

Achieving PCI DSS Compliance with Thales Data Protection



Contents

3	Introduction
3	Purpose of PCI Data Security Standard
4	Why Does PCI DSS Compliance Matter?
5	PCI DSS Requirements in a Nutshell
6	Overview of the Thales Data Protection Portfolio
7	Data-at-Rest Encryption
7	Key Management
7	File-system, Database, and Application Encryption
7	Cloud Encryption
7	Tokenization with Dynamic Data Masking
7	Enterprise Key Management
7	Cloud Key Management
8	Data-in-Motion Encryption
8	Hardware Security Modules (HSMs)
8	General Purpose HSM
8	Cloud HSM
8	Payment HSM
9	Authentication and Access Control
9	Addressing PCI DSS Requirements with the Thales Data Protection Portfolio
9	Requirement 2: Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters
10	Requirement 3: Protecting Stored Cardholder Data
13	Requirement 4: Encrypting Account Data in Transit
14	Requirement 6: Develop and Maintain Secure Systems and Applications
14	Requirement 7: Restricting Access to Cardholder Data
15	Requirement 8: Authenticating Access to System Components
16	Requirement 9: Restrict Physical Access to Cardholder Data
17	Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data
19	Top 10 Critical Steps to Achieve PCI DSS Compliance
20	About Thales
20	References:

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 2019 Thales Data Threat Report – Financial Services Edition¹, 62% of U.S. financial services organizations say they have been breached at any time in their history, with 41% breached in the last year. Despite recognizing the importance of protecting sensitive data, encryption rates among U.S. financial companies is surprisingly low (only 31%).

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 3.2.1 requirements² 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.

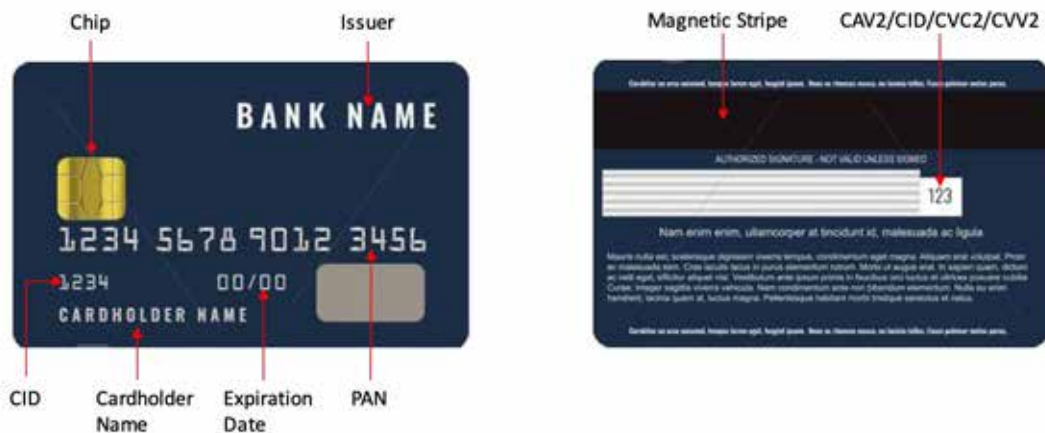
Purpose of PCI Data Security Standard

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 3.2.1 was made in May 2018.

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
<ul style="list-style-type: none">Primary Account Number (PAN)	<ul style="list-style-type: none">Full track data (on magnetic stripe or chip)
<ul style="list-style-type: none">Cardholder Name	<ul style="list-style-type: none">CAV2/CID/CVC2/CVV2
<ul style="list-style-type: none">Expiration Date	<ul style="list-style-type: none">Personal Identification Number (PIN) entered by cardholder
<ul style="list-style-type: none">Service Code	



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 \$5000 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 Framework². 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 a firewall configuration to protect cardholder data.	
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.	*
Protect Cardholder Data	3. Protect stored cardholder data.	*
	4. Encrypt transmission of cardholder data across open, public networks.	*
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs.	
	6. Develop and maintain secure systems and applications.	•
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know.	•
	Identify and authenticate access to system components.	•
	Restrict physical access to cardholder data.	
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data.	•
	Regularly test security systems and processes.	
Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel.	

For more details on the PCI DSS version 3.2.1 requirements go to: https://www.pcisecuritystandards.org/document_library

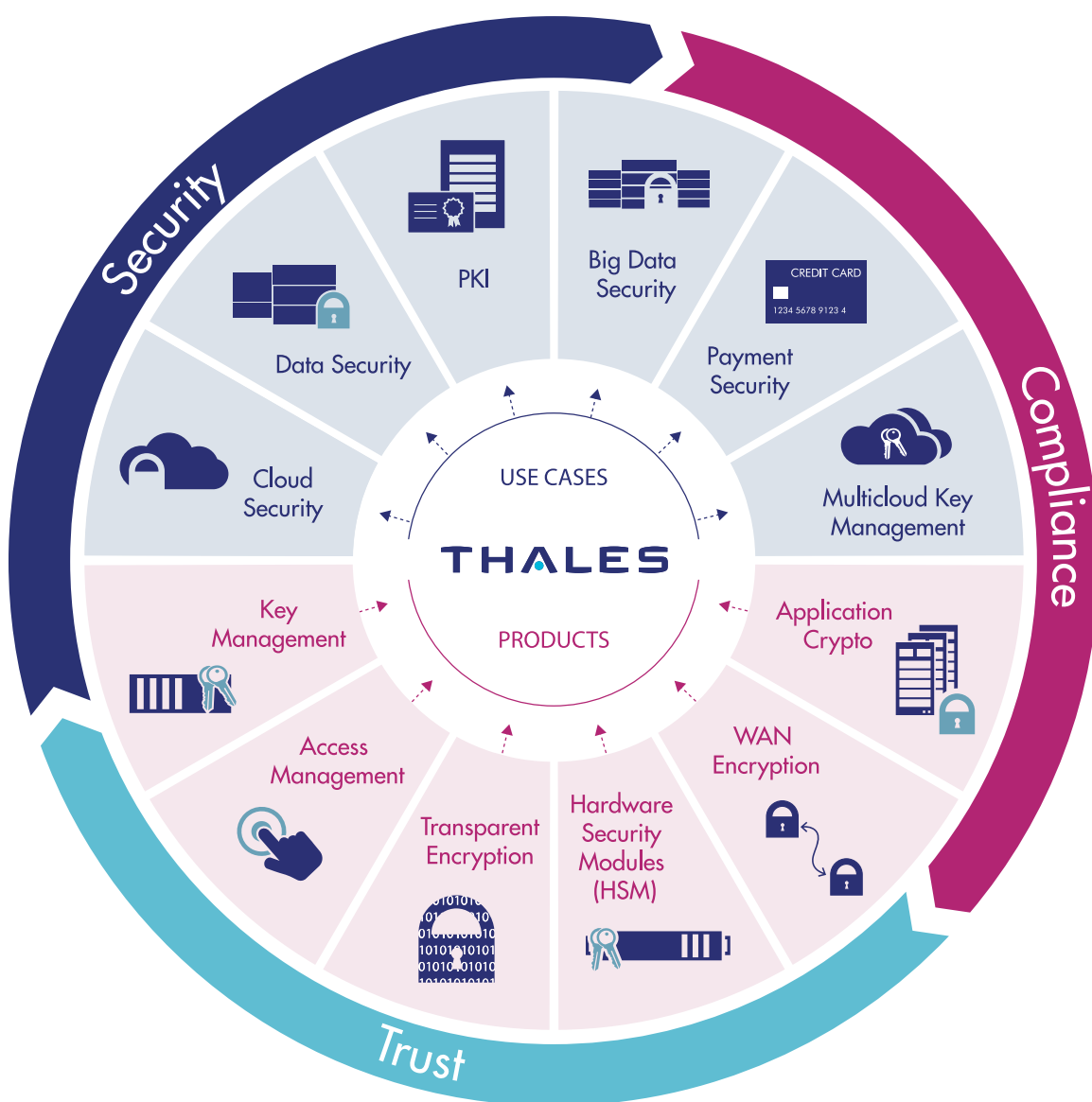
Note that, PCI DSS can ensure data security at the snapshot of time when the compliance audit is conducted, but does not guarantee data protection all the time, unless you continuously monitor your environment and update security controls as your IT infrastructure evolves.

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 1: Thales Data Protection Product Portfolio and Use-cases Supported



Data-at-Rest Encryption

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

Key Management

Vormetric Data Security Manager 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

Vormetric Transparent Encryption (VTE) 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. VTE is designed to meet PCI DSS requirements and best practices with minimal disruption, effort, and cost.

Cloud Encryption

CypherTrust Cloud Key Manager manages encryption keys for Salesforce, Microsoft Azure and AWS 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

Vormetric Tokenization Server makes it easy to add format-preserving tokenization to protect Payment Account Numbers (PAN) and supports policy-based dynamic data masking to enable portions of PAN data visible to specific users/groups based on their authorization rights. Static data masking and bulk encryption or tokenization is made quick and simple with Vormetric Batch Data Transformation.

Enterprise Key Management

Vormetric Key Manager provides unified key management and secure key storage for third-party Transparent Data Encryption (TDE) and KMIP-compliant clients as well as securely storing certificates.

Cloud Key Management

CipherTrust Cloud Key Manager manages Bring Your Own Keys (BYOK) and provider created keys for Salesforce, Microsoft Azure and AWS while addressing enterprise needs to meet compliance and best practices for managing encryption key life cycles outside of their native environments, without the need for enterprises to become cryptographic experts.

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.

Addressing PCI DSS Requirements with the Thales Data Protection Portfolio

Requirement 2: Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters

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

Req.	Requirement Description	Thales Data Security solution
2.2.1	<p>Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)</p> <p>Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.</p>	<p>Thales solutions enable multi-tenancy and separation of duties to ensure that only authorized users can access the secure data.</p> <p>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.</p>
2.2.3	<p>Implement additional security features for any required services, protocols, or daemons that are consider to be insecure— for example, use secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file sharing, Telnet, FTP, etc.</p>	<p>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.</p>
2.3	<p>Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</p>	<p>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.</p>
2.6	<p>Shared hosting providers must protect each entity's hosted environment and cardholder data.</p>	<p>Thales solutions enable clear and secure distinction between different clients even in multi-tenant, shared environments.</p>

Requirement 3: Protecting Stored Cardholder 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

Req.	Requirement Description	Thales Data Security solution
3.1	Limit cardholder data storage and retention time to that which is required for the business, legal, and/or regulatory purposes, as documented in your data 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.
3.2	Do not store sensitive authentication data after authorization (even if it is encrypted). Render all sensitive authentication data unrecoverable upon completion of authorization process.	Thales SafeNet Trusted Access does not retain any authentication data after authorization, when it is integrated with the payment processing applications.
3.3	Mask PAN when displayed, so that authorized people with legitimate business need can see more than the first six or last four digits of the PAN.	<p>The Vormetric 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.</p> <ul style="list-style-type: none"> • 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 <p>Strong cryptography underpinned by key management and data access policies.</p>
3.4	Render PAN unreadable anywhere it is stored – including portable digital media, backup media, in logs, and data received from or stored by wireless networks.	Thales' data-centric approach to data security means that once data is encrypted at the primary site, it is automatically secured when replicated to disaster recovery sites and archives. Without access to the keys, the data is unreadable regardless of where it is stored.
3.4.1	If disk encryption is used (rather than file or column-level database encryption), logical access must be managed separately and independently of the native OS authentication and access control mechanisms).	Thales Vormetric Data Security Manager and Luna HSMs enable central management of encryption keys independent of the user credentials on the native OS.
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Thales Vormetric Data Security 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.

3.5.1	<p>Additional requirements for service providers only: Maintain a documented description of the cryptographic architecture that includes:</p> <ul style="list-style-type: none"> • Details of algorithms, protocols, and keys used to protect card holder data. • Description of key usage for each key. • Inventory of any HSMs and other SCDs used for key management. 	<p>Thales Vormetric Data Security Manager and Luna support this documentation process:</p> <ul style="list-style-type: none"> • 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.
3.5.2	<p>Restrict access to cryptographic keys to the fewest number of custodians necessary.</p>	<p>Thales Vormetric Data Security Manager and Luna HSM provide role-based access control to only those users and groups who have key custodian responsibility.</p>
3.5.3	<p>Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:</p> <ul style="list-style-type: none"> • 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. 	<p>Thales Vormetric DSM 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.</p>
3.5.4	<p>Store cryptographic keys in the fewest possible locations.</p>	<p>Thales Vormetric DSM centralizes the management and storage of encryption keys in a high-availability cluster of appliances that is centrally managed. Vormetric DSM 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.</p>
3.6	<p>Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:</p>	<p>While customers must document the key-management processes used within their organization and ensure that key custodians understand and acknowledge their responsibilities, Vormetric DSM and Luna HSM support compliance with the technical requirements associated with 3.6.</p>
3.6.1	<p>Generation of strong cryptographic keys</p>	<p>Cryptographic keys are generated by the Vormetric DSM or Luna appliances which are fully compliant with FIPS standards.</p>
3.6.2	<p>Secure cryptographic key distribution</p>	<p>Clear text keys never leave the Luna HSM or DSM or. When keys are distributed to Vormetric agents, they are encrypted with a onetime-use AES 256 key and sent over a mutually authenticated TLS connection.</p>
3.6.3	<p>Secure cryptographic key storage</p>	<p>Cryptographic keys are stored by the Vormetric DSM or Luna appliances that are fully compliant with FIPS standards. DSM customers can choose to cache cryptographic keys on the host server. DSM's highly secure agents protect these keys from unauthorized access, even from root administrators.</p>

3.6.4	Cryptographic key changes for keys that have reached end of their crypto-period, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines.	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. Vormetric Transparent Encryption offers Live Data Transformation capabilities to allow for key rotation without taking services offline.
3.6.5	Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened, or keys are suspect of being compromised.	Vormetric DSM 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. Vormetric Transparent Encryption makes this easy and without downtime using its Live Data Transformation capability.
3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.	With Vormetric 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. DSM protects against any one person having access to key material by supporting "no knowledge" and configurable split knowledge and dual control policies.
3.6.7	Prevention of unauthorized substitution of cryptographic keys	Access control policies defined within DSM govern access to key creation and other key management activities, restricting access to authorized key custodians only. DSM 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 DSM archive into a new or replacement instance.
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key custodian responsibilities.	Vormetric DSM 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 below 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 3.2
	CAV2/CVC2/CVV2/CID	No	Cannot store per requirement 3.2
	PIN/PIN Block	No	Cannot store per requirement 3.2

Requirement 4: Encrypting Account Data in Transit

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

Req.	Requirement Description	Thales Data Security solution
4.1	<p>Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:</p> <ul style="list-style-type: none"> Only trusted keys and certificates are accepted The protocol in use only supports secure versions or configurations The encryption strength is appropriate for the encryption methodology in use 	<p>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.</p> <p>The Vormetric platform can be used to encrypt or tokenize data at rest, and then this secured data can be safely transmitted meeting PCI DSS recommendations.</p>
4.2	Never send unprotected PANs by end user messaging techniques (for example e-mail, instant messaging, SMS, chat, etc.)	Thales HSEs encrypts all application data transmitted over a network. In addition, Vormetric Platform can be used to encrypt, tokenize or mask PANs ahead of sharing.
4.3	Ensure that security policies and operational procedures for encrypting transmissions for cardholder data are documented, in use, and known to all affected parties.	Thales products are used to support data encryption policies between parties. Customers are responsible for documenting operational procedures.

Requirement 6: Develop and Maintain Secure Systems and Applications

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 Requirements 6

Req.	Requirement Description	Thales Data Security solution
6.3	<p>Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:</p> <ul style="list-style-type: none">• In accordance with PCI DSS (for example, secure authentication and logging)• Based on industry standards and/or best practices.• Incorporating information security throughout the software-development life cycle	<p>The 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.</p>

Requirement 7: Restricting Access to Cardholder Data

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 Requirement7

Req.	Requirement Description	Thales Data Security solution
7.1	<p>Limit access to system components and cardholder data to only those individuals whose job requires such access.</p>	<p>Thales Vormetric 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 VTE, 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.</p>
7.2	<p>Establish an access control system(s) for system components that restrict access based on user's need to know, and is set to "deny all" unless specifically allowed.</p>	<p>Vormetric 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.</p> <p>With Vormetric 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.</p>
7.3	<p>Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.</p>	<p>Customers are responsible for documenting operational procedures.</p>

Requirement 8: Authenticating Access to System Components

Ensuring individual accountability for their actions can be achieved by assigning unique identification (ID) to each person, and the actions taken by them on critical data and systems can be traced to known and authorized users. This requirement is focused on designing a robust authentication and access control system.

Table 10: Details of PCI DSS Requirement 8

Req.	Requirement Description	Thales Data Security solution
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	<p>Thales products, acting as components in the PCI DSS solution, can be set up for unique, multifactor administrative access.</p> <p>In addition, Thales SafeNet Trusted Access enables you to centrally manage unique user identities for cloud and web-based applications that handle cardholder data.</p>
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	<p>Thales products allow for control of addition, deletion, and modification of user IDs, credentials, and other identifier objects via local databases or LDAP integrations.</p> <p>In addition, SafeNet Trusted Access to centrally add/delete/modify user credentials for cloud and web-based applications.</p>
8.1.3 to 8.1.8	<p>8.1.3. Immediately revoke access for any terminated users.</p> <p>8.1.4. Remove/disable inactive user accounts at least every 90 days</p> <p>8.1.5. Manage IDs used by third parties to access, support, or maintain system components via remote access.</p> <p>8.1.6. Limit repeated access attempts by locking out the user ID after not more than six attempts.</p> <p>8.1.7. Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.</p> <p>8.1.8. If a session has been idle for more than 15 min. require the user to re-authenticate to re-activate the session.</p>	<p>Vormetric DSM allows administrators to revoke access to any terminated users. It does not automatically revoke access to terminated users.</p> <p>DSM allows administrators to remove/disable inactive user accounts periodically as a manual step.</p> <p>DSM provides REST apis for third-parties to access, support and maintain system components.</p> <p>DSM also limits repeated failed logins to 3 attempts by default, and the number of attempts, lockout duration and idle timeout are configurable.</p> <p>SafeNet Trusted Access (STA) can immediately revoke access to any terminated user, by disabling them in the STA console that manages single sign-On for each user to all applications that handle card holder data.</p>
8.2	<p>In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as biometric. 	<p>Thales data protection portfolio of products support multifactor authentication.</p> <p>SafeNet Trusted Access allows you to configure separate risk-based authentication policies for users and administrators. The policies have options to configure various authentication methods - regular passwords, one-time passwords/tokens, smartcards or use of biometric authentication for based on the risk acceptable to each application.</p>

8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	SafeNet Trusted Access can be used to authenticate remote access via VPN and VDI using multi-factor authentication.
8.7	<p>All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:</p> <ul style="list-style-type: none"> • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). 	Vormetric Transparent Encryption provides control at the file system level, below the database. When a database is protected with Vormetric, all access to the data in the database must come from the database process. All other sources are denied access. Database admins can be allowed direct access via policy.

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 personnel gain access to cardholder data, they will not be able to decrypt and make sense out of it.

Table 11: Details of PCI DSS Requirement 9

Req.	Requirement Description	Thales Data Security solution
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	<p>Should encrypted data not be adequately cleaned from media, the data will not be viewable in clear text unless the data owners Vormetric DSM or Vormetric Tokenization Server is available to authorize the decryption of the data on that media.</p> <p>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.</p>

Requirement 10: Track and Monitor all Access to Network Resources 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 12: Details of PCI DSS Requirement 10

Req.	Requirement Description	Thales Data Security solution
10.1	Implement audit trails to link all access to system components to each individual user.	<p>Thales products all maintain audit trails to system access of individual users.</p> <p>For example, VTE 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.</p>
10.2	<p>Implement automated audit trails for all system components to reconstruct the following events:</p> <p>10.2.1: All individual user accesses to cardholder data</p> <p>10.2.2: All actions taken by any individual with root or administrative privileges</p> <p>10.2.3: Access to all audit trails</p> <p>10.2.4: Invalid logical access attempts</p> <p>10.2.5: Use of and changes to identification and authentication mechanisms</p> <p>10.2.6: Initializing, stopping, or pausing of audit logs</p> <p>10.2.7: Creation and deletion of system-level objects</p>	<p>All products in the Thales data protection portfolio produce audit records that log any encryption key lifecycle operations (creation/deletion/rotation) and other administrative functions that can be used to reconstruct events.</p> <p>In addition, VTE also creates audit logs of file and database access as described in 10.1.</p> <p>SafeNet Trusted Access monitors changes to identification and authentication mechanisms.</p>
10.3	<p>Record at least the following audit trail entries for all system components for each event:</p> <p>10.3.1 User identification</p> <p>10.3.2 Type of event</p> <p>10.3.3 Date and time</p> <p>10.3.4 Success or failure indication</p> <p>10.3.5 Origination of event</p> <p>10.3.6 Identity or name of affected data, system component, or resource.</p>	<p>Vormetric provides detailed auditing at the file system level, generating audit entries that include:</p> <ul style="list-style-type: none"> • User-name and group membership. (10.3.1) • Type of event. (10.3.2) • Date and time. (10.3.3) • Success or failure indication. In the case of a permitted action, the event data also includes whether the access was to clear text or to encrypted data. (10.3.4) • Origination of the event. (10.3.5) • Host and the full path to the file that was the target of the access request. (10.3.6)

10.4.1	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Critical systems have the correct and consistent time	The DSM can be configured to synchronize with a Network Time Protocol (NTP) server.
10.5	Secure audit trails so they cannot be altered.	<p>There are software controls in place in DSM to prevent unauthorized access and alteration to its internals including the audit logs</p> <p>If log and audit files are sent to a centralized log server, this external log repository can be protected and safeguarded with Vormetric Transparent Encryption and access control. The VTE solution can be used to secure logs for other PCI DSS Components as well.</p>

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 Protection³.

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. The Changing Face of Data Security, 2019 Thales Data Threat Report – Financial Services Edition
2. PCI DSS Requirements and Security Assessment Procedures, v3.2.1, May 2018
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.



Americas

Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalessec.com

Asia Pacific – Thales Transport & Security (HK) Ltd

Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa

350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> cpl.thalesgroup.com <

