PKWARE® | SMARTCRYPT

MEET PCI DSS REQUIREMENTS WITH SMARTCRYPT

WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of industry-mandated security requirements for credit and debit card transaction processing. PCI DSS applies to stores, online retailers and other organizations, and covers a broad range of security topics including network configuration, data protection, internal control and policy development.

A council composed of major credit card corporations is responsible for maintaining PCI DSS requirements. While compliance is not mandated by United States federal law, some state laws require that payment processors comply with PCI DSS or similar standards.

HOW DOES PCI DSS AFFECT MY ORGANIZATION?

Any organization that processes credit or debit card transactions, or that transmits or stores any form of cardholder data, is required to comply with PCI DSS. Specific obligations can vary based on an organization's transaction volumes. Merchants processing several million transactions per year, for example, are subject to more frequent and more rigorous compliance assessments than smaller merchants. However, all organizations must meet high standards for protection of cardholder data:

- PCI DSS Requirement 3.4 states that an account number should be rendered "at a minimum, unreadable anywhere it is stored." The requirement emphasizes that encryption is a critical component of cardholder data protection and that strong cryptography with key management is recommended.
- Requirement 4.1 states that strong cryptography should be used to "safeguard sensitive cardholder data during transmission over open, public networks."
- Requirement 4.2 states that cardholder data should never be sent in an unencrypted email.

Organizations that fail to meet PCI DSS requirements are subject to a range of penalties including fines, increased transaction fees and cancellation of processing privileges.

HOW DOES SMARTCRYPT HELP MEET PCI DSS REQUIREMENTS?

PKWARE's Smartcrypt platform allows organizations to protect cardholder data with strong encryption, satisfying several PCI DSS requirements.

- Smartcrypt applies persistent data-level protection, using AES strong encryption (up to 256-bit) that exceeds PCI DSS requirements. Encrypted information remains unreadable by unauthorized users, even in the event of a security breach.
- Smartcrypt ensures that even the most sensitive information can be sent via open, public networks without additional layers of protection. Smartcrypt encryption meets the enhanced PCI DSS requirements for data transmission that took effect in July 2016.
- The integration of ZIP compression with strong security not only ensures that information is secure, but it enables portability and efficient exchange of information across all major enterprise computing platforms.

With cross-platform functionality and a robust management console, Smartcrypt makes it easy to apply security policies across the entire enterprise, ensuring that the organization maintains control over encryption activities.

CUSTOMER SUCCESS STORY: PCI DSS COMPLIANCE

A major discount retailer in the U.S. experienced a security breach involving sensitive information from thousands of credit and debit card transactions. An assessment by the Federal Trade Commission revealed weaknesses in the company's data security practices.

After reviewing several possible alternatives, the retailer selected PKWARE's smart encryption solution to encrypt its transaction data in transit and in storage. No other software offered the ability to encrypt data across all of the company's computing platforms, including z/OS mainframes and AIX servers.

Today, the retailer is able to demonstrate full compliance with all PCI DSS requirements, ensuring consumer confidence and avoiding industry and regulatory sanctions. In addition, PKWARE's compression technology has reduced data transit times by 75%, allowing the company to transmit and store its data much more efficiently.

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

CORPORATE HEADQUARTERS

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

+ 1 866 583 1795

EMEA HEADQUARTERS

79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249