Improving Data Security and PCI Compliance through Key Management Controls
Table of Contents

Introduction

Executive Summary 5
Leveraging this White Paper 5

Business Impact: Data protection and the Impact of PCI DSS

Regulatory Oversight and the PCI Data Security Standard 6
Consequences of Non-Compliance 6
Repeating the Benefits 7
Encryption and Manual Management Challenges 8
Industry Movement and Best Practices 8

Technical Impact: Enterprise Key Management and PCI DSS

Enterprise Key Management 10
PCI DSS and Key Management 11
Private Key Management 12
PCI DSS and Security Vulnerabilities 13
Beyond PCI: Key Management Recommendations 16

PCI DSS and the Venafi Solution

The Venafi Systems Management Approach 17
Venafi Encryption Director 18

PCI DSS Requirements and the Venafi Solution Details 20

Conclusion 25
Executive Summary

Introduction

Organizations of all sizes and industries maintain extensive financial, customer and mission-critical business data. When sensitive information is misused or compromised, organizations often pay a heavy price. Recent high-profile security breaches have cost organizations millions in revenue and lost opportunities. These fears, along with new security standards and regulations, have driven IT professionals to deploy encryption more broadly.

In this model, the encryption keys used to secure data become the figurative “keys to the kingdom.” The key (and not the data itself) becomes the entity that must be safeguarded. Efforts to manage these keys manually, however, represent a significant security risk and become operationally challenging, especially as encryption is deployed across disparate systems and applications. A much broader, systems management approach is required.

Such an approach includes automating the creation and management of encryption keys and certificates, configuring the applications that use them and providing comprehensive tools to monitor, control access and report on the status of each component being managed. Venafi invented the industry’s first holistic, enterprise-wide encryption management platform to help organizations simplify the management of encryption keys and certificates across their diverse operating and infrastructure environments.

Leveraging this White Paper

This white paper is broken into four sections in an effort to provide information pertinent to different users and their needs, including business, technical and PCI DSS regulation-specific sections. Readers need not read the entire document, but can browse and consume only those sections that address their functional responsibilities and interests. By reading this piece, you will learn how to achieve compliance and better protect data through true enterprise key management, while improving data security, operational efficiency and audit readiness.
Data protection and the Impact of PCI DSS

Regulatory Oversight and the PCI Data Security Standard

With the proliferation of sensitive data and in a world of increasingly sophisticated and malicious hackers, organizations must recognize the imperative for digital security and protect sensitive data wherever it resides or moves. Encryption is a critical element of any security strategy and is widely leveraged to protect data, combat emerging threats and satisfy a growing body of government and industry regulations. Yet managing the increasing key and certificate volumes has reached a tipping point as enterprises increase encryption deployments to better safeguard information. Poorly managed, lost or stolen encryption keys can lead to failed audits, data breaches and system downtime.

A series of industry regulations and government directives have sprung up in an effort to reduce costly breach and fraud incidents and to protect consumers. The Payment Card Industry Data Security Standard (PCI DSS), launched in 2005 by a consortium of the world’s largest credit card issuers, is the industry’s response to credit card misuse and sensitive data loss. The standard was developed to encourage and enhance cardholder security by stipulating consistent data security measures and guidelines, and establishes a body of common processes and precautions that governs the handling, storage, processing and transmission of cardholder data.

The Payment Card Industry’s Data Security Standard and other regulations like it mandate numerous controls around the protected data, including the management of and access to cryptographic keys. How are these keys protected against loss, misuse or theft? These become especially important questions given that the majority of data breaches are executed from inside organizations.

PCI DSS is intended to protect cardholder data wherever it moves or resides, ensuring that merchants and service providers achieve and maintain the highest levels of information security. The standard has direct applicability for both data in transit and stored data. The PCI security standards council provides testing procedures and a compliance assessment tool for auditing and reporting purposes. All merchants and service providers are required to comply with the standard, including financial institutions, processors, merchant service providers and third-party service providers. The standard is administered by the Payment Card Industry (PCI) Security Standards Council. The PCI DSS is not an audit, but rather a set of guidelines that must be followed to achieve certification.

Consequences of Non-Compliance

Non-compliance can be costly and places organizations at great risk, leaving the business and its customers and partners vulnerable. When information protected by PCI DSS is mismanaged or compromised, organizations are subject to severe consequences, including fines ranging from $250,000 to more than $20 million.

In addition, organizations experience increased card processing fees and can lose their ability to accept payment cards. Additional costs include less tangible damages like loss of trust, employee dissatisfaction and reputational erosion—consequences likely to have a far more significant impact on an organization’s bottom line.

Some companies are dragged into compliance kicking and screaming, but there’s nothing like the prospect of brand reputation damage and lawsuits to get them to do what’s necessary to secure systems and respond properly when there is a breach.3

The cost of preventative measures—including automated management tools—is often far less than the total cost of a breach, particularly when long-term costs like lost business opportunities are considered. According to The Ponemon Institute’s 2009 Cost of a Data Breach study, “The investment required to prevent a data breach is dwarfed by the resulting costs of a breach. With average breach costs totaling $6.6 million, the return on investment (ROI) and justification for preventative measures is clear.” If nothing else, fines and other financial incentives make a strong business case for a PCI compliance program.
Reaping the Benefits

Organizations that understand and implement the security measures required by these new standards not only avoid costly fines, but also can reduce the risk of an actual data loss or breach. Implementing management systems for controlling the new tools also improves operational efficiency and reduces downtime through improved processes.

As is the case with any regulation or standard, achieving PCI compliance may seem like a daunting, even insurmountable task. At its core, however, the standard is nothing more than a set of security best practices. Companies that institute programs to better protect cardholder data can also leverage and extend these efforts throughout their business, ensuring that other sensitive customer, employee and partner data is better protected.

As part of their overall PCI security efforts, compliant organizations often reap the benefits of enterprise-wide encryption and associated encryption key management strategies. When properly deployed and managed, security-conscious organizations protect their data more effectively—and at far less cost—than their counterparts with less mature practices. The way to improve business results and to reduce exposure, data loss and financial expense is to increase compliance and risk management competencies and implement best practices. The more mature these practices are, the better the business results will be.

Recent research supports this view. In its annual IT Governance, Risk and Compliance report, the IT Policy Compliance Group outlines the business and security benefits of organizational compliance programs. According to their research, data protection efforts are paying leading organizations big dividends. In fact, firms with the most mature IT compliance, data protection and access management practices generate an average of 8.5 percent more revenue than similar companies operating in the middle of the normative range.5

---

Figure 1 — Many of the world’s leading organizations have quantified the business value of enterprise-wide, holistic approaches to encryption key and certificate management. To learn more, download Making the Business Case for Systems Management for Encryption from www.venafi.com/collateral_library or request a copy from a Venafi salesperson. The document reviews the challenges of encryption management, proposes systems to alleviate these problems and provides a series of ROI formulas to calculate the associated hard and soft costs. See Figure 2 for a sampling of the formulas.
Encryption and Manual Management Challenges
Independent of industry or organizational size, encryption is widely accepted as the best-practice approach for securing data. When the data is properly protected with encryption—and when encryption keys are properly managed—sensitive data is safe from loss, misuse and fraud. According to many state breach laws, once credit card information and other personally identifiable information (PII) is protected with cryptographic functions, then, even if a breach occurs, it becomes a non-event and need not be reported since the data remains inaccessible.

Regulations, executive mandates and departmental security policies have driven IT professionals to deploy encryption more broadly. Yet managing the increasing key and certificate volumes manually without simultaneously increasing the staff to manage the impacted systems and assets exposes new security threats. Encryption is critical in protecting data and ensuring compliance, but encryption technologies—especially certificates and the associated keys—require regular maintenance, monitoring, rotation and secure distribution for encryption systems to function properly. The increased operational burden exposes additional vulnerabilities, caused either by human error or by malicious insiders with unfettered access to the keys.

When data is protected by encrypting it with a key and a certificate (an asymmetric key pair), the private key becomes the data that must be protected. If the private key is not well managed and protected, the risk of data loss or theft increases dramatically. This threat becomes particularly acute when data is protected by keys that reside in a container or “keystore” (or on multiple keystores) with shared access. The keys that protect the data are often accessible to multiple administrators with no audit or access controls, and are often distributed widely and insecurely within organizations. This places organizations at greater risk of a data loss or breach.

Yet traditional approaches to encryption lifecycle management have proven limited, especially when keys and certificates are deployed across disparate systems, applications and business silos. Simply encrypting the data is not enough to ensure compliance with the PCI data security standard or to pass audits. And yet, organizations have begun to rely solely on the Payment Card Industry’s Data Security Standard—or any other industry or government regulation—alone to safeguard their data.

Recent events demonstrate that organizations can be held liable for PCI security compliance failures, even when they have been found fully compliant with the standard. A passed PCI audit is no guarantee of secure data. Organizations must be aware that privileged-access insiders can cause substantially more damage than outside hackers. Security audits should be conducted regularly, and should not be limited to items required by PCI DSS.

The PCI standard also requires that cryptographic keys be appropriately generated, secured, managed and monitored with proper access controls. In order to maintain compliance effectively, management systems should, at a minimum, allow administrators to set policies, enforce the application of those policies and audit ongoing operations against those policies.

Industry Movement and Best Practices
Enterprise key management and accompanying initiatives have been among the most “hot-topic” IT and security trends in recent years. Yet, according to industry analysts, large organizations with vast encryption deployments are overly focused on protecting data and managing the encryption keys within specific technology silos (such as databases, file servers and endpoints).

To be successful, they need to view the encryption management challenge more holistically. Organizations should evaluate more enterprise-focused encryption management solutions. Such solutions must address key and certificate lifecycle management across the entire infrastructure, independent of the encryption provider, encryption asset, application or operating environment.

In order to better support the management of these broad encryption deployments—and to reduce the cost of managing encryption—leading organizations will leverage solutions that increase automation and provide a more centralized, heterogeneous, and secure approach to key and certificate lifecycle management.

Automated, cost-effective enterprise data protection solutions are now available to secure data both within an organization and among business partners. Centralized management of encryption solutions allows information protection to be aligned with corporate security policies and regulatory or business-partner mandates. A holistic approach to data protection – at rest, in motion and in use – allows security best practices to be automatically enforced throughout the enterprise."

A much broader, systems management approach is required that accounts for the diverse systems, platforms and applications that exist throughout the infrastructure. Such an approach will, by necessity, include automating the generation, distribution and management of keys and certificates, configuring the applications that use them and monitoring and reporting on the status of each component being managed with logging and audit trails.

Venafi invented the industry’s first enterprise-wide encryption management platform that helps organizations manage, monitor and provision keys and certificates across their diverse operating and infrastructure environments and on different certificate authorities (CAs). See the “PCI DSS and the Venafi Platform” section for more information.
Figure 2 — Above are five of the eleven ROI formulas contained in the document Making the Business Case for Systems Management for Encryption, which addresses some of the common challenges associated with encryption management and regulatory compliance. These formulas should be used to determine the hard and soft return on investment of implementing a systems management approach to key and certificate management.
Enterprise Key Management and PCI DSS

Enterprise Key Management

For years, security practitioners have employed a sequence of well-defined, manual steps for managing encryption. To manage encryption keys, including both symmetric and private key encryption (PKI), the following, basic steps are required (see Figure 3):

- First, a key or a key pair must be generated
- Next, the key or key pair is stored to ensure it is secured
- Backup copies of the key(s) are often made
- The key or keys must then be distributed for use
- Finally, the key(s) must be rotated

A closer, more nuanced investigation, however, reveals challenges with implementing this model (see Figure 4). In most cases, companies do not have the luxury of starting at “ground zero” with their key management initiatives. Rather, typical organizations already have large key and certificate volumes that are deployed throughout their environments. Enterprise key management solutions must, from the outset, be able to discover where encryption assets exist across the infrastructure—from the desktop to the datacenter.

The following is a more detailed, step-by-step outline of the required processes for encryption key lifecycle management:

1. **Discover**: A critical first step is to determine where keys and certificates have been deployed.
2. **Generate**: New and renewed keys must be generated and systems should support the central generation of keys. Key lengths and algorithms should be determined at this stage via pre-defined policy.
3. **Store**: Keys must be stored in keystores (software- or hardware-based) and aliases, labels, and key IDs used to identify keys within keystores should be tracked so that multiple keys can be stored and managed in the same keystore.
4. **Distribute**: Keys must be distributed from the keystore to the applications, platforms and devices that will use them, to encrypt data. The keys must be properly secured and protected from loss and/or misuse as they are moved throughout the infrastructure.
5. **Archive/Backup**: Keys must be backed up to a secure location to assure rapid recovery. Access to backed-up keys should be controlled through policy, access rights, and secret encryption keys.
6. **Rotate**: Keys should be periodically rotated based on expiration dates and best practices. Reviews and approvals should occur at each step in the rotation process.
7. **Alert**: One of any organization’s biggest challenges is ensuring that the right people are notified when encryption key or system issues arise. The notifications should be customizable and allow for automated escalations.
8. **Monitor/Validate**: Once keys are deployed, the health and operation of those keys and corresponding encryption systems must be monitored.
9. **Control Access**: The access to and responsibility for individual keys should be assigned to separate administrators to achieve Separation of Duties (SoD) requirements. Granular rights should enable security measures like dual control for separation between individuals responsible for configuration and those who review and approve specific operations on keys.
10. **Initialize/Manage Keystore**: There are a wide variety of keystores in use to store keys on platforms and applications. Each has different configuration parameters, security options, and best practices for management.
11. **Configure Application**: In addition to managing the keystore, it is critical that each application is properly configured for encryption.
12. **Index (Metadata)**: Organizations must be able to apply metadata to their keys for tracking. This information can include department, business application, business owner, key purpose, key lifetime, cost center, etc.
The same steps are required for managing all types of encryption, including certificates, symmetric, asymmetric (public/private keys), and even password. These requirements apply to lifecycle management as a whole and must be performed—either manually or automatically—in order to maintain a successful and secure encryption environment. If encryption keys are not deployed and managed correctly, the risk of negative results (breaches, system downtime) are increased within the systems and applications that leverage the encryption.

Manual approaches to key lifecycle management make it difficult to implement and enforce policies or execute workflows. Equally challenging is the requirement to generate audit logs, especially on legacy systems or on applications where minimal management capabilities exist. Ideally, key management activities should be automated centrally (except on HSMs), including the key generation, distribution, archiving, recovery, rotation, and other operations. This ensures better alignment with corporate policies and industry requirements.

PCI DSS and Key Management
PCI DSS has been a key driver in security-related initiatives in recent years. The standard has led to vast encryption deployments, which have generally been combined with limited, manual key-management implementations. Most of these deployments, however, are focused narrowly on departmental security needs and/or specific technology implementations and tend to leverage the (typically minimal) native key management tools provided within a given encryption system.

The PCI standard provides guidelines for achieving and maintaining compliance. Six primary requirements called “control objectives” are broken further into twelve specific sub-requirements. The technical requirements for verifying PCI compliance are discussed in detail in the sections that follow, particularly as they apply to cryptographic key management functions. See the “Solution Details” section for specific PCI requirements and sub requirements and the associated challenges of manual management.

Requirements 3.5 and 3.6 of Section 2 provide specific language that defines how encryption keys are to be managed to achieve compliance. The standard states:

“Requirement 3.5: Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.”

“Requirement 3.6: Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.”

Note that the standard does not distinguish or suggest priority treatment between symmetric and private key management. Both key types must be properly secured in order to be PCI DSS compliant. The management of symmetric keys is commonly referred to as key management. Such an understanding, however, does not take into account the true nature of the key management discipline.
As industry pundits and auditors are aware, true enterprise key management solutions will also address the full lifecycle management of asymmetric keys (public-private key pairs) and the certificates required for encrypting data in motion and applications that use encryption for authentication. The PCI data security standard makes this broader, holistic perspective regarding key management explicit.

PCI requirement 3 mandates proper key management to protect against “both disclosure and misuse” and must be fully “documented and implemented” for all key types. PCI DSS does not distinguish between symmetric and asymmetric keys and the management requirements of the standard apply equally to both. See the “Solution Details” section for more information.

Private Key Management

Two of the twelve so-called “digital dozen” PCI DSS requirements apply specifically to the use and proper management of SSL certificates and the private keys they rely on to ensure protection of data in transit (see Figure 5 for common use cases where private keys and certificates are used to protect credit-card data in the infrastructure). Specifically, requirement 2.3 states that administrators must: “Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.”

Requirement 4.1 states: “Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are: The Internet, Wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).”

The two most terrifying words to those involved in encryption are key management (KM)…. If your encryption effort is being driven primarily by compliance requirements, KM becomes even more important. It has often been said that effective KM is as important as protecting the data itself.”

These requirements mandate that data in motion must be protected from unauthorized access using the SSL/TLS, IPSEC and other encryption protocols. Transactions that come either from credit card swipe terminals or over the Web via a browser and that require access to the data for processing must be protected in this way to ensure compliance and security. SSL is the de-facto standard in use to protect the data as it is transmitted, and relies on certificates and their associated private keys.

Section two of the PCI standard mandates that cardholder data be encrypted when stored or transmitted over open networks. The data is protected as long as the decryption or private key is protected—as the encrypted data cannot be decrypted and consumed without the key. A lost or mismanaged key can mean that companies may become locked out from their own data.

Most organizations today manage these encryption keys manually. Here is a list of the typical steps an administrator must perform to generate a key pair (which includes a private and public key) and obtain the needed certificate:

• Create a keystore, if one doesn’t already exist
• Assign the keystore(s) a password to protect its contents, including the private key(s)
• Generate a key pair (public and private key)
• Generate a certificate signing request (CSR)
• Submit the CSR to the certificate authority (CA)
• Retrieve the end entity certificate from the CA
• Install needed CA root certificate(s) in the keystore
• Install the end entity certificate in the keystore
• Backup the private key (if deemed necessary)
• Extract the private key and certificate so they can be placed on other systems (e.g. for load balanced configurations)

How do typical organizations secure and manage private keys—the keys required to encrypt data in transit? How are the keys protected against loss, misuse or theft? These become especially important questions given that, according to Gartner, the majority of data breaches are executed from inside organizations. In most cases, the private keys are not being protected.

The PCI DSS requirements for private key management cannot be accomplished in an IT environment that relies on manual processes. There are both security risks and operational challenges when administrators attempt to perform these steps manually.
The problem with administrators performing these steps manually is that doing so exposes organizations to a host of security vulnerabilities, either because the administrators are not following best practices (including those in PCI DSS) or because they have malicious intent. In fact, in spite of best-practice suggestions and specific key management requirements in the PCI standard, private encryption keys are not well protected—both from lax distribution processes as well as the poor and infrequent keystore password rotation practices—and are frequently protected with the same password across hundreds of administrative keystores. Administrators also often have direct access to the keystore(s) and duplicate the keys in them for distribution, and reuse them on other systems and applications throughout the infrastructure.

These keys—shared by all and protected by none—are, in essence, the keys to the kingdom. With them, an insider with privileged keystore access can, working alone or with an outside hacker, gain access to the protected data or even to the authentication (user name and password) information meant to secure it.

**PCI DSS and Security Vulnerabilities**

There are a multitude of use-case scenarios where proper key management is critical to data security and PCI DSS compliance. The following is a common use case. As part of its normal course of business, an organization needs to collect, store, and retrieve customer information. Based on PCI or some other regulation, an organization decides to deploy encryption in two different places: first, on the network where the information is transferred to and from an end user, and second, within the database to encrypt the columns that contain the personally identifiable information (PII).

The encryption within the database is typically done using symmetric key encryption. This is due to both performance considerations as well as being the most common method used by enterprise database vendors. The transmission of the PII data across the network is typically done using industry standard SSL, which uses asymmetric (public and private) key pairs. The threat to the data is that a hacker or malicious insider can access credit card or password data as is transmitted—both inside or outside the firewall—with the private key.

The same security measures used for symmetric key management also need to be followed for private key management. The data protected by private keys and certificates as it is accessed within the infrastructure and beyond organizational boundaries by partners and customers is no less sensitive or valuable than the data at rest protected by symmetric keys. The data is often the same, and the keys used to protect it must be managed with equal vigor and according to the same standards and industry regulations.

Gartner recommends that companies encrypt all sensitive data in transit—even when the data is being transmitted over internal, private networks. This goes beyond what PCI DSS requires, yet is certainly a best practice. The Gartner report also calls out the importance of properly protecting decryption keys, which for data in transit means private keys. This implies an inherent security risk in poorly managed private keys used to secure network traffic. Gartner states:

---

**Figure 5 — Private keys are used extensively to protect credit card data—from the desktop to the datacenter**

---
The PCI standard does not require the encryption of data that flows over private enterprise networks; however, Gartner recommends that card-accepting enterprises consider this measure because it renders the data useless if it’s stolen (unless, of course, the thief has access to the decryption key).”

Gartner

When SSL is used to encrypt data in transit, the certificate is used to authenticate the client to the server and then the public key contained in the certificate is used to encrypt a symmetric key that is used to encrypt the ensuing two-way communication. Thus, if administrators are able to gain access to the “decryption key”, which in this case is the private key that resides on the server, you can access the symmetric key and decrypt the data. This can be done asynchronously if the network stream was captured. Thus, if the wrong person has access to or obtains of copy of that key, then the data is at risk.

The need to protect these keys with good key management and access control systems from bad guys (the “thief” referenced in the Gartner quote above) becomes even more significant in the context of Gartner’s other finding: The Gartner survey found that retailers are mostly concerned about unauthorized access to their systems by insiders, not outsiders…. Insiders typically cause the most damage because they know where to find sensitive corporate personal, financial account and other information” and “As you secure your enterprise systems, remember that insiders with privileged and knowledgeable access can cause significantly more damage than an outside hacker acting alone.” See the section entitled “PCI DSS and Venafi” for more information.

Figure 6 — Typical private key security risks
In most organizations, these private keys are not being protected—from either external or internal threats. In fact, despite best practices and specific key management requirements in the PCI DSS standard, keys are not rotated at appropriate intervals and are frequently protected with the same password across hundreds of keystores.

**Multiple Access Points to Keys:** Because of organizational failover, redundancy, and capability requirements—in both ecommerce and swipe terminal environments—systems must be able to recover and load balance. This requirement necessitates that the same private key and certificate are copied and placed across multiple systems. Generally this means that more than one administrator is involved and all have multiple points of access to the exposed key(s).

**Keystore Passwords Seldom Changed:** Administrators typically share keystore passwords across multiple keystores managed by a team, as well as with system and application owners, as they share oversight of managing a group of systems. These shared passwords are seldom changed. This can lead to individuals having access to private keys for systems that they have no responsibility for managing, and frequently have no authority to use.

**Same Password Used Across Multiple Keystores:** Administrators often use the same keystore password on multiple—sometimes hundreds—of systems across the infrastructure in order to more easily remember them for application and system maintenance. Each keystore contains the “secure” storage and access to the private key. Such a configuration represents a security risk and a violation of the PCI security standard.

**Private Key(s) Manually Shared Between Applications:** Organizations deploy technologies to monitor outbound network traffic (data loss prevention, customer experience and performance monitoring tools, for instance). Each of these monitoring applications must look at the data stream in order to perform its role. If this data is encrypted then the private key must be supplied to the system to allow it to decrypt the data so that it can be read.

**Keystore Passwords Rarely Changed:** Administrators often struggle to comply with corporate password rotation policies for keystore passwords (e.g. change every 90 days) and will often use the same password for years.

See Figure 7 and the “Solution Details” section for more information on how Venafi addresses these challenges.
Beyond PCI: Key Management Recommendations

Beyond the specific PCI DSS applicability of these requirements, there are numerous additional sensitive or regulated data types that pass across the network and over the Internet that should also be properly protected with appropriate private key lifecycle management. For example:

- Insurance information
- Individual healthcare records
- Employee salary and benefits information
- Corporate financial information
- Stock account information
- Corporate trade secrets

Below are several, additional best-practice recommendations that should be considered as organizations safeguard their most critical company data with private keys and certificates:

- **Automate:** Use an automated key and certificate management system that reduces or removes the need for administrators to access keystores directly and the passwords that protect them
- **Rotate Passwords:** Change keystore passwords regularly
- **Separation of Duties and Roles:** Require that separate groups of administrators manage keystore passwords and the systems where the keystores reside
- **Proactively Change Keys:** Change private keys (and the corresponding certificates) each time an administrator who has had access is reassigned or leaves the organization

---

**Figure 7 — Venafi private key management improvements**
PCI DSS and the Venafi Platform
The Venafi Systems Management Approach
At Venafi, we’ve spent the last several years working in tandem with our customers—including some of the world’s most prestigious organizations in financial services, telecommunications, government, healthcare, airlines, restaurants and other industries—to improve the protection of sensitive data with encryption, by learning how to manage the keys and certificates. With our systems management for encryption approach, Venafi helps organizations become compliant with eight of the twelve PCI Data Security Standards (see Figure 8).

Policy and Audit Readiness
To ensure audit readiness and compliance to industry regulations and organizational policies, Venafi allows administrators to maintain a detailed record of all encryption keys and certificates and their locations. Mandatory enterprise-wide encryption policies can be established, enforced and inherited down to individual systems. Divisional, departmental or group policies can also be set and locked in the same manner. Auditors can now track and expect that these requirements are implementable with a platform that offers these controls.

<table>
<thead>
<tr>
<th>PCI DSS Overview</th>
<th>Venafi Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1</td>
<td>Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td>Section 2</td>
<td>Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Section 3</td>
<td>Protect stored cardholder data and encryption keys</td>
</tr>
<tr>
<td>Section 4</td>
<td>Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Section 5</td>
<td>Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td>Section 6</td>
<td>Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Section 7</td>
<td>Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td>Section 8</td>
<td>Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td>Section 9</td>
<td>Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Section 10</td>
<td>Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td>Section 11</td>
<td>Regularly test security systems and processes</td>
</tr>
<tr>
<td>Section 12</td>
<td>Establish an information security policy that and communicate to employees and contractors</td>
</tr>
</tbody>
</table>

Figure 8 — PCI Summary Coverage with Venafi

“The reality is that if you want to encrypt sensitive data wherever it lives or goes, you have to manage hundreds if not thousands of encryption keys and certificates across different applications, platforms, appliances and even organizational silos. Venafi offers an extensible, platform approach to encryption management that spans the environment and enables IT to transcend technical and organizational barriers.”

IBM

Monitoring
The Venafi monitoring capabilities allow administrators to demonstrate that processes are in place to notify owners of certificates and keys whenever issues are detected or attention is required. Certificates and keys can also be assigned to specific owners so they can be reminded of scheduled maintenance. Administrators, managers, business owners and auditors are notified whenever pre-defined policies are modified or violated configuration elements are found. Meta data tags let administrators generate reports by department, cost center, associated applications, regulatory requirement, and so on; as well as maintain forensically durable logs of discovery results and renewal alerts.
Automation
The automation capabilities provided by Venafi protect organizations from costly and time-consuming repeat audits. The Venafi platform automates key and certificate management, thereby removing the need for administrators to access keystores directly and the passwords that protect them. Venafi also allows organizations to remedy non-compliant systems by automatically applying compliant system configurations and inspect systems to ensure they are compliant with external regulations and internal policies.

Logging
With the ability to maintain forensically durable logs of all encryption management operations, security professionals can quickly and easily demonstrate that a standard of due care has been met, and are consistent with safe harbor requirements by illustrating the breadth and depth of encryption deployments and management processes.

Access Control
Venafi’s workflow engine enables organizations to implement access control for certificate and private key issuance and renewal processes that are consistent with internal policies and procedures. Venafi also ensures Separation of Duties and dual-access controls are deployed and met, by enforcing that a different set of administrators manage keystore passwords than the administrators who manage the systems where the keystores reside. Venafi helps enterprises avoid costly follow-up audits, fines, and lawsuits caused by failed audits by regularly conducting self-compliance inspections. See the “Solution Details” section for more information.

Venafi Encryption Director
Venafi Encryption Director is an enterprise encryption management platform that helps organizations simplify the management of encryption keys and certificates across their diverse operating systems and infrastructure environments—from the desktop to the datacenter. Director performs four progressively more-valuable operations, including Discovery, Monitoring, Enrollment and Provisioning. These operations deliver four key benefits to our customers: Enhanced data security; Increased critical system uptime; Improved operational efficiency; and Refined compliance management and reporting.

Discovery
The first step in managing encryption is to determine where keys and encryption certificates are deployed within the enterprise environment, and assess where imminent risks exist (such as which systems are using weak key strengths, which certificates and keys are about to expire, where rogue certificate authorities are in use, etc.).

To utilize the discovery services in Venafi Encryption Director, administrators simply enter an IP address or range of IP addresses and define the relevant ports to inspect. The discovery engine systematically and non-invasively queries each host for certificates (including SSL, SSL-EV, TLS, SMTP and self-signed) from any CA, collects information about the certificates, and presents a status report to the administrator. Users can then easily identify systems that are at risk or require attention, and place those certificates under management. The discovery engine can be configured to regularly survey the infrastructure on a schedulable basis, and alert administrators whenever anything new is found.

Figure 9 — Policy compliance interface in Venafi Encryption Director
Monitoring

Once keys are deployed across an enterprise, it is critical to track the health and operation of those keys and corresponding encryption systems. Venafi Encryption Director performs continuous monitoring and assessment of encryption certificates and technologies—including status and expiration dates—for all root, intermediate root, SSL, VPN, authentication, code signing and other types of certificates.

Administrators are able to enter information about the applications and systems where certificates and keys are deployed for improved inventory and asset management. When a certificate nears its expiration or other issues are encountered, Director automatically sends notifications to the correct owner at user-defined intervals prior to expiration, and will automatically escalate if no action is taken. The contents of the notification messages are fully configurable, ensuring that certificate renewal instructions are provided consistent with organization-specific policies and procedures.

Policy-based monitoring is critical, for instance, when an automated maintenance process becomes delayed or fails. Active monitoring ensures business continuity and helps organizations move quickly and proactively to remedy problems before they result in service interruptions. The built-in reports in Director provide visibility into the status of managed encryption assets, allowing administrators to troubleshoot problems easily, perform operational reviews, verify compliance with corporate policies and regulations, and quickly respond to audit requests.

Enrollment

When the time comes for a certificate to be renewed or for a key to be rotated, Venafi Encryption Director can manage the entire process from start to finish via the native workflow engine. Using its patented technology, Director can concurrently manage the enrollment of encryption certificates by multiple certificate authorities (CAs), and interfaces directly with all leading CAs, including VeriSign, Microsoft and others.

Venafi Encryption Director also provides full, end-to-end automation of encryption lifecycle management—from the CA all the way down to the target application or platform. Director automatically replaces expired certificates and out-of-date keys on the target platforms, replacing formerly manual processes including: key and CSR generation, CSR submission to CAs, approvals at the CA, issued certificate retrieval, certificate installation, operational validation, private key backup, and certificate renewal.

Administrators now find it simple to migrate certificates from one CA to another, and the system allows for multiple approval steps throughout the process. This centralized and automated lifecycle management not only helps reduce administrative costs, but also reduces the errors common in manual work (that often requires nearly thirty steps per certificate renewal) and ensures compliance with corporate policies and regulations.
PCI DSS and the Venafi Solution Details

PCI DSS Section 2 – Do not use vendor-supplied defaults for system passwords

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</td>
<td>There are challenges inherent in managing self-signed certificates.</td>
<td>Venafi helps organizations assure that self-signed certificates are identified and replaced, wherever possible in the infrastructure.</td>
</tr>
<tr>
<td>2.2.4</td>
<td>Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, an unnecessary web servers.</td>
<td>If is difficult to discover web servers and ports that are no longer in use without the ability to discover certificates that have been expired for a long period of time.</td>
<td>Venafi automatically discovers inactive web sites via expired certificates.</td>
</tr>
<tr>
<td>2.3</td>
<td>Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</td>
<td>Private keys and certificates are the basis of encryption and the security of SSL/TLS, IPSEC and other transport encryption protocols. Private keys must be managed based on the requirements outlined in PCI DSS that apply to cryptographic keys. The challenges to meet those requirements with manual management are immense.</td>
<td>Venafi fully automates the management of all SSL/TLS private keys and certificates. The automated management enables the private keys and certificates used to protect non-console administrative access to be secured and managed in compliance with PCI-DSS. Out-of-the-box drivers can also be developed to support the automated management of certificates on other systems, such as VPN.</td>
</tr>
</tbody>
</table>

PCI DSS Section 3 – Protect stored cardholder data

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5</td>
<td>Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.</td>
<td>The direct access to private keys required by administrators in manual management processes increase the possibility of disclosure and misuse.</td>
<td>With Venafi, administrators do not require access to private keys in order to provision and manage them. Separation of duties (thru granular access controls), dual control [via workflow], and automated audit logging further protect keys against disclosure and misuse.</td>
</tr>
<tr>
<td>3.51</td>
<td>Restrict access to cryptographic keys to the fewest number of custodians necessary.</td>
<td>Many keystores only allow a single password per key or keystore, requiring the same password to be shared amongst multiple administrators, requiring that passwords and keys to be changed each time an admin is reassigned.</td>
<td>Access to private keys can be limited to only those who require it. Admin entitlement reports are available to show assigned rights for each administrator.</td>
</tr>
<tr>
<td>3.52</td>
<td>Store cryptographic keys securely in the fewest possible locations and forms.</td>
<td>With manual distribution, keys are transferred via file servers, email, thumb drive, etc, thereby exposing them to loss and misuse</td>
<td>Private keys are only stored at the management server and on the systems where they are used.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
<td>Challenges of Manual Management</td>
<td>Venafi Solution</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>----------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>3.6</td>
<td>Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.</td>
<td>Proper key management procedures are difficult to implement, enforce, and audit manually due to complexity and the distributed nature of organizations.</td>
<td>Venafi provides fully automated key and certificate lifecycle management that requires only approvals for stages where review is deemed necessary by custodians. Organizations are able to configure, implement, monitor, and report on procedures, administrative entitlements, dual control/approvals, audit logging and other aspects of keys management processes. Keys are only stored on Venafi servers and systems where they are needed.</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Generation of strong cryptographic keys.</td>
<td>Organizations rely on administrators to comply with key strength policies and must somehow validate to assure compliance.</td>
<td>Venafi supports policy-based setting and enforcement of key lengths and compliance reporting. Organizations leverage policy-based enforcement and reporting of key strengths.</td>
</tr>
<tr>
<td>3.6.2</td>
<td>Secure cryptographic key distribution</td>
<td>Manual private key distribution is accomplished by transferring password protected files via ftp, email, or other methods using passwords to protect keys in transit, thus increasing the possibility that key are copied and compromised.</td>
<td>With Venafi, keys are securely distributed without requiring administrators to handle keys directly and dual control can be enforced to assure oversight over all distribution operations.</td>
</tr>
</tbody>
</table>
| 3.6.5       | Retirement or replacement of old or suspected compromised cryptographic keys | The direct access to private keys required by administrators in manual management processes dictates that keys should be replaced each time administrators are reassigned. This is operationally untenable for most organizations and consequently rarely performed. | Venafi fully automates:  
- Generation of new key pair,  
- CSR generation,  
- CSR submission to CA,  
- Certificate retrieval from CA  
- Certificate installation  
Fully automated lifecycle management enables replacement at the click of a button if a key is suspected compromised. However, the removal of direct admin access to keys reduces the need to replace private keys when administrators are reassigned. |
| 3.6.6       | Split knowledge and establishment of dual control of cryptographic keys. | Dual control over keystores is difficult to implement. The single password protection of keystores makes split knowledge and dual control difficult if not impossible, to implement. | Because administrators do not have direct access to keys, there is no “knowledge” to split. Dual control can be enforced with required approvals at one or more stages in key management/distribution processes. |
| 3.6.7       | Prevention of unauthorized substitution of cryptographic keys. | On a frequent basis, custodians must manually validate that keys have not be changed. | Venafi automates validation of keystore contents and operation, where possible. |
### PCI DSS Section 4 – Encrypt transmission of cardholder data across open, public networks

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are: The Internet, Wireless technologies, Global System for Mobile communications (GSM), General Packet Radio Service (GPRS).</td>
<td>Private keys and certificates are the basis of encryption and provide the security of SSL/TLS, IPSEC and other transport encryption protocols. Private keys must be managed based on the requirements outlined in Section 3 of PCI DSS.</td>
<td>Venafi fully automates the management of all SSL/TLS private keys and certificates. This automated management enables the private keys and certificates used to protect cardholder data to be secured and managed in compliance with PCI-DSS.</td>
</tr>
</tbody>
</table>

### PCI DSS Section 7 – Restrict access to cardholder data by business need-to-know

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: Controlling access to keystore passwords and private keys is difficult in manual environments. Manual key management often provides administrator direct access to private keys.</td>
<td>Private keys are sensitive “system components.” Controlling access to private keys is difficult in manual environments since keystore passwords must be shared amongst multiple administrators.</td>
<td>With Venafi, granular access controls enable access limited to job requirements. Administrative entitlement reports enable audits of assigned rights.</td>
</tr>
<tr>
<td>7.1.1</td>
<td>Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.</td>
<td>Unique user IDs for each admin and granular access controls enable privileges to be limited to those required to perform job responsibilities.</td>
<td></td>
</tr>
<tr>
<td>7.1.2</td>
<td>Assignment of privileges is based on individual personnel’s job classification and function</td>
<td>Controlling access to keystore passwords and private keys is difficult in manual environments. The password-based protection of many keystores does not meet privileged user ID or least privileges requirements.</td>
<td>Granular access controls enable privileges to be limited to those required by to perform job responsibilities.</td>
</tr>
<tr>
<td>7.1.4</td>
<td>Implementation of an automated access control system.</td>
<td>Access controls are difficult to implement, track and enforce across multiple systems and keystores.</td>
<td>With Venafi, users are required to authenticate themselves and access is controlled. Central automated access control system and entitlement reporting is included.</td>
</tr>
</tbody>
</table>
### PCI DSS Section 8 – Assign a unique ID to each person with computer access

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.5.4</td>
<td>Immediately revoke access for any terminated users.</td>
<td>Manual key management often provides administrators direct access to private keys, making it possible to make duplicate copies. Keys in any password-protected keystores, must be replaced each time an admin is reassigned or terminated in order to revoke access.</td>
<td>Administrators do not require access to private keys in order to provision and manage them in the Venafi systems, so keys and certificates do not need to be changed when administrators are reassigned or terminated. Account access to the Venafi management platform can be revoked immediately with one change or via Active Directory.</td>
</tr>
<tr>
<td>8.5.8</td>
<td>Do not use group, shared, or generic accounts and passwords.</td>
<td>Password protected keystores typically only have a single password, making it impossible to not use shared passwords and comply with this requirement.</td>
<td>Each user in Venafi has a different account. Granular access rights enable separation of roles (e.g. the administration of certificate, private key, each system where they will be deployed, and the administration of keystore passwords can each be assigned to different individuals).</td>
</tr>
</tbody>
</table>

### PCI DSS Section 10 – Track and monitor all access to network resources and cardholder data

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.</td>
<td>Access to keystore passwords and private keys is difficult to track. As keystore passwords are shared with administrators, it is difficult to reliably link “access” to each individual admin.</td>
<td>With Venafi, the assignment of granular access rights guarantees that only the access needed is granted. Administrative entitlement reports enable linking of administrators to the system components and assets to which they have access.</td>
</tr>
<tr>
<td>10.2</td>
<td>Implement automated audit trails for all system components to reconstruct the following events: (specified in 10.2.1-7)</td>
<td>Many keystore management applications do not create or maintain logs of actions, making the implementation of complete audit trails difficult with manual management.</td>
<td>Venafi provides automated audit logging with detailed events logged for each step in the key management process. Audit trails of all operations are automatically created and maintained enabling all critical key management operations and events to be reconstructed.</td>
</tr>
<tr>
<td>10.3</td>
<td>Record at least the following audit trail entries for all system components for each event: User identification, type of event, date and time, success or failure indication, origination of event, identity or name of affective data, system component, or resource.</td>
<td>Manual management procedures are difficult to audit and track. This information is difficult to collect for password protected keystores that are manually managed.</td>
<td>Venafi provides automated audit logging with detailed, automated audit logs for each step in the key management process, including all information specified by this requirement.</td>
</tr>
</tbody>
</table>
### PCI DSS Section 11 – Regularly test security systems and processes

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.5</td>
<td>Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.</td>
<td>Standard file monitoring tools can be used to monitor keystores but must be updated each time a key is changed or they will report false positives.</td>
<td>Venafi performs automated management that enables keystore integrity validation on a regular basis to assure the proper certificates and keys are present, including when keys are certificates are replaced.</td>
</tr>
</tbody>
</table>

### PCI DSS Section 12 – Maintain a policy that addresses information security

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Challenges of Manual Management</th>
<th>Venafi Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>Establish, publish, maintain, and disseminate a security policy that accomplishes the following: 12.1.1 Addresses all PCI DSS requirements.</td>
<td>Documenting and disseminating (i.e. providing training for) a policy for the manual management of private keys that addresses all PCI DSS requirements is a daunting challenge.</td>
<td>Venafi enables policies to be defined, enforced, and tracked. By eliminating most of the manual work involved in managing keys, the dissemination, training, and implementation of policies is possible.</td>
</tr>
<tr>
<td>12.2</td>
<td>Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).</td>
<td>Developing and implementing operational procedures that meet all PCI DSS requirements using manual management will be nearly impossible.</td>
<td>Venafi enables organizations to meet PCI DSS requirements for private key management by automating critical, daily operational security procedures. Notifications are also sent to the appropriate administrators when exceptions are detected.</td>
</tr>
</tbody>
</table>
Conclusion

Encryption is a critical element of any security strategy and is growing in use due to emerging threats as well as new regulations. Organizations are struggling to deploy encryption where it is needed to secure critical resources and effectively manage deployed encryption systems to prevent downtime on mission critical systems.

The PCI Data Security Standard mandates numerous controls around protected data management and access. Demonstrating compliance around these mandates is challenging in situations where no software platform exists. Venafi invented the industry’s first automation platform allowing organizations to more effectively implement and maintain encryption throughout their varied and disparate environments.

Venafi Encryption Director represents the next-generation Systems Management for Encryption platform that assists in applying best practices and compliance-ready solutions to the enterprise.

Learn more about Venafi Encryption Director and our PCI and other compliance-management solutions at www.venafi.com/Director today.