White Paper

PCI DSS 4.0: Stronger Mandates, Broader Coverage

Simplifying Compliance Through Architectural Abstraction

Table of Contents

Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive framework that defines requirements for security policy management, procedures, network and software design, and other safeguards to ensure the protection of cardholder data. Although originally designed for bank card information security, PCI DSS recommendations extend to general data protection. Any organization that stores, processes, or transmits confidential data can use the PCI DSS framework as a blueprint for data security policies and practices.

PCI DSS 4.0 marks a significant evolution in payment security. An impactful addition is the acknowledgement that cardholder data remains vulnerable when processed or displayed, meaning that limiting data protection to the storage layer is no longer sufficient by these standards. As of March 31, 2025, new mandates require organizations to extend the protection of cardholder data beyond storage to include data in transit and data in use, requiring primary account numbers (PANs) to be masked when displayed. The standard also requires the regular assessment of cryptographic ciphers and protocols and plans for migrating to stronger cryptography as threats continue to evolve. For merchants, processors, issuers, acquirers, and service providers, these updates mean stronger defenses are required against modern attack vectors, but this also presents new challenges in achieving and maintaining a strong security posture.

Meeting the new compliance requirements can be made easier by adopting a data-centric security strategy that consistently protects critical cardholder data. This paper outlines the key changes in PCI DSS 4.0, their practical implications, and how organizations can employ modern data-centric, crypto-agile approaches to adapt easily to future PCI DSS changes without constant re-work of their applications. Applying application-level data protection with centralized policy management and decentralized execution enables organizations to protect cardholder data, safeguard payment applications, and future-proof systems from evolving threats and regulatory changes.

Evolution

The focus of PCI DSS has evolved from storage-only to full lifecycle protection. Earlier versions of the standard emphasized encryption and access control for stored data. PCI DSS 3.2.1 Requirement 3 mandated disk or file-level encryption, truncation, and strong key management. At the time, version 3.2.1 justified stored cardholder data as the most obvious target. Today, the payment ecosystem has changed. Modern applications now use APIs, cloud services, and distributed architectures, exposing sensitive cardholder data to new threats outside of storage. Attackers exploit vulnerabilities in transmission channels, processing environments, and even within applications, making data in transit and in use just as vulnerable, if not more susceptible, targets than stored data.

PCI DSS 4.0 responds to this reality with a holistic approach. The standard has raised the bar on security by making previously recommended best practices mandatory for compliance.

Key changes include:

- Requiring robust protection of cardholder data not only in storage, but also in transit and in use.
- Mandating periodic reviews and updates of cryptographic ciphers and protocols to eliminate outdated and weak methods.
- Introducing the concept of crypto-agility to ensure that organizations can quickly and seamlessly adapt cryptographic methods as threats and standards evolve.

Requirements Overview

Of the 12 security requirements defined in the latest PCI DSS release, seven directly address data protection, access controls, key management, and crypto-agility. The core security requirements include:

1. Install and maintain network security controls.
2. Apply secure configurations to all system components.
3. Protect stored account data.
4. Protect cardholder data with strong cryptography during transmission over open, public networks.
5. Protect all systems and networks against malicious software.
6. Develop and maintain secure systems and software.
7. Restrict access to system components and cardholder data by business need-to-know.
8. Identify users and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Log and monitor all access to system components and cardholder data.
11. Test security of systems and networks regularly.
12. Support information security with organizational policies and programs.

Requirements that specifically impact cardholder data security can be grouped into four categories:

- Protecting account data in storage and in transit – Requirements 2, 3, and 4 apply to securing the configurations to all system components. Disk or partition encryption alone cannot be the only mechanism used to protect PANs.
- Controlling access to cardholder data – Requirements 7 and 8 address access controls, requiring authorized users to have the right permissions and be authenticated before accessing system components.

- **Logging and monitoring** – Requirement 10 addresses the need to maintain a record of all activity related to cardholder data protection for auditing purposes.
- **Cryptographic strength and agility** – Requirement 12 addresses the assessment of cryptographic ciphers to ensure they are up to the task of protecting cardholder data considering ever-changing threats and ability to quickly adapt through an agile architecture.

Associated with the strong data protection mandates established in the standard, there is also the requirement for robust cryptographic key management using a hardware root of trust. An outline of the above requirements aligned with the state of cardholder data is presented below in Table 1.

Table 1. PCI DSS protection requirements aligned with the state of cardholder data.

State	Requirement	Implications
Data in Storage	• Requirement 3.3.3: Sensitive authentication data (SAD) must be encrypted using strong cryptography. • Requirement 3.5.1.1: All PANs must be hashed to render them unreadable. • Requirement 3.5.1.2: Disk encryption alone is insufficient - additional compensating controls are required.	Application-level data protection with robust encryption and tokenization secures structured and unstructured data the moment it is created so it remains unreadable not only in storage but also in transit and in use.
Data in Transit	• Requirement 4.2.1: PANs must be transmitted only with strong cryptography (TLS 1.2 or higher). • Certificates and keys must be valid, trusted, and not expired or revoked. • All transmission points must be assessed and secured.	Certificate lifecycle management and strong TLS enforcement are now compliance ***requirements***, not recommendations.
Data in Use	• PCI DSS requirements apply to entities with environments where cardholder data and authentication data is not only stored or transmitted but also processed. • Requirement 3.4.1: PANs must be masked when displayed; only users with legitimate business needs may view full PANs.	Organizations must extend controls over sensitive cardholder and authentication data to processing environments using techniques such as in-use encryption, tokenization, masking, and redaction with fine-grained access controls.

Across all the cardholder data protection mandates outlined above, there is also the requirement to document and regularly review the cryptographic cipher suites and protocols in use. Stipulated in Requirement 12.3.3, the standard provides guidance promulgating crypto-agility, the ability to rapidly replace algorithms as threat levels and standards change. Use of crypto-agile architecture not only ensures resilience against advances in computing technology, including post-quantum cryptography, but also enables systems to quickly swap algorithms without having to rewrite applications. Applying this security architecture prioritizes flexibility and abstraction, reducing reliance on hard-coded cryptography.

Meeting the Requirements

PCI DSS 4.0 encourages a risk-based security model to minimize unnecessary exposure of cardholder data. Compliance requires robust controls that protect data not only while in storage but everywhere it moves across the system. A data-centric security approach permits organizations to effectively protect data from the moment it is entered into an application. Techniques used to enable this approach to data protection include:

- **Application-level data protection:** Encrypting or tokenizing data before it touches the storage or transmission layers.
- **Format-preserving encryption (FPE):** Maintaining usability of fields like card numbers while keeping them protected.
- **Digital signing and hashing:** Safeguarding the integrity and authenticity of data.
- **Fine-grained access controls:** Ensuring that only authorized applications and individuals can access clear-text data.
- **Masking and redaction:** Preventing unnecessary exposure of cardholder data to users without the right privileges.

The data-centric security approach reduces risks and PCI DSS audit scope and facilitates compliance while positioning organizations to continue ensuring compliance as requirements evolve over time in response to changing threats.

Security Abstraction

The modern approach to application-level data protection abstracts security functionality from business applications while centralizing data protection policy and decentralizing its execution and enforcement. This architectural model delivers significant advantages including:

- **End-to-end protection:** Cardholder data is safeguarded in storage, in transit, and in use.
- **Operational efficiency:** Centralized security policies enforce consistently, while decentralized execution ensures conformance to local needs for optimum performance.
- **Crypto-agility:** Algorithms and protocols can be updated without having to rewrite applications.

- **Reduced audit scope:** Sensitive data is protected before it enters the PCI DSS environments.
- **Integration with a hardware root of trust:** Cryptographic keys underpin the security of the entire system, and operations need to be anchored in certified hardware, satisfying PCI DSS requirements for tamper resistance and key lifecycle management.

By decoupling security functionality from applications, cardholder data protection becomes agnostic, and this enables organizations to apply a consistent protection policy across deployments, regardless of the platforms, technology stacks, or the programming languages used. And whenever changes to the security policy are required, these can be made in a centralized location rather than having to make changes to each individual application.

Role of Hardware Security Modules (HSMs)

PCI DSS includes requirements for the secure management and safekeeping of cryptographic keys that underpin all encryption and tokenization methods.

HSMs are hardened devices that provide:

- Robust key generation: Ensuring that keys are derived using approved random number generators.
- Tamper-resistant storage: Protecting master and working keys against theft or misuse.
- Standards compliance: Meeting FIPS 140-2/3 requirements for validated cryptographic modules.
- Centralized key lifecycle management: Supporting secure rotation, revocation, and renewal of cryptographic keys.
- Separation of duties: Enforcing operational boundaries between administrators and cryptographic functions.

PCI DSS places strong emphasis on the security of cryptographic keys and the use of FIPS-approved HSMs is a critical part in meeting these requirements. When integrated with an abstraction-based solution, HSMs ensure that all encryption, tokenization, signing, and hashing operations are anchored in certified hardware, satisfying PCI DSS requirements while enabling scalable, crypto-agile data.

Building a Future-Proof Strategy

To align with PCI DSS requirements, facilitate compliance, and prepare for inevitable changes in operational demands and regulatory requirements, organizations must:

- Map the cardholder data lifecycle: Identifying where PANs and SAD are stored, transmitted, and processed.
- Inventory cryptographic assets: Documenting all algorithms, protocols, and keys currently in use.
- Adopt centralized policy management: Decoupling cryptography from applications to simplify updates.
- Implement crypto-agile architecture: Ensuring algorithms and keys can be swapped with minimal disruption.

Aligning requirements to specific objectives and mapping these outcomes will enable organizations to plan for compliance and ensure a future-proof security strategy. A recommended checklist to facilitate this process is presented in Table 2.

Table 2. PCI DSS requirements and how modern data protection addresses them.

Requirement	Objective	How Modern Approaches Address It
No. 2. **Secure configurations.**	Harden all system components.	Centralized security policy ensures uniform hardening across diverse environments.
No 3. **Protect stored data.**	Encrypt and tokenize cardholder data to render it unreadable.	Application-level encryption, tokenization, and HSM-backed key storage protect data in storage and beyond.
No. 4. **Protect data in transit.**	Secure open networks.	TLS 1.2+, certificate lifecycle management and crypto-agile protocols protect data in transit.
No. 7. **Restrict access.**	Limit exposure by business need-to-know.	Fine-grained access controls, masking, and redaction ensure data is only available to users with the right permissions.

No. 8. **Identify and authenticate users.**	Strong identity assurance.	Role-based and multi-factor authentication integration ensure that only authorized users have access to systems and data.
No. 10. **Log and monitor access.**	Detect and respond to misuse.	Centralized audit trails tied to cryptographic operations document what is presented to auditors.
No 12. **Support security policy and programs.**	Ensure governance and agility.	Centralized key and crypto-policy management ensures a strong data security posture.

Conclusion

PCI DSS 4.0 represents a pivotal shift from a storage-centric defense posture to a comprehensive lifecycle-driven security model. As organizations embrace this shift, they will be better prepared for the impact that disruptive technologies such as quantum computing will have on evolving threats and the future regulatory landscape.

By adopting a data-centric security model, abstracting data protection functionality, centralizing policy management, and decentralizing its execution, enterprises can mitigate their exposure to risk, reduce the scope of audits, and facilitate compliance. Building crypto-agility into their security architecture further strengthens security posture and prepares organizations for future challenges.

How Can Prime Factors Help?

Prime Factors helps organizations that store, process, or transmit sensitive information to protect their critical data and facilitate compliance with PCI DSS, including the new expanded requirements dictated by version 4.0.

Prime Factors' EncryptRIGHT is a data security platform that delivers the broad security techniques needed to protect cardholder data in storage, in transit, and in use. It is built on a crypto-agile architecture that abstracts data protection from applications that process, transmit, and store cardholder data. The platform enables enterprises to adapt seamlessly to evolving regulatory demands and future PCI DSS changes, which reduces development costs, minimizes complexity, and simplifies security updates.

EncryptRIGHT delivers:

- Strong data protection leveraging a variety of security techniques, including encryption, tokenization, data masking, hashing, and redaction to protect cardholder data everywhere.
- Granular role-based access controls to ensure that only authorized users with the right permissions have access to the protected cardholder data.
- Robust cryptographic key lifecycle management to ensure critical keys are always protected and available.
- Extensive audit logging and reporting functionality that supports external security information and event management (SIEM) platform integration for traceability and compliance.
- Support for most common operating systems from mainframe to Windows and the ability to deploy on-premises, in the cloud, and across hybrid environments to secure your data in whatever environment(s) works for your business.

Prime Factors built EncryptRIGHT to empower enterprises with the flexibility they need to stay ahead of evolving data protection and privacy challenges. All the functionality delivered by EncryptRIGHT deploys in a single code base that integrates in a few lines of code, without needing developers to be security or cryptography experts.

To experience the benefits of EncryptRIGHT firsthand,

visit **PrimeFactors.com/Free-Trial**.