Encryption & PCI DSS:

7 Easy Ways to Meet and Exceed Compliance

The PCI DSS (Payment Card Industry Data Security Standard) provides a baseline for businesses large and small who need to protect and process all data associated with credit and debit cards. As part of its most recent standards revisions in April, the PCI Security Standards Council continued to advocate for the adoption of strong, data-centric encryption (or P2PE) to provide the utmost protection against sophisticated business information threats.

PKWARE developers and sales teams have worked with numerous customers to add easy-to-use encryption that covers PCI requirements and extends security for the way today's business share, store and access data. From that experience, PKWARE engineers have crafted these seven suggestions for businesses looking to gain end-to-end data protection while at the same time covering PCI compliance expectations.

1 SECURE WHAT IS MOST VALUABLE

Disk encryption (a.k.a. whole disk encryption, or WDE) satisfies some elements of PCI, but doesn't guard data as it moves across systems, devices and applications.

With disk encryption, data is only protected when the endpoint is powered down; when a laptop or other device running disk encryption is turned "on" and the operating system is running, the data is in motion, unencrypted and vulnerable. Using disk encryption alone leaves gaps in data sharing and access.

SOURCE: PCI DSS V3.1, REQUIREMENT 3, PG. 41

Suggestion: Data-centric encryption gives protection and covers PCI. By emphasizing protection of the information rather than the device, data-centric encryption satisfies PCI and shields data at its core. Additionally, adding multi-factor authentication (MFA, or two-factor authentication) provides an extra access buffer for businesses and administrators handling cardholder information.

2 REMOVE RELIANCE ON SSL AND TLS

PCI requires encryption of cardholder data as it is transmitted across open, public networks. Starting July 1, 2016, encryption methodologies known as "transport layer" encryption (such as SSL or TLS) will not be considered sufficient for PCI data transmission guidelines.

SOURCE: PCI DSS V3.1, REQUIREMENT 2, PG. 34

Suggestion: Existing implementations that use SSL and/or early TLS must utilize a formal Risk Mitigation and Migration Plan if needed prior to the 2016 cutoff date. Rather than rely on transport layer security—which has been the source of such flaws as Heartbleed—focus on encryption of the data itself as part of a wider infosec strategy.

3 SCRAMBLE ALL PAN

Personal Account Numbers (PAN) must be rendered unreadable in whatever system or storage which they reside, including portable digital media, backup media and server logs.

SOURCE: PCI DSS V3.1, REQUIREMENT 3, PG. 40

Suggestion: A few ways PCI supports obscuring or scrambling PAN text include: one-way hashes (based on industry-tested cryptography); truncation; index tokens and pads; and strong cryptography. Going the route of strong cryptography, PCI advises not to use "homegrown" encryption or a proprietary algorithm that isn't vetted along industry standards.

4 PROTECT BEFORE YOU SEND

Never send unprotected PANs through end-user messaging technologies such as email, instant messaging, SMS, or chat. In version 3.1 of its procedures outline, PCI states: “do not utilize these messaging tools to send PAN unless they are configured to provide strong encryption.”

SOURCE: PCI DSS V3.1, REQUIREMENT 3, PG. 42

Suggestion: Ensure PAN is determined to be unreadable or secured with strong cryptography if using end-user technologies to send cardholder data. Establish that processes and procedures are in place to explain that unprotected PANs are not to be sent by end-user messaging services. Additional user certificates give businesses peace of mind that information is accessed by the correct recipient.

5 HIDE THE KEYS

Encryption keys themselves should be guarded from insider threats and external risks. Those keys should be encrypted with the same, strong level of security used to lock down data. Other methods for protecting crypto keys include: store keys in an HSM (hardware security module) or PTS-approved point-of interaction device; or “as at least two, full-length key components or key shares,” in accordance with an industry-vetted methodology.

SOURCE: PCI DSS V3.1, REQUIREMENT 4, PG. 48

Suggestion: While encryption of keys is not mandatory, keys used for the protection of cardholder data must be safeguarded against “disclosure and misuse.” The PCI Security Standards Council offers encryption of keys as a solid key protection practice. When researching key libraries and encryption methods, opt for automatic and industry-vetted asymmetric key encryption.

6 SPLIT CONTROL OVER KEYS

Operations must be managed using split knowledge and dual control if manual clear-text cryptographic key-management operations are used, according to the PCI Security Standards Council. Examples of manual key-management operations include key generation, transmission, loading, storage and destruction. The use of split knowledge and dual control ensure that no single person has access to the whole key, and thus, all related encrypted data.

SOURCE: PCI DSS V3.1, REQUIREMENT 3, PG. 45

Suggestion: Implement a split key tactic where the key components are dictated to at least two people and only those two people have knowledge of their respective key component. For encryption desired for highly sensitive information, a method of “dual control” can be implemented so that at least two people are needed to perform an access function. For true control over protection, seek encryption vendors that can provide key separation in a manner where the vendor also has no unwarranted key or data access.

7 PREVENT “RUNAWAY” CRYPTO

PCI expects businesses to assign unique identification to each person with access, while protecting authentication credentials during transfer. When IDs and related passwords are transmitted unencrypted, they are “readable” and have proven to be a steady source for attacks on business systems and sensitive information.

SOURCE: PCI DSS V3.1, REQUIREMENT 8, PG. 67

Suggestion: By designing identification to each person, businesses and administrators are given a trail of action and responsibility if a breach, leak or hack were to occur. To prevent a “worst-case scenario” incident, businesses should also adopt emergency encryption keys (or “contingency keys”) as well as processes to make sure encrypted data leaving the organization can be scanned by Data Loss Prevention (DLP) systems.

PKWARE’s Smart Encryption solutions armor data at its core, eliminating vulnerabilities everywhere data is used, shared or stored. For nearly three decades, PKWARE has provided encryption and compression software to more than 30,000 enterprise customers and over 200 government agencies. PKWARE continues to innovate its creation, .ZIP, the world’s most widely used file-based open standard.

PKWARE, INC., 201 E. PITTSBURGH AVE. STE 400, MILWAUKEE, WI 53203

WWW.PKWARE.COM