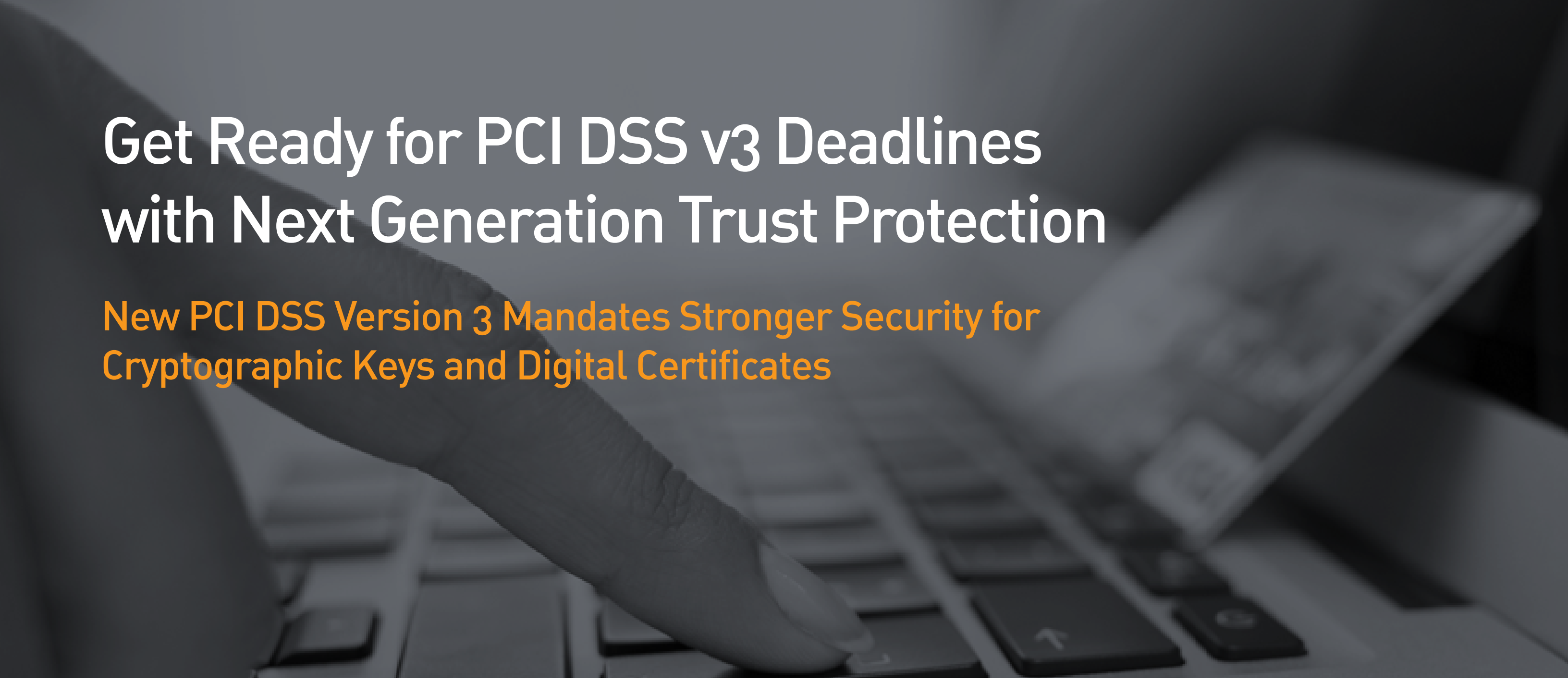

Get Ready for PCI DSS v3 Deadlines with Next Generation Trust Protection

New PCI DSS Version 3 Mandates Stronger Security for Cryptographic Keys and Digital Certificates

The Facts

January 1, 2015
DEADLINE
When most new PCI DSS v3 requirements are due[1]

17K
WIDE REACH
Keys and certificates in an average network[2]

100%
ALREADY COMPROMISED
Companies attacked in the last 24 months using compromised keys and certificates[2]

50%
PERFECT ATTACK VECTOR
According to Gartner, the percentage of network attacks that will use SSL by 2017[3]

The new Payment Card Industry Data Security Standard (PCI DSS) v3 demands more visibility and security over keys and certificates than most organizations can deliver. But the Payment Card Industry Security Standards Council (PCI SSC) understands the importance of keys and certificates that establish the trust on which businesses depend—securing data, keeping communications safe and private, and establishing trust between communicating parties.

Don't Undermine Your CSCs

Why is securing keys and certificates so important now? As we have come to rely more heavily on keys and certificates, cybercriminals have made them more of a target. They want to use keys and certificates to be authenticated and evade detection, bypassing other security controls and keeping their actions cloaked. And keys and certificates are especially attractive when they secure sensitive data such as payment card information. These threats range from exploits of accidental vulnerabilities, like Heartbleed, to advanced persistent threats designed to circumvent and misuse keys and certificates such as APT1, Mask, Energetic Bear, Crouching Yeti, and Zombie Zero—just to name a few.

To learn more visit
Venafi.com/PCI

Organizations layer security controls to create a defense-in-depth approach to protecting their business and meeting PCI DSS compliance. But a lack of key and certificate security undermines a minimum of 40% of the Critical Security Controls (CSCs) listed by the SANS Institute.[4] For example, according to Gartner, 25% to 50% of all traffic in organizations is encrypted.[3] Most security controls, like malware, boundary defenses, and data protection, do not decrypt data, but instead rely on keys and certificates to determine trust.

As organizations struggle to secure their keys and certificates against the latest trust-based attacks, the new version of the PCI DSS is mandating stronger security for cryptographic keys and digital certificates, including inventory capabilities, malware protection, authentication requirements, and more. The vast majority of organizations rely on internal scripts or manual processes to manage their cryptographic keys and certificates, and lack the security, automation, and scalability needed for ongoing PCI DSS audit success.

Achieving PCI DSS v3 Compliance for Keys and Certificates

Many view keys and certificates as a management issue, but with all of the attacks on keys and certificates, organizations need Next Generation Trust Protection to ensure they stay secure. If only one critical key or certificate is compromised, the digital trust an organizations has established is eliminated. Venafi Next Generation Trust Protection delivers key and certificate security, including automated and policy-based tools that help enterprises easily implement regulatory processes and demonstrate PCI DSS compliance.

Table: Summary of New PCI DSS v3 Requirements that Impact Keys and Certificates*

New Req. #	Requirement Description	How Venafi Helps
New Req. 2.4	Maintain an inventory of all in scope system components	Delivers a complete key and certificate inventory with monitoring, baseline, and anomaly detection
Req. 5 Change to Title New Req. 5.1.2	Protect *all* systems against malware Review systems uncommonly affected by malware to see if protection has become necessary	Provides malware mitigation and remediation for keys and certificates by breaking the attack chain: • Continuous monitoring • Policy enforcement • Anomaly detection • Risk evaluation • Replacement of keys and certificates if there is a breach
New Req. 8.6	Certificates for authentication must be assigned to an individual account, not shared	Offers an easy-to-use, web-based, self-service portal for fast deployment of new certificates with strict usage policies
Business-as-Usual Processes	Security controls for compliance should also be part of the business-as-usual security strategy	Delivers fully automated key and certificate protection, automatically remediating so that errors, oversights, and attacks do not become breaches

** Table highlights new PCI DSS v3 changes that impact keys and certificates—does not cover the previously established key and certificate provisions throughout the standard*

To learn more visit
Venafi.com/PCI

Requirement 2.4: Inventory of All Keys and Certificates

New requirement 2.4: Maintain an inventory of all in scope system components

PCI DSS v3 introduces a few new provisions that stress visibility. One such provision is requirement 2.4 which requires organizations to maintain an inventory of all system components in scope of the standard. But most organizations lack the ability to discover all of the keys and certificates that are in their network and then accurately determine which are in scope of the PCI DSS.

On average, there are 17,000 keys and certificates in an enterprise network, but 51% of organizations are unaware of how many certificates and keys are actively in use.[2] And discovering these keys and certificates is usually a manual, labor-intensive exercise, conducted only periodically to achieve compliance. There is no ongoing monitoring to provide on-demand access of this information.

How Venafi Helps Address Requirement 2.4

Venafi rapidly conducts key and certificate discovery to deliver insight into the entire key and certificate inventory. This inventory is maintained through continuous monitoring, establishes a baseline of normal usage, and detects anomalies that alert administrators to potential trust-based attacks. And reports provide on-demand audit support.

Requirement 5: Malware Using Trust-based Attacks

Requirement 5 clarification: Protect all systems against malware

New requirement 5.1.2 : Periodically review systems uncommonly affected by malware to determine if protection has become necessary

With changes to Requirement 5, the PCI SSC wanted to stress that *all* systems should be protected from malware, and even systems uncommonly impacted by malware should be reviewed periodically to determine if malware protection has become necessary. Although keys and certificates may be viewed as a system uncommonly affected by malware, falling under the new requirement, in truth, today they should be considered commonly impacted targets of malware and protected.

Attacks that target keys and certificates go back to at least as early as 2009 and have dramatically increased. For example, malware signed with legitimate certificates more than tripled from 2012 to 2013.[5] Then in March 2014, the severity and scope of Heartbleed put a spotlight on this vulnerability that, for full remediation, requires companies to replace all keys and certificates. According to Ponemon Institute research, every major enterprise has been attacked in the last 24 months using compromised keys and certificates.[2] And experts believe that these attacks are only going to increase. Gartner predicts that "50% of network attacks will use SSL by 2017."[3]

Cybercriminals leverage keys and certificates to create the illusion of trust and bypass traditional defense-in-depth security, undermining critical security controls. These threats underscore the importance of strong security and remediation capabilities for keys and certificates.

How Venafi Helps Address Requirement 5

For protection against malware, Venafi provides malware mitigation and remediation for cryptographic keys and digital certificates by breaking the attack chain. Venafi continuously monitors keys and certificates and enforces policies, enabling organizations to establish a baseline, detect anomalies, evaluate new risks, and refresh and replace the key and certificate infrastructure if there is a breach.

Requirement 8.6: Certificates Used for Authentication

New requirement 8.6: When certificates are used for authentication, they must be assigned to an individual account and not shared

In this latest PCI DSS version, certificates are specifically called out as a means of authentication. But, as stated in the new Requirement 8.6, when using certificates, organizations must be able to assign them to an individual account that prevents shared usage. This requires a certificate security solution that applies strict certificate usage policies while also enabling ease of distribution and maintenance.

How Venafi Helps Address Requirement 8.6

Venafi provides an easy-to-use, web-based, self-service portal as well as flexible policies to allow authorized system administrators, application owners, and end users to quickly request new certificates while also enabling strict certificate usage policies to limit access.

Previously Established Key and Certificate PCI DSS Provisions

In addition to the new requirements, Venafi also covers the previously established key and certificate provisions throughout the PCI standards. Venafi offers a robust policy framework to ensure selection of a secure algorithm; use of strong, protected, securely stored, and securely distributed keys; limitation of access and locations; designation of cryptoperiods; key rotation, retirement, and replacement where needed; and more.

Delivering Business-as-Usual Compliance

The new version of the PCI DSS also emphasizes that security controls implemented for compliance should also be part of the organization's business-as-usual security strategy. This enables organizations to maintain compliance on an ongoing basis.

To deliver business-as-usual security processes, Venafi provides fully automated key and certificate protection for end-to-end provisioning of complex, load-balanced encryption environments. This automation eliminates the vulnerabilities that can arise from error-prone manual processes, rapidly scales new encryption-dependent applications, and provides automatic remediation so that errors, oversights, and attacks do not become breaches.

Accomplishing Successful PCI DSS v3 Audits

The PCI DSS is meant to serve as a minimum security standard. A company's security program should meet and exceed the PCI DSS requirements, achieving compliance as a by-product of implementation. If organizations are not meeting the PCI DSS requirements, not only are they not compliant, they are not secure—providing opportunities for cybercriminals.

Cryptographic keys and digital certificates are the foundation for providing trust in data protection, authorization, and authentication of servers, devices, software, cloud, and privileged administrators and users. The PCI DSS recognizes the importance of securing keys and certificates and includes requirements for them throughout the standard. With Venafi, organizations can meet these PCI DSS v3 requirements—simplifying and ensuring repeated audit success while continually defending against trust-based attacks.

For More Information

Learn more about how Venafi can help you achieve PCI DSS v3 compliance at www.venafi.com/pci.

About Venafi

Venafi is the market-leading cybersecurity company in Next Generation Trust Protection. As a Gartner-recognized Cool Vendor, Venafi delivered the first trust protection platform to secure cryptographic keys and digital certificates that every business and government depends on for secure communications, commerce, computing, and mobility. Venafi customers are among the world's most demanding, security-conscious organizations.

Part number: 1-0026-0914

To learn more visit
Venafi.com/PCI

[1] Source: PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard, Version 3*. November 2013 (PCI DSS v3 goes into effect on January 1, 2015, but a few new requirements are best practices until June 30, 2015.)

[2] Source: Ponemon. *2013 Annual Cost of Failed Trust Repot: Threats & Attacks*. 2013.

[3] Source: D'Hoinne, Jeremy and Hils, Adam. Gartner. *Security Leaders Must Address Threats from Rising SSL Traffic*. Gartner RAS Core Research Note G00258176. December 9, 2013.

[4] Source: Council on CyberSecurity. *The Critical Security Controls for Effective Cyber Defense, Version 5*. February 2014.

[5] Source: McAfee. *McAfee Labs Threats Report*. Fourth Quarter 2013.