Brought to you by:

THALES

PCI Compliance & Data Protection

for dummies®
A Wiley Brand

- Explore the PCI DSS requirements
- Understand the importance of data protection
- Discover ways to reduce scope

Thales eSecurity Limited Edition

Ian Hermon
Peter Spier, QSA

About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services, delivering trust wherever information is created, shared or stored. We ensure that company and government data is secure and trusted in any environment – on premise, in the cloud, in data centers and in big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices.

Thales provides everything an organization needs to protect and manage its data, identities, and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control, and by meeting the highest standards of certification for high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

About Fortrex Technologies

Since 1997, Fortrex Technologies has served as a trusted security and risk management advisor to its clients throughout the world. Fortrex focuses exclusively on IT security, operational risk, and regulatory compliance and helps organizations throughout the world identify, assess, remediate, and manage their operational risks through consulting, audit, vendor management and human capital assistance. By providing expert technical assessments, Fortrex ensures the confidentiality, integrity and availability of data and systems through world-class, enterprise-wide information security services and solutions. Powered by a team of security and risk management experts and the industry's leading technology, Fortrex's in-depth risk assessments and solutions ensure that its clients' information assets remain safe and secure.

PCI Compliance & Data Protection

Thales eSecurity Limited Edition

by Ian Hermon and Peter Spier

for dummies®
A Wiley Brand

PCI Compliance & Data Protection For Dummies®, Thales eSecurity Limited Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate Chichester, West Sussex, www.wiley.com

Registered Office

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

ISBN 978-1-119- 41869-6 (pbk); ISBN 978-1-119- 41870-2 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Kathy Simpson

Project Editor: Jennifer Bingham

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Frazer Hossack

Production Editor: Antony Sami

Special Help: Thanks to Charles Goldberg, Tim Arnold and Jim DeLorenzo from Thales eSecurity and Cady Ann Chin QSA and Samuel P. Hinson, QSA, PA-QSA from Fortrex for their assistance with content and reviews during the creation of this book.

Table of Contents

Introduction

If your business transmits, processes, or stores cardholder data — or provides services to organizations that do — the payment brands require you to comply with the Payment Card Industry Data Security Standard (PCI DSS). Whether you work in information technology (IT) security, auditing, risk management, compliance operations, or even finance, this book can help you successfully fulfill necessary reporting requirements.

About This Book

We intend this book to serve as an easy-to-understand introduction to protecting payment card data, as well as a reference guide you can use as you work with architects, operations, analysts, and assessors. We cover not just the PCI DSS requirements themselves, but also ways in which you can employ data protection controls (such as encryption and tokenization) and access controls (such as authentication and authorization methods) to reduce your PCI scope.

The goals, approaches, and benchmarks within the standard have general applicability, and adopting them will almost certainly improve your overall security posture, support your broader privacy obligations, and protect your reputation. We hope that this information makes your life easier and saves you money.

How This Book Is Organized

The book is divided into five chapters and three appendices. Here's what you'll find:

- **Chapter 1: Why Focus on Protecting Account Data?** A refresher on the goals of PCI DSS and its structure, as well as the requirements associated with account data protection.
- **Chapter 2: Examining Data Protection and Access Control Requirements:** Specific requirements for protecting data at all times (in transit, in storage, and in use), restricting

and monitoring access to data and system components with references to technology options, and key management fundamentals required by PCI DSS.

- **Chapter 3: Choosing a Data Security Solution:** Practical issues to consider when planning your implementation, including the pros and cons of various approaches to reduce scope.
- **Chapter 4: Managing Your Data Security Operations:** What to consider when establishing your policies to control access to data and systems, together with the need for comprehensive monitoring and audit trails.
- **Chapter 5: Ten Keys to PCI DSS Success:** Suggested guidance to help keep your data protection efforts focused and on the track to success.
- **Appendix A: Making Stored PAN Information Unreadable:** A brief summary of the technology options available to render PAN information unreadable.
- **Appendix B: PCI Security Standards That Complement the PCI DSS:** A quick look at some of the other security standards that are used in the payments industry that complement PCI DSS that you may need to consider.
- **Appendix C**: **Glossary:** A list of abbreviations we use in this book together with some others you may find in supporting documents.

Foolish Assumptions

The main assumptions that we make in this book are that you're involved directly or indirectly with protecting cardholder data and that a data breach is definitely not in your interest. We also assume that you're not quite sure of all the things that need to be done to comply with PCI DSS and that you need assistance from the data security community.

Although the PCI DSS specification contains only 12 requirements, it's a meaty document with extensive supporting guidance released in various supplements. Therefore, we assume that you don't have the time to read and digest all this information and that instead, you want to understand what you need to do.

We assume that the aspects of compliance of most interest to you (and for which we can offer the best practical advice) are those connected to data security, such as cryptography — most notably encryption. With this assumption in mind, we tailored the book to address the best practices for delivering data security and keeping your cardholder data safe, wherever it resides.

Please feel free to use the table of contents page to identify the main topics of interest and jump straight to them. We hope that we can help you in your mission to secure your data.

Icons Used in This Book

As you read this book, you'll notice the following icons located in the margins. These icons highlight important points and information.

Tips are suggestions or shortcuts that could simplify your path to PCI DSS compliance.

The Remember icon points out important issues to keep in mind as you consider your path forward.

Warnings are words of caution about issues that could hold you back or trigger unintended consequences.

This icon points out information that you have no pressing need to know but may find interesting anyway. If you choose to skip a Technical Stuff passage, you can do so without losing the knowledge you gain from the book.

Where to Go From Here

As we state in various places throughout the book, the definitive set of PCI DSS specifications and official guidance is available in the document library section of the PCI Security Standards Council website (`https://www.pcisecuritystandards.org/document_library`). This site is where you find the unabridged

documents that define what you need to achieve PCI DSS compliance, the approved vendor solutions available to help you, and lots of tips and guidance on avoiding potential pitfalls.

You should be aware that all specification documents are updated periodically, so you should keep a lookout for new requirements that you need to satisfy.

To supplement the extremely useful documentation provided by the PCI Security Standards Council, you may also want to check out the solutions, practical advice, and guidance provided by the companies to which the authors of this book belong:

- Thales eSecurity (`www.thalesesecurity.com/solutions/compliance/pci-dss`) has a solution page on its website dedicated to PCI DSS. This page is updated regularly to reflect the latest information and provides a wealth of detail on the products and services it supplies, which can simplify your PCI DSS compliance effort.
- Fortrex Technologies has a team of senior Qualified Security Assessors or QSAs who have been delivering PCI compliance solutions for more than a decade. The Fortrex web page (`www.fortrex.com/pci-dss.html`) describes the organization's service offerings (including expert assessment, gap analysis, self-assessment questionnaire support, and consultation), which you may want to consider as a way to fast-track your way to PCI DSS compliance.

The content of these sites, like PCI DSS itself, keeps evolving. You should visit them on a regular basis to keep track of the latest information.

IN THIS CHAPTER

- Introducing PCI DSS
- Recognizing the core requirements of the standard
- Reducing the scope of assessment
- Using PCI DSS principles to protect other information assets

Chapter 1
Why Focus on Protecting Account Data?

Malware, identity theft, insider threats, state-sponsored attacks, and hacktivism affect virtually every business. According to a recent study by Thales, organizations around the world increase cybersecurity spending year after year. Still, more than one in four respondents reported a data breach during the preceding year.

In this chapter, we provide a primer on the Payment Card Industry Data Security Standard (PCI DSS) and show you how to use it to safeguard your valuable cardholder data.

Seeing Why the PCI DSS Matters

Before you dive into the details in this chapter, it's important to consider how the PCI DSS fits into the broader security landscape. Protecting payment-related data is certainly important, but similar concerns about a much wider range of sensitive personal information — such as medical records, criminal backgrounds, and employment information — have elevated the issue of data

protection, triggering numerous privacy laws and data-breach-disclosure obligations.

WARNING

Compliance, of course, is mandatory. Failure to take the appropriate steps would at the very least damage your reputation and put you at a competitive disadvantage. Worse, if you experienced a data breach, you'd be hit by fines and accusations of negligence would come thick and fast. Those fines might be levied by the card brands themselves and/or your acquirer (the organization that processes transactions on your behalf and that might be responsible for vouching for your PCI DSS compliance to the payment card brands). You'd also face increased transaction fees and potential litigation.

Avoiding all this trouble makes it easy to see why complying with the PCI DSS is in your organization's best interest. There's another benefit: You can use many of the same technologies and processes you use to achieve PCI DSS compliance to protect a wide variety of data across your enterprise.

Safeguarding account data

Regulation is nothing new to the payments industry. Technology mandates such as the protection of personal identification numbers (PINs) and other authentication credentials at ATMs and point-of-sale (POS) terminals have been in place for many years now. The PCI DSS expands this protection to include other types of data, such as cardholder names, card expiration dates, and primary account numbers (PANs).

This evolution sounds logical, but it raises some new and quite important issues. PINs, for example, are used transiently to authorize transactions and are rarely stored — which isn't the case for other types of account data. Names, account numbers, and expiration dates are frequently stored for a variety of reasons, often to enhance the user experience. Table 1-1 presents the most common reasons for storing account data according to Qualified Security Assessors (QSAs), the people responsible for assessing compliance for organizations that are ineligible for self-assessment.

TABLE 1-1 Most Common Reasons for Storing Account Data, As Reported by QSAs

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

Source: Ponemon Institute

While we're on the topic of QSAs, it's worthwhile to give you a little background on their roles. QSAs are certified by the PCI Security Standards Council to conduct PCI DSS assessments. They must be employed by validated QSA companies; there are no freelance QSAs. The rules vary slightly by card brand, but in most cases, entities at merchant reporting category levels one and two and at service provider level one are required to use QSAs. Other entities may be able to substitute an appropriate self-assessment questionnaire. But whether or not you're required to use them, QSAs can be valuable sources of information and guidance as you prepare for assessment, achieve compliance, and thereafter maintain compliance.

WARNING

Check with your acquirer to make sure that you understand your reporting requirements.

Maintaining a universal security standard

Account data can easily find its way into a wide variety of business systems, ranging from transaction processing to customer relationship management and added-value systems such as loyalty and customer support. The challenge is that all these environments need to be protected to achieve compliance with the PCI DSS. As a result, this standard has a breadth and depth that far exceed those of other privacy and data security mandates. In fact, security experts tend to agree that it also well represents and aligns with industry best practices. Although some aspects of

the standard may be new to your organization, it likely addresses areas of genuine risk.

REMEMBER

The standard was designed to be applied consistently by all companies around the world, from one-man bands to huge multinational corporations. In practice, however, assessments also have to take legal, regulatory, and business requirements into account.

Understanding the Core Requirements of PCI DSS

The PCI DSS consists of 12 published requirements, which in turn contain multiple subrequirements. The requirements are organized in six groups (see Table 1-2).

TABLE 1-2 PCI DSS Requirements

Group	Requirements
Build and Maintain a Secure Network	*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data.
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	*Requirement 3:* Protect stored cardholder data.
	Requirement 4: Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	*Requirement 5:* Protect all systems against malware and regularly update antivirus software or programs.
	Requirement 6: Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	*Requirement 7:* Restrict access to cardholder data by business need to know.
	Requirement 8: Identify and authenticate access to system components.
	Requirement 9: Restrict physical access to cardholder data.

Group	Requirements
Regularly Monitor and Test Networks	*Requirement 10:* Track and monitor all access to network resources and cardholder data.
	Requirement 11: Regularly test security systems and processes.
Maintain an Information Security Policy	*Requirement 12:* Maintain a policy that addresses information security for all personnel.

Source: PCI Security Standards Council

Clarifying the requirements

REMEMBER

You may notice in Table 1-2 that the requirements refer to *cardholder data*, whereas so far in this book, we've also used the term *account data*. Just remember that the term *account data* relates to all types of information that the PCI DSS is designed to protect. Account data includes *cardholder data* (personal account number [PAN], cardholder name, expiration date, service code) as well as *sensitive authentication data* (personal identification number [PIN], PIN block, contents of magnetic stripe, card verification code/value).

TIP

It's easy to see how confusion about the PCI DSS can arise. The PCI Security Standards Council website (`https://www.pcisecuritystandards.org`) is a good source of clarification and guidance. For starters, we recommend that you review "Ten Common Myths of PCI DSS" (`https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf`).

Focusing on data flow

Almost by definition, the PCI DSS is a data-focused standard. Data (in this case, account data) flows through an entire organization, which raises a variety of interesting issues that we attempt to address throughout this book:

- Data that passes through different parts of the IT infrastructure may be owned by different teams.
- Data is subject to various security technologies that are already in place — some old, some new, some in line with the PCI DSS, some not.

THE EVOLUTION OF THE PCI DSS

The PCI DSS is revised periodically to address changes in the current threat landscape and industry trends. When threats to point-of-interaction (POI) devices increased, for example, the standard was amended to include Requirement 9.9. Similarly, after Secure Sockets Layer (SSL) and early Transport Layer Security (TLS) transmission protocols were compromised, guidance was released and the standard was revised to require migration to later TLS versions and interim mitigation of affected deployments. Typically, as the standard evolves, new requirements are considered to be best practices pending formal PCI DSS adoption.

- Data is used and stored for different reasons, and each reason is subject to different business drivers and constraints.
- Data exists in structured, unstructured, and even paper forms.
- Data finds its way into end users' email messages, spreadsheets, and thumb drives — effectively beyond the control of IT staff.

REMEMBER

Although most of the 12 requirements address issues such as security policies, access controls, antimalware software, and avoidance of default passwords, Requirements 3 and 4 focus on protection of the data itself. These two requirements collectively protect data as it moves over vulnerable networks and is stored. This area is where the PCI DSS overlaps most with many more-generic privacy mandates and data-breach-disclosure laws. Yet Requirements 3 and 4 can represent some of the most taxing aspects of PCI DSS compliance, often requiring unfamiliar technologies and practices (such as key management; see Chapter 2) and involving multiple touchpoints within organizations, crossing business silos and political domains.

The relative complexity of protecting data and satisfying Requirements 3 and 4 requires us to cover this topic extensively throughout the book. As we get into the details, you see that data-protection technologies such as tokenization aren't just ways to help achieve compliance with these two requirements. They also have the

potential to reduce the scope of your overall PCI DSS compliance obligation — a topic that we discuss in the next section.

Seeking the Holy Grail of Scope Reduction

If you're transmitting, processing, or storing payments, at least some of your environment is exposed to account data, which requires PCI DSS compliance. Even if you extensively outsource, you still have to ensure that your service provider adheres to the standard.

Fortunately, in December 2016, the PCI Security Standards Council published "Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation" (`www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf`). This document defines out-of-scope system components as those that don't connect to the cardholder data environment (CDE). It also includes system components that can't directly or indirectly affect CDE security as being out-of-scope. The document also clarifies that open public networks such as the Internet are not in scope.

Nevertheless, effective scope-reduction strategies may reduce the cost, complexity, and effort of achieving compliance.

Before you consider scope reduction, it's important that you clearly understand your obligations under Requirements 3 and 4 and the technologies that they mandate. We discuss these topics further in Chapter 2.

Protecting Other Data Using PCI DSS Principles

You're going to be investing a lot of time and money in building a secure infrastructure and supporting processes to meet PCI DSS security requirements. The PCI DSS is primarily concerned with the protection of cardholder data. What about all the other data that your company handles that has nothing to do with payments? Some of it may benefit from similar levels of protection.

By thinking beyond what you're doing to meet PCI DSS requirements, you can leverage those security principles to build additional solutions that support your organization's critical assets. You could do any of the following:

- Encrypt all the network traffic inside your organization to ensure that only those who need to see the data can do so.
- Protect all data at rest across your whole enterprise by using encryption and/or tokenization and ensuring that only those who are authorized to decrypt that data have access to it.
- Protect all sensitive data at the point of capture (the point at which it enters your organization) by encrypting selected fields in the data record.
- Keep security under your full control by encrypting data and managing the keys locally before sending data to any cloud service provider you use. (We discuss cloud providers in Chapter 3.)
- Implement a layered security approach so that your infrastructure doesn't have a single vulnerable point of attack, which makes it much more difficult for an attacker (inside or outside your organization) to gain unauthorized access to your data.


TIP

If you adopt a security-conscious approach to all data and to data access within your organization, meeting the specific PCI DSS requirements is much simpler.

IN THIS CHAPTER

- Securing data in storage
- Making data safe in transit
- Restricting and authenticating access to data and systems
- Tracking data access

Chapter 2
Examining Data Protection and Access Control Requirements

Protection of account data is prevalent throughout the 12 requirements of the PCI DSS, which we cover in Chapter 1. In this chapter, we focus on the security of cardholder data, including restricting and monitoring authentication and access.

The standard addresses the security of account data in storage and transit in Requirement 3 (Protect stored cardholder data) and Requirement 4 (Encrypt transmission of cardholder data across open, public networks). These requirements incorporate multiple subrequirements and testing procedures, which we can summarize as follows:

- Don't store cardholder data unless required for legal, regulatory, or business reasons.
- Protect cardholder data everywhere it's stored, from data centers to tape backups to faxes and copiers.

- Encrypt cardholder data (and any other type of account data) as it moves over any vulnerable network, particularly wireless networks and the Internet.
- Make sure that the way you're protecting data is well documented and easy to audit.

In the first part of this chapter, we cover Requirements 3 and 4 in detail, along with some technologies you can use to address them. The second part of the chapter focuses on Requirements 7, 8, and 10, which are dedicated to restricting, authenticating, and monitoring access to cardholder data and the systems where the data is located.

Protecting Stored Cardholder Data (Requirement 3)

At the heart of the PCI DSS is the need to protect any cardholder data that you store. The standard provides examples of suitable protection methods, such as encryption, tokenization, truncation, masking, and hashing.

WARNING

This section assumes that you're familiar with these security-related technologies. If you need background information on them, see Appendix A.

By using one or more of these protection methods, you can effectively make stolen data unusable. For one thing, the attackers won't have access to the cryptographic keys that encrypted the data in the first place.

TIP

Protecting stored data isn't a "one size fits all" concept. You should think of Requirement 3 as being the minimum level of security that you should implement to make life as difficult as possible for potential attackers.

Knowing the data storage rules

You need to know all locations where data is stored (a big incentive to minimize your data footprint). Requirement 3 also provides guidance about which data can — and can't — be stored. Here are a few examples:

- Under no circumstances (unless you are an issuer) can you store sensitive authentication data (full magnetic stripe data, card verification codes/values, personal identification numbers [PINs], PIN blocks, and so on) after authorization takes place.
- When you no longer need certain data, you must delete it securely.
- You can store only certain data items (see Table 2-1).

REMEMBER

One of the best pieces of advice in this requirement is "If you don't need it, don't store it."

TABLE 2-1 Cardholder Data Protection and Storage Requirements

Account Data	Storage Permitted?	Render Unreadable?
Cardholder data		
Primary account number	Yes	Yes
Cardholder name	Yes	No
Service code	Yes	No
Expiration date	Yes	No
Sensitive authentication data		
Full magnetic strip data or equivalent on a chip	No	N/A
Card security code	No	N/A
PIN/PIN block	No	N/A

Source: PCI Security Standards Council

Making stored data unreadable

The PCI DSS standard requires you to render a primary account number (PAN) unreadable anywhere it's stored, including portable storage media, backup devices, and even audit logs (which are often overlooked). The deliberate use of the word *unreadable* by the PCI Security Standards Council allows the council to avoid mandating any particular technology, which in turn futureproofs the

requirements. Despite this fact, Requirement 3.4 provides several options:

- One-way hashes based on strong cryptography in which the entire PAN must be hashed
- Truncation, which stores a segment of the PAN (not to exceed the first six and last four digits)
- Tokenization, which stores a substitute or proxy for the PAN rather than the PAN itself
- Strong cryptography underpinned by key management processes and security procedures

Managing keys securely

Whatever approach you intend to use to render your stored data unreadable, you need to secure the associated cryptographic keys. Strong encryption is useless if it's coupled with a weak key management process. The standard provides detailed guidance on managing keys — guidance that's significantly similar to the way banks and other financial institutions are required to secure their cryptographic keys. Key management efforts should include:

DECIPHERING CARD SECURITY CODES

The various card brands use different terminology to describe the three- or four-digit card security codes printed on the front or back of their payment cards. You may encounter the following acronyms to describe the codes on your payment cards:

- **CID:** Card identification number used by American Express and Discover
- **CAV2:** Card authentication value used by JCB
- **CVC2:** Card verification code used by Mastercard
- **CVN2:** Card validation number used by UnionPay
- **CVV2:** Card verification value used by Visa

- Use keys of appropriate cryptographic strength to align with recognized industry standards.
- Ensure that the keys you use to encrypt other keys are at least equal in strength to those that you use to encrypt your data.
- Store the keys you use to encrypt cardholder data separately from the keys you use to encrypt other keys or data (to prevent a single point of attack).
- Store keys in as few locations as possible.
- Restrict key access to the smallest number of key custodians necessary.
- Protect your keys by using technology such as hardware security modules (HSMs)
- Distribute your keys securely.

Additional requirements call on you to fully document the way you implement and manage various keys throughout their life cycles. Following are some of the important aspects you need to cover:

- The method you use to ensure that keys are replaced at the end of their valid cryptoperiod (which may require assistance from your software vendors) or when the integrity of the keys are weakened
- The process you use to securely delete or archive keys when you no longer need them
- How you ensure that retired or replaced keys are no longer available for encryption operations
- How you prevent unauthorized key substitution

Your success in managing keys depends on having good cryptographic key custodians: people you trust who won't collude to attack your systems. These people are required to formally acknowledge that they understand and accept their key-custodian responsibilities.

WARNING

When key custodians who know any part of a clear-text cryptographic key change roles or leave your company, be sure to rotate your cryptographic keys.

Also, you must ensure that security policies and operational procedures for protecting stored cardholder data are documented, used, and known to all affected parties within your organization.

WARNING

Don't underestimate the critical importance of strong key management, and don't try to take shortcuts. Your Qualified Security Assessor (as we describe in Chapter 1) will find your errors, and attackers may find them too.

Masking the PAN before displaying

The standard provides some very specific advice regarding the display of a PAN: Display the full range of digits (normally, 16) only to those personnel who must view it for business reasons. In all other cases, you must implement masking to ensure that no more than the first six digits and the last four digits of the PAN are displayed.

Encrypting Account Data in Transit (Requirement 4)

Sensitive data is quite vulnerable when it's transmitted over open networks, including the Internet, public or otherwise untrusted wireless networks, and cellular networks. The PCI Security Standards Council takes a very hard line on this situation, requiring the use of trusted keys/certificates, secure transport protocols, and strong encryption. The council also assigns you the ongoing task of reviewing your security protocols to ensure that they conform to industry best practices for secure communications.

Blocking eavesdroppers

Many potential attackers are eavesdroppers who are trying to exploit known security weaknesses. The standard includes specific requirements and guidance on establishing connections to other systems:

- Proceed only when you have trusted keys/certificates in place. You're expected to validate these keys and/or certificates and to make sure that they haven't expired.
- Configure your systems to use only secure protocols, and don't accept connection requests from systems using weaker protocols or inadequate encryption key lengths.

- Implement strong encryption for authentication and transmission over wireless networks that transmit cardholder data or that are connected to the cardholder data environment (CDE).

Securing end-user messaging

Much of the PCI DSS focuses on protecting PANs. Requirement 4 sets forth some specific rules about transmitting PANs across open networks. As a result, technologies that your organization normally uses (such as end-user messaging technologies) may need to be adapted, replaced, or discontinued when cardholder data is being transmitted. The main constraints of Requirement 4 are as follows:

- PANs must never be sent unprotected over commercial technologies such as email, instant-messaging, and chat applications.
- Before using any of these end-user technologies, you must ensure that PANs have been rendered unreadable via strong cryptography.
- If a third party requests a PAN, that third party must provide a tool or method to protect the PAN, or you must render the number unreadable before transmission.

REMEMBER

When you encrypt cardholder data as part of your network communications process, you must define the appropriate security policies and operational procedures. In addition, you must make sure that the relevant documents are kept up to date, made available to, and followed by all relevant people in your organization.

Restricting Access to Cardholder Data (Requirement 7)

A considerable portion of the PCI DSS concerns access control mechanisms, which must be sufficiently robust and comprehensive to deliver the protection required for cardholder data. Requirement 4 of the standard, for example, declares that PANs must be rendered unreadable by a method such as encryption or tokenization, but if you think that encryption or tokenization is the end of your responsibility for protecting PANs, you're wrong.

Requirement 7 clearly states that you must restrict data access. You have to ensure that critical data can be accessed only by authorized personnel and that you have the appropriate systems and processes in place to limit access based on business needs and job responsibilities. The requirement also calls for you to immediately remove access when access is no longer needed.


TIP

Try to keep the number of people who need access to data to the absolute minimum, with access needs identified and documented according to defined roles and responsibilities.

Managing your access policy

The standard requires you to think very carefully about who in your organization has access to system components and the effect of that access on the security of your CDE. This task becomes much more complex if you have multiple office locations or data centers, or if you use cloud-based service providers to host some of your data.

You're required to manage your access control policy at quite a granular level, carefully defining the various user roles in your organization (user, administrator, and so on) and specifying which parts of your system and data they can access.

In practice, you need to implement sufficient controls to create a practical, effective access control policy, so spend sufficient planning time to devise the best mechanism to satisfy your needs.

Assigning "least privilege" access rights

The standard is prescriptive in that it forces you to grant "least privilege" access rights to all user accounts with requests for access documented and approved. The logic is that you grant each person only enough access to the various bits of the system or data he needs to perform his job functions. An administrator, for example, could define an access policy for another user to view the cardholder data, but she herself wouldn't be able to read the data directly.

Depending on your environment, you may need to address multiple system types and varying levels of access for network, host, and application-level use and administration. This task can prove to be complex when, for example, you need to give multiple types of users different access rights to your databases.


TIP

It's best to disable access to data by default and then enable any access that's required. This method makes it easier to prevent access-granting mistakes that could lead (in the worst-case scenario) to a data breach.

Revoking data access

When a user has a change of role internally, document the change, and modify that user's privileges as appropriate. Similarly, when a user leaves your company, you need to document the change and then disable or delete his user account in alignment with your organization's policy and procedure.


TIP

An established, consistent process can help ensure strong privilege management. In addition, we recommend that you periodically run queries on user accounts to verify account activity. You might run a scheduled script on a quarterly basis, for example.

Authenticating Access to System Components (Requirement 8)

Strong security is essential for protecting your systems and data from unauthorized access. Requirement 8 of the PCI DSS contains many elements that you need to address in your access control and password policies for staff members and third parties alike. We discuss some of these elements in the following sections.

Ensuring individual accountability

It's important to ensure that every user (internal or external) who needs access to your systems has a unique identifier so that no dispute occurs later about who performed a particular task. (For details on handling nonrepudiation, for example, see PCI DSS Requirement 8.1.) Strict enforcement of unique identifiers for each user inherently prevents the use of group-based or shared identities (see PCI DSS Requirements 8.1.5 and 8.5).

You also need to ensure full accountability whenever new users are added, existing credentials are modified, or the accounts of users who no longer need access are deleted or disabled. This accountability includes revoking access immediately for a terminated user, such as an employee who has just left your company (see PCI DSS Requirements 7.1.4 and 8.1.2).

Making access management flexible

Having a compliant user access policy is all well and good, but that policy takes you only part of the way to compliance with the PCI DSS. You're required to underpin your user access policy with an access management system that spells out various tasks, such as the following:

- Restricting data access by third parties (such as vendors that require remote access to service or support your systems). Grant access only when those parties need it, and monitor their use of your system. Never offer unrestricted 24/7 access.
- Locking out users who make multiple unsuccessful login attempts over a specified period (to make automated password attacks more difficult).
- Making the system unavailable to any user after a specified period of inactivity and requiring a repeat login to continue (to minimize the risk of impersonation).
- Enforcing multifactor authentication methods (normally, tokens or smart cards) for people who attempt nonconsole administrative or remote access to CDE system components. This enhanced security approach raises the bar for attackers.

Beefing up authentication

For all types of access, the standard expects a strong authentication system. You won't be surprised to find that the standard doesn't stop there; it also provides details on implementing and managing this authentication system. In the case of passwords, for example, PCI DSS Requirement 8.2 directs you to do the following:

- Use strong cryptography to render all authentication credentials (such as passwords or passphrases) unreadable during transmission and storage on all system components, thereby devaluing data where it's most vulnerable to an insider attack.
- Set strict conditions for passwords. As a fundamental requirement, all passwords must be changed every 90 days as a minimum. You must enforce a minimum of seven

alphanumeric characters for any given password. The reuse of previous passwords must be prohibited

- Supply an initial password to each new user, and require her to change that password the first time she accesses your system.
- Prohibit group shared passwords.

After you establish an authentication policy, provide it to all users to help them understand and follow the requirements.


TIP

In Chapter 4, we provide practical guidance on using existing security solutions to meet the standard's access control and password management requirements.

Monitoring Access to Cardholder Data (Requirement 10)

If you don't have precise details on how and when your data is being accessed, updated, or deleted, you'll struggle to identify attacks on your systems. Also, you'll have insufficient information to investigate if something goes wrong, especially after a data breach.

Fortunately, Requirement 10 calls for keeping, monitoring, and retaining comprehensive audit logs, as we discuss in the following sections.

Maintaining audit trails

The standard mandates that certain activities — especially reading, writing, or modifying data (see PCI DSS Requirement 10.2) — be recorded in automated audit trails for all system components. These components include external-facing technologies and security systems, such as firewalls, intrusion-detection and intrusion-prevention systems, and authentication servers.

In addition, the standard describes how to record specific details so that you know the who, what, where, when, and how of all data accesses. Any root or administrator user access, for example, should be logged, especially when a privileged user escalates his privileges before attempting data access.

REMEMBER

PCI DSS Requirement 10.4 also calls for all CDE system components to be configured to receive accurate time-synchronization data. If you don't already have this capability, you may need to upgrade your systems.

One important piece of information to log is any failed access attempt — a good indicator of a brute-force attack or sustained guessing of passwords, especially if the access log has lots of entries. You must also record additions and deletions, such as increased access rights, lower authentication constraints, temporarily disabling of logs, and software substitution (which could be a sign of malware).

Preventing unauthorized modification of logs

After you create your audit logs, you must ensure that the logs are secured in such a way that they can't be altered. You must use a centralized logging solution (see PCI DSS Requirement 10.5.3) with restricted access and sufficient capacity to retain at least 90 days' worth of log data from all system components within the CDE, with the remainder of a full year available for restoration if needed.

Making regular security reviews

As well as ensuring that required details are generated, centrally stored, and secured against unauthorized access or modification, you must monitor your logs and security events on at least a daily basis, with alerts requiring review at any time of day or night (see PCI DSS Requirements 10.6 and 12.10.3). This requirement helps you identify anomalies and suspicious activity.

TIP

Look to implement a centralized logging solution that accounts for future capacity and includes reporting tools.

IN THIS CHAPTER

- Keeping stored cardholder data secure
- Employing encryption
- Giving third parties access

Chapter 3
Choosing a Data Security Solution

In Chapter 2, we summarize the PCI DSS requirements that focus explicitly on data protection and access management. In this chapter, we shift our perspective to implementation choices.

REMEMBER

Any part of your organization that comes into contact with account data must be assessed against the full set of PCI DSS requirements.

There's no one-size-fits-all solution for protecting account data; every organization is different, faces different threats, and has different security objectives that (ideally) go beyond PCI DSS compliance. This chapter presents a general framework that you can apply to your own organization while highlighting the pros and cons of the choices that you'll make along the way.

TIP

It's always best to approach data protection as a strategic investment rather than as a purely compliance-driven obligation.

Protecting Stored Data

In this section, we provide an overview of various technologies you can use to protect your stored data. Although protecting data on end-user devices (such as mobile devices, laptops, and flash drives) is important, in this chapter, we focus on business applications and enterprise infrastructure.

TIP

Data can spread rapidly across an organization, piling up in data repositories and archives, and inadvertently spilling over into test locations, audit logs, and forensic reports. Always try to minimize the amount of account data you must store well before you figure out how to protect it. Simply limiting the spread of account data is the easiest way to limit PCI DSS scope.

DON'T LOSE YOUR KEYS!

All approaches to protecting stored data must involve some element of key management, which (as we explain in Chapter 2) can be a thorny topic. Key management isn't just about protecting access to keys to meet compliance obligations; it's also a business-continuity issue. Protecting stored data with persistent encryption gives rise to the need to manage keys over the long term. Lose the keys, and you lose the data.

The good news is that in most cases, systems can be easily configured to support hardware security modules (HSMs). These devices can support the enforcement of key management policies, provide physical protection against tampering, and establish clear separation of duties between security officers and storage administrators.

When security professionals take key management seriously, encrypting stored data is a win for everyone. Proper key management not only addresses compliance requirements, but also improves your organization's overall security posture.

Encrypting Data

One of the most common and most effective approaches to protecting stored data is *encryption* — the process of encoding sensitive data so that only authorized parties can read it.

TIP

Both hardware- and software-based encryption (cryptographic) solutions are available. Choose a secure solution that offers easy key management and scalability.

The Ponemon Institute has been conducting global research for many years on the strategy and adoption of encryption by enterprises. In an April 2017 research report, they report it is evident that more and more organizations are using encryption especially in conjunction with HSMs. Figure 3-1 shows the year-on-year rise in HSM usage.

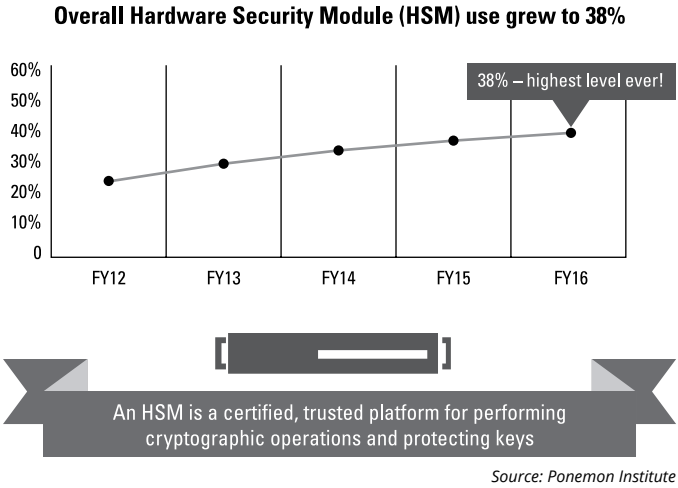
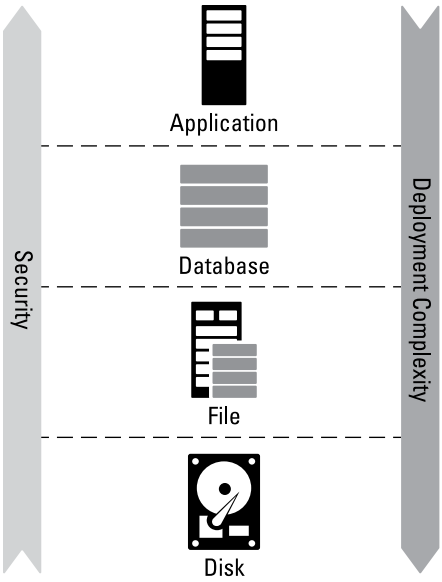


FIGURE 3-1: Increased use of HSMs by enterprises.

Encryption is typically employed on four layers of the technology stack (see Figure 3-2):

- Disk (or media)
- File
- Database
- Application



Source: Thales

FIGURE 3-2: Layers of the technology stack where encryption is applied.

Generally, when you employ encryption lower in the stack, it's less likely to interfere with operations in the layers above. If encryption occurs on the disk layer, for example, there's little risk of any effect on the file, database, and application layers, which continue to have access to decrypted data and are unaware of the encryption applied on the disk layer.

WARNING

Unfortunately, this simple technique delivers little protection. When a user boots the media with the encryption key, all the data is in the clear, fully exposed to threats both inside and outside your organization. For PCI DSS compliance, the implementation must rely on a logical access method that's separate from the native operating system (Requirement 3.4.1).

Alternatively, if you decide to apply encryption (and/or tokenization) on the application layer, data is encrypted right at the source before it leaves the application or e-commerce server. This approach significantly increases security, as it protects the data from unauthorized access, but it's typically complex, costly, and time-consuming to implement. These drawbacks occur because application developers need to modify each application that

requires access to the encrypted data and to support all the associated key management processes.

In the following sections, we look at the four layers of the technology stack in detail, explaining the advantages and disadvantages of applying encryption on each layer.


TIP

Before selecting a solution, it's important to evaluate technology support. Solutions can have limited support for operating systems, databases, and file types. If your organization deploys a wide range of technologies, selecting the solution that has the broadest technology support helps you establish an enterprise-wide encryption strategy, and saves you time and money in the long run.

Full-disk encryption

The simplest way to encrypt your stored data is to employ full-disk encryption (FDE) or self-encrypting drives, which may be free options that come with your storage hardware. These solutions encrypt all information as it's written to the disk and decrypt the information as it's read off the disk.

The main advantage of such an approach is that it's transparent to applications, databases, and users. In addition, you may experience little or no degradation in disk read and write times, because the encryption is typically done in hardware.

The major disadvantage of this approach is that it addresses a limited set of threats, offering data protection only if the physical drive is stolen. When the drive is booted and the encryption key is accepted, all the data on that drive is available to any user who can gain access to the system.

FDE makes sense for laptops, which are highly susceptible to loss or theft. This encryption approach, however, isn't suitable for the most common risks faced by your organization, and it frequently fails to meet the standard or industry best practices for the following reasons:

- FDE doesn't offer safeguards against advanced persistent threats, malicious insiders, or external attackers.
- If an attacker gains access to an application through an authorized user's credentials, FDE doesn't prevent the attacker from decrypting the data.

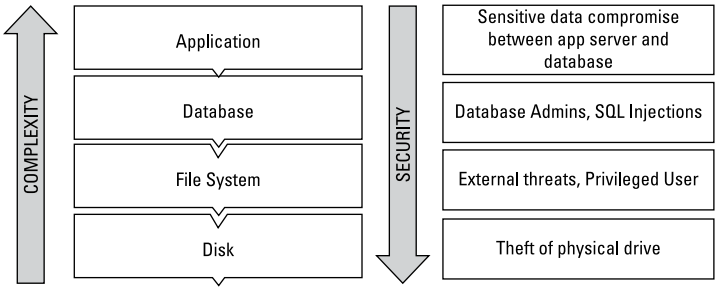
» FDE leaves a limited audit trail, which means that administrators have little or no ability to report on what files have been accessed — only on whether the drive was booted and authenticated with the encryption key.

File-system encryption

If you need something more comprehensive and flexible than full-disk encryption, file-system encryption may be the solution for you.

When you apply protection within the file system or database, that protection can be more granular and can integrate seamlessly with a wide range of access controls, activity monitoring solutions, and auditing tools. Encryption at the level of storage media tends to be an all-or-nothing experience. But one advantage of using encryption within the file system — and particularly within databases — is that it makes it easier to target individual tables, columns, or even cells. Other benefits are that file-system encryption is transparent to your users, so you're unlikely to need to change your applications or any associated business processes.

Before we get into any more detail, we should point out the need to consider what types of threats you're trying to mitigate by choosing to apply encryption on any layer. Figure 3-3 summarizes the protection you gain by employing the appropriate technology solution on each layer of the stack.



Source: Thales

FIGURE 3-3: The threats mitigated by encryption on each layer of the technology stack.

By employing encryption at file level, you can establish strong controls that guard against abuse by privileged users within your organization — which stands to reason, as the recent Thales Data Threat Report (`https://www.thalesesecurity.com/about-us/newsroom/news-releases/2017-thales-data-threat-report-security-spending-decisions-leave`) shows that most respondents identified privileged-user threats as their greatest concern.

TECHNICAL STUFF

Although this encryption method may seem to be more complex than low-level encryption of storage media, you can deploy it in a way that's transparent to your business applications by installing data security software agents within the operating system. You can get the necessary software agents from a specialist data security vendor such as Thales eSecurity. The agents intercept all read and write calls to disks and then apply policies to determine whether the data should be encrypted or decrypted. In addition to offering encryption, some advanced file-system solutions incorporate controls that enable you to create policies governing access and file-system functions based on criteria such as users, groups, and processes.

WARNING

One disadvantage of file encryption is that it doesn't guard against some threats that may be important to you. If you encrypt database files, for example, the data is still vulnerable to a malicious database administrator or SQL injection attack. You may also have to consider adding a compensating control such as database activity monitoring to your data security environment.

Database encryption

While approaches vary from solution to solution, by implementing encryption at the database layer, you can encrypt a specific subset of data within the database (such as a column) or the entire database file.

The main advantage of using database encryption is that it safeguards against a wide range of threats, including malicious insiders and even malicious database administrators. In addition, you don't need to modify your applications.

Unfortunately, database encryption has a significant potential down side. One problem is that database-specific encryption policies, cryptographic keys, and other features apply only to the vendor's databases. This arrangement may be fine if your organization uses a single database vendor (such as Oracle or Microsoft).

If your organization has a mix of applications and databases, however, administrating multiple vendor-specific solutions can be time-consuming and complex, with keys and policies being managed in different ways, with separate system management tools and unique user interfaces.

Several database vendors offer encryption capabilities in their products. Customers that run specific versions of Oracle or Microsoft SQL Server databases, for example, can take advantage of Transparent Data Encryption (TDE) functionality. Additionally, security vendors such as Thales eSecurity offer encryption products that support multiple database offerings with a consistent centralized management platform.

WARNING

When you use multiple solutions, you lack centralized administration across different technologies, which can lead to security risks and compliance gaps. The PCI DSS requires separation of administrative duties, in the event that clear-text key management operations are in use, to prevent a single administrator from having complete control of sensitive assets and services. As a result, your organization may need to have controls in place to ensure that one set of administrators manages cryptographic keys and another group manages organizational databases.

Application encryption

Application-layer encryption (or, equally, tokenization) applies data protection on a higher layer than the database or file layer. Logically, the application is an excellent choice to protect account data, because it's the only thing that actually knows what account data is and how it's allowed to be used. You can protect individual primary account number (PAN) records selectively, for example, by making them unreadable on a record-by-record and user-by-user basis.

Under this approach, existing applications are updated to call new application programming interfaces (APIs) to govern the encryption or tokenization of the data. Often, application encryption solutions use a collection of software libraries and languages (such as C, Java, or .NET) to enable the encryption of specific types of application data. Complementary tokenization solutions may use representational state transfer (REST) APIs. Alternatively, cryptographic APIs may integrate with an organization's existing hardware security modules (HSMs).

TECHNICAL STUFF

REST is a term associated with client server systems promoting an architectural design style that uses standard interfaces and protocols. REST is typically used in web service developments in which resources (both data and functionality) are consumed in a stateless manner so that multiple servers can be configured to handle any client request, providing easier scaling of processing capacity and/or redundancy.

In general, the advantage of using application encryption is that the solution typically protects specific subsets of data, such as PANs. Other data elements can remain in the clear without disrupting any of your other applications. In addition, the protection spans multiple layers, from application to disk; guards against a range of threats; and ensures that a PAN is never exposed in the clear anywhere in your environment after initial capture and processing by your application. This solution works with any vendor's database and eliminates some of the limitations of database encryption (discussed in the preceding section).

As you might expect, you have to make some trade-offs for this level of control and granularity. The main challenge is that compared with file, database, and disk encryption, application encryption must be tightly integrated with the application, which requires significant development efforts and resources. Also, this type of encryption may change column sizes, potentially necessitating changes in database schema. If data format preservation is required, tokenization or solutions such as format-preserving encryption (FPE) can be integrated with the application, as we discuss in the next section.

TIP

If you apply protection on the application layer, downstream systems such as databases, file systems, and storage environments are exposed only to encrypted or tokenized PANs, which may help you limit scope.

REMEMBER

Sharing encrypted data between applications means sharing keys. This approach relies on trust and may require shared security management systems, all of which must comply with the PCI DSS. The same is true of tokenization (see the next section).

Tokenization

The goal of tokenization is to render the data valueless to an attacker. For the purposes of PCI DSS compliance, a token must bear no resemblance to the original PAN. Per the guidance of the

PCI Security Standards Council, the security of a token is determined by the infeasibility of determining the original PAN based on the resulting token. The council further stresses that the tokenization of sensitive authentication data (including magnetic strip data or the equivalent on a chip, card verification codes or values, and PINs/PIN blocks) is not permitted.

REMEMBER

In some cases you may wish to use FPE tokenization (as described in Appendix A) to maintain some of the structural properties of the PAN. It is important not to confuse FPE tokenization with other encryption techniques, such as hashing, which is a one-way encryption technique. FPE tokens are reversible and can be decrypted to produce unencrypted plain text.

The main advantage of using tokens is that they minimize potential for exposure of sensitive data to accidental or unauthorized access. Applications generally can operate with tokens; a small number of trusted applications can be permitted to detokenize when strictly necessary for an approved business purpose.

To reduce maximum risk, the tokenization system must be logically isolated and segmented from systems and applications that previously processed sensitive cardholder data. An advantage is that only the tokenization system can tokenize data to create the tokens in the first place. When the reverse process is required, only this system can transform the tokenized data back to its original state. Further, the token-generation method must block attackers from using direct attacks, cryptoanalysis, side-channel analysis, token-mapping table exposure, or brute-force detokenization techniques.

TECHNICAL STUFF

Although tokenization may make your life easier in terms of PCI DSS compliance, a potential disadvantage is that a larger burden may fall on others within your organization. Table 3-1 summarizes at a high level what is in scope and what is out of scope for PCI DSS when you use tokenization.

Tokenization types

The payments industry uses two main types of tokenization, which are initiated and controlled by different distinct entities in the ecosystem:

- Issuer
- Acquirer

Both methods replace a PAN with a surrogate value (or token). Each method, however, has a different objective and is used by different parts of the payments ecosystem. Depending on your role, you may need to support one type or both types in your environment.

TABLE 3-1 What Is in Scope for Tokenization

In Scope PCI	Out of Scope PCI
Token servers and supporting system components	Application servers storing tokens without access to detokenize tokens
Application servers which can detokenize tokens	Database servers storing tokens without access to detokenize tokens
Administrators on systems who can detokenize tokens	

WARNING

The payment industry often uses multiple terms when describing tokenization and therefore you may see references to *nonpayment tokenization* or *network tokenization,* which we are covering under *acquirer tokenization* in this book. The terms are interchangeable.

Issuer tokenization is used to segregate payment channels, ensuring that any data breached in one channel is invalid for use in another. Typically, an issuer creates a separate, logically unique token for each payment type or method associated with the same consumer account. Three different tokens, for example, could be assigned to the same debit card account: one for contactless mobile payments in a store, one for use when shopping on the Internet, and one for making payments using consumer devices such as bracelets. The main advantage of using a token rather than the real PAN for the account is that if compromise occurs, only the token needs to be replaced — not the PAN and associated payment card. Individual issuers (or their third-party token service providers) maintain the lookup tables between PANs and tokens for their customers, and protect the PAN in the lookup table by using encryption.

Acquirer tokenization is designed to protect the merchant from data breaches. The merchant doesn't have to store even the encrypted PAN, which reduces its scope for PCI DSS compliance. Typically, the real PAN is used for the payment transaction up to the authorization stage. At the point where the merchant needs to store

customer account data to assist with business processes such as chargebacks, after-sales returns, and loyalty programs, the merchant uses a token rather than the real PAN. Normally, the token is generated and controlled by the acquirer or the card network and provided to the merchant as a substitute for the PAN in the authorization response. The main advantages of this system are that merchants reduce their PCI DSS compliance scope, business processes don't have be redesigned, and the risk of exposure of sensitive data is dramatically reduced.

REMEMBER

All elements of the tokenization system — including tokenization, detokenization, and PAN storage — are considered to be part of the cardholder data environment (CDE) and, therefore, parts of your system that are assessed for compliance with PCI DSS. Also, any system component or process that has access to the tokenization system or the tokenization/detokenization process is considered to be in scope. Systems that handle tokens without access to cardholder data, the detokenization process, or detokenized data, however, may be out of scope of the PCI DSS, depending on the company's tokenization system — including but not limited to system segmentation. (That is, the system may not reside within CDE network segments.)

Guidelines for tackling tokenization

The PCI Security Standards Council first issued specific guidance about tokenization in August 2011, in a document called "Information Supplement: PCI DSS Tokenization Guidelines" (`https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf`). This document describes the major components of a tokenization system and its primary security aspects, including how tokens are generated, mapped to PANs, and protected during storage, as well as how access to the system is controlled. The document also deals with distinguishing tokens from real PAN values — an important task from an assessment point of view, because it's necessary to prove that data objects that look like PAN data are in fact only tokens.

In April 2015, the council published an additional document called "Tokenization Product Security Guidelines," which is available at `https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf`. This supplementary document, which was developed in conjunction with technology vendors and security assessors, provides technical

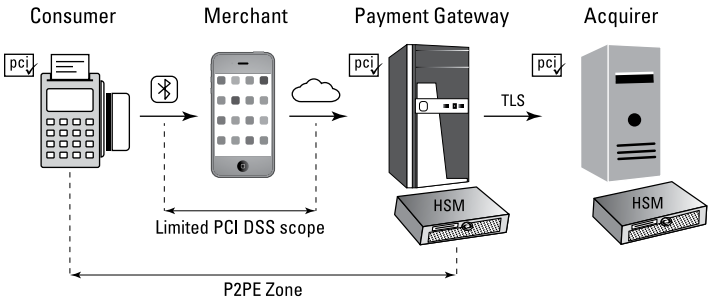
guidelines for evaluating tokenization products. Further, the document offers best practices on topics including token generation, storage in back-office systems, and attack mitigation.

Both documents are essential reading if you're contemplating using tokenization to limit your stored-cardholder-data footprint.

Point-to-point encryption

Point-to-point encryption (P2PE) protects vulnerable payment infrastructure. This method is used almost exclusively in point-of-sale (POS) environments to protect data as it travels from the merchant's environment to a payment gateway or acquirer.

P2PE encrypts data at the point of capture (the POS terminal or mobile POS reader). Thereafter, this data is maintained in an encrypted state and can be decrypted only inside the HSM at a payment gateway or acquirer. At this point, the HSM may encrypt the data again for a new P2PE zone established for the next segment of the processing chain — normally, the card network. Figure 3-4 illustrates how P2PE is used in a mobile POS environment.



Source: Thales

FIGURE 3-4: P2PE securing the data from the point of capture to the payment gateway.

If you're a merchant, the main advantage of using P2PE is that no clear-text cardholder data flows through your systems. Just as important, you have no means of decrypting the data because you don't have access to the necessary cryptographic keys. Your acquirer or payment service provider takes care of this process on your behalf. Therefore, P2PE is effective in reducing the scope of PCI DSS compliance for you, as well as in devaluing data in a

segment of the payments ecosystem where data breaches used to be widespread (and lucrative for attackers). The main potential drawback to implementing P2PE is that you may need to purchase a hardware upgrade for your POS systems to support the data encryption process. This upgrade may be costly if you have a large number of terminals that aren't suitable for a software-only upgrade.


TIP

The PCI Security Standards Council provides a list of approved P2PE solutions for merchants, acquirers, and service providers at `https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions`.

Sharing Data with Third Parties

If you're considering sharing account data with third parties, we recommended that you first review the PCI Security Standards Council publication "Information Supplement: Third-Party Security Assurance Guidance" (`https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf`). Here are some of the points to consider:

- These third parties should appear in the list of approved or compliant service providers published by the relevant payment brands (see PCI DSS Requirement 12.8).
- These entities and the services that they provide should be included in your annual risk assessment efforts for completeness.
- You should perform necessary due diligence, including vendor review, risk assessment, evidence of the entity's PCI DSS compliance status, and definition of its PCI DSS compliance responsibilities.
- Any contract should include the service provider's acknowledgement of its responsibility for the security of account data that it possesses, transmits, processes, and/or stores on your behalf.

Some payment card brands maintain lists of service provider compliance status, which you can review to check a provider's

initial PCI DSS compliance status and assessed service information. We advise that you also review the provider's attestation of compliance and supporting material.

Protecting data in the cloud

The term *cloud* means different things to different people. The National Institute of Standards and Technology offers a definition in its Special Publication 800-145 (`http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf`): "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

You may be surprised to discover that the PCI Security Standards Council doesn't use the word *cloud* in the PCI DSS requirements. Instead, in March 2016, the council released a useful supplementary document titled "Third-Party Security Assurance and Shared Responsibilities" (`https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf`) that covers circumstances in which organizations outsource some or all of their CDEs to a third party.

The general industry terms for such entities are *cloud service provider* and *third-party service provider*. If you choose to use such an entity, it becomes an integral part of your CDE and affects both your CDE security and your PCI DSS compliance.

To secure your interface with a cloud provider in a way that ensures PCI DSS compliance, make sure that you address the following:

- Security of your critical data, regardless of where it resides in the cloud environment
- Verifiable evidence that data is maintained in compliance with PCI DSS requirements
- Proof that if a data breach occurs, the keys used to encrypt your data weren't compromised
- Data security that you control (no sole reliance on a third party)

TIP

Consider leveraging the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) (`https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview`) to help you select the most appropriate cloud service provider offering for your needs. Similar to the PCI SSC, participation in the CSA is welcomed and helps organizations to have direct input in its ongoing development.

TECHNICAL STUFF

In "Third-Party Security Assurance and Shared Responsibilities" (discussed earlier in this section), the PCI Security Standards Council states, "Ultimate responsibility for compliance resides with the entity, regardless of how specific responsibilities may be allocated between an entity and its third-party service provider(s)."

Some reasons to consider using the cloud include reducing costs, achieving greater scalability, and realizing flexibility in CDE security. Many cloud providers already have their environments assessed for PCI DSS compliance, so ideally, their services will support many of your compliance needs.

TIP

Third-party relationships should be carefully assessed and monitored. Services provided, due diligence, written agreements, compliance status, access requirements, and applicable PCI DSS requirements should be documented, and the details should be reviewed annually (see Requirement 12.8). Solutions such as VendorPoint and VendSure from Fortrex can help organizations accomplish this task and manage associated risks effectively.

The critical point to bear in mind is that these providers don't manage the storage, transmission, and processing of your cardholder data. Instead, they create a platform that enables you to manage your data in a secure, standard-compliant manner.

WARNING

The cloud deployment model that you adopt will have a major effect on the operational and security procedures that you manage as part of PCI DSS compliance. You and the provider will share many security implementations, and your ability to operate under this shared-responsibility model will almost certainly affect the technical knowledge and operating structure that your organization requires.

Keeping control of cryptographic keys

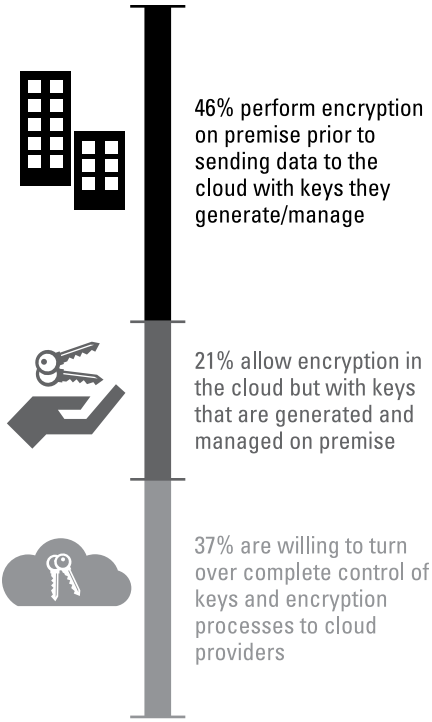
As you further explore third-party service provider relationships, you'll want to consider various deployment options for encryption and key management. Here are a few important questions that you should answer:

- **Are you in control of your cryptographic keys?** You may need to change service providers or take cryptographic key management processes in-house at some point.
- **How well do you understand your applications?** If you wrote your own business application, there's a good chance that you know how the application uses cryptographic keys. If you're deploying commercial software, however, you may not know what keys exist within those systems, let alone how well they're being protected.
- **What logical access controls exist?** Even if you're comfortable that your application protects keys appropriately, the risk still exists that the application itself may be misused. You must implement — and enforce — strong access controls that limit user privileges (see Chapter 2).
- **Are physical controls necessary?** Virtually all software-based systems are susceptible to physical tampering or theft. PCI DSS Requirement 9 forces you to consider the physical environment of your systems, including those that contain keys.

Organizations continue to show a preference for control over encryption in the cloud as shown in Figure 3-5.


TIP

For peace of mind regarding good security practice and key management when using commercial software, be sure to verify that your payment application software is validated for the Payment Application Data Security Standard (PA-DSS; see Appendix B), visit `https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php`). The payment card brands require this validation, which assures you that the software has received a thorough, independent security validation performed by certified Payment Application Qualified Security Assessors (PA-QSAs).



Source: Ponemon Institute

FIGURE 3-5: Control over encryption in the cloud.

IN THIS CHAPTER

- Defining access control policies
- Enforcing appropriate authentication
- Recording all activities

Chapter 4
Managing Your Data Security Operations

Given the challenge of managing your day-to-day security operations, maintaining strict access control and comprehensive data monitoring are equally important — and essential, in the case of the PCI DSS. The off-the-shelf security mechanisms that come with operating systems and databases probably aren't sufficient for your ongoing needs. What you really need to complement these mechanisms are additional layers of security controls.

In this chapter, we discuss suggested security control strategies addressing access controls, authentication, and monitoring to support organizational efforts to limit access to authorized personnel, systems, and processes — the overarching theme of PCI DSS Requirement 7, Restrict access to cardholder data by business need to know (see Chapter 1). We also offer some practical ways to provide administrative access to sensitive data without affecting your compliance status.

Controlling Data Access

When you design your access-control policy to comply with the PCI DSS, one of your main objectives is to limit access to system

components and cardholder data to those people whose jobs require such access. The most effective way to implement this policy is to add a security control on top of the operating system's native access-control system, which simplifies management of the cardholder data environment (CDE).

TIP

Some off-the-shelf data security software agents can supplement defined access controls to prevent administrators and privileged users from accessing cardholder data without stopping them from performing their assigned duties.

REMEMBER

You need to know exactly who can access your systems and data. Limiting access to as few people as possible makes this task much easier.

For each person or role that has access to CDE system components or data, it's important to prevent exposure of cardholder data where appropriate and prevent administrators from granting themselves unauthorized access. This policy effectively implements a "need to know" approach and has no effect on operational tasks such as backups and normal administrative actions. Keeping readable metadata associated with files in the clear, for example, is imperative; administrators must be able to identify files that need to be backed up but don't need access to the data inside those files.

These important considerations can make designing an access-control policy easier:

- **Be selective.** No administrator or root user should be granted access to the CDE unless your organization has a legitimate business need to provide such access.
- **Document all accesses.** For all access to data, it's important to document the user's job classification, role, and business responsibilities, as well as the time of data access and the systems that were accessed.
- **Document all changes.** Keep records of all access control rights that you grant or change to ensure that appropriate approvals are recorded.
- **Take no chances.** A default "deny all access" approach works best. Add access rights to users and applications by enforcing the principle of least privilege. If access isn't required, access shouldn't be authorized.

Managing and Authenticating Users

Having effective access controls for both users and applications ensures that only authorized users are authenticated before you grant access and make data accessible.

To prevent eavesdropping and unauthorized access, make sure that all authentication credentials (such as passwords and passphrases) are strong and unreadable during both transmission and storage. You can achieve this goal by using a complex password transmitted via a secure communication channel and stored with transparent encryption, for example. (See the nearby sidebar "Making passwords strong.")

Look for easily integrated solutions that use existing directory services such as Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory. Focus on solutions that offer centralized control so that you don't have to enter the same configuration information multiple times for each location. This type of system can also simplify cryptographic key management and prevent problems with integrity and continuity.

Here are some important points to consider in deciding how to authenticate users:

- **Strive for flexible authentication.** Look for solutions that allow scalability and support the three fundamental authentication methods, such as something you have (tokens, smart cards), something you are (biometric), and/or something you know (passwords), because different user roles may have different authentication requirements.

  
  REMEMBER

  All nonconsole administrative and remote access requires multifactor authentication. Multifactor authentication must incorporate at least two of the three authentication methods, which must be independent in such a way that access granted by one factor doesn't affect any other factor. For details, see the PCI Security Standards Council's "Multi-Factor Authentication" information supplement (`https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf`).

- **Don't reinvent the wheel.** Leverage any existing directory services that your organization uses, such as LDAP or Microsoft Active Directory.

TIP

MAKING PASSWORDS STRONG

A strong password typically has these characteristics:

- It's at least seven characters long.
- It includes capitalized letters, lowercase letters, and numbers in combination with special characters (such as !@#$%^&*-+=).
- It's rotated at least every 90 days.
- It's different from the user's previous four passwords.

To enable such complexity throughout your organization, be sure to define password requirements in your organizational access-control policy and procedures. Also, make vendors and subcontractors subject to the same password requirements, and promptly revoke their access rights when they're no longer under contract.

» **Encrypt stored credentials.** Ensure that your strong password practices (see the nearby sidebar "Making passwords strong") are supported by secure password storage.

Monitoring and Auditing All Activities

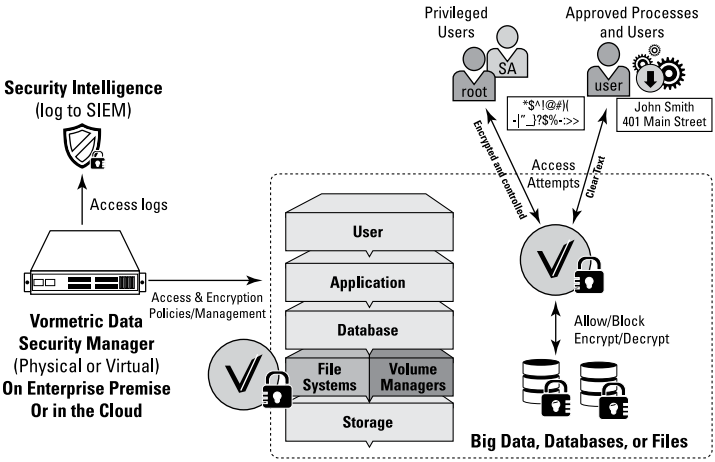
The security of your audit logs is just as important as the data that they contain. After all, there's no point in having detailed logs if you can't trust their contents!

The PCI DSS demands that you generate and retain audit logs of all successful and failed accesses to CDE system components, encrypted data access and use, and administrative actions. Further, you must analyze such events at least once a day and monitor alerts around the clock (see PCI DSS Requirements 10.6 and 12.10.3).

REMEMBER

Encryption solutions that log encryption-key requests but don't track continuous data access and use typically aren't sufficient for PCI DSS compliance. You need to be able to control and track all activities, even those of privileged users.

To give you a high-level view of how such enforcement works in practice, Figure 4-1 shows an example data security solution that enforces least-privilege policies on privileged users.



Source: Thales

FIGURE 4-1: Enforcing least privilege policies on privileged users.

Looking for Specific Solution Features

Any solution that you consider should have the following capabilities and associated access policies:

- **Granularity:** The policies that you define should be flexible enough to ensure that you monitor individual accesses of cardholder data, including logging the activities of root or administrative users.
- **Prevention:** Establish policies that prevent privileged users from accessing data in the clear but still enable them to perform their day-to-day duties.
- **Recording:** The solution must log both failed and successful events to view cardholder data so that you can ascertain whether an attack on your system is being launched.
- **Alerts:** Administrators should be able to set policies that generate automated alerts whenever activities that require special monitoring occur.

- **Centralization:** Individual logs must be promptly backed up to a central location for further analysis. This task can be facilitated by a security information and event management system.
- **Time synchronization:** All CDE system components should be configured to receive accurate time from a designated internal source, and only designated hosts should be permitted to receive the time from authoritative external sources.
- **Flexibility:** Any solution in which you invest should not only satisfy today's requirements, but also migrate with you to new environments, such as Big Data and the cloud. Make sure that your solution doesn't lock you into a specific platform. Select a solution that supports a range of platforms to meet new requirements and offer growth opportunities.

IN THIS CHAPTER

- Understanding what you need to do
- Managing an effective program
- Aligning compliance efforts with business goals

Chapter 5
Ten Keys to PCI DSS Success

This chapter details ten critical steps that can help you with your PCI DSS compliance efforts. We start by looking at some aspects of what you need to do to secure your cardholder data environment (CDE) to help you understand the types of data protection technology you may need and the comprehensive documentation and processes that are necessary to support them. Then we cover the program management aspects of your compliance efforts, offering practical advice on where you can get assistance and how to prevent some common pitfalls. Finally, we explore areas where the need to satisfy the PCI DSS requirements may be in conflict with your business goals and strategy. Some of the common issues encountered during Qualified Security Assessor (QSA) assessments are described together with ideas for how they can be addressed to align with typical organizational business goals.

Hopefully these steps presented in a logical and easy-to-follow manner will continue to prove relevant guidance as you consider future developments.

Analyze Data Flows

To understand the components of your CDE to which the PCI DSS applies, follow these steps:

1. **Identify all cases in which cardholder data is being transmitted.**

   This in one of the fundamental things you need to get right early on so that you know precisely all places that cardholder data is present. Ensure you make it easy to update your findings as your system evolves.

2. **Document all communication points that are involved from start to finish (end to end), as well as the connection methods or protocols that are used.**

   This is where you will uncover areas where insecure protocols or weak encryption methods are used which will almost certainly need to be updated or replaced.

3. **Detail all applicable authorization, capture, and settlement data flows, as well as all boundaries between trusted and untrusted components that are implemented to protect and isolate the traffic.**

   Pay particular attention to identifying all links to third parties that may have access to (or the capability to affect) your CDE and how you are securing communications with them and protecting the data that you are sharing with them. An important consideration is how you are preventing unauthorized access to your CDE which may involve different approaches as you may have multiple types of applications, operating systems and databases to support.

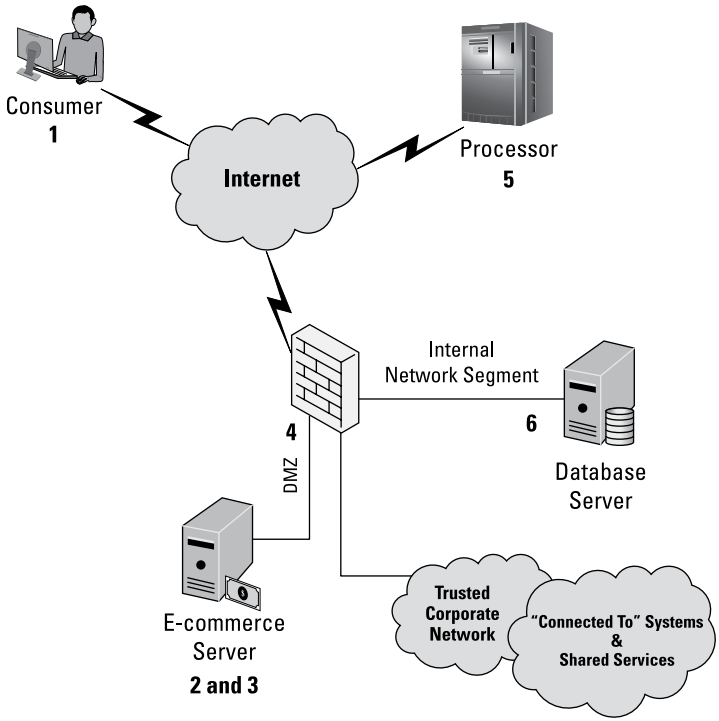
REMEMBER

We discussed how best to define your access control policies in Chapter 4 and specifically how to enforce least privilege policies on privileged users.

TIP

After identifying all data flows, you may want to annotate your high-level network diagram or build a flow chart to aid compliance with PCI DSS Requirement 1.1.3.

Figure 5-1 shows a sample data flow chart for a typical e-commerce implementation.



Source: Fortrex

FIGURE 5-1: A typical e-commerce implementation.

This chart involves the following steps:

1. A consumer enters his credit card into your web-based shopping cart.
2. Your web server receives the transmission in nonvolatile memory.
3. The web server calls a processor application programming interface (API).
4. The API securely transmits the cardholder data for authorization.
5. The processor returns an authorization and processes the transaction.
6. The cardholder data is written to an internal network segment located database server, where it's encrypted and stored until it's no longer required for legal, regulatory, and/or business purposes.

Identify Cardholder Data Storage

When you understand all data flows in your CDE (refer to "Analyze Data Flows" earlier in this chapter), you should identify all cases in which cardholder data is stored, in whole or in part, and for how long (temporary and prolonged periods). Document these data storage repositories, including details on all elements of cardholder data that's stored in each location, how the data is made unreadable (refer to Chapter 2); and how access is logged (refer to Chapter 2). Further document retention requirements in organizational data handling and retention policies and procedures (see PCI DSS Requirement 3.1).

REMEMBER

In Chapter 2 we explain in detail the various PCI DSS requirements relating to the storage of cardholder data, however, it is in Chapter 3 where we provide analysis of the pros and cons of the various encryption technologies that you can use to render data unreadable when stored. The importance of key management and keeping control of your keys, especially when you are sharing data with third parties, cannot be overstated and this is probably the area where you will need most assistance from your security vendor.

TIP

We recommend the use of open-source or commercial tools to help identify all instances of cardholder data storage. Include the results in your scoping documentation or, if they are not necessary, securely delete the data according to industry standards for data destruction (see PCI DSS Requirement 9.8).

Understand and Document Scope

Further define your CDE scope by following these steps:

1. **Review the PCI Security Standards Council document "Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation."**

   This December 2016 document is available at `https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf`.

   Be sure to note that systems that share a network segment with those that process, transmit, and/or store cardholder

data are in scope of assessment. Additionally, all systems that connect to and/or provide shared services to the CDE are in scope to the extent that requirements apply to them and that they affect the security of the CDE and its assets.

2. **Create a high-level network diagram.**

   Include all system components that process, transmit, and/or store cardholder data; share a network segment with systems that do; connect to; or provide shared services to the CDE.

   By *high-level*, we mean executive-friendly, not necessarily beloved by network engineers.

3. **Create an inventory of identified system components and critical software, vendor, make/model, and role/functionality.**

   Although such inventory is required by PCI DSS Requirement 2.4, it may also serve to support configuration standards and management database processes. Further, though documentation of your CDE's cryptographic architecture, though Requirement 3.5.1 relegates the activity to service providers, its inclusion easily proves valuable for merchants as well.


TIP

We mention frequently throughout the book any ability to reduce your exposure to cardholder data by using technology options may help reduce your PCI scope. If you are not already using solutions involving tokenization or point-to-point encryption then it may be worth reading again our comprehensive sections in Chapter 3 relating to these technologies to establish whether they could be of immediate use and help reduce your ongoing compliance costs.

Know Your Reporting Requirements

To identify the payment card brand reporting requirements that apply to your organization, follow these steps:

1. **Define your organization.**

   The organization can be a merchant (sells to consumers), a service provider (provides services to merchants and/or other service providers), an issuer (issues payment cards), or a combination of one or more of these.

2. **Ask your acquiring bank or payment processor to find out how many annual transactions your organization completes and which reporting category level it accepts.**

   Service providers which lack acquiring bank or payment processor relationships may, alternatively, consult with the payment brands directly.


REMEMBER

Merchants report compliance to their acquiring banks or payment processors. Service providers report to the payment brands themselves after applicable registration processes. Issuers follow service provider reporting level requirements and provide compliance attestations to their acquiring banks. Also, an entity may be classified as a combination of these categories dependent on its role and payment card responsibilities.

Document Everything

Being control-rich and documentation-poor is no way to achieve the compliance you need. Compliance with the PCI DSS requires you to do what you say and say what you mean. Most requirements call for explicit documentation, often in the form of organizational policies and procedures. You should also document the other important activities including change management efforts, code reviews, security awareness programs, training sessions, and program authorizations.


REMEMBER

Carefully review each requirement and its associated testing procedure, and keep in mind the fact that sub-requirements inherit their parents' language. PCI DSS Requirement 8.1.1 (Assign all users a unique ID before allowing them to access system components or cardholder data), for example, must be incorporated into the identity management policies and procedures set forth by Requirement 8.1.


TIP

Although many PCI DSS requirement mapped policy templates are available, not all of them are truly comprehensive or meet the scrutiny of every Qualified Security Assessor (QSA). We recommend coordinating with your QSA in your selection and being certain to customize your selected policy to reflect your organization's actual implementation practices and established processes. A portion of a typical security operations checklist that your QSA may provide that could be adapted for your specific requirements is shown in Figure 5-2.

Action	Procedures	Assigned	Date of Completion	Notes
Daily				
File Integrity Monitoring Log Review				
Audit Log Review				
Security Log Review				
IDS/IPS Alert Review				
Third-party Vulnerability Alert Review				
Monthly				
Installation of all critical new security patches				
Quarterly				
Review of all stored cardholder data to ensure that retention requirements have not been exceeded				
Password rotation				
Review of retention requirements for visitor logs				
Review of retention requirements for video camera data				
Media inventory for hardcopy and electronic back-up media				
Review of audit log retention requirements				
Wireless Analyzer Scanning				
Internal Network Vulnerability Scans				
Internal Host Vulnerability Scans				
Internal Application Vulnerability Scans				
External Approved Scanning Vendor (ASV) vulnerability scans				

Source: Fortrex

FIGURE 5-2: An extract from a security operations checklist.

Consider Business Requirements and Risk

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 applicable QSAs. Nevertheless, it's almost always better to comply with a requirement as written than to attempt to position business needs or risk in opposition to that requirement.

Requirement 3.1, for example, which addresses organizational retention of cardholder data, requires cardholder data to be securely deleted at least quarterly or when it's no longer needed based on legal, regulatory, and/or business requirements. The fact that it's easier to retain data indefinitely than to establish a secure deletion process is not a business need. In this case, business need may be better supported by a contractual agreement.

Similarly, Requirement 6.2 allows the implementation of vendor-supplied security patches within an appropriate period based on prioritization and risk. The PCI DSS states that low-risk patches can be implemented within two to three months, as opposed to the one month required for riskier patches.

WARNING

Don't interpret this requirement to mean that you can patch a database system that stores cardholder data once per quarter if the system doesn't have direct Internet access. Database system components are most commonly categorized as critical assets.

Correct Deficiencies

During your assessment, you'll probably identify control deficiencies. As you identify such deficiencies, it's best to document them and manage the status of remediation efforts in a consolidated tracking mechanism. A quality QSA is likely to be able to assist with a suitable tool to make this process more efficient, and focused, while enabling better prioritization to be implemented.

REMEMBER

Even evidence requests that you don't complete during the assessment period may be considered to be deficiencies.

Further, this type of tool makes it easy to understand overall assessment state, and it may be useful in ongoing monitoring and future assessments.

Think Carefully About Compensating Controls

On occasion, business and/or technical constraints prevent you from complying with one or more PCI DSS requirements. In such cases, you can implement a compensating control and document it

on the Compensating Control Worksheet, provided in Appendix C of the PCI DSS. The constraints must be for business or technical reasons as opposed to preference, however.

REMEMBER

It's almost always best, if not easiest, to comply with PCI DSS requirements as written.

Compensating controls must meet the intent and rigor of the affected requirement and must go above and beyond other requirements. Other requirements may be considered when they produce a unique result in an area where they're not normally considered. All compensating controls must be maintained and periodically reexamined to validate both the original constraints and their effectiveness.

TIP

As commercial security solutions get more sophisticated you may find that you are able to upgrade some of your existing technology to remove the need for some of your compensating controls.

TECHNICAL STUFF

Consider the required use of a proprietary software vendor's application that depends on the insecure Telnet protocol. When the cost of migrating to a secure solution is unaffordable, you might consider a compensating control that communicates the Telnet protocol through a Secure Shell Home (SSH)-based tunnel to secure the transmission. You might also implement firewall-based access control lists to limit and log network and host-based communications using the SSH protocol.

Review Your Program Strategy Regularly

Becoming compliant with the PCI DSS is one thing; maintaining compliance is quite different (and challenging). Take the time to formalize your PCI DSS compliance program including definition of roles and responsibilities (see Requirements 12.4 and 12.5). For example, role and responsibility should be defined which ensures regular communication among team members and identified stakeholders as well as for appropriate incident escalation.

Additionally, whereas Requirement 12.11 states that service providers must conduct reviews at least quarterly to ensure ongoing compliance, merchants would be wise to do the same. Similarly, Requirement 12.4.1 requires that service providers assign responsibilities for overall accountability, definition of program charter,

and required executive management communications. This also is advised and should prove considerably valuable to your efforts to continually develop program maturity.


TIP

Roles and responsibilities required by the PCI DSS are excellent guides, but we also recommend adding more responsibilities, such as monitoring the documents and knowledge base of the PCI Security Standards Council and participating in regional meetings. In some circumstances, you may want to join the board of advisors or a special interest group to help shape the future direction of the standard. For more information, see the PCI Security Standards Council document "Get Involved: Make a Difference to Our Industry" which can be found at `https://www.pcisecuritystandards.org/get_involved`. You will find many leading security technology vendors as official PCI "Participating Organizations" and attending the various regional events held each year is an excellent way to learn more about the latest products to help simplify your PCI DSS compliance efforts.

Get Management Support

PCI DSS Requirements 12.4 and 12.5 formally assign responsibility for information security, but they don't provide explicit guidance on program oversight. Nevertheless, as is the case with other programs, effective governance can support program efforts. It's critical to get the support of your organization's stakeholders and senior management to ensure alignment of your compliance program with business goals and with other compliance and cybersecurity initiatives. As a bonus, getting leadership directly involved in developing future compliance strategies enables your organization to more readily adapt and respond to changing threat environments.


REMEMBER

Your success depends on getting everyone within your organization to perform effectively as part of a team. Seek senior level buy-in to underpin your critical time and resource investments

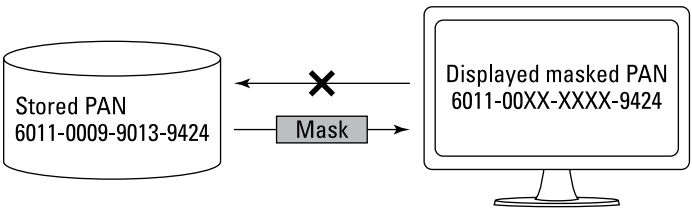
Appendix A

Making Stored PAN Information Unreadable

Throughout the book, we introduce various technologies that you can use as part of your strategy to render stored information — especially primary account numbers (PANs) — unreadable. This appendix briefly describes the most popular methods in use today.

Masking

Masking relates to maintaining the confidentiality of data when it's presented to a person. The process is familiar to anyone who has used a payment card in a restaurant or shop and then checked the printed receipt; certain digits of the PAN are shown as Xs rather than the actual digits (see Figure A-1). Per PCI DSS Requirement 3.3, PAN display should be limited to the minimum number of digits necessary to perform job functions and should not exceed the first six and last four digits.

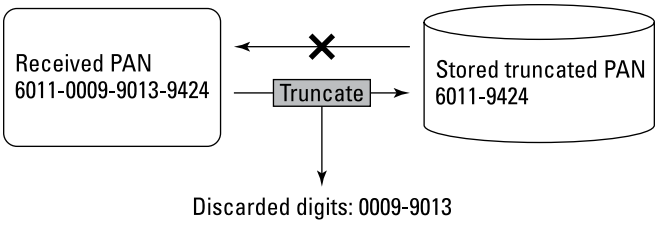


Source: Thales

FIGURE A-1: Masking a PAN for display purposes.

Truncation

Truncation renders stored data unreadable by ensuring that only a subset of the complete PAN is stored (see Figure A-2). As in masking, no more than the first six and last four digits can be stored.



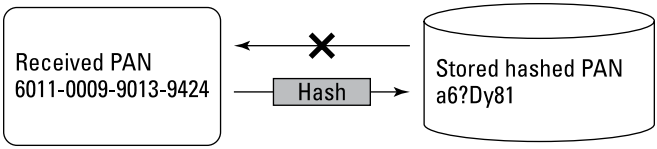
Source: Thales

FIGURE A-2: Truncating a PAN.

One-Way Hashing

A *hash function* is a well-defined, provably secure cryptographic process that converts an arbitrary block of data (in this case, a PAN) to a different, unique string of data. In other words, every PAN yields a different result. The one-way hash process is irreversible (which is why it's called *one-way*); it's commonly used to ensure that data hasn't been modified, because any changes in the original block of data would result in a different hash value.

Figure A-3 illustrates the use of the hash function in the context of the PCI DSS. The technique provides confidentiality (it's impossible to re-create a PAN from a hashed version of that PAN), but like truncation, it makes using the stored data for subsequent transactions impossible.



Source: Thales

FIGURE A-3: One-way hash of a PAN.

REMEMBER

You can't retain truncated and hashed versions of the same payment card within your cardholder data environment unless you implement additional controls to ensure that the two versions can't be correlated to reconstruct the PAN.

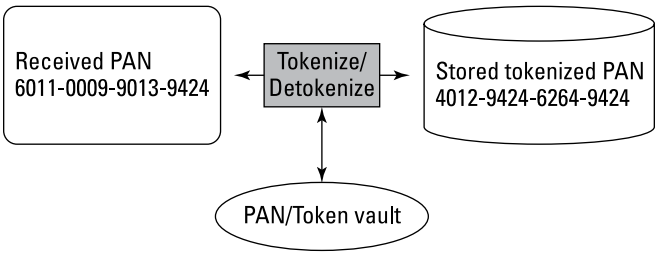
Tokenization

Tokenization is a process that replaces the original PAN with surrogate data — a token that may look like a legitimate PAN but has no value to an attacker. In most implementations, the process is reversible; tokens can be converted back to the original PANs on request. Tokenization is used when stored PANs need to be accessible for subsequent transactions.

You can create tokens in a variety of ways. Following are two common approaches:

- **Tokens calculated directly from the original PAN value:** This method yields the same token for each given PAN in a process that's said to be *deterministic.*
- **Tokens generated randomly:** This method yields different tokens every time except when an exhaustive lookup of previous PANs is made so that a previously issued token can be reused.

The degree to which the tokenization process is deterministic can be important in certain scenarios. Everything depends on how the tokens are being used. In some cases, it's desirable to preserve not just the format of the PAN during the tokenization process, but also certain digits of the PAN (see Figure A-4).



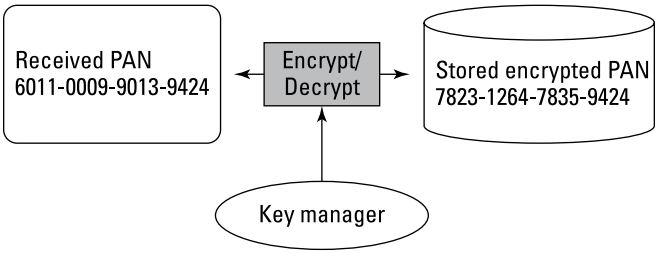
Source: Thales

FIGURE A-4: Tokenization of a PAN (last four digits preserved).

Encryption

In some ways, the goals of encryption are similar to those of tokenization, in that PAN data is replaced by data that has no intrinsic value to an attacker. Encryption uses standardized cryptographic algorithms and keys to derive the encrypted PAN from the original data. The algorithms are widely known, so the security of the process hinges on the strength and handling of the cryptographic keys, which is why hardware security modules are widely involved.

The encryption process generally changes the format of the data. Typically, data size increases when that data is encrypted. For the same reason that tokenization attempts to preserve the format of the original PAN data — to minimize changes in existing systems that come into contact with the data — organizations often employ format-preserving encryption (FPE; see Figure A-5).



Source: Thales

FIGURE A-5: Encryption of a PAN (with FPE and preservation of last four digits).

Appendix B

PCI Security Standards That Complement PCI DSS

Numerous PCI security standards complement the PCI DSS in providing a robust cardholder data environment (CDE) for the secure use of payment applications, payment cards, point-of-sale (POS) devices, and hardware security modules (HSMs). We summarize those standards in this appendix.


TIP

For more detailed information (including details of specification changes from previous versions, supporting guidance, and frequently asked questions), visit the Document Library on the PCI Security Standards Council's website (`https://www.pcisecuritystandards.org/document_library`).

The specifications are sorted into various sections (that we cover in the remainder of this Appendix) so you can go straight to your area of interest and from there explore the various documents within that section.

PCI PA-DSS

The Payment Application Data Security Standard (PA-DSS) applies specifically to payment applications that store, process, or transmit cardholder data as part of a payment authorization or settlement process. The standard is intended to ensure that the software is implemented and operated in compliance with the PCI DSS.

This specification is used by Payment Application Qualified Security Assessors who conduct payment application validations to assess whether or not the payment application being reviewed complies with the PA-DSS requirements. Merchant and/or service provider PCI DSS assessments will include verification that the

payment application is configured and implemented according to the payment application's validated implementation guide.

WARNING

If you are using a PA-DSS compliant application, that in itself does not make your environment PCI DSS compliant since the application must be implemented in a PCI DSS compliant manner.

PCI PTS

The PCI Security Standards Council and the payment brands use the term PIN Transaction Security (PTS) to cover a range of security requirements, testing methods, and approval processes for devices used in payment transaction processing. All organizations that store, process or transmit cardholder data need to comply with the standards. The vendors who supply products to such organizations must ensure that they meet all the applicable security standards covered in the various PTS specifications, necessitating comprehensive evaluation before deployment.

The following security specifications are included within the scope of the PTS standard:

- **Hardware Security Module:** This specification relates to HSMs, wherein a protected hardware device provides physical or logical security services for cryptographic processes and is used for encryption or decryption of account data and key management. The PCI HSM standard is very payment industry-specific covering aspects of device and key management (required for PCI compliance) which are getting much stricter as the standard evolves to address new threats.
- **PIN Security:** PIN Security ensures that all personal identification numbers (PINs) are securely transmitted, managed, and handled during online or offline transaction processing performed by hardware terminals (such as ATMs) or attended or unattended POS terminals. The primary users of the specification are the various acquiring institutions (such as large banks) and their agents (normally third party processors) who are responsible for PIN transaction processing and who must ensure that PINs are secured at all times as they are routed through the payment network. For many years each of the payment brands implemented their own proprietary PIN security program – now all brands have

REMEMBER

adopted the PCI PIN Security standard together with the associated testing, assessment and certification programs.

HSM functionality that's used in the generation, translation, or validation of PINs must meet the PIN Security requirements.

- **Point-of -Interaction (POI) Modular Security:** This specification is a set of security requirements for vendors that submit devices for PTS approval. Devices covered by the standard are segregated into categories: PIN entry devices, unattended payment terminals, non-PIN acceptance POI devices, encrypting PIN pads, and secure components used in POS terminals. These devices are typically in consumer-facing environments and hence must meet high levels of physical security including the fundamental requirement to erase any master keys stored immediately on detection of a tamper attack. The secure generation of keys and their loading into the devices involve high levels of security which are covered in the specifications and associated approval processes.

PCI P2PE

The Point-to-Point Encryption (P2PE) standard applies to third-party developed, P2PE Assessor validated and PCI Security Standards Council approved solutions which provide a secure process for transmitting data from the point-of-interaction to the secure decryption environment where HSMs are deployed. The primary objective is to increase the protection of cardholder data by effectively removing clear-text account data (most notably the PAN) between the point of capture and decryption environment, where data breaches historically have been most prevalent. Many merchants have seen reduced PCI scope for their CDE due to their adoption of POS technology incorporating P2PE.

The P2PE documentation set is mainly intended for solution providers that provide P2PE components or P2PE applications as part of an overall P2PE approved solution and P2PE Assessors. However, a listing of SSC approved P2PE solutions is also maintained which is easily accessible via the council's web site (`https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions`).

PCI TSP

The Token Service Provider (TSP) standard defines security controls for providers that generate and issue Europay Mastercard Visa (widely known as EMV) payment tokens. The standard is intended to protect physical and logical tokenization services within the token data environment. According to the PCI Security Standards Council, the definition of a Token Service Provider is "An entity that provides a Token Service comprised of the Token Vault and related processing. The Token Service Provider will have the ability to set aside licensed ISO BINS as Token BINs to issue Payment Tokens for the PANs that are submitted according to this specification."

The documentation provided by the council defines the security controls needed to protect environments where the tokenization services occur. Many of the early EMV-compliant tokenization services for mobile payments have been provided by the major payment brands themselves rather than third party providers.

Card Production

The Card Production standard applies to entities that perform card-issuing services. The standard defines logical and physical security requirements (in separate specification documents) associated with card production (for both magnetic stripe and EMV-compliant chip cards), such as data preparation, pre-personalization, card personalization, PIN generation, and PIN mailers.

The development, manufacture, transport, and personalization of payment cards and their components have a strong impact on the security structures of the payment systems, issuers, and vendors involved in their issuance. You will find that data security has a very high profile in the various documents that comprise the Card Production standards.

Appendix C

Glossary

Throughout this book we have incorporated numerous abbreviations that are commonly used in the payments industry. To provide you with a quick reference, we have included them in this appendix together with some other terms you are likely to encounter when reading the various PCI security standards covered in Appendix B.

TIP

For a more comprehensive glossary, visit the PCI Security Standards Council's website (`https://www.pcisecuritystandards.org/pci_security/glossary`).

2FA: Two factor authentication

AOC: Attestation of compliance

API: Application programming interface

ATM: Automated teller machine

CCM: Cloud controls matrix

CDE: Cardholder data environment

CSA: Cloud security alliance

CVC: Card verification code

CVV: Card verification value

DMZ: Demilitarized zone

DSS: Data Security Standard

E2EE: End-to-end encryption

EMV: Europay Mastercard Visa

FDE: Full disk encryption

FPE: Format preserving encryption

HSM: Hardware Security Module

LDAP: Lightweight Directory Access Protocol

MAC: Message authentication code

MPOS: Mobile point-of-sale

NTP: Network time protocol

P2PE: Point-to-point encryption

PAN: Primary account number

PA-QSA: Payment Application Qualified Security Assessor

PCI: Payment Card Industry

PCIP: Payment Card Industry Professional

PED: PIN entry device

PIN: Personal identification number

POI: Point-of-interaction

POS: Point-of-sale

QSA: Qualified Security Assessor

REST: Representational state transfer

ROC: Report on compliance

SAD: Sensitive authentication data

SQL: Structured query language

SSC: Security Standards Council, also referred to as "the council"

SSH: Secure Shell Home

SSL: Secure sockets layer, an insecure protocol

TDE: Transparent data encryption

TLS: Transport layer security

VM: Virtual machine

Need help with your PCI DSS compliance?

If your business relies on card payments and faces the challenge of maintaining ongoing compliance with PCI DSS, this book is for you. It will be useful whether you work in risk management or business planning. This book explains the requirements for protecting account data, controlling access to the data, and the associated monitoring and logging activities that you need to adopt. Various technology options available to protect data are explained in detail together with strategies you could adopt to help reduce scope. Ultimately, the book acts as a valuable and practical reference guide that you can come back to time and again to assist with your ongoing compliance and help you avoid the common pitfalls that can lead to serious data breaches or failed audits.

Inside...

- Why protecting payment card data is important
- What PCI DSS scope of compliance means and how you can reduce it
- Where best to deploy data security in your cardholder environment
- Why key management is so important and how to tackle it
- How to control and monitor all activities, even those of privileged users

THALES
FORTREX

Ian Hermon is a product marketing manager for Thales eSecurity who participates in a wide range of industry organizations to help improve the security of financial transactions. **Peter Spier** is the Managing Director PCI and Risk Assurance for Fortrex Technologies, helping numerous organizations with PCI DSS compliance in his capacity as a PCI QSA, PA-QSA, and PCIP.

for dummies®
A Wiley Brand

ISBN: 978-1-119-41869-6
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.