cpl.thalesgroup.com

THALES
Building a future we can all trust

Get Ready for PCI DSS 4.0 with Thales Data Protection

White Paper

Contents

Introduction

Consumers' payment data continues to be a compelling target for criminals, and IT security defenses enacted to guard these assets continue to be circumvented. Virtually every major financial institution, retailer, and scores of payment processors have been the victims of devastating data breaches. According to the 2022 Thales Data Threat Report – Financial Services Edition[1], 52% of U.S. financial services organizations say they have been breached at any time in their history, with 29% breached in the last year. Additionally, 43% reported an increase in the volume, severity, and/or scope of cyberattacks in the last year.

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) is critical for any business that stores, processes and transmits payment card information and the service providers that enable their businesses. This paper looks in detail at many of the vital PCI DSS 4.0 requirements[2] set out for securing sensitive cardholder data, and reveals how the encryption, key management, and access control products from the Thales Data Protection portfolio address them to streamline your compliance needs.

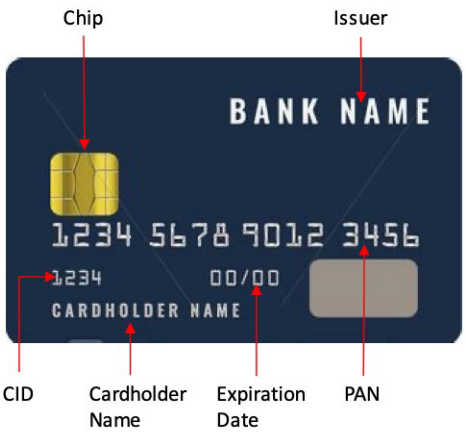
Purpose of PCI Data Security Standard

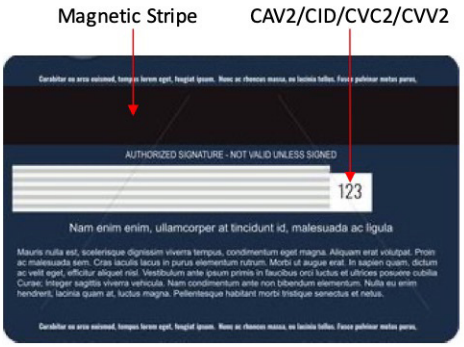
The Payment Card Industry Data Security Standard (PCI DSS) was jointly developed by American Express, Discover, JCB, MasterCard and Visa, back in 2008, to standardize the security controls that need to be enforced by businesses processing payment card data. The last updates to PCI DSS requirements version 4.0 was made in March 2022.

The goal of the PCI Data Security Standard (PCI DSS) is to protect cardholder data and sensitive authentication data wherever it is stored, processed or transmitted. The security controls and processes required by PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. It also applies to all entities that store, process, or transmit cardholder data and/or sensitive authentication data as shown in Table 1 below.

Table 1: Payment Card Account Data

Cardholder Data	Sensitive Authentication Data
• Primary Account Number (PAN)	• Full track data (on magnetic stripe or chip)
• Cardholder Name	• CAV2/CID/CVC2/CVV2
• Expiration Date	• Personal Identification Number (PIN) entered by cardholder
• Service Code	





The Goals for PCI DSS 4.0

The new version of the standard was released on March 31, 2022. Building on the previous version 3.2.1, the top level goals for PCI DSS v4.0 are to:

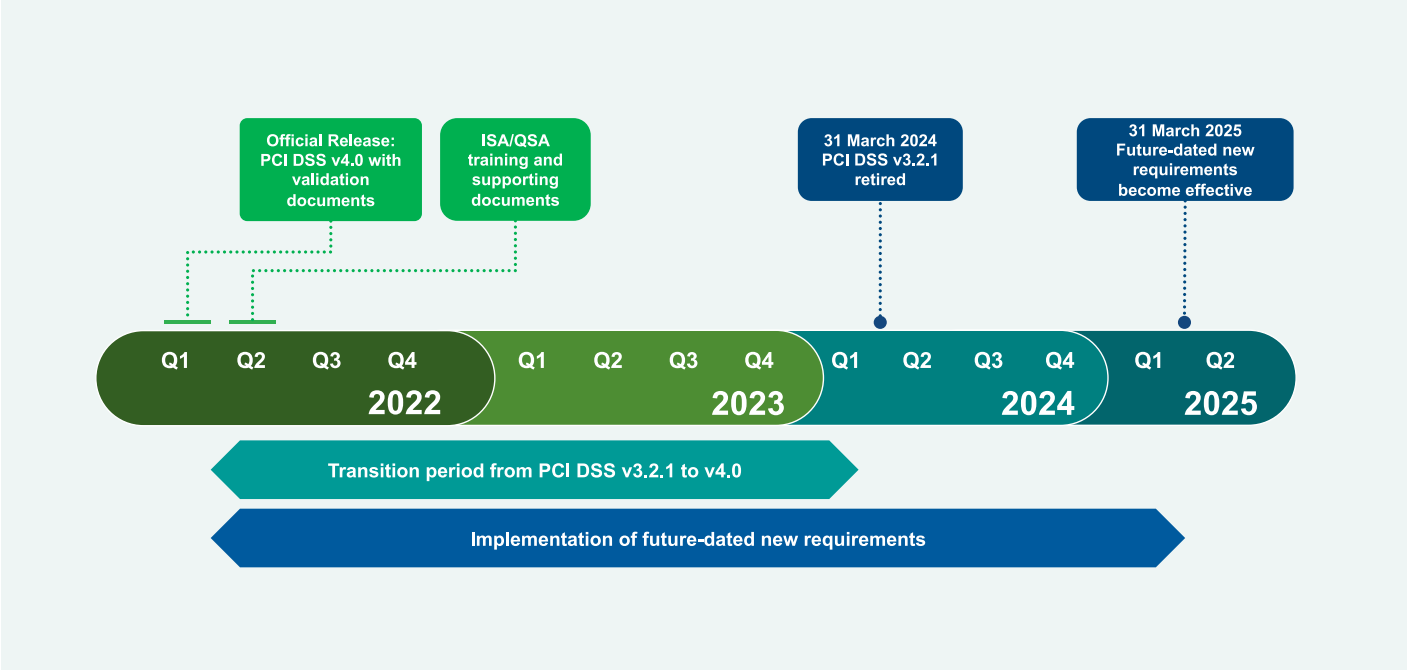
- Continue to meet the security needs of the payment industry
- Promote security as a continuous process
- Add flexibility for different methodologies
- Enhance validation methods

Details about the updates can be found in the PCI DSS v4.0 Summary of Changes document on the PCI SSC website.

When will PCI DSS 4.0 take effect?

PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organizations time to become familiar with the new version, and plan for and implement the changes needed. The implementation timeline is shown in Figure 1.

Figure 1: Implementation Timeline



Why Does PCI DSS Compliance Matter?

PCI DSS compliance is mandatory for financial institutions, online payment processors, merchants that accept payment cards, and any organization that processes payment card transactions, stores or accesses payment card information, and any service providers that enable business anywhere in the card processing eco-system.

If merchants and service providers fail to comply with PCI DSS, then it can result in penalties ranging from $5,000 to $100,000 USD per month. These penalties depend on the volume of transactions, the level of PCI-DSS that the service provider should be on, and the time that it has been non-compliant.

This regulation mandates protection of personal identification information (PIN) and other authentication credentials at ATMs or point-of-sale (POS) terminals, which are used transiently to authorize transactions, but are rarely stored. PCI DSS expands this protection to include other types of data that are more permanent in nature, such as cardholder names, card expiration dates, and primary account numbers (PANs), which are frequently stored for a variety of reasons, often to enhance user experience. Table 2 lists the most common reasons for storing account data according to Qualified Security Assessors (QSAs), who are the people certified by the PCI Security Standards Council to conduct PCI-DSS assessments.

Table 2: Most Common Reasons for Storing Account Data, as Reported by QSAs

Reason for Storing Account Data	Frequency
Chargebacks	83%
Customer service	68%
Recurring subscription	61%
Card reuse	32%
Marketing analytics	19%
Other reasons	2%

Source: Ponemon Institute

Account data can easily find its way into a wide variety of business systems, ranging from transaction processing to customer relationship management, and value-added systems such as loyalty and customer support. The challenge is to protect cardholder data in all these environments to achieve compliance with PCI DSS.

PCI DSS Requirements in a Nutshell

PCI DSS covers technical and operational systems connected to cardholder data and/or sensitive authentication data. It consists of 12 requirements that mirror security best practices defined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework[2]. Table 3 below provides a summary of the PCI DSS requirements addressed by the Thales Data Protection portfolio of products.

Table 3: The PCI DSS Data Security Requirements Addressed by Thales

Goals	PCI DSS Requirements	Addressed by Thales
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls	
	2. Apply secure configurations to all system components	√
Protect Cardholder Data	3. Protect stored account data	√
	4. Protect cardholder data with strong cryptography during transmission over open, public networks	√
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software	
	6. Develop and maintain secure systems and software	√
Implement Strong Access Control Measures	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	
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data	√
	11. Test security of systems and networks regularly	
Maintain an Information Security Policy	12. Support information security with organizational policies and programs	√

For more details on the PCI DSS version 4.0 requirements go to: https://www.pcisecuritystandards.org/document_library

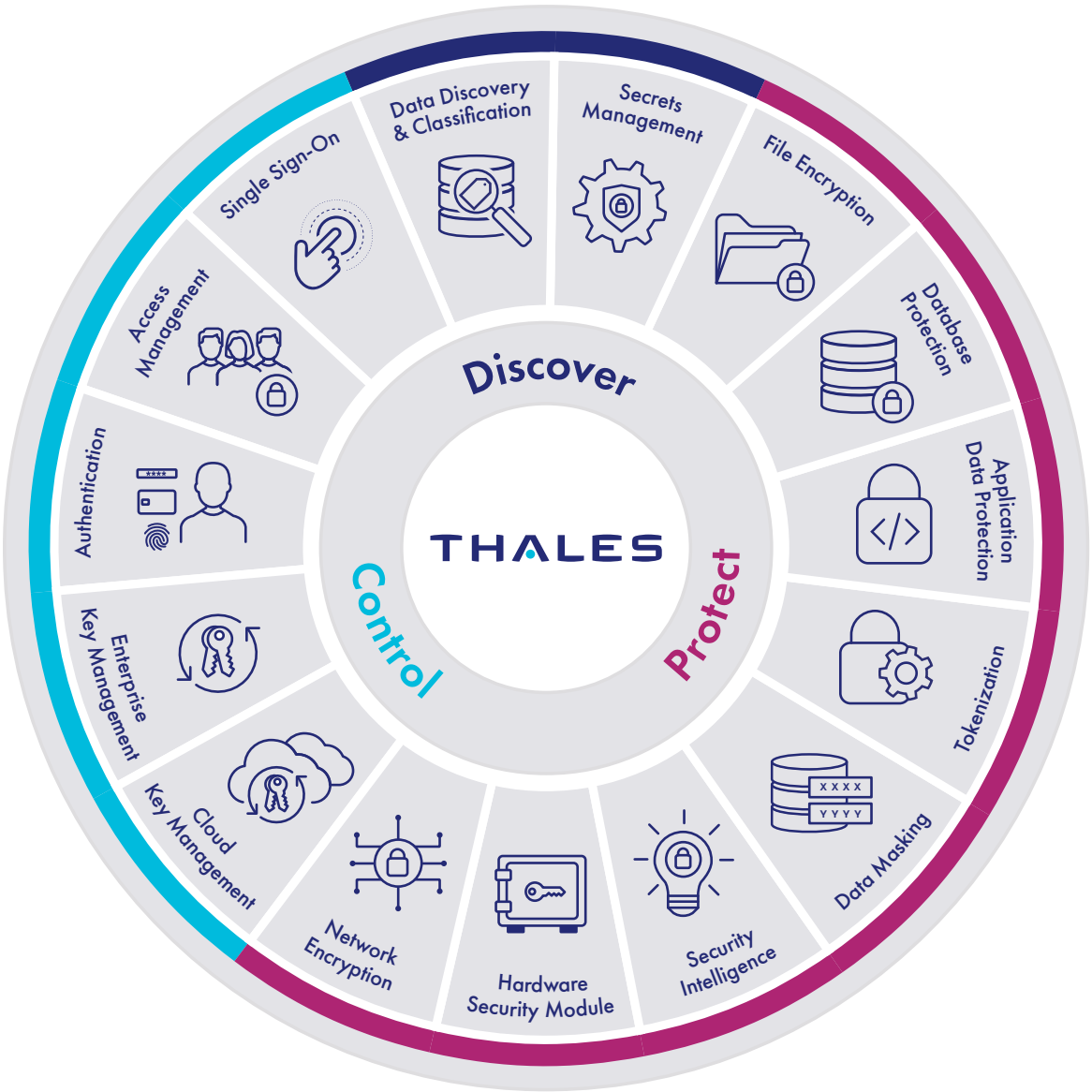
Note that, PCI DSS can ensure data security at the snapshot of time when the compliance audit is conducted, but does not guarantee data protection all the time, unless you continuously monitor your environment and update security controls as your IT infrastructure evolves.

Overview of the Thales Data Protection Portfolio

One of the most common and effective approaches to protecting data is **key management and encryption** – the process of encoding sensitive data so that cyber criminals cannot read it even if they gain unauthorized access in a data breach. This section provides an overview of the Thales data security portfolio of products that can protect data-at-rest and data-in-motion in enterprise infrastructure and business applications, which process cardholder data either on-premises or in private or public cloud.

The industry leading data protection portfolio of products from Thales shown in the Figure 1 below, include key management, tokenization, transparent encryption, application crypto, along with the payment and general purpose hardware security module(HSM) and high speed encryptors (HSEs). In addition, Thales offers products that deliver centralized authentication access control functionality.

Figure 2: Thales Data Protection Product Portfolio and Use-cases Supported



Data-at-Rest Encryption

The CipherTrust Data Security Platform from Thales, features an integrated suite of products that protect any data at rest including any sensitive cardholder data that is required to comply with PCI DSS.

Key Management

CipherTrust Manager (CM) centralized key lifecycle management and user/group-based policy control of encryption keys. It includes a web-based console, CLI, SOAP, and REST APIs. Its available as FIPS 140-2 and common criteria certified virtual and physical appliances.

File-system, Database, and Application Encryption

CipherTrust Transparent Encryption (CTE) delivers data-at-rest encryption at the OS/File-system, database, and application levels. It also encrypts data across multiple clouds, big-data, and container environments. CTE is designed to meet PCI DSS requirements and best practices with minimal disruption, effort, and cost.

Cloud Encryption

CipherTrust Cloud Key Management (CCKM) manages encryption keys for Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure (OCI), Salesforce and SAP to address enterprise needs and meet compliance requirements for managing encryption key life cycles outside of their native environments, enabling you to encrypt cardholder data in multi-cloud environments.

Tokenization with Dynamic Data Masking

CipherTrust Tokenization is offered both vaulted and vaultless, and can help reduce the cost and complexity of complying with data security mandates for PCI-DSS. Static data masking and bulk encryption or tokenizaton is made quick and simple with CipherTrust Batch Data Transformation.

Enterprise Key Management

CipherTrust Manager (CM) enables organizations to centrally provide centralized key management for third-party devices including a variety of KMIP Clients, Transparent Data Encryption (TDE) Agents on Oracle and Microsoft SQL Servers, and Linux Unified Key Setup (LUKS) Agents on Linux Servers.

Cloud Key Management

CipherTrust Cloud Key Management (CCKM) streamlines Bring Your Own Key (BYOK), Hold Your Own Key (HYOK), and native key management for Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure (OCI), Salesforce and SAP while addressing enterprise needs to meet compliance and best practices for managing encryption key life cycles outside of their native environments.

Data Discovery and Classification

CipherTrust Data Discovery and Classification (DDC) enables organizations to discover and classify sensitive data — both structured and unstructured — across the cloud, big data, and traditional data stores. DDC provides a streamlined workflow from policy configuration, discovery, and classification, to risk analysis and reporting — helping to eliminate security blind spots and complexities so organizations can understand risks, uncover gaps, and make better decisions about closing security gaps, prioritizing remediation, and securing cloud transformation.

Data-in-Motion Encryption

Thales offers High Speed Encryptors (HSEs) that provide network independent data-in-motion encryption (Layers 2,3 and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our HSE solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception — all at an affordable cost and without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps.

Hardware Security Modules (HSMs)

PCI DSS-regulated organizations use Thales **Hardware Security Modules** to sign code for hardware payment devices in point-to-point encryption implementations and software used in payment applications to comply with the Payment Application Data Security Standard (PA-DSS). Thales offers the industry leading product family of hardware security modules (HSMs), which are the highest performing, most secure and easiest to integrate in the market today. They act as trust anchors to protect the master keys that encrypt your data and digital identities in a high assurance FIPS 140-2 Level 3-certified, tamper-resistant appliance. Thales offers the following types of purpose-built HSMs:

General Purpose HSM

Luna HSMs come in several form-factors — a network attached appliance, an embedded PCI module, and a portable USB appliance. They can be easily integrated with a wide-range of applications to accelerate general cryptographic operations, secure crypto key life cycles and act as a root of trust for your entire crypto infrastructure.

Cloud HSM

Data Protection On Demand (DPoD) is a cloud-based platform that provides a wide range of Cloud HSM and key management services through a simple on-line marketplace. With DPoD, security is made simpler, more cost effective and easier to manage because there is no hardware to buy, deploy and maintain.

Payment HSM

payShield 10K delivers a suite of payment security functionality including transaction processing, sensitive data protection, payment credential issuing, mobile card acceptance and payment tokenization. It is used throughout the global payment ecosystem by issuers, service providers, acquirers, processors and payment networks.

Authentication and Access Control

Thales SafeNet Trusted Access is an industry leading authentication and access management solution that enables organizations to centrally manage and secure access to enterprise web-based and cloud-based applications. It offers smart single-signon to multiple web-based applications with the broadest range of authentication methods including – One-Time Passwords (OTP), PKI credentials, Kerberos, Google Authenticator, biometric and many more. All authentication methods are available in multiple form factors, such as smart cards, USB token, mobile app, and hardware tokens. Refer to Get Ready for PCI DSS 4.0 with Thales SafeNet Trusted Access -Solution Brief for more information on how SafeNet Trusted Access helps with PCI DSS v4.0.

Addressing PCI DSS Requirements with the Thales Data Protection Portfolio

Requirement 2: Apply Secure Configurations to All System Components

Thales data protection solutions enable you to meet several of the requirements in PCI DSS section 2, as listed in Table 4 below, which pertain to separation of critical primary functions per server with virtualization, using secure protocols to protect insecure services, encrypting all non-console administrative access using strong cryptography.

Table 4: Details of PCI DSS Requirement 2

Requirement	Requirement Description	Thales Data Security solution
2.2.3	2.2.3 Primary functions requiring different security levels are managed as follows: Only one primary function exists on a system component, OR Primary functions with differing security levels that exist on the same system component are isolated from each other, OR Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	Thales solutions enable multi-tenancy and separation of duties to ensure that only authorized users can access the secure data. In addition, **Thales Luna HSM** can be separated into one-hundred cryptographically isolated partitions, with each partition acting as if it were an independent HSM. This provides a tremendous amount of scalability and flexibility, as a single HSM can act as the root of trust that protects the cryptographic key lifecycle of one-hundred dependent applications.
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	Operating at Layer 2, 3 and 4 of the network stack, Thales **High Speed Encryptors (HSE)** encrypt all data that traverses an open network. All the appliances use strong cryptography and are certified FIPS 140-2 L3 and Common Criteria.
2.2.7	All non-console administrative access is encrypted using strong cryptography.	Thales appliances' non-console administrative access is encrypted using strong cryptography to prevent unauthorized access. In addition, Thales **Luna HSMs** can protect TLS server keys and certificates used by products with web-based management, while SafeNet Authentication solutions can be used to provide even greater levels of security for non-console administrative access.

Requirement 3: Protect Stored Account Data

Entities accepting and processing cardholder data are expected to protect it and prevent its unauthorized exposure or use – wherever it is stored locally, or transmitted over internal private networks or external public networks to a remote server or service provider. Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. As listed in Table 5, Thales delivers a variety of encryption solutions that support standard, robust algorithms to ensure the security of sensitive data. These solutions can encrypt cardholder data in files, folders, applications, and databases in both traditional and cloud or virtualized environments.

Table 5: Details of PCI DSS Requirement 3

Requirement	Requirement Description	Thales Data Security solution
3.2	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.	At the end of data retention periods, encryption keys can be destroyed, digitally shredding all instances of the data, no matter where it is currently stored, backed up, or may have migrated. Additionally, to establish a data security program that keeps account data storage to a minimum using controls and technology, organizations need to have visibility into where sensitive data resides. **CipherTrust Data Discovery and Classification** can be used to efficiently locate structured and unstructured regulated data across the cloud, big data, and traditional data stores in your organization so you can prioritize remediation.
3.4.1 & 3.5.1	PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN. PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key-management processes and procedures.	The **CipherTrust Tokenization** solution includes several dynamic data masking options, enabling the ability to display the first six or last four digits of the PAN or the full 16-digit PAN, depending on the role of the user. • One way hashing of the entire PAN based on strong cryptography • Partial masking, that masks a segment of the PAN (first 6 or last 4 digits) • Tokenization and masking, which stores a substitute or proxy for digits in the PAN Strong cryptography underpinned by key management and data access policies.

Requirement	Requirement Description	Thales Data Security solution
3.6.1	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	Thales **CipherTrust Manager and Luna HSM** centrally manage the key lifecycle and access policies in a FIPS certified hardware. The administrative separation of duties, logging, and other capabilities support PCI DSS procedures.
3.6.1.1	Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices.	Thales **CipherTrust Manager** and Luna support this documentation process: • Centralized management of keys with clear description of the key strength and algorithm used for encryption. • It should be able to work with internal or external HSMs that provides the root-of-trust for keys along with an inventory.
3.6.1.3	Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	Thales **CipherTrust Manager** and **Luna HSM** provide role-based access control to only those users and groups who have key custodian responsibility.
3.6.1.2	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with key-encrypting keys are at least as strong as the data-encrypting keys, and it is stored separately from data-encrypting keys. • Stored within a secure cryptographic device (such as a HSM or a PTS approved point-of-interaction device). • As at least two full-length key components or key shares, in accordance with an industry accepted method.	Thales **CipherTrust Manager** and **Luna HSM** are certified up to FIPS 140-2 Level 3 for key storage. Using these products assures the keys are stored separate from the data and meet industry accepted methods.

Requirement	Requirement Description	Thales Data Security solution
3.6.1.3	Cryptographic keys are stored in the fewest possible locations.	Thales **CipherTrust Manager** centralizes the management and storage of encryption keys in a high-availability cluster of appliances that is centrally managed. CipherTrust Manager can function as central key manager for multiple external encryption platforms including third party platforms. Similarly, Luna HSM can be set up in a centrally managed high-available estate.
3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	While customers must document the key-management processes used within their organization and ensure that key custodians understand and acknowledge their responsibilities, **CipherTrust Manager** and **Luna HSM** support compliance with the technical requirements associated with **3.6.**
3.7.1	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	Cryptographic keys are generated by the **CipherTrust Manager** or Luna appliances which are fully compliant with FIPS standards.
3.7.2	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	Clear text keys never leave the **Luna HSM** or **CipherTrust Manager** or. When keys are distributed to CipherTrust Connectors, they are encrypted with a onetime-use AES 256 key and sent over a mutually authenticated TLS connection.
3.7.3	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	Cryptographic keys are stored by the **CipherTrust Manager** or Luna appliances that are fully compliant with FIPS standards. CipherTrust Managers customers can choose to cache cryptographic keys on the host server.
3.7.4	Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod	Cryptographic keys can be changed by key custodians based upon the organization's policies for cryptographic periods. When a key is retired by a custodian, it can be permanently deleted. Key change procedures need to specify a process for re-encrypting data with new keys before making old keys obsolete. **CipherTrust Transparent Encryption** offers Live Data Transformation capabilities to allow for key rotation without taking services offline.

Requirement	Requirement Description	Thales Data Security solution
3.7.5	Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leave the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	**CipherTrust Manager** includes detailed auditing/logging of all key state changes, administrator access and policy changes. Administrators can rotate keys when any suspicious activity is detected. When a key is changed by a custodian, it can be permanently deleted. Key change procedures will need to include a process for re-encrypting data with new keys before making old keys obsolete. CipherTrust Transparent Encryption makes this easy and without downtime using its Live Data Transformation capability.
3.7.6	Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented including managing these operations using split knowledge and dual control.	With the **CipherTrust Platform** solutions, administrators don't have to do manual management of keys in clear text. Custodians can create keys, but key values are not visible to the custodian. CipherTrust Manager protects against any one person having access to key material by supporting "no knowledge" and configurable split knowledge and dual control policies.
3.7.7	Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	Access control policies defined within **CipherTrust Manager** govern access to key creation and other key management activities, restricting access to authorized key custodians only. CipherTrust Manager supports an "m-of-n" sharing scheme for backing up keys. A specific number of shares must be provided in order to restore the encrypted contents of a CipherTrust Manager archive into a new or replacement instance.
3.7.8	Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**CipherTrust Manager** policy configurations enable you to communicate key custodian responsibilities to key administrators.

Requirement 3 also provides guidelines on which cardholder data can and cannot be stored. Sensitive data on magnetic strip or **chip** must never be stored after authorization. If your organization stores PAN data, it is critical to render it unreadable (see table 6 for PCI DSS guidelines).

Table 6: Cardholder Data Protection and Storage Requirements

Account Data	Data Element	Storage Permitted?	Render Unreadable?
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data	Full Track Data	No	Cannot store per requirement 3.3
	CAV2/CVC2/CVV2/CID	No	Cannot store per requirement 3.3
	PIN/PIN Block	No	Cannot store per requirement 3.3

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Sensitive data must be encrypted during transmission over private or public networks, since they can be intercepted by malicious individuals who can gain access to card holder data and commit fraud.

Table 7: Details of PCI DSS Requirement 4

Requirement	Requirement Description	Thales Data Security solution
4.2.1	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	Thales offers **High Speed Encryptors (HSEs)** for data in motion encryption across the network, ensuring card holder data is secure as it moves from site-to-site on public or private networks. Operating at Layer 2, 3 or 4 of the network stack, Thales HSEs from encrypt all data that traverses an open network. The appliances use strong cryptography and are certified FIPS 140-2 L3, Common Criteria, NATO and UC APL. The **CipherTrust platform** can be used to encrypt or tokenize data at rest, and then this secured data can be safely transmitted meeting PCI DSS recommendations.
4.2	PAN is protected with strong cryptography during transmission.	Thales **HSEs** encrypts all application data transmitted over a network. In addition, The CipherTrust Platform can be used to encrypt, tokenize or mask PANs ahead of sharing.

Requirement 6: Develop and Maintain Secure Systems and Software

Digital signatures help maintain the electronic integrity and authenticity of code by associating it with an application vendor's unique signature. Without assurance of an application's integrity and knowledge of who published an application, it's difficult for end users to know how much to trust that software.

A certificate is a set of data that completely identifies an entity, and it is issued by a certification authority (CA). The data set includes the entity's public cryptographic key. To obtain a certificate from a CA, an application provider must meet the criteria for a commercial publishing certificate. It is recommended that applicants generate and store their private key using a dedicated hardware solution, such as an HSM.

Table 8: Details of PCI DSS Requirement 6

Requirement	Requirement Description	Thales Data Security solution
6.1 & 6.5	Processes and mechanisms for developing and maintaining secure systems and software are defined and understood. Changes to all system components are managed securely.	The **Thales Luna HSM** protects the identity, whether it is a physical or virtual server, or the user. Thales HSMs take this level of security one step further by storing the signing material in a hardware device, thus ensuring the authenticity and integrity of an application code file.

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

To ensure sensitive cardholder data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on a need to know and according to job responsibilities. The logic is based on "least privilege", where you grant each person just enough rights to perform his/her job function.

Table 9: Details of PCI DSS Requirement 7

Requirement	Requirement Description	Thales Data Security solution
7.1	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Thales **CipherTrust Data Security Platform** offers a range of capabilities to implement least privileged access controls and deny unauthorized access to protected cardholder information. For example, using CipherTrust Transparent Encryption, root systems administrators can be granted access to perform administration tasks on systems they're responsible for, without being able to decrypt the data on those systems.
7.2	Access to system components and data is appropriately defined and assigned.	The **CipherTrust Platform** solutions enable security teams to enforce policies that authorize users and applications to access cardholder data storage. Only authorized users and applications can access data in clear text. With CipherTrust Platform solutions, administrators can be given access to files containing cardholder data, but without gaining the permissions needed to decrypt the file. Default policy is to deny access to all, except those who have explicit authorization.

Requirement 9: Restrict Physical Access to Cardholder Data

Any physical access to data or systems that house cardholder data provides the opportunity for unauthorized personnel physically present on the entity's premises to steal data. Thales data protection solutions enable you to encrypt data at rest, so even when unauthorized personal gain access to cardholder data, they will not be able to decrypt and make sense out of it.

Table 10: Details of PCI DSS Requirement 9

Requirement	Requirement Description	Thales Data Security solution
9.4.7	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	Should encrypted data not be adequately cleaned from media, the data will not be viewable in clear text unless the data owners **CipherTrust Manager** or **CipherTrust Tokenization Server** is available to authorize the decryption of the data on that media. Similarly, if encryption keys are stored in Luna HSMs, the data on the media is unrecoverable without authorized access to the HSMs. And Once the encryption keys are destroyed, the data cannot be accessed in clear text.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Ability to track user activity with continuous monitoring are critical to detecting, alerting, and minimizing the impact of data breaches. Determining the cause of data breaches is difficult, if not impossible, without tracking system log activity.

Table 11: Details of PCI DSS Requirement 10

Requirement	Requirement Description	Thales Data Security solution
10.1	Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.	Thales products all maintain audit logs to system access of individual users. For example, **CipherTrust Transparent Encryption** directly supports by providing detailed logging at the file system level. Any read, write, or other access requests for sensitive data is audited. The audit records contain details such as host machine, directory, file, or resource accessed; specific user and user group; policy invoked; application; and time of day.
10.3 & 10.5	Audit logs are protected from destruction and unauthorized modifications. Audit log history is retained and available for analysis.	There are software controls in place in **CipherTrust Manager** to prevent unauthorized access and alteration to its internals including the audit logs. If log and audit files are sent to a centralized log server, this external log repository can be protected and safeguarded with CipherTrust Transparent Encryption and access control. It can be used to secure logs for other PCI DSS Components as well.
10.6.1	System clocks and time are synchronized using time-synchronization technology.	The **CipherTrust Manager** can be configured to synchronize with a Network Time Protocol (NTP) server.

Requirement 12: Support Information Security with Organizational Policies and Programs

The organization's overall information security policy sets the tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

Table 12: Details of PCI DSS Requirement 12

Requirement	Requirement Description	Thales Data Security solution
12.5	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes identifying all data flows for the various payment stages and acceptance channels.	**CipherTrust Data Discovery and Classification** can be used to facilitate identifying all sources and locations of PII (Personally Identifiable Information), including PAN, and to look for PAN that resides on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE. The solution enables you to efficiently locate structured and unstructured regulated data across the cloud, big data, and traditional data stores in your enterprise, so you can make better decisions about closing your gaps and prioritizing remediation.
12.10.7	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected. This includes remediating data leaks or process gaps that resulted in the account data being where it was not expected.	Thales has created an automatic workflow that links **CipherTrust Data Discovery and Classification** with **CipherTrust Transparent Encryption**, called CipherTrust Intelligent Protection. Using this combined solution you can discover, classify, and use policy-based data encryption to automate data remediation if PAN was found outside the CDE or in an unexpected place within the defined CDE.

Top 10 Critical Steps to Achieve PCI DSS Compliance

This section provides the ten critical steps that can help you with your PCI DSS compliance efforts. For a more comprehensive guide on how you could secure your cardholder data environment (CDE), you can read the Dummies Guide® on PCI Compliance & Data Protection[3].

1. **Scope: Establish where cardholder data is present and how you are protecting it on its journey**

   Review and document in detail all processes involving capture, authorization and settlement of payment transactions where cardholder data is present to understand the components of your cardholder data environment (CDE). Ensure you identify all trusted, untrusted, and third-party connections and any mechanisms deployed to prevent unauthorized access to the CDE.

2. **Assess: Know where your stored data is located and how you rendered it unreadable**

   Document precisely what elements of cardholder data you are storing, all locations where it is stored and why your organization needs to store it. Recording how you have rendered the data unreadable and how access is logged are of critical importance. Knowing how long you need to retain the data and when you can securely delete it should involve business, legal and regulatory considerations.

3. **Report: Consult with your reporting contacts to ensure you get it right**

   PCI DSS compliance and reporting requirements are enforced by the payment brands depending on your role and annual transaction volume. Ensure that assessor and/or entity complete required documentation (e.g. Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls.

4. **Attest: Complete the appropriate attestation of compliance (AOC)**

   Companies must attest to PCI DSS compliance annually, if it handles credit card data electronically. This involves delivering 2 or 3 of the following packages – 1) Self-Assessment Questionnaire; 2) Regular network and web-site scanning by an Approved Scanning Vendor (ASV); 3) Report on Compliance by a Qualified Security Assessor (only needed by the very largest companies).

5. **Submit: All requested documents to the acquirer or to the payment brand/requestor**

   Submit the SAQ, ROC, AOC and other requested supporting documentation such as Approved Scanning Vendor (ASV) scan reports to the acquirer (for merchants) or to the payment brand/requester (for service providers).

6. **Remediate: Perform remediation to address requirements, and compensatory controls where remediation is not possible**

   If required, perform remediation tasks to address requirements. Sometimes, business and/or technical constraints can prevent you from complying with one or more PCI DSS requirements. In these instances, compensating controls, which can include encrypting card holder data that can mitigate unauthorized access.

7. **Business-goals: Ensure PCI DSS compliance complements your enterprise risk management efforts**

   Practical application of the PCI DSS requirements means considering intent as well as business needs and assessed risk. Your efforts should include reviewing PCI DSS guidance, reading PCI Security Standards Council publications, and consulting with your QSAs to better understand how to reasonably apply required controls without harming defined business requirements.

8. **Review: Program strategy regularly to promote greater team involvement**

   Manage your compliance efforts by establishing ongoing processes, regular team communications and staying abreast. Establish a defined program including documented roles and responsibilities to help ensure that your CDE and supporting processes remain compliant of developments within the industry.

9. **Sponsorship: Seek senior level buy-in to underpin your critical time and resource investments**

   Identify executive sponsors and stakeholders and ensure their involvement and awareness to help align your program with enterprise business goals and intra-organizational initiatives, and make you better prepared for changes in the threat environment.

10. **Document: Use comprehensive documentation to support your compliance policies**

    Organizational policies and procedures require explicit documentation to tightly align with the various PCI DSS requirements and sub requirements for critical pieces of your compliance effort. It is essential to document important activities including change management, code reviews, security awareness programs, training sessions, and other programs to reflect your overall approach to security.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

References:

1. 2022 Thales Data Threat Report – Financial Services Edition
2. PCI DSS Requirements and Testing Procedures, Version 4.0, March 2022
3. Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1, July 2019
4. PCI Compliance & Data Protection, Dummies Guide, by Ian Hermon and Peter Spier, 2017.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <