaller groups of well trained data custodians, organizations should look towards automated, policy based encryption solutions that identify, encrypt and log all sensitive email, especially that containing cardholder data. Many email encryption products now offer tight integration with content-monitoring solutions. These integrated solutions can automatically recognize credit card and other sensitive data, and automatically encrypt outgoing

email, eliminating user error as a cause of inadvertent disclosure of sensitive data. In addition, email encryption products offer enhanced auditing and logging, allowing you to easily demonstrate compliance for email encryption requirements to auditors.

Beware of the hidden costs of blocking sensitive emails

When organizations investigate sensitive email needs, the issue of blocking typically arises. While blocking is a reasonable measure for many emails that contain inappropriate content, blocking emails originating from approved cardholder data custodians can interrupt business processes and significantly impact productivity.

Consider the following scenario of a large distributed merchant that discovered that up to 500 emails with credit card numbers were being sent every day to customers. While determining email encryption needs, this merchant considered leveraging their content-monitoring and filtering solution as a blocking mechanism. Upon blocking a message, an email would be sent to the customer service representative who would then have to go retrieve the email, remove the credit card number and resend. Below are the related costs for two scenarios: Automated blocking vs. automated encryption.

Scenario: Automated Blocking (Send – receive blocking message- read message - remove and resend)

Rep Time Required: 5 minutes per email

500emails*5minutes = 2500 minutes/day or approximately:

42 hours of productivity lost per day

5 work weeks lost per week

260 work weeks lost per year

Assume cost of \$2000 per week per customer service representative – Office space, benefits, salary, vacation

Result: \$520,000 a year in lost productivity

Does not include: Cost of helpdesk calls

Scenario: Automatically encrypt based on credit card data present in email content

Rep time required: 0 extra seconds

Rep Training Cost: \$0 (automated encryption)

Management overhead = \$12,000 per year (.1 FTE)

Cost of solution = \$40,000 per year*

*Costs can be less or more based on implementation.

**Does not include: Cost savings through leveraging Voltage SecureMail
in place of existing processes**

In this case, automated policy based encryption at the gateway would save this organization over \$400,000 per year in costs, protect information in storage and also build positive customer relationships through providing them with a secure method of communicating with service representatives. In addition, the email encryption solution would also support additional PCI and other regulatory compliance initiatives.

Ensure the email solution provides encryption in storage, both locally and anywhere it is stored

Many secure mail gateway solutions provide an encrypted “pipe” via transmission over SSL. While this method provides compliance with **Requirement 4: Encrypt transmission**, it leaves the organization out of compliance with **Requirement 3: Protect stored data**. Organizations should carefully evaluate the nature of the email encryption solution to determine if, sent emails are always stored encrypted and how. This is critical to ensure that information is protected as it is backed up to tape and archived as well as in the user’s sent folder itself. Ensuring this information is encrypted in storage greatly simplifies the auditability and effectiveness of the PCI compliance program.

Place a Premium on Usability

With so many technical requirements in the PCI Standard, it can be easy for IT decision-makers to lose sight of human factors that can affect security. Usability in a merchant environment is critical to extend the reach of encrypted email to employees, customers and business partners. Key usability issues to explore include:

- ▶ Can the solution send encrypted email without download of client software?
- ▶ How intimidating is the encryption process to the end-user?
- ▶ Are key changes and revocation issues left to the user’s discretion?

Addressing PCI Challenges:

Developing a comprehensive disk encryption strategy

With a steady stream of news stories about lost or stolen laptops in the media in recent years, the loss of an employee laptop containing sensitive information is a top risk to merchants. Due to the . A lost PC would not only incur costs due to data breach disclosure laws, but could also incite an in-depth investigation of PCI practices. Implementing comprehensive disk encryption for sensitive data is a logical preventive remedy for this potential liability. However, strategies for encrypting data-at-rest must be developed carefully to avoid loss of data, high overhead of helpdesk calls for technical issues and password recovery, and performance degradation. Important criteria to meet to ensure a successful implementation include:

- ▶ Meets requirements for PCI strong encryption.
- ▶ Ensure minimal performance impact.
- ▶ Enable robust system management that can guarantee control of assets and allow for the demonstration of compliance.
- ▶ Enable directory integration to leverage existing user/machine information for ease of deployment
- ▶ Provide for the ability to recover passwords without a help desk call

Summary

While delivering encryption for PCI requirements and beyond can seem daunting, technology has advanced to the point where key management has become more automated, email encryption is now economically and broadly possible, and disk encryption can be centrally managed. When planning security technology purchases, PCI-covered entities should carefully manage requirements and always look for the ROI and broader applicability silver linings in the PCI cloud. If planned with a eye toward delivering value above and beyond PCI requirements, these technologies will not only demonstrate compliance, but also greatly reduce the risk of a successful consumer data security breach. These initiatives can also streamline communication throughout the organization, and differentiate customer offerings in ways that can add value and drive increased revenue.

Appendix: Voltage Solutions for PCI

Voltage Security empowers users to perform their responsibilities, travel with data and ensure access to systems while allowing organizations to maintain control over sensitive information. Voltage Security offers easy-to-manage, easy-to-use policy-based encryption for laptops and email that easily integrates with existing infrastructure. The matrix below describes how solutions from Voltage Security can help your organization implement stronger data protection for PCI and beyond.

REQUIREMENT	DETAIL	VOLTAGE SOLUTIONS
REQUIREMENT 3	Protect Stored Data	
3.3	<p>Mask account numbers when displayed. (the first six and last four digits are the maximum number of digits to be displayed)</p> <p>Note that this does not apply to those employees and other parties with a specific need to see full credit card numbers.</p>	<p>With Voltage Identity Based Encryption solutions, account numbers and other sensitive information can be easily masked through encryption to all except those who have a specific need to know credit card numbers. Voltage Security’s unique ability to provide “one click” encryption to groups delivers the most efficient means of controlling access to sensitive information in storage, transit and access.</p>
3.4	<p>Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, backup media, in logs and data received from or stored by wireless networks) by using any of the following approaches:</p> <ul style="list-style-type: none"> • one-way hashes (hashed indexes), such as SHA-1 (Truncation) • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures <p>The MINIMUM account information that needs to be rendered unreadable is the payment card account number</p>	<p>Voltage Security provides strong cryptography, including Triple-DES 128-bit and AES 256-bit, one way hashes with SHA-1 for cardholder information in storage with strong yet easy-to-administer key management processes.</p>
3.5	<p>Protect encryption keys against both disclosure and misuse</p>	<p>Voltage Security protects encryption keys through encrypted transit and storage, as well as the ability to institute a “no storage” policy for private keys, as they can easily and securely be re-generated based on a need to use.</p>
3.5.1	<p>Restrict access to keys to the fewest number of custodians necessary</p>	<p>With Voltage Key Management, access to keys can be restricted to a single custodian. Unlike other key management structures where multiple custodians are required for manual key generation and extensive management of certificate revocation lists, the Voltage System uses existing authentication mechanisms and revokes keys based on time (e.g. one week). The result is completely automated and auditable policy-based key management.</p>

REQUIREMENT	DETAIL	VOLTAGE SOLUTIONS
3.5.2	Store keys securely in the fewest possible locations and forms	Voltage Key Management enables a “storeless” policy for keys. Keys can be automatically generated instead of being maintained on the centralized server. In addition, keys can also be stored locally.
3.6	Fully document and implement all key management processes and procedures, including:	
3.6.1	Generation of strong keys	Voltage Key Generation techniques are fully documented and tested.
3.6.2	Secure key distribution	Voltage distributes keys over secure sockets layer (SSL) only after an individual has authenticated using the corporate defined process for strong authentication
3.6.3	Secure key storage	Voltage does not store private keys on the central key server. Private keys can be stored encrypted locally, or re-generated during each use using existing strong authentication methods.
3.6.4	Periodic key changes	Voltage key management provides automatic key changes without the overhead of certificate revocation lists (CRLs). The automation provided delivers the lowest management and user overhead of any key management system.
3.6.5	Destruction of old keys	Voltage key management capabilities provide automatic destruction of keys either on demand or automatically via integration with active directory and/or an administrator configurable time-based policy.
3.6.6	Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key to reconstruct the key)	Voltage key management delivers the ability to split control over administrative decryption keys.
3.6.7	Prevention of unauthorized substitution of keys	Every action in the Voltage system, including key substitution, is automatically logged to provide separation of duties.
3.6.8	Replacement of known or suspected compromised keys	Replacement of compromised keys can easily be performed on demand, without the difficulty of CRLs.
3.6.9	Revocation of old or invalid keys (mainly for RSA keys)	Voltage solutions do not require key revocation, as keys are automatically regenerated (e.g. weekly) based on the organizational policy

REQUIREMENT	DETAIL	VOLTAGE SOLUTIONS
REQUIREMENT 4	<p>Encrypt transmission of cardholder and sensitive information across public networks</p> <p>Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit</p>	
	<p>4.1 Use strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks</p>	<p>Voltage Security solutions encrypt all information in transit, including SecureMail and FTP using standardized encryption algorithms, including SSL.</p>
	<p>4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless LAN. Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.</p>	<p>Voltage SecureMail provides the foundation to support a consistent policy of encrypting emails that contain credit card numbers over wireless networks.</p>
	<p>4.2 Never send cardholder information via unencrypted email.</p>	<p>Voltage SecureMail provides the ability to encrypt email on demand, or automatically based on policy, including recognition of cardholder information in emails and attachments.</p>
REQUIREMENT 5	<p>Use and regularly update anti-virus software or programs.</p> <p>Many vulnerabilities and malicious viruses enter the network via employees' email activities. Anti-virus software must be used on all email systems and desktops to protect systems from malicious software.</p>	<p>Voltage SecureMail seamlessly integrates with Anti-Virus software to automatically scan encrypted messages and attachments for malicious software.</p>
REQUIREMENT 7	<p>Restrict access to data by business need-to-know</p> <p>This ensures critical data can only be accessed in an authorized manner.</p>	
	<p>7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.</p>	<p>Voltage SecureDisk and SecureFile limit access to cardholder information based on groups, or individual users.</p>
	<p>7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.</p>	<p>Voltage SecureFile encryption capabilities can serve as a mechanism to restrict access to files based on individual users or groups.</p>