# Payment Card Industry
# 3-D Secure (PCI 3DS)

## Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server

Version 1.0

October 2017

# Document Changes

| Date | Version | Description |
|---|---|---|
| October 2017 | 1.0 | Initial version |

# Table of Contents

# Introduction

This document, the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (hereafter referred to as the "PCI 3DS Core Security Standard"), defines physical and logical security requirements and assessment procedures for entities that perform or provide the following functions, as defined in the *EMV® 3-D Secure Protocol and Core Functions Specification:*

- 3DS Server (3DSS)
- 3DS Directory Server (DS)
- 3DS Access Control Server (ACS)

The requirements in this PCI 3DS Core Security Standard are organized in two parts:

- **Part 1: Baseline Security Requirements** – A baseline of technical and operational security requirements designed to protect the 3DS data environment (3DE)
- **Part 2: 3DS Security Requirements** – Security requirements to protect 3DS data and processes

This standard does not address how an entity would meet the requirements in the *EMV® 3-D Secure Protocol and Core Functions Specification*. Rather, this document defines the security controls needed to protect environments where specific 3DS functions occur. Entities performing these functions may be subject to the requirements in this document. To determine whether an entity is required to meet these requirements, confirm with the payment brand for which the functions are performed.

> ***Note:** Whether an entity is required to validate to the PCI 3DS Core Security Standard is determined by payment brand compliance programs.*

The requirements in this standard cover EMV® 3-D Secure implementations. Table 1 provides a high-level overview of the PCI 3DS Core Security Standard requirements.

### Table 1: Overview of PCI 3DS Core Security Standard Requirements

| PCI 3DS Part 1: Baseline Security Requirements | |
|---|---|
| **1. Maintain security policies for all personnel** | 1.1 Maintain security policies<br>1.2 Evaluate risk<br>1.3 Educate personnel<br>1.4 Screen personnel |
| **2. Secure network connectivity** | 2.1 Protect 3DS systems from untrusted systems and networks<br>2.2 Protect 3DS systems from network threats |
| **3. Develop and maintain secure systems** | 3.1 Secure application development<br>3.2 Configuration standards<br>3.3 Change management |
| **4. Vulnerability management** | 4.1 Protect against malicious software<br>4.2 Address vulnerabilities and security weaknesses |
| **5. Manage access** | 5.1 Access management<br>5.2 Account management<br>5.3 Authentication |
| **6. Physical security** | 6.1 Restrict physical access<br>6.2 Secure media |
| **7. Incident response preparedness** | 7.1 Incident response plan<br>7.2 Audit logs |

| PCI 3DS Part 2: 3DS Security Requirements | |
|---|---|
| **1. Validate scope** | 1.1 Scoping |
| **2. Security governance** | 2.1 Security governance<br>2.2 Manage risk<br>2.3 Business as usual (BAU)<br>2.4 Manage third-party relationships |
| **3. Protect 3DS systems and applications** | 3.1 Protect boundaries<br>3.2 Protect baseline configurations<br>3.3 Protect applications and application interfaces<br>3.4 Secure web configurations<br>3.5 Maintain availability of 3DS operations |
| **4. Secure logical access to 3DS systems** | 4.1 Secure connections for issuer and merchant customers<br>4.2 Secure internal network connections<br>4.3 Secure remote access<br>4.4 Restrict wireless exposure<br>4.5 Secure VPNs |
| **5. Protect 3DS data** | 5.1 Data lifecycle<br>5.2 Data transmission<br>5.3 TLS configuration<br>5.4 Data storage<br>5.5 Monitoring 3DS transactions |
| **6. Cryptography and key management** | 6.1 Key management<br>6.2 Secure logical access to HSMs<br>6.3 Secure physical access to HSMs |
| **7. Physically secure 3DS systems** | 7.1 Data center security<br>7.2 CCTV |

## Terminology

Definitions for PCI terminology used throughout this document are provided in the general PCI Glossary on the PCI SSC website: https://www.pcisecuritystandards.org/pci_security/glossary.

Additionally, the following terms are used in this PCI 3DS Core Security Standard:

- **Authentication Value (AV)** – As defined in the *EMV® 3-D Secure Protocol and Core Functions Specification:* A cryptographic value generated by the ACS to provide a way, during authorization processing, for the authorization system to validate the integrity of the authentication result. The AV algorithm is defined by each Payment System.
- **3-D Secure (3DS)** – As defined in the *EMV® 3-D Secure Protocol and Core Functions Specification:* An authentication protocol that enables the secure processing of payment and non-payment card transactions.
- **3DE** – Acronym for 3DS data environment. The 3DE is a secure area within which ACS, DS, and/or 3DSS functions are performed, as described in the *EMV® 3-D Secure Protocol and Core Functions Specification.*
- **3DS data** – Covers a number of discrete data elements as defined in the *EMV® 3-D Secure Protocol and Core Functions Specification*, and generally includes any data transmitted within 3DS messages.
- **3DS entity** – Term used to describe entities that perform 3DSS, ACS, and/or DS functions as defined in the *EMV® 3-D Secure Protocol and Core Functions Specification.*
- **3DS messages** – A set of messages—for example, PReq, PRes, CReq, CRes, etc.—that are used to convey information between 3DS components, as described in the *EMV® 3-D Secure Protocol and Core Functions Specification*.
- **3DS sensitive data** – Specific data elements requiring additional protection as defined in the *PCI 3DS Data Matrix*. Data in this category includes 3DS authentication data, public-key data, authentication challenge data (CReq/CRes), and cardholder challenge data.
- **3DS system** – General description for any system component—for example, network device, server, computing device, or application—that performs or supports a 3DS function or comprises the 3DE infrastructure.
- **Consumer Device Information (CDI)** – Data provided by the Consumer Device that is used in the authentication process. The Consumer Device—for example, a smartphone, laptop, or tablet—is used by a cardholder to conduct payment activities, including authentication and purchase.
- **Cardholder Verification Method (CVM)** – A process used to confirm that the person presenting a payment card (or payment token) is the legitimate cardholder. Examples of static CVM data include online PIN, offline PIN, challenge-response, shared secret/static password, and biometric. Examples of dynamic CVM data include a one-time passcode (OTP).

Definitions and terminology related to the 3-D Secure Protocol can be found in the *EMV® 3-D Secure Protocol and Core Functions Specification* (www.emvco.com).

## Roles and Responsibilities

There are several stakeholders involved in maintaining and managing PCI standards. The following describes the high-level roles and responsibilities as they relate to the PCI 3DS Core Security Standard.

### PCI SSC

PCI SSC maintains various PCI standards, supporting programs, and related documentation. In relation to the PCI 3DS Core Security Standard, PCI SSC:

- Maintains the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (this document, hereafter referred to as the PCI 3DS Core Security Standard).
- Maintains supporting documentation including reporting templates, attestation forms, frequently asked questions (FAQs), and guidance to assist entities implementing and assessing to the PCI 3DS Core Security Standard.
- Provides training for assessors evaluating 3DS entities in accordance with the requirements and assessment procedures in the PCI 3DS Core Security Standard.
- Maintains the list of qualified assessors on the PCI SSC Website.
- Maintains a quality assurance program for qualified assessors.

### Participating Payment Brands

The Participating Payment Brands develop and enforce their respective programs related to compliance with PCI standards including, but not limited to:

- Requirements, mandates, and deadlines for compliance to PCI standards.
- Which organizations are required to comply with a PCI standard.
- Validation methods and frequency.
- Fines or penalties for non-compliance.

### EMVCo

EMVCo is the global technical body owned by American Express, Discover, JCB, MasterCard, UnionPay, and Visa that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Specifications and related testing processes. Adoption of EMV Specifications and associated approval and certification processes promotes a unified international payments framework, which supports an advancing range of payment methods, technologies, and acceptance environments.

Additionally, the following EMV® 3-D Secure entities are identified for the purpose of this standard:[1]

### 3DS Access Control Server (ACS)

The ACS contains the authentication rules and is controlled by the Issuer. The ACS verifies whether authentication is available for a card number and device type, and authenticates specific transactions. Specific ACS functions include:

- Verifying whether a card number is eligible for 3DS authentication.
- Verifying whether a Consumer Device type is eligible for 3DS authentication.
- Authenticating the Cardholder for a specific transaction.

### 3DS Directory Server (DS)

The DS maintains lists of card ranges for which authentication may be available and coordinates communication between the 3DSS and ACS to determine whether authentication is available for a particular card number and device type. DS functions include:

- Authenticating the 3DS Server and the ACS.
- Routing messages between the 3DS Server and the ACS.
- Validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
- Defining specific program rules (for example, logos, time-out values, etc.).
- Onboarding 3DS Servers and ACSs.
- Maintaining ACS versions and 3DS Method URLs.

### 3DS Server (3DSS)

The 3DSS provides the functional interface between the 3DS Requestor Environment flows and the Directory Server (DS). Functions performed by the 3DS Server include:

- Collecting necessary data elements for 3DS messages.
- Authenticating the DS.
- Validating the DS, the 3DS SDK, and the 3DS Requestor.
- Ensuring that message contents are protected.

The 3DS Server may also link to the Acquirer and initiate authorization requests.

[1] For further information about 3DS roles and functions, refer to the *EMV® 3-D Secure Protocol and Core Functions Specification*.

# Scope of PCI 3DS Core Security Standard

The PCI 3DS Core Security Standard applies to environments where ACS, DS, and/or 3DSS functions are performed. Typically, this will consist of the 3DS Environment (3DE), which contains system components involved in performing or facilitating 3DS transactions, as well as system components supporting the 3DE. The term "system components" includes network devices, servers, computing devices, and applications. Examples of system components include but are not limited to:

- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the 3DE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- Any other component or device located within or connected to the 3DE.

## 3DS Data

3DS transaction processes involve a number of discrete data elements that may be also used for purposes other than performing 3DS transactions. Requirements in this standard that address "3DS data" apply where such data is part of a 3DS transaction process or is otherwise present where ACS, DS, and/or 3DSS functions occur—that is, within a 3DE. Data that exist outside of a 3DE and used only for purposes unrelated to 3DS transactions are not in scope for this standard.

## Relationship between PCI 3DS Core Security Standard and PCI DSS

There is an independent relationship between the PCI 3DS Core Security Standard and PCI DSS. A 3DE could be part of a cardholder data environment (CDE) or be completely separate from any CDE. If a 3DE contains account data, it may be subject to PCI DSS and/or the PCI 3DS Core Security Standard in accordance with payment brand compliance programs.

Where a 3DS entity has already applied PCI DSS to protect its 3DE as part of its CDE, the 3DS entity may be able to leverage the results of its PCI DSS assessment to meet the PCI 3DS Part 1: Baseline Security Requirements. Refer to Appendix B, "Alignment between PCI 3DS and PCI DSS Requirements," for details.

Whether a 3DS entity is required to validate to PCI DSS, to the PCI 3DS Core Security Standard, or to both is defined by individual payment brand compliance programs.

# Use of Third-Party Service Providers / Outsourcing

3DS entities will often outsource or rely on a third-party service provider for certain functionality of the 3DE. Common examples include hosting of applications, management of network devices or databases, and maintenance of physical security. Additionally, a 3DS entity may outsource aspects of the 3DS transaction process—for example, performing risk-based analysis of 3DS transactions—to an external third party. Where a third-party service can impact 3DS functionality or the security of the 3DE, the applicable PCI 3DS requirements will need to be identified and implemented for that service.

Critical steps in the process include understanding which 3DS functions and system components can be impacted by the service provider and identifying which PCI 3DS requirements are the responsibility of the service provider(s) and which are the responsibility of the 3DS entity.

It is expected that a 3DS entity will have processes in place to manage risks associated with third-party providers, including:

- Performing due diligence prior to engagement.
- Clear definition of security responsibilities.
- Periodic verification that agreed-upon responsibilities are being met.
- A written agreement to ensure both parties understand and acknowledge their security responsibilities.

While the ultimate responsibility for the security of the 3DE and 3DS Data lies with the 3DS entity, service providers may be required to demonstrate compliance with the applicable PCI 3DS requirements based on the provided service. The service provider may do so by either:

(a) Undergoing a PCI 3DS assessment and providing evidence to its 3DS entity customers to demonstrate its compliance to applicable PCI 3DS requirements; or

(b) For each of its 3DS entity clients' assessments, providing the required evidence to demonstrate compliance with the applicable PCI 3DS requirements.

The evidence provided by service providers should be sufficient to verify that the scope of the service provider's 3DS assessment covered the services applicable to the 3DS entity, and that the relevant PCI 3DS requirements were examined and determined to be in place. The specific type of evidence provided will depend on the how the assessments are managed. For example, if the service provider undergoes its own PCI 3DS assessment, the service provider's 3DS Attestation of Compliance (AOC) and/or relevant sections of the service provider's 3DS Report on Compliance (redacted to protect any confidential information) could provide some or all of the information. If the service provider does not have a 3DS AOC or Report on Compliance, the evidence provided should encompass the specific requirements being assessed, and be consistent with the validation methods described for each requirement.

# 3DS Security Requirements and Assessment Procedures

The security requirements and assessment procedures in this PCI 3DS Core Security Standard are presented in the following format:

- **Requirements** – The specific security control or objective that a 3DS entity is required to meet.
- **Validation Methods** – The assessment activities to be performed to determine whether a requirement has been met.
- **Implementation Guidance*** – Additional information to help entities and assessors understand how a requirement could be met. The guidance may include examples of controls or methods that— when properly implemented—could meet the intent of a requirement, as well as best practices that should be considered. This guidance is not intended to preclude other methods that an entity may use to meet a requirement, nor does it replace or extend the requirement to which it refers.

  **** The examples and practices in the Implementation Guidance column are not requirements.***

## Risk-Management Approach to Requirements

To ensure security controls continue to be properly implemented and are appropriate to address applicable security risks, the PCI 3DS Core Security Standard requires periodic identification and evaluation of evolving risks to 3DS environments. The rigor of certain security requirements (for example, the timing and frequency of system patching) will depend on the 3DS entity's risk-management strategy. While this approach provides the 3DS entity with flexibility to implement security controls based on its assessed risk, it also requires implementation of a robust risk-management practice as an integral part of the entity's "business as usual" operational processes.

Where a PCI 3DS requirement does not define a minimum frequency for periodic or recurring activities (for example, audit log reviews), the 3DS entity may define the frequency as appropriate for its business. The frequency defined by the 3DS entity must be supported by the 3DS entity's security policy and risk-management strategy. The 3DS entity should also be able to demonstrate that the frequency it has defined is appropriate for the activity to be effective and meets the intent of the requirement.

## Validating Requirements

The validation methods identified for each requirement describe the expected activities to be performed by the assessor to validate whether the entity has met the requirement. The intent behind each validation method is described as follows:

- **Examine:** The assessor critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- **Observe:** The assessor watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, system configurations/settings, environmental conditions, and physical controls.
- **Interview:** The assessor converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The validation methods are intended to allow the 3DS entity to demonstrate how they have met a requirement. They also provide the 3DS entity and the assessor with a common understanding of the assessment activities to be performed. The specific items to be examined or observed and personnel to be interviewed should be appropriate for both the requirement being assessed and each entity's particular implementation.

When documenting the assessment results, the assessor identifies the validation activities performed and the result of each activity. While it is expected that an assessor will perform all the validation methods identified for each requirement, it is also possible for an implementation to be validated using different or additional methods. In such cases, the assessor should document why they used validation methods that differed from those identified in this document.

The PCI 3DS Reporting Template and Attestation documents (available on the PCI SSC Website) should always be used to document the results of a PCI 3DS security assessment.

## Compensating Controls

Compensating controls may be considered when, due to legitimate technical or documented business constraints, an entity cannot meet a PCI 3DS requirement as stated but has sufficiently mitigated the risk associated with the requirement through implementation of alternative, or compensating, controls. Refer to Appendix A for details and requirements on the use of compensating controls.

## 3DS Assessment Process

The PCI 3DS assessment process typically includes the following steps:

1. The 3DS entity completes EMVCo functional testing for ACS, DS, and/or 3DSS and receives a Letter of Approval from EMVCo.
2. Confirm the scope of the PCI 3DS assessment.
3. Perform the PCI 3DS assessment, following the requirements and assessment procedures in this PCI 3DS Core Security Standard.
4. Complete the 3DS assessment report and attestation in accordance with applicable templates, guidance, and instructions.
5. Submit the assessment report and attestation, along with any other requested documentation, to the applicable payment brand(s).
6. If required, perform remediation to address requirements that are not in place, and provides an updated report.

# Part 1: 3DS Baseline Security Requirements

## Requirement P1-1. Maintain security policies for all personnel

| | Overview | Requirements |
|---|---|---|
| **P1-1** | Security policies define rules and requirements for all personnel to protect the security and integrity of the entity's resources and protect against identified risks. | 1.1 Maintain security policies<br>1.2 Evaluate risk<br>1.3 Educate personnel<br>1.4 Screen personnel |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-1.1 Maintain Security Policies** | | | |
| **P1** | 1.1.1 An organizational security policy(s) is established and disseminated to all relevant personnel. | • Examine documented policies and procedures.<br>• Interview personnel. | A strong security policy, or policies, should set the security tone for the entity as a whole and inform personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. The security policy should be updated as needed in response to changes in the environment, results of risk assessments, implementation of new technologies, and changes in business objectives.<br>Personnel should be aware of all policies and policy updates, including their applicable responsibilities. Methods of communicating policies should include a mechanism for personnel to acknowledge they have received and read the policy or policy update. Personnel acknowledgment may be in writing or electronic.<br>All security policies and policy updates should be approved by management to ensure they are aligned with the entity's security strategy and business objectives. Any exception to the policies should require management sign-off to ensure the appropriate due diligence is done and approval obtained. |
| **P1** | 1.1.2 Security policies are reviewed and updated as needed to reflect changes to business objectives or the risk environment. | | |
| **P1** | 1.1.3 Policy updates are communicated to applicable personnel. | | |
| **P1** | 1.1.4 The security policy is approved by management | | |
| **P1** | 1.1.5 Personnel acknowledge that they have read and understood the security policy, including updates to the policy. | • Examine evidence of acknowledgments.<br>• Interview personnel. | |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-1.2 Evaluate Risk** | | | |
| **P1** | 1.2.1 A risk-assessment process is documented. | - Examine documented policies and procedures.<br>- Interview personnel. responsible for risk-assessment process. | Risks to 3DS environments should be assessed at least annually and upon significant changes. The risk assessment should identify assets, threats, likelihood, and potential impacts. Risk considerations should include internal and external attacks—e.g., for cybercrime, fraud, or theft—internal control failures, and malware. Risks should be prioritized and resources allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized. Considerations should include regulatory obligations and changes in technology—e.g., deprecation of encryption algorithms.<br>*Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.* |
| **P1** | 1.2.2 The documented risk-assessment process is performed at least annually and upon significant changes. | | |
| **P1-1.3 Educate personnel** | | | |
| **P1** | 1.3.1 A security awareness program is implemented that provides awareness to all applicable personnel about security policy and procedures. | - Examine documented policies and procedures.<br>- Examine security awareness materials. | The security awareness program should result in personnel understanding the security policy and procedures, and their responsibilities for following secure processes. All personnel—including full-time, part-time and temporary employees, contractors, and consultants—with access to or the ability to impact the security of the 3DE should be required to complete training. Training should be required upon hire and include periodic refresher sessions at appropriate intervals. The frequency of training should be aligned with the entity's policies for education and security awareness, and commensurate with personnel job function. |
| **P1** | 1.3.2 Personnel receive security awareness training at defined intervals, as appropriate for their job function. | - Examine records of attendance.<br>- Interview personnel. | |
| **P1** | 1.3.3 Personnel are aware of the security policy and responsibilities as applicable to their job function. | - Interview personnel. | |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-1.4 Screen personnel** | | | |
| **P1** | 1.4.1 Personnel are screened (background checks) prior to being granted access to the 3DE. | • Examine documented policies and procedures.<br>• Interview personnel.<br>• Examine results of screening process. | The intent of screening personnel is to reduce the risk of fraud and unscrupulous behavior from an internal resource. Role descriptions should describe the level of security or access required for the role, and the level of screening should be appropriate for the particular position. Positions requiring greater responsibility or that have administrative access to critical data or systems may warrant more detailed background checks than positions with less responsibility and access. The policy should also cover internal transfers where personnel in lower-risk positions, and who have not already undergone a detailed background check, are promoted or transferred to positions of greater responsibility or access. The specific roles to be screened will depend on the entity's personnel and security policies. For example, an entity may have a policy that requires detailed screening for all personnel or defines different levels of screening for different job functions.<br>Examples of criteria that may be appropriate include employment history, criminal records, credit history, and reference checks. |
| **P1** | 1.4.2 The screening process includes established criteria and a decision process for background check results. | | |

## Requirement P1-2. Secure network connectivity

| | Overview | Requirements |
|---|---|---|
| **P1-2** | Network connectivity controls provide secure pathways to the entity's systems while protecting those systems from unauthorized access and network-based threats. | 2.1 Protect 3DS systems from untrusted systems and networks<br>2.2 Protect 3DS systems from network threats |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-2.1 Protect 3DS systems from untrusted systems and networks** | | | |
| **P1** | 2.1.1 A security policy(s) and procedures for protection of 3DS environment boundaries are maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | Policies for the protection of 3DS environment boundaries should define the purpose, scope, roles, and responsibilities of defined boundaries to protect system components from untrusted networks. The policy should be kept up to date, approved by management, and communicated to applicable personnel. |
| **P1** | 2.1.2 Up-to-date network and data flow information is maintained for all 3DS communication paths. | • Examine network and data flow information.<br>• Observe methods used to maintain up-to-date network and data flow information. | Network and data flow information—for example, diagrams or network mapping tools—accurately document how the entity's 3DS networks are configured, the identity and location of all 3DS systems, how 3DS systems are connected to each other and to other systems, and all communication paths with trusted and untrusted networks. |
| **P1** | 2.1.3 Access between trusted and untrusted networks, systems, and applications is limited via physical and/or logical controls. | • Examine documentation describing controls.<br>• Observe physical and/or logical controls. | Documentation illustrating authorized communications, both internal and external—including source and destination systems, interface connections, security controls for those connections, and the type of data being sent—will assist in meeting these requirements.<br>Protection mechanisms may include technologies such as network gateways, routers, firewalls, encryption, API controls, and virtualization techniques. Controls may be a combination of software and hardware—for example, use of packet-filtering capability based on header information, advanced filtering/inspection tools, and implementation of dedicated physical network devices or channels to separate network segments.<br>Many security devices and software provide rule sets and settings that can validate the existence and methodologies used to secure network connectivity. |
| **P1** | 2.1.4 Traffic to/from 3DS systems is restricted to only that which is necessary, with all other traffic specifically denied. | • Examine documentation identifying necessary traffic.<br>• Observe configurations of ingress and egress controls. | |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 2.1.5 Network connectivity controls are monitored and/or periodically reviewed to confirm configurations are effective. | • Examine documented methods for monitoring and/or periodically reviewing network connectivity controls.<br>• Observe implemented methods and processes. | Reviewing device configurations allows the entity to identify and remove any unneeded, outdated, or incorrect rules and confirm that only authorized connections, ports, protocols, services, and APIs are allowed as defined in the documented business justifications. All other services, protocols, and ports should remain disabled or be removed through periodic reviews. Review processes may include real-time monitoring and analysis, periodic maintenance cycles to ensure the controls are accurate and working as intended, and periodic reviews of network traffic connectivity across ports, protocols, and services. For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance—e.g., NIST, ENISA, OWASP, etc. |
| **P1-2.2 Protect 3DS systems from network threats** | | | |
| **P1** | 2.2.1 Controls are implemented to detect and/or block known and unknown network attacks. | • Examine documented controls/configuration standards.<br>• Observe implemented controls. | Controls should be implemented at the perimeter and critical systems points, and include consideration of both network-based and application-based attack vectors. Methods of detection may include signature-based, behavioral, and other mechanisms that analyze traffic flows. Examples of tools include IDS/IPS, host firewalls, and real-time traffic analysis tools. All mechanisms—such as detection engines, baselines, and signatures—should be configured, maintained, and updated per vendor instructions to ensure optimal protection. |
| **P1** | 2.2.2 Suspicious traffic is blocked or generates an alert that is investigated and responded to. | • Examine documented procedures.<br>• Observe implemented controls and processes. | If suspicious traffic is not automatically blocked, an alert should be generated that is actively monitored and immediately investigated.<br>Where suspicious traffic is automatically blocked, a record of the traffic should also be generated and investigated to determine whether action is needed to prevent further attack. |

## Requirement P1-3. Develop and maintain secure systems

| | Overview | Requirements |
|---|---|---|
| **P1-3** | Security risks and events can occur at any time during the lifetime of a system or application. Integrating secure processes throughout the lifecycle provides assurance that system integrity is maintained at all times. | 3.1 Secure application development<br>3.2 Configuration standards<br>3.3 Change management |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-3.1 Secure application development** | | | |
| **P1** | 3.1.1 A security policy(s) and procedures for secure management of the Software Development Life Cycle (SDLC) is maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | Where software is developed by the 3DS entity or bespoke or custom software is developed by a third party for the 3DS entity, the software development process should employ secure coding practices to address common vulnerabilities applicable to the particular technology. The entity should remain up to date with vulnerability trends and update its secure coding practices and developer training as needed to address new threats. Examples of current best practices include OWASP, SANS CWE Top 25, and CERT Secure Coding.<br>Application developers should be properly trained to identify and resolve issues related to common coding vulnerabilities. Having staff knowledgeable of secure software development practices minimizes the number of security vulnerabilities accidentally introduced through poor coding practices. Training for developers may be provided in-house or by third parties and should be appropriate for the technology used.<br>Common methods for software security testing include threat modeling, code reviews, fuzz testing, and penetration testing. Software security testing should be performed by someone other than the developer of the code to allow for an independent, objective review. Automated tools or processes may also be used in lieu of manual reviews, but keep in mind that it may be difficult or even impossible for an automated tool to identify some coding errors or other security issues.<br>*(Continued on following page)* |
| **P1** | 3.1.2 Personnel involved in software development are trained in secure software development practices. | • Examine evidence of training.<br>• Interview developer personnel. | |
| **P1** | 3.1.3 Software development procedures include processes to address common coding vulnerabilities. | • Examine documented procedures.<br>• Interview developer personnel. | |
| **P1** | 3.1.4 Software security testing is conducted during the software development lifecycle using methodologies documented in the SDLC processes. | • Examine documented software security testing procedures.<br>• Examine results of software security testing.<br>• Interview personnel. | |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 3.1.5 The software security testing process identifies defects and security vulnerabilities. | • Examine documented software security testing procedures.<br>• Examine results of software security testing.<br>• Interview personnel. | Correcting identified software defects before the software is deployed prevents it from exposing the environments to potential exploit. Requiring a formal review and sign-off by management should verify that the software is approved and has been developed in accordance with policies and procedures. |
| **P1** | 3.1.6 Identified software defects and security vulnerabilities are addressed prior to release. | | |
| **P1** | 3.1.7 Results of software security testing are signed off by management prior to software release. | | |
| **P1-3.2 Configuration standards** | | | |
| **P1** | 3.2.1 A security policy(s) and procedures for system build and configuration management are maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | The policy document should be able to explain the purpose, scope, roles and responsibilities, methods of access for different account types, configuration management, monitoring methodology, and controls to address known risks. |
| **P1** | 3.2.2 An up-to-date inventory of all 3DS system components is maintained. | • Examine system inventory.<br>• Interview personnel. | Maintaining a current inventory of all system components enables an organization to accurately and efficiently apply security controls to protect the assets. The inventory should be periodically confirmed by either manual or automated process—for example by correlation with the results of vulnerability scans or penetration testing—to confirm it is up to date. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 3.2.3 Configuration standards are defined and implemented for all 3DS system types. | • Examine system configuration standards and build procedures for all system component types.<br>• Examine system configurations.<br>• Interview personnel. | System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being deployed in the environment.<br>System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. Examples of industry-accepted configuration standards include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS) Institute, and National Institute of Standards Technology (NIST).<br>The implemented controls should provide assurance that all 3DS systems have known secure configurations. |
| **P1** | 3.2.4 Configuration standards address all known security vulnerabilities and are based on industry-accepted system hardening standards. | | |
| **P1** | 3.2.5 Configuration standards and build procedures include:<br>• Changing all vendor-supplied default accounts and system settings.<br>• Removing or disabling all unnecessary system or application functionality.<br>• Preventing functions that require different security levels from co-existing on the same system component. | • Examine system configuration standards and build procedures for all system component types.<br>• Examine system configurations.<br>• Interview personnel. | |
| **P1-3.3 Change management** | | | |
| **P1** | 3.3.1 Change-control procedures are defined and implemented for all changes to system components, including “emergency changes.” | • Examine documented change-control procedures.<br>• Examine records of changes and compare to system configurations.<br>• Interview personnel. | Defined change-control procedures should be followed for any change that impacts a 3DS system or the 3DE. The impact of the change should be documented so that all affected parties can plan appropriately for any processing changes. Changes should be authorized by appropriate parties, as defined by the change-management policy, to verify the change is legitimate.<br>Thorough testing should be performed to verify that the security of the environment is not reduced by implementing a change; and there should be documented back-out procedures in case the change fails or adversely affects the security of any system component. |
| **P1** | 3.3.2 All changes are authorized and the security impact understood prior to implementing the change. | | |
| **P1** | 3.3.3 All changes are tested in a non-production environment. | | |
| **P1** | 3.3.4 Rollback procedures are prepared for all changes. | | |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 3.3.5 Unauthorized changes to system or application configurations are prevented and/or detected and addressed. | • Examine documentation of controls and/or processes.<br>• Observe implemented controls.<br>• Interview personnel. | The implemented process should be able to either prevent or detect and address the unauthorized addition, removal, or modification of system critical files such as configuration file contents, operating system programs, and application executables. If the implemented solution relies on detection, processes should be in place to ensure that unauthorized changes are detected and addressed as soon as possible. Where unauthorized change attempts are automatically blocked, a record of the attempted change should also be generated and investigated to determine whether action is needed to prevent further attempts.<br>The controls could include change-detection solutions, such as file-integrity monitoring, or a frequent re-load of a trusted build to restore the system component to a known secure state. |

# Requirement P1-4. Vulnerability management

| | Overview | Requirements |
|---|---|---|
| **P1-4** | New vulnerabilities are continually being discovered and can enter the network from both internal and external sources. An ongoing cycle of testing and remediation helps ensure that security controls continue to be effective in a changing environment. | 4.1 Protect against malicious software<br>4.2 Address vulnerabilities and security weaknesses |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-4.1 Protect against malicious software** | | | |
| **P1** | 4.1.1 A security policy(s) and procedures for protecting systems against malware are maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | Controls should prevent the introduction and execution of malicious software (malware) on 3DS systems. A combination of methods, tools, and programs may be used—for example, anti-malware software, application whitelisting, host-based and network-based intrusion-prevention tools, and system instrumentation. A combination of real-time protection and periodic scans should be considered.<br>The implemented controls should be kept current—e.g., updated signatures, baselines, etc.—as applicable for the technology. Anti-malware controls should not be disabled unless specifically authorized by management on a case-by-case basis for a limited time period. |
| **P1** | 4.1.2 Controls to prevent and/or detect and remove malicious software are implemented, active, and maintained. | • Examine documented controls/configurations.<br>• Observe implemented controls and processes.<br>• Examine evidence of malware prevention and/or detection and removal.<br>• Interview personnel. | |
| **P1-4.2 Address vulnerabilities and security weaknesses** | | | |
| **P1** | 4.2.1 A security policy(s) and procedures for identifying, ranking, and protecting against vulnerabilities are maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | Policies and procedures define the methods employed to identify and remediate vulnerabilities that could affect 3DS systems, and include; monitoring vulnerability lists, performing vulnerability scans and penetration tests, and establishing bug bounty programs. Reputable outside sources should be used for security and vulnerability information. |
| **P1** | 4.2.2 Vulnerability scans, both internal and external, are performed at least quarterly to identify and address vulnerabilities. | • Examine vulnerability scanning reports<br>• Interview personnel. | Vulnerability scans and all required remediation should be completed as frequently as needed to ensure vulnerabilities are addressed in a timely manner. Rescans should be performed to verify vulnerabilities have been addressed. In addition to a regular scanning process, vulnerability scans should also be performed after any significant change to the environment. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 4.2.3 Vulnerability scans are performed by qualified personnel:<br>- External scans are performed by a PCI SSC Approved Scanning Vendor (ASV).<br>- Internal scans are performed by qualified personnel. | - Examine vulnerability scanning reports.<br>- Interview personnel. | Internal vulnerability scans can be performed by qualified, internal staff or outsourced to a qualified third party. For scans managed by the entity, the entity should ensure that scanning engines and vulnerability fingerprints are up to date and the scanning engine configured in accordance with vendor guidance documentation.<br>Internal personnel should have sufficient knowledge to review and understand the scan results, and determine appropriate remediation. Internal personnel who interact with the ASV should also be knowledgeable in the network architecture and implemented security controls in order to provide the ASV with information needed to complete the scan. |
| **P1** | 4.2.4 Identified vulnerabilities are ranked to determine the criticality of the vulnerability. | - Examine documented procedures for ranking vulnerabilities.<br>- Interview personnel. | Vulnerabilities should be ranked and prioritized in accordance with an industry-accepted methodology or organizational risk-management strategy. |
| **P1** | 4.2.5 Penetration tests are performed at least annually. | - Examine penetration test reports.<br>- Interview personnel. | Penetration tests should be performed at regular intervals and after significant changes to the environment. The penetration-testing methodology should be based on industry-accepted approaches and incorporate both application-layer and network-layer testing. The scope of testing should cover the 3DE perimeter and critical systems, and include testing from both inside and outside the network. Testing should also be performed to verify all segmentation controls are operational and effective, and that out-of-scope systems and networks do not have access to the 3DE. The specific methodology, depth, and frequency of the testing should be based on the entity's risk-assessment strategy, and be updated as needed to consider new threats and vulnerabilities. |
| **P1** | 4.2.6 Penetration tests are performed by qualified personnel. | - Examine penetration test reports.<br>- Interview personnel. | Tests should only be performed by qualified personnel who can demonstrate knowledge and experience, and are organizationally independent of the environment being tested. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 4.2.7 Vulnerabilities and penetration testing findings considered as high risk are addressed within one month. All other vulnerabilities and identified security issues are addressed in a timely manner. | • Examine results of penetration tests and vulnerability scanning reports.<br>• Examine evidence of remediation to address vulnerabilities and security issues.<br>• Interview personnel. | Security patches and fixes should be implemented based on risk ranking. Where high-risk vulnerabilities cannot be addressed within one month, a formal exception process should be followed, including approval by personnel with appropriate responsibility and accountability. (See Requirements P2-2.1.2 and P2-2.1.3.)<br>Once remediation activities have been performed—for example, implementing a patch or updating a configuration file to address a vulnerability or security flaw—rescans and penetration tests should be performed as necessary to verify the remediation is effective and the identified vulnerability or security issue has been mitigated.<br>A record of remediation activities should be maintained—for example, via change-control records, configuration file updates, and audit logs. All updates and patches should be managed in accordance with change-control processes. Where applicable, changes to system configurations should be reflected in the configuration build standards. |

## Requirement P1-5. Manage access

| | Overview | Requirements |
|---|---|---|
| **P1-5** | Strong access controls protect systems and data from unauthorized access and can limit the likelihood of a compromised system being used to gain access to other systems and networks. | 5.1 Access management<br>5.2 Account management<br>5.3 Authentication |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-5.1 Access management** | | | |
| **P1** | 5.1.1 A security policy(s) and procedures for assigning access are maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | Policies and procedures should include details of processes for role assignments, oversight processes, business justifications, and user and group privilege controls. |
| **P1** | 5.1.2 Roles and responsibilities are defined for groups and accounts with access to 3DS systems. | • Examine defined roles and responsibilities.<br>• Interview personnel. | Determining who has access to what, for how long, and what level of access they have should be based on established roles and responsibilities. This includes the processes used to maintain, monitor, and approve administrative and user access to 3DS systems and data. |
| **P1** | 5.1.3 Least privileges are assigned based on individual job function and periodically reviewed. | • Observe assigned access privileges.<br>• Examine evidence that access privileges are periodically reviewed.<br>• Interview personnel. | Access to 3DS systems and data should be restricted based on business need, while also accounting for the sensitivity of the data being transmitted between the 3DS systems. Access privileges should be reviewed by responsible personnel as defined by the 3DS entity. The frequency of reviews should be defined in accordance with the entity's defined policies and be appropriate for the level of privilege assigned. |
| **P1-5.2 Account management** | | | |
| **P1** | 5.2.1 A security policy(s) and procedures for managing accounts are maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | Established processes and oversight includes approval process for provisioning, monitoring, changing, and revocation of accounts with the ability to access a 3DS system. |
| **P1** | 5.2.2 Individuals are assigned a unique account ID. | • Examine documented procedures.<br>• Observe account settings. | Assigned unique IDs should allow the organization to maintain individual responsibility for actions and an effective audit trail per employee. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 5.2.3 Controls are implemented to protect the confidentiality and integrity of accounts and credentials. | • Examine documented procedures.<br>• Observe implemented controls. | Implemented controls should protect the confidentiality and integrity of accounts for both local and remote users. The controls should include ensuring that account and credential information is securely transmitted and stored—for example, using strong cryptography—at all times. |
| **P1** | 5.2.4 Controls are implemented to prevent misuse of accounts. | • Examine documented procedures.<br>• Observe implemented controls. | Processes for prevent misuse of accounts should include, at a minimum, the use of account lockouts, lockout durations, session timeouts, and reactivation processes. Inactive user accounts should be removed or disabled within a timely manner. All processes should align with the entity's security policies and procedures. |
| **P1** | 5.2.5 Access for third parties is identified, controlled, and monitored. | • Examine documented procedures.<br>• Observe implemented controls. | Configuration and connection requirements should be defined and implemented for all access by third-party personnel—for example, ensuring accounts are enabled only during the time needed and disabled when not in use, and monitoring account activity when in use. |
| **P1-5.3 Authentication** | | | |
| **P1** | 5.3.1 All access to 3DS systems requires strong authentication prior to access being granted. | • Examine documented procedures.<br>• Observe implemented controls. | Authentication may be consist of one or more of:<br>• Something you know, such as a password or passphrase<br>• Something you have, such as a token device or smart card<br>• Something you are, such as a biometric<br>Where passwords are used, documented requirements should include considerations for entropy (strength/complexity), password history and reuse, reset processes, and other best practices for secure password use. Passwords should meet a minimum level of strength, as defined by the entity's security policy, that provides reasonable assurance they are not guessable and would withstand a brute-force attack. |

## Requirement P1-6. Physical Security

| | Overview | Requirements |
|---|---|---|
| **P1-6** | Individuals with physical access to systems or media could potentially bypass logical access controls and gain access to sensitive data. Strong physical access controls also protect against the unauthorized addition, modification, removal, or damage of systems and data. | 6.1 Restrict physical access<br>6.2 Secure media |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-6.1 Restrict physical access** | | | |
| **P1** | 6.1.1 A security policy(s) and procedures for securing physical access to 3DS systems is maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | The entity should define the physical access controls required to prevent 3DS systems being physically accessed by unauthorized persons. The controls should cover all physical access points and include procedures for managing onsite employees and third parties. Specific procedures should be defined for managing visitors, including a visible means for identification and escorts by authorized personnel.<br>Physical access and monitoring controls should include use of video cameras and/or access-control mechanisms. Data from video cameras and/or access-control mechanisms should be logged to provide an audit trail of all physical access to the 3DE. Access logs should be retained in accordance with the entity's audit log policy. (Refer to Requirement P1–7.2.) Monitoring and periodic reviews of physical access controls and audit logs should be performed to allow early identification of incorrect controls and for timely response to suspicious activities. Personnel should be trained to follow procedures at all times.<br>All suspicious activity should be managed per incident security procedures. (Refer to Requirement P1-7.1.) |
| **P1** | 6.1.2 Facility entry controls are in place to limit and monitor physical access to systems in the 3DE. | • Observe physical access controls. | |
| **P1** | 6.1.3 Physical access for personnel to 3DE is authorized and based on individual job function. | • Examine assigned access permissions.<br>• Interview personnel.<br>• Observe personnel access procedures. | |
| **P1** | 6.1.4 Personnel access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. | • Examine documented procedures.<br>• Examine evidence of access revocation and return of physical access mechanisms.<br>• Interview personnel. | |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-6.2 Secure media** | | | |
| **P1** | 6.2.1 Strict control is maintained over the storage and accessibility of media. | • Observe implemented controls.<br>• Interview personnel. | Controls and processes should cover secure storage, transport, and disposal of all storage media used in the 3DE. Procedures and technical controls should provide assurance that media cannot be removed, stolen, or copied by unauthorized persons. The specific controls and level of rigor required to protect media should be appropriate for the sensitivity of the data stored on the media. |

## Requirement P1-7. Incident response preparedness

| | Overview | Requirements |
|---|---|---|
| **P1-6** | An effective incident response plan allows an entity to respond to potential security issues quickly and effectively, and minimize the potential impact of a security incident or breach. | 7.1 Incident response plan<br>7.2 Audit logs |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1-7.1 Incident response plan** | | | |
| **P1** | 7.1.1 A security policy(s) and procedures for managing and responding to security incidents is maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | The policy should define plans, procedures, and technologies to detect, analyze, and promptly respond to security incidents. Defined procedures should include response activities, escalation, and notification, and cover all assets and processes that could impact 3DS operations or data. Procedures should be updated in alignment with operational/business changes and the organization's risk strategy. |
| **P1** | 7.1.2 An incident response plan is in place that includes:<br>• Roles and responsibilities<br>• Communication and contact strategies<br>• Specific incident response procedures<br>• Business recovery and continuity procedures<br>• Data back-up processes<br>• Analysis of legal requirements for reporting compromises<br>• Coverage and responses of all critical system components<br>• Consideration of payment brands' response requirements | • Examine documented incident response plans and procedures.<br>• Interview personnel. | The incident response plan should be comprehensive and include coverage of all 3DS systems.<br>Communication and contact strategies should include notification of the payment brands, at a minimum.<br>Incident response personnel/teams should be trained and knowledgeable in incident response procedures, and be available to respond immediately to an incident. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 7.1.3 The plan is reviewed and tested at least annually. | • Examine documented procedures.<br>• Examine evidence of reviews and testing.<br>• Interview personnel. | The incident response plan should be periodically reviewed, tested, and updated to incorporate lessons learned. Relevant staff should be included in the testing and be briefed on the post-test review. Testing should include validation that system, audit, and monitoring logs are available and contain all needed data. |
| **P1-7.2 Audit logs** | | | |
| **P1** | 7.2.1 A security policy(s) and procedures for generating and managing audit logs is maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | The policy should cover requirements for the generation, collection, management and retention of audit logs for all system components in the 3DS environment. |
| **P1** | 7.2.2 Audit logs are implemented to:<br>• Link all access to 3DS systems to an individual user.<br>• Record security events. | • Examine system configurations.<br>• Observe access attempts.<br>• Examine audit log files. | Recording all personnel access, both physical and logical, to 3DS systems should help the entity identify any misuse of accounts, and ensure that each individual is accountable for their actions.<br>The determination of “security event” will vary for each organization and may include consideration for the type of technology, location, and function of the system. Logging of security events should include notifications or alerts related to suspicious or anomalous activities—for example, as defined in Requirements P1-2.2.2 and P1-3.3.5. The level of detail logged should be sufficient to identify who, what, where, when, and how an event occurred in the 3DS environment. This requirement does not encompass 3DS transaction logs. |
| **P1** | 7.2.3 Time synchronization is implemented on 3DS systems to ensure system clocks are synchronized and have the correct and consistent time. | • Examine system configurations. | Designated central time server(s) should be defined to receive time signals from trusted external sources, based on International Atomic Time or UTC. Central time server(s) should peer with one another to keep accurate time. Systems receive time only from designated central time server(s).<br>Time-synchronization technology should be kept current and time data protected from unauthorized modification. |
| **P1** | 7.2.4 Logs and security events are monitored and/or periodically reviewed for all 3DS systems to identify anomalies or suspicious activity. | • Examine evidence of reviews of logs and security events.<br>• Interview personnel. | Real-time monitoring and/or periodic reviews should be in place for all security events, critical system logs, and security system logs—for example, firewalls, IDS/IPS, authentication servers, e-commerce redirection servers, etc. The frequency of reviews should be aligned with the associated risk.<br>The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P1** | 7.2.5 Audit logs are secured so they cannot be altered. | - Examine controls/configurations.<br>- Observe attempts to modify audit logs | Only individuals who have a job-related need should be able to view audit log files. Audit logs should be promptly backed up to a centralized log server or media that is difficult to alter. Physical and logical access controls should be in place to prevent unauthorized modifications to audit logs. File-integrity monitoring or change-detection software can be implemented to ensure that any changes to saved log data generates an alert. |
| **P1** | 7.2.6 Audit and monitoring logs are retained for least one year, with a minimum of three months immediately available for analysis. | - Examine audit log files.<br>- Interview personnel. | Log-retention policies should include storage and retrieval procedures. If stored in off-line locations, procedures should include assurance that log data can be retrieved in a timely manner. The logs to be retained include at least those defined in Requirement P1-7.2.2. |

# Part 2: 3DS Security Requirements

## Requirement P2-1. Validate scope

| | Overview | Requirements |
|---|---|---|
| **P2-1** | Scoping involves the identification of the facilities, people, processes, and technologies that interact with or could impact the security of 3DS data or systems. Once scope is properly identified, the appropriate security controls can be applied. | 1.1 Scoping |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-1.1 Scoping** | | | |
| **P2** | 1.1.1 All networks and system components in-scope for these PCI 3DS security requirements are identified. | • Examine documented results of scope reviews.<br>• Interview personnel. | A scope verification exercise includes identifying all locations and flows of 3DS data, as well as the systems performing 3DS functions (ACS, DS, and/or 3DSS) and any systems that are connected to or could impact the 3DE. Network mapping tools, data flow diagrams, and process documentation can often assist with this process. The scoping process should also include consideration of backup/recovery sites and fail-over systems.<br>The scoping exercise should also include identifying personnel with access to 3DS data, as well as the physical locations where 3DS systems are housed.<br>Validation of scope should be performed as frequently as needed to ensure the scope is known and scope documentation remains accurate and up to date. The results of scoping exercises should help to confirm that security controls are applied to all applicable systems, and that all connections to third-parties—for example, service providers and business partners—are identified and properly secured. |
| **P2** | 1.1.2 All out-of-scope networks are identified with justification for being out of scope and descriptions of segmentation controls implemented. | • Examine documented results of scope reviews.<br>• Examine data flow and network diagrams.<br>• Observe segmentation controls. | |
| **P2** | 1.1.3 All connected entities with access to the 3DS environments are identified. | • Examine documentation.<br>• Interview personnel. | |

# Requirement P2-2. Security governance

| | Overview | Requirements |
|---|---|---|
| **P2-2** | A security governance program provides oversight and assurance that an entity's information security strategies are aligned with its business objectives and adequately address risks to the entity's data and systems. | 2.1 Security governance<br>2.2 Manage risk<br>2.3 Business as usual (BAU)<br>2.4 Manage third-party relationships |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-2.1 Security governance** | | | |
| **P2** | 2.1.1 Security objectives are aligned with business objectives. | • Examine documentation.<br>• Interview personnel. | The security objectives should be defined as part of an overarching security strategy that supports and facilitates business objectives. The security strategy should provide the foundation for the entity's security policies and procedures and provide a benchmark against which the health of security controls is monitored and measured. |
| **P2** | 2.1.2 Responsibilities and accountability for meeting security objectives are formally assigned, including responsibilities for the security of 3DS processes. | • Examine documentation.<br>• Interview personnel. | The assignment of specific roles and responsibilities should include monitoring and measurement of performance to ensure security objectives are met. Roles and responsibilities may be assigned to a single owner or multiple owners for different aspects.<br>Ownership should be assigned to individuals with the authority to make risk-based decisions and upon whom accountability rests for the specific function. Duties should be formally defined, and owners should be able to demonstrate an understanding of their responsibilities and accountability. |
| **P2** | 2.1.3 Responsibility for identifying and addressing evolving risks is assigned. | • Examine documentation.<br>• Interview personnel. | |
| **P2-2.2 Manage risk** | | | |
| **P2** | 2.2.1 A formal risk-management strategy is defined. | • Examine documentation.<br>• Interview personnel. | The risk-management strategy defines a structured approach for identifying, evaluating, managing, and monitoring risk. The strategy should include requirements for regularly reviewing and updating the entity's risk-assessment processes as well as methods to monitor the effectiveness of risk-mitigation controls. |
| **P2** | 2.2.2 The risk-management strategy is approved by authorized personnel and updated as needed to address changing risk environment. | • Examine documentation.<br>• Interview personnel. | The risk-management strategy should be approved by personnel with appropriate responsibly and accountability. (See Requirements P2-2.1.2 and P2-2.1.3.) |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-2.3 Business as usual (BAU)** | | | |
| **P2** | 2.3.1 Review and/or monitoring is performed periodically to confirm personnel are following security policies and procedures. | • Examine evidence of reviews and/or ongoing monitoring.<br>• Interview personnel. | Periodic reviews and/or ongoing monitoring of personnel and activities should ensure security is included as part of normal business operations on an ongoing basis. Reviews should be performed by responsible personnel as defined by the entity. The frequency of reviews should be defined in accordance with the entity's risk assessments and be appropriate for the particular job function. |
| **P2** | 2.3.2 Processes to detect and respond to security control failures are defined and implemented. | • Examine documented processes.<br>• Observe implemented processes.<br>• Interview personnel. | The entity should be able to detect any failures in security controls and respond to them in a timely manner. Processes for responding to security control failures should include:<br>• Restoring the security control<br>• Identifying the cause of failure<br>• Identifying and addressing any security issues that arose during the failure of the security control<br>• Implementing mitigation (such as process or technical controls) to prevent the cause of the failure recurring<br>• Resuming monitoring of the security control |
| **P2-2.4 Manage third-party relationships** | | | |
| **P2** | 2.4.1 Policies and procedures for managing third-party relationships are maintained and implemented. | • Examine documented policies/procedures.<br>• Interview personnel. | Policies and procedures for managing third-party relationships should consider the risk that each relationship represents, as well as how third-party performance and behavior will be monitored. The policy should be kept up to date, approved by management, and communicated to applicable personnel. |
| **P2** | 2.4.2 Due diligence is performed prior to any engagement with a third party. | • Examine documented procedures.<br>• Examine results of due diligence efforts<br>• Interview personnel. | Due-diligence processes should include thorough vetting and a risk analysis prior to establishing a formal relationship with the third party. Specific due-diligence processes and goals will vary for each entity and should provide sufficient assurance that the third party can meet the entity's security and operational needs. |
| **P2** | 2.4.3 Security responsibilities are clearly defined for each third-party engagement. | • Examine documentation<br>• Interview personnel. | The specific approach for defining security responsibilities will depend on the type of service as well as the particular agreement between the entity and third party. The entity should have a clear understanding of the security responsibilities to be met by the third party and those to be met by the entity. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 2.4.4 The 3DS entity periodically verifies that the agreed-upon responsibilities are being met. | • Examine results of periodic verification.<br>• Interview personnel. | The specific type of evidence provided by the third party will depend on the agreement in place between the two parties. The evidence should provide assurance that the agreed-upon responsibilities are being met on a continual basis. The frequency of verification should be aligned with the entity's risk analysis of the service being provided. |
| **P2** | 2.4.5 Written agreements are maintained. | • Examine documentation.<br>• Interview personnel. | Agreements should promote a consistent level of understanding between parties about their applicable responsibilities, and be acknowledged by each party. The acknowledgement evidences each party's commitment to maintaining proper security in regard to the 3DS services. |

## Requirement P2-3 Protect 3DS systems and applications

| | Overview | Requirements |
|---|---|---|
| **P2-3** | To maintain the security of 3DS environments, controls need to be designed and implemented to protect the confidentiality, integrity, and availability of 3DS technologies, processes, and data. | 3.1 Protect boundaries<br>3.2 Protect baseline configurations<br>3.3 Protect applications and application interfaces<br>3.4 Secure web configurations<br>3.5 Maintain availability of 3DS operations |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-3.1 Protect boundaries** | | | |
| **P2** | 3.1.1 Traffic to and from ACS and DS is restricted to only that which is relevant to the 3DS functions. | • Examine log files.<br>• Observe implemented controls. | The only permitted traffic should be for the purposes of 3DS transactions, or to support a 3DS function, or support the 3DS system component—for example, for security or management purposes. Systems within the 3DE should be limited to those necessary for performing or supporting 3DS functions.<br>All types of interfaces should be identified, including physical, logical, and virtual. |
| **P2** | 3.1.2 Traffic to and from ACS and DS is permitted only via approved interfaces. | | |
| **P2-3.2 Protect baseline configurations** | | | |
| **P2** | 3.2.1 Controls are implemented to protect the confidentiality and integrity of system configurations and documentation that define security settings. | • Examine log files.<br>• Observe implemented controls. | Examples of the types of files requiring protection include baseline configuration files, system build data, system images, and build procedures. The controls should protect both integrity and confidentiality of such data, to prevent an attacker from changing the secure configuration of a 3DS system component, installing their own configuration, or using the information to identify security gaps they can then exploit. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-3.3 Protect applications and application interfaces** | | | |
| **P2** | 3.3.1 Applications and programs are protected from unauthorized changes once in a production state. | - Examine log files.<br>- Observe implemented controls. | Ensuring the integrity of applications and programs in production requires more than an effective change-control process. A combination of strict access controls, monitoring, and programmatic controls should be considered. Examples of additional mechanisms include software authentication codes, digitally signed modules, or execution within an SCD. The use of a protection technique is only effective if the system confirms the results (for example, is the digital signature valid?) and acts on the results. |
| **P2** | 3.3.2 The mechanisms to protect applications and programs from unauthorized changes are monitored and maintained to confirm effectiveness. | - Observe implemented controls for monitoring and maintaining protection mechanisms<br>- Interview personnel. | Protection mechanisms should be kept up to date and monitored to ensure they are working as intended and continue to be effective. Cryptographic techniques used for API code protection may require updating as computation capabilities and cryptanalysis improvements evolve. |
| **P2** | 3.3.3 All APIs that interface with the 3DS environment are identified, defined, and tested to verify they perform as expected. | - Examine network and data-flow diagrams<br>- Observe implemented controls.<br>- Examine results of testing<br>- Interview personnel. | All exposed APIs need to be periodically reviewed and tested to ensure that they are functioning as intended. Use of industry best practices and guidance is recommended—for example, the OWASP REST (REpresentational State Transfer) Security Cheat Sheet provides best practices for REST-based services. |
| **P2** | 3.3.4 Controls are implemented to protect APIs exposed to untrusted networks. | | |
| **P2-3.4 Secure web configurations** | | | |
| **P2** | 3.4.1 Only those HTTP request methods required for system operation are accepted. All unused methods are explicitly blocked. | - Examine log files.<br>- Observe implemented controls.<br>- Interview personnel. | All functionality not explicitly required for system operation should be disabled or blocked; and configurations should be designed to prevent common application attack scenarios such as XSS, Clickjacking, and injection attacks. Applications should be configured to restrict content and functionality from external sources to only that which is necessary for business purposes. If functionality or content from trusted external sources—for example, third-party websites—is necessary for business purposes, then those sources and the methods in which they are permitted to provide such content (e.g., as iframes, direct posts, etc.) should be explicitly authorized, and all other sources and methods blocked. |
| **P2** | 3.4.2 The use of HTTPS is enforced across all application pages/resources and all communications are prevented from being sent over insecure channels (e.g., HTTP). | - Examine log files.<br>- Observe implemented controls.<br>- Interview personnel. | |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 3.4.3 Applications (or the underlying systems) are configured to reject content provided by external sources by default. Exceptions are explicitly authorized. | • Examine documented controls.<br>• Observe implemented controls.<br>• Interview personnel. | *(See previous page)* |
| **P2** | 3.4.4 Applications are configured to prevent content from being embedded into untrusted third-party sites/applications. Exceptions are explicitly authorized. | • Examine documented controls.<br>• Observe implemented controls.<br>• Interview personnel. | Similarly, content provided by the 3DS provider should be prevented (to the extent possible) from being embedded in the sites of untrusted third parties. Otherwise, those parties might use the content of the 3DS entity to impersonate the 3DS entity in an attempt to hijack 3DS transactions and/or commit fraud. |
| **P2** | 3.4.5 Security features native to the development framework and/or application platform are enabled, where feasible, to protect against common client-side attacks (such as XSS, Injection, etc.). | • Examine documented controls.<br>• Observe implemented controls.<br>• Interview personnel. | Native security functions are available in most modern development platforms and frameworks, and are effective at protecting against common client-side attacks without requiring additional security functionality to be written into the application code. Methods to restrict such content and functionality include the use of Content Security Policy (CSP) directives and HTTP Strict Transport Security (HSTS). Other security features native to the development framework that should be considered include automated compile-time security checks that are performed as part of the application build process.<br>Where native security controls such as those described above are not used, 3DS entities should document the controls that have been implemented to protect applications and systems from common client-side attacks (such as XSS, XSRF, Injection attacks, etc.) and provide justification for why native features were not used. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-3.5 Maintain availability of 3DS operations** | | | |
| **P2** | 3.5.1 Availability mechanisms are implemented to protect against loss of processing capability within the 3DS infrastructure. | • Examine documented controls.<br>• Observe implemented controls. | 3DS components should be architected with high availability as a key factor in the software, system, and infrastructure design to maintain the integrity of the 3DS ecosystem. Security policies should reflect availability requirements of 3DS components and security resources in support of 3DS platform and clusters—for example, review of catastrophic testing results, failover results, and change-control processes. The controls should ensure security resources are working correctly and according to policy within the respective testing processes.<br>The plan for availability should allow the entity to withstand denial-of-service (DoS) attacks that could force fallback to less secure verification methods or provide cover for other attacks against a system or the infrastructure. The implemented controls should demonstrably reduce this risk through, for example, a combination of fault-tolerance and rapid response/recovery capabilities as well as the use of application isolation, data and system restraints, and load balancing. Documentation and domain architectures should be reviewed for denial-of-service utilities and network load-balancing capabilities. Testing of back-up process and data should be performed. |
| **P2** | 3.5.2 The availability mechanisms implemented are monitored and maintained to confirm effectiveness. | • Observe implemented controls for monitoring and maintaining the availability mechanisms.<br>• Interview personnel. | The mechanisms intended to maintain availability of the 3DS infrastructure should be maintained and monitored to ensure they are working as intended and continue to be effective. Continuous monitoring of processing availability and rapid reporting of outages aid in timely response to potential failures.<br>Availability mechanisms and technologies evolve and may require periodic refresh. Additionally, the sophistication of attacks that may adversely impact availability or that may exploit a degraded system continues to evolve. |

## Requirement P2-4. Secure logical access to 3DS systems

| | Overview | Requirements |
|---|---|---|
| **P2-4** | In addition to ensuring strong access controls and account management for the 3DS environment, certain types of access present a higher risk and require more stringent controls to prevent them from being misused or compromised. | 4.1 Secure connections for issuer and merchant customers<br>4.2 Secure internal network connections<br>4.3 Secure remote access<br>4.4 Restrict wireless exposure<br>4.5 Secure VPNs |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-4.1 Secure connections for issuer and merchant customers** | | | |
| **P2** | 4.1.1 Access by issuer and merchant users to their assigned issuer and merchant interfaces—for example, via API or web portal—for purposes of managing only their own account, is restricted to authorized personnel and requires a unique user ID with strong password and another form of strong authentication. | • Examine documented procedures.<br>• Observe implemented controls. | This requirement is intended for scenarios where the 3DS entity provides issuer and merchant users with access to 3DS services and data through defined issuer and merchant interfaces, such as an API or web portal. In this scenario, the issuer and merchant personnel require a unique user ID with a strong password and another form of strong authentication. Strong authentication techniques should align with industry-accepted practices and may include:<br>• One-time passcodes/passwords (OTP)<br>• Certificate-based authentication (CBA/SAML) where a public and private key is unique to the authentication device and the person who possesses it<br>• Context-based authentication where additional information is required to verify whether a user's identity is authentic<br>• Restriction of connections to only predefined and authorized system components–e.g., via IP filtering or site-to-site VPN<br>These merchant/issuer users have access only to their own merchant/issuer account and are not able to access any other account or impact the configuration of any application, system component, or network. While multi-factor authentication is not required for this type of access, it is recommended. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-4.2 Secure internal network connections** | | | |
| **P2** | 4.2.1 Multi-factor authentication is required for all personnel with non-console access to ACS, DS, and 3DSS. | • Examine documented procedures.<br>• Observe implemented controls. | Multi-factor authentication (MFA) requires the completion of at least two different authentication methods—that is, something you know, something you have, and something you are—prior to access being granted. The authentication mechanisms used should be implemented to ensure their independence such that access to one factor does not grant access to any other factor, and the compromise of any one factor does not affect the integrity or confidentiality of any other factor. Additionally, no prior knowledge of the success or failure of any factor should be provided to the individual until all factors have been presented. Refer to industry standards and best practices for further guidance on MFA principles.<br>MFA can be applied at the network level, system level, or application level. For example, MFA could be applied when connecting to the 3DE secure network or network segment, or when connecting to an individual 3DS system component.<br>MFA is required for all personnel connections to the ACS, DS, and 3DSS that occur over a network interface. Examples of access include for purposes of maintenance, configuration, updating, administration, or general management of the 3DS component. MFA is not required for application or system accounts performing automated functions. |
| **P2-4.3 Secure remote access** | | | |
| **P2** | 4.3.1 Multi-factor authentication is required for all remote access originating from outside the entity's network that provides access into the 3DE. | • Examine documented procedures.<br>• Observe implemented controls. | Multi-factor authentication (MFA) is required for all personnel—both user and administrator, and including third-party access for support or maintenance—accessing the 3DE from outside the entity's network.<br>Where MFA is implemented to grant access to the 3DE, additional MFA is not required for access to individual systems or applications within the 3DE. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 4.3.2 Remote access to the 3DE is controlled and documented, including:<br>- System components for which remote access is permitted<br>- The location(s) from which remote access is permitted<br>- The conditions under which remote access is acceptable<br>- Individuals with remote access permission<br>- The access privileges applicable to each authorized use | - Examine policies and procedures.<br>- Observe remote access controls.<br>- Interview personnel. | Remote access processes should be fully documented to ensure access is only granted to users or systems that have been previously approved for such access. Disconnection of remote access sessions after a period of inactivity should be considered. Policies and operational procedures should be kept up to date so personnel understand the proper processes and to prevent unauthorized access to the network. |
| **P2** | 4.3.3 Where remote access using personally owned devices is permitted, strict requirements for their use are defined and implemented to include:<br>- Device security controls are implemented and maintained as equivalent to corporate-owned devices.<br>- Each device is explicitly approved by management. | - Examine policies and procedures.<br>- Observe remote access controls.<br>- Interview personnel. | Remote access using a personally owned device should only be permitted under a strictly defined process that includes management approval and verification that the device could not impact the security of 3DS systems.<br>Devices should be verified as meeting at least the same rigor of security as defined in the entity's security policies. Devices should be maintained and monitored via a centralized, secure device-management solution. Approval for the use of a personal device should be explicitly provided on a case-by-case basis, by an appropriate person who has assigned responsibilities for security. (See Requirement P2-2.1.2.) |
| **P2** | 4.3.4 Remote access privileges are monitored and/or reviewed at least quarterly by an authorized individual to confirm access is still required. | - Examine documented processes.<br>- Examine evidence of monitoring and/or reviews.<br>- Interview personnel. | Remote access privileges should be regularly reviewed, at least quarterly, by an authorized individual. Documentation of reviews should be retained. Results of these reviews should include identification and removal of any unneeded or incorrect access, and should ensure that only individuals with a current business need are granted remote access.<br>Automated processes may be used to assist in reviewing access privileges—for example, to generate notifications when an account has not been used for a period of time. Organizational processes to actively review and change access when an individual changes job function can also assist. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-4.4 Restrict Wireless Exposure** | | | |
| **P2** | 4.4.1 3DS components (ACS, DS, 3DSS) do not use or connect to any wireless network. | • Examine network diagrams.<br>• Observe implemented controls.<br>• Interview personnel. | To prevent 3DS components from being exposed to wireless networks, wireless-enabled devices should not be present within the 3DE. Additionally, ACS, DS, and 3DSS system components should not use or be connected to any wireless-enabled components.<br>Any wireless networks and devices used or supported by the 3DS entity—for example, for remote users—should be properly secured and configured in accordance with industry standards. |
| **P2-4.5 Secure VPNs** | | | |
| **P2** | 4.5.1 All VPNs that provide access to 3DE are properly configured to provide strong security communications and protect against eavesdropping, replay attacks, and man-in-the-middle attacks. | • Examine configuration standards.<br>• Observe VPN controls.<br>• Interview personnel. | VPN configurations should be reviewed against industry-recommended implementations to verify security features are enabled. Use of a trusted CA, a third party that utilizes a chain-of-trust model to provide assurance for a particular certificate, is recommended. If an internal CA is used the internal CA also needs to be verified as meeting industry requirements such as TS101456. |

## Requirement P2-5. Protect 3DS data

| | Overview | Requirements |
|---|---|---|
| **P2-5** | Minimizing the distribution and amount of data to only that which is necessary helps to reduce the risk of data exposure. The use of data-specific controls provides a critical layer of protection when data is exposed to public or untrusted environments, and can also protect data in trusted environments in the event other security controls are circumvented. | 5.1 Data lifecycle<br>5.2 Data transmission<br>5.3 TLS configuration<br>5.4 Data storage<br>5.5 Monitoring 3DS transactions |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-5.1 Data lifecycle** | | | |
| **P2** | 5.1.1 Policies and procedures for usage, flow, retention, and disposal of 3DS data are maintained and implemented. | • Examine documented policies.<br>• Examine evidence of data usage, flow, retention and disposal.<br>• Interview personnel. | Policies should address protection of 3DS data throughout its lifecycle and be based on data sensitivity and legal and business requirements. Protection for data in transit, persistent storage, temporary storage, and memory should be defined. Documentation should explain the purpose, scope, retention goals, disposal requirements, and applicable legal and business requirements. Local or applicable laws supersede any defined practices regarding data storage—for example, PII Laws and breach notification laws should be included in data-classification and retention policies. Data should be classified according to its security need. |
| **P2** | 5.1.2 3DS data is retained only as necessary and securely deleted when no longer needed. | • Examine data retention schedule and data disposal process<br>• Interview personnel.<br>• Observe data storage. | Data-retention schedules should be defined to identify what data needs to be retained, for how long, where that data resides, and procedures for its secure destruction as soon as it is no longer needed. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-5.2 Data transmission** | | | |
| **P2** | 5.2.1 Strong cryptography and security protocols are used to safeguard 3DS sensitive data during transmission. | • Examine documentation describing methods for encrypting data.<br>• Examine configuration standards.<br>• Observe implemented controls. | Controls should be applied at all interfaces and locations where 3DS sensitive data (as defined in the *PCI 3DS Data Matrix*) is transmitted or received. This includes all transmissions over open or public networks, internal networks, and transmissions within and between 3DS system domains. 3DS sensitive data should be protected to a level that is at least equivalent to that identified in Annex D of the current version of *EMV® 3DS Protocol and Core Functions Specification*.<br>Secure transmission of 3DS data requires use of trusted keys/certificates, a secure protocol for transport, and strong cryptography to encrypt the 3DS data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted. |
| **P2** | 5.2.2 Fallback to insecure cryptographic protocols and configurations is not permitted. | | |
| **P2-5.3 TLS configuration** | | | |
| **P2** | 5.3.1 All TLS communications between ACS, DS, and 3DSS for the purpose of 3DS transmissions use only approved cipher suites with at least the minimum key sizes, as defined in the *EMV® 3DS Protocol and Core Functions Specification*. | • Examine configuration standards and TLS configurations.<br>• Observe TLS communications. | Refer to Annex D, "Approved Transport Layer Security Versions," in the current version of the *EMV® 3DS Protocol and Core Functions Specification*, to identify those cipher suites that shall be supported and those that must not be offered or supported. The Implementation Notes in Annex D may also contain additional considerations for TLS implementations.<br>The use of 3DES and SHA-1 should be phased out, as they may be deprecated in future versions of the *EMV® 3DS Protocol and Core Functions Specification*. |
| **P2** | 5.3.2 3DS components (ACS, DS, and 3DSS) do not offer, support, or use any cipher suite identified as "not supported" in the *EMV® 3DS Protocol and Core Functions Specification*. | • Examine configuration standards and TLS configurations.<br>• Observe TLS communications. | |
| **P2** | 5.3.3 TLS configurations do not support rollback to unapproved algorithms, key sizes, or implementations. | • Examine configuration standards and TLS configurations.<br>• Observe TLS communications. | TLS configurations may not support rollback to unapproved algorithms, key sizes, or implementations. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 5.3.4 Controls are in place to monitor TLS configurations to identify configuration changes and to ensure secure TLS configuration is maintained. | • Observe implemented controls for monitoring and maintaining TLS configurations.<br>• Interview personnel. | A combination of tools and processes should be considered to ensure an appropriate level of monitoring is implemented. Examples of controls include real-time monitoring, change-detection software, and analysis of audit logs. Continuous monitoring is recommended to prevent, detect, and allow timely response to unauthorized modifications or use of non-permitted configurations. The implemented controls should provide continued assurance that TLS is properly configured and using only approved cipher suites. |
| **P2-5.4 Data storage** | | | |
| **P2** | 5.4.1 Storage of 3DS sensitive data is limited to only permitted data elements. | • Examine data flows and 3DS transaction processes.<br>• Observe data storage. | The *PCI 3DS Data Matrix* identifies storage restrictions for 3DS sensitive data elements. Where storage of a particular data element is not permitted, the 3DS entity should be able to confirm that the data element is not stored to any persistent media—including to any hard drive, portable media or other data storage device—for any period of time or for any reason. The presence of these data elements in volatile memory is permitted as needed for 3DS transaction purposes; however, controls should be implemented to prevent data in memory being inadvertently copied to persistent media. |
| **P2** | 5.4.2 Strong cryptography is used to protect any permitted storage of 3DS sensitive data. | • Examine documentation describing methods for protecting stored data.<br>• Observe implemented controls and configurations. | 3DS sensitive data—as identified in the *PCI 3DS Data Matrix*—should be protected wherever it is stored, using industry-recognized methods for strong cryptography. The cryptographic control may be applied either to the individual data elements or to the entire data packet or file that contains the data element. For example, where an element of 3DS sensitive data is contained in a transaction log with other data, encryption may be applied to the entire log or to only the sensitive data elements within the log.<br>Strong cryptographic controls include one-way hash functions that use an appropriate algorithm and a strong input variable, such as a “salt.” Hash functions are appropriate when there is no need to retrieve the original data, as one-way hashes are irreversible. Alternatively the data can be protected using cryptography based on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm) with strong cryptographic keys. Associated key-management processes and procedures are defined in Requirement P2-6. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.). |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-5.5 Monitoring 3DS transactions** | | | |
| **P2** | 5.5.1 3DS transactions are monitored to identify, log, and alert upon anomalous activity. | - Examine documented procedures and configuration standards.<br>- Examine log files.<br>- Observe implemented controls.<br>- Interview personnel. | Maintaining a baseline of normal 3DS traffic and transaction patterns will assist in identifying anomalous behaviors and developing use cases. All identified deviations should be ranked by risk level and responded to accordingly. In addition to real-time monitoring and analysis, frequent reviews of network traffic and correlation of audit logs may identify potentially suspicious activity.<br>Response processes should include specific investigative activities, escalation, and notification, in accordance with the entity's incident response plan. |
| **P2** | 5.5.2 Anomalous or suspicious transaction activity is investigated and addressed in a timely manner. | | |

## Requirement P2-6 Cryptography and Key Management

| | Overview | Requirements |
|---|---|---|
| **P2-6** | Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key-management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect. | 6.1 Key management<br>6.2 Secure Logical access to HSMs *(For ACS and DS only)*<br>6.3 Secure Physical access to HSMs *(For ACS and DS only)* |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-6.1 Key management** | | | |
| **P2** | 6.1.1 Policies and procedures for managing cryptographic processes and keys are maintained and implemented. | • Examine documented policies and procedures.<br>• Interview personnel. | Policies should cover all cryptographic keys and processes used to protect the confidentiality and integrity of 3DS data and messages during transmission and storage, as well as all respective key-encrypting keys. Cryptographic key-management processes should be monitored and maintained to ensure adherence to the defined policies. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 6.1.2 ***For ACS and DS only:*** All key management activity for specified cryptographic keys (as defined in the *PCI 3DS Data Matrix)* is performed using an HSM that is either:<br>• FIPS 140-2 Level 3 (overall) or higher certified, or<br>• PCI PTS HSM approved. | • Examine documented key-management procedures.<br>• Interview personnel. | The requirement to use an HSM applies to ACS and DS entities. The *PCI 3DS Data Matrix* identifies 3DS cryptographic key types required to be managed in an HSM. Key-management activities include key-encryption and decryption operations, as well as key lifecycle functions such as key generation and storage.<br>The HSM approval documentation verifies the HSM is either:<br>• Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3 (overall) or higher. Refer to http://csrc.nist.gov.<br>• Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device under the approval class "HSM."<br>While an HSM is required only for the keys specified in the *PCI 3DS Data Matrix*, use of an HSM for other 3DS keys is strongly recommended. All 3DS keys should be evaluated in accordance with the 3DS entity's risk-management policy to determine whether they should be managed in an HSM.<br>It is not required that 3DSS entities use an HSM to manage 3DS keys; however it is strongly recommended. 3DSS entities are subject to all other key management requirements in this standard. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 6.1.3 ***For ACS and DS only:*** The HSM is deployed securely, in accordance with its approved security policy, as follows:<br>• If FIPS-approved HSMs are used, the HSM uses the FIPS-approved cryptographic primitives, data-protection mechanisms, and key-management processes for account data decryption and related processes.<br>• If PCI PTS-approved HSMs are used, the HSM is configured to operate in accordance with the security policy that was included in the PTS HSM approval, for all operations (including algorithms, data protection, key management, etc.). | • Examine HSM approval documentation / security policy (as applicable).<br>• Observe HSM configurations. | An integral component of a PCI PTS or FIPS certification is the HSM security policy, which defines how to configure and operate the HSM in accordance with the certification.<br>The security policy enforced by the HSM should not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required to support specified functionality should be disabled before the HSM is commissioned. When HSMs are connected to online systems, controls should be in place to prevent the HSM being used to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration. |
| **P2** | 6.1.4 A documented description of the cryptographic architecture exists that includes:<br>• Description of the usage for all keys<br>• Details of all keys used by each HSM (if applicable) | • Examine documented description of the cryptographic architecture.<br>• Interview personnel.<br>• Examine HSM approval documentation. | Cryptographic keys must be stored and functions handled securely to prevent unauthorized or unnecessary access that could result in the exposure of keys and compromise cardholder data. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 6.1.5 Cryptographic keys are securely managed throughout the cryptographic lifecycle including:<br>• Generation<br>• Distribution/conveyance<br>• Storage<br>• Established crypto periods<br>• Replacement/rotation when the crypto period is reached<br>• Escrow/backup<br>• Key compromise and recovery<br>• Emergency procedures to destroy and replace keys<br>• Accountability and audit | • Examine documented key-management procedures.<br>• Observe key-management activities.<br>• Interview personnel. | A good key-management process, whether manual or automated, is based on industry standards and addresses all elements of the key lifecycle. Applicable standards include NIST Special Publication 800-57 (all parts), Special Publication 800-130, ISO 11568, and ISO/IEC 11770—including associated normative references cited within as applicable. For example, the generation and use of deterministic random numbers should conform to NIST Special Publication 800-90A, ISO/IEC 18031, or equivalent.<br>Keys should only be distributed in a secure manner, never in the clear, and only to designated custodians or recipients. Procedures for distribution apply both within the entity and across 3DS domains. Secret and private keys should be encrypted with a strong key-encrypting key that is stored separately, or be stored within a secure cryptographic device (such as a HSM), or be stored as at least two full-length key components or key shares, in accordance with an industry-accepted method. The existence of clear-text keys during data-encryption/decryption operations should be limited to the minimum time needed for its purpose—for example, where clear-text keys may temporarily exist in memory, they should be securely purged from memory upon completion of the encryption/decryption operation.<br>A crypto period should be identified for each key based on a risk assessment, and keys changed when this period is reached. Additionally, keys should be destroyed and replaced immediately upon suspicion of a compromise.<br>Secure key-management practices include minimizing access to keys to the fewest number of custodians necessary, enforcing split knowledge and dual control for activities involving clear-text keys or key components, and defining roles and responsibilities for key custodians and key managers. |
| **P2** | 6.1.6 Cryptographic key-management processes conform to recognized national or international key-management standards. | • Examine documented key-management procedures.<br>• Observe key-management activities.<br>• Interview personnel. | |
| | 6.1.7 Cryptographic keys are used only for their intended purpose, and keys used for 3DS functions are not used for non-3DS purposes. | • Examine documented key-management procedures.<br>• Interview personnel. | Cryptographic keys should only be used for the purpose they were intended—for example, a key-encryption key should never be used to encrypt 3DS sensitive data. Similarly, public and private keys should only be used for a single defined purpose—private keys should be used either for decryption or for creating digital signatures, and public keys used only for encryption or for verifying digital signatures.<br>Keys used to protect 3DS transactions or data should not be used for any business function other than their 3DS purpose. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 6.1.8 A trusted Certificate Authority is used to issue all digital certificates used for 3DS operations between 3DSS, ACS, and DS components. | • Examine documented evidence of Certificate Authority validation (e.g., security assessments, certifications).<br>• Observe implemented digital certificates. | Entities need to ensure that the Certificate Authority (CA) that they use has robust security controls to ensure the security of 3DS protocols and to verify a chain of trust. Refer to Section 6.1, "Links," in the current version of the *EMV® 3DS Protocol and Core Functions Specification* to identify connections between 3DSS, ACS, and DS components that require digital certificates. The CA could be approved by a payment brand or could undergo a security assessment, conducted by the entity or other third party, against an industry-standard framework such as ISO 27001. The assessment should confirm the CA has robust controls around security, processing integrity, confidentiality, online privacy, and availability. Entities can also leverage WebTrust, an assurance service jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). |
| **P2** | 6.1.9 Audit logs are maintained for all key-management activities and all activities involving clear-text key components. The audit log includes:<br>• Unique identification of the individual that performed each function<br>• Date and time<br>• Function being performed<br>• Purpose<br>• Success or failure of activity | • Examine documented key-management procedures.<br>• Examine audit logs.<br>• Interview personnel. | Recording the function or key-management activity being performed (for example, key loading), and the purpose of the affected key (for example, 3DS data encryption) provides the entity with a complete and concise record of key-management activities. Identifying whether the activity resulted in success or failure confirms the status upon conclusion of the activity. By recording these details for the auditable events, a potential compromise can be quickly identified with sufficient detail to know who, what, where, when, and how. |
| **P2** | 6.1.10 Incident response procedures include activities for reporting and responding to suspicious or confirmed key-related issues. | • Examine documented incident response procedures.<br>• Interview personnel. | The appropriate personnel should be notified immediately of any breach impacting the keys. Documented procedures should explain how this issue would be escalated for further investigation and resolution, including initiation of the entity's incident response procedures. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-6.2** | **Secure logical access to HSMs *(For ACS and DS only)*** | | |
| **P2** | 6.2.1 Personnel with logical access to HSMs must be either at the HSM console or using an HSM non-console access solution that has been evaluated by an independent laboratory to comply with the following sections of the current version of ISO 13491:<br>• Annex A – Section A.2.2: Logical security characteristics.<br>• Annex D – Section D.2: Logical security characteristics. *(Note: The use of single DEA message authentication codes is not permitted.)*<br>• Annex E – Section E.2.1: Physical security characteristics, and Section E.2.2: Logical security characteristics. *(Note: Only random number generators meeting the requirements of SP 800-90A are allowed.)*<br>• Annex F – Section F.2.1: Physical security characteristics, and Section F.2.2: Logical security characteristics.<br>• If digital signature functionality is provided: Annex G – Section G.2.1: General considerations, and Section G.2.2: Device management for digital signature verification. | • Examine system configurations<br>If non-console access is used:<br>• Examine documented evidence (e.g., lab certification letters, solution technical documentation, or vendor attestation) that the solution has been validated to applicable ISO requirements<br>• Observe implemented solution | HSMs have high security needs, and additional controls are necessary to restrict and protect logical access to these systems. If personnel have network (non-console) access to HSMs, the security of the HSM non-console access solution is critical to the overall security of the HSM itself. Examples of personnel access include for purposes of maintenance, configuration, updating, administration, and general management of the HSM. Use of non-console access solution is not required for application or system accounts performing automated functions.<br>An HSM non-console access solution is typically comprised of both hardware components (for example, network appliances and smart cards) and software components (for example, client-side applications) that define and manage how non-console access is handled. For additional assurance that only authorized persons can access the HSM, the use of multi-factor authentication for all personnel access should also be considered.<br>An independent laboratory is one that is organizationally independent of the non-console management solution vendor and is not otherwise subject to any commercial, financial, or other commitment that might influence its evaluation of the vendor's product. |
| **P2** | 6.2.2 All non-console access to HSMs originates from a 3DE network(s). | • Examine network and system configuration settings | To ensure that non-console access to HSMs originates from a secure location, such access may only be provided to systems located within a 3DS environment (3DE) that is protected in accordance with the requirements in this standard. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 6.2.3 Devices used to provide personnel with non-console access to HSMs are secured as follows:<br>• Located in a designated secure area or room that is monitored at all times.<br>• Locked in room/rack/cabinet/ drawer/safe when not in use.<br>• Physical access is restricted to authorized personnel and managed under dual control.<br>• Authentication mechanisms (e.g., smart cards, dongles, etc.) for devices with non-console access are physically secured when not in use.<br>• Operation of the device requires dual control and multi-factor authentication.<br>• Devices have only applications and software installed that are necessary.<br>• Devices are verified as having up-to-date security configurations.<br>• Devices cannot be connected to other networks while connected to the HSM.<br>• Devices are cryptographically authenticated prior to the connection being granted access to HSM functions. | • Observe locations of devices used for non-console access to HSMs.<br>• Observe device configurations.<br>• Observe HSM authentication mechanisms. | The term “devices” refers to the endpoint device (for example, a PC, laptop, terminal, or secure cryptographic device) that an individual is using to access the HSM via a non-console connection. The implemented physical and logical security controls should provide assurance that devices are being used only as intended, and only by authorized personnel. The specific security configurations for each device will depend on its particular technology and function. In order to prevent malicious individuals from “piggy-backing” on an authorized connection, devices should only be connected to the network used to access the HSM. For example, connectivity on multi-homed devices should be disabled for all but the interface accessing the HSM, and any VPN/SSH tunnels to other networks should be closed before opening a tunnel to the HSM.<br>Methods to verify that only authorized devices are permitted to connect to the HSM can include digital signatures and other cryptographic techniques.<br>All non-console access to HSMs should occur only over a secure communication channel, such as a VPN that meets Requirement 4.4. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 6.2.4 The loading and exporting of clear-text cryptographic keys, key components, and/or key shares to/from the HSM is not permitted over a non-console connection. | • Examine device configurations. | Non-console access to HSMs should only be used for the purpose of HSM maintenance/administration. Because the loading and export of clear-text keys, key components, and key shares requires a higher assurance of physical security, all such activities are required to be performed at the HSM. |
| **P2** | 6.2.5 Activities performed via non-console access adhere to all other HSM and key-management requirements. | • Examine policies and procedures.<br>• Interview personnel.<br>• Examine HSM configurations and observe connection processes. | If personnel are not physically at the HSM console, additional controls may be necessary to ensure that the 3DS entity's policies and procedures around key management and HSM usage are adhered to. For example, if the ability to access an HSM function or key-management activity requires dual control, and the activity or function can be accessed by personnel physically at the HSM console or over a non-console (network) connection, the requirements for dual control need to be enforced over both methods of access. |
| **P2-6.3 Secure physical access to HSMs *(For ACS and DS only)*** | | | |
| **P2** | 6.3.1 HSMs are stored in a dedicated area(s). | • Examine 3DS device inventory.<br>• Observe physical locations of HSMs. | Physical access to HSMs requires passing an additional physical control—e.g., via locked cabinets or cages, or a separate secure room. HSMs could be in multiple racks within the same dedicated physical space, or in one or more dedicated rooms, and so on.<br>Where HSMs are in a data center managed by the 3DS entity, the HSMs should be in a space dedicated to HSMs and HSM-management devices. Where a 3DS entity's HSMs are in a shared data center, such as a co-location facility, the 3DS entity's HSMs should be in a space that is dedicated to the entity's systems and is physically separate from all other customers of the co-location facility.<br>Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another. |
| **P2** | 6.3.2 Physical access to the HSMs is restricted to authorized personnel and managed under dual control. | • Examine documented procedures.<br>• Observe access controls. | |

## Requirement P2-7 Physically secure 3DS systems

| | Overview | Requirements |
|---|---|---|
| **P2-7** | As ACS and DS systems are critical components of the 3DS infrastructure, they require a secure facility with elevated physical security controls to restrict, manage, and monitor all physical access. | 7.1 Data center security<br>7.2 CCTV |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2-7.1 Data center security** | | | |
| **P2** | 7.1.1 ACS and DS systems are hosted in data center environments. | • Observe ACS and DS locations. | Data centers should apply controls across a number of levels—for example, door-entry controls may be applied at room level within the data center, at an outer level that must be passed through to access the data center, or a combination of both. Some controls may also be applied at rack level—for example, where the 3DS component is in a secured rack. However the controls are implemented, they must ensure that access to the 3DS component is controlled and monitored as defined in these requirements. |
| **P2** | 7.1.2 Data centers supporting ACS and DS are equipped with a positively controlled single-entry portal (e.g., mantrap), that:<br>• Requires positive authentication prior to granting entry; and<br>• Grants entry to a single person for each positive authentication. | • Observe data center entry points. | A positively controlled mantrap is typically a small room with an entry door on one wall and an exit door on the opposite wall. One door of a mantrap cannot be unlocked and opened until the opposite door has been closed and locked.<br>Access controls can be a combination of automated (for example, electronic access cards and physical barriers) and manual (for example, a human security guard performing visual verification and confirmation of identity). These controls ensure that the second door is not opened until authentication is complete, and that only one individual is provided access per authentication. |
| **P2** | 7.1.3 Doors to areas within the data center that contain 3DS systems are fitted with an electronic access-control system (e.g., card reader, biometric scanner) that controls and records all entry and exit activities. | • Observe all entrances to the 3DE.<br>• Examine audit logs and/or other access records. | Electronic access-control systems, such as a keypad with individually assigned PIN codes or individually assigned access cards, provide assurance that the individual gaining access is who they claim to be. To provide additional protection against the unauthorized use of an individual's credential, multi-factor authentication should be considered. |

| Requirements | | Validation Methods | Implementation Guidance |
|---|---|---|---|
| **P2** | 7.1.4 Multi-factor authentication is required for entry to telecommunications rooms that are not located within a secure data center. | - Examine access controls.<br>- Observe access events. | A telecommunications room is a room or space where communications are consolidated and distributed. Telecommunications rooms typically house communications equipment (such as switches and routers), cable termination points, and cross-connects serving a specific area and/or floor. Examples of multi-factor authentication for physical access include use of an access card with PIN/passcode and use of an access card with a biometric reader. Visual verification of government-issued photo ID by an authorized guard at the entry point may also be acceptable as one of the two factors.<br>Multi-factor authentication is not required for physical access to telecommunications rooms housed within a data center environment that meets the requirements in this standard. |
| **P2** | 7.1.5 Entry controls prevent piggy-backing by granting access to a single person at a time, with each person being identified and authenticated before access is granted. | - Observe personnel entering the data center. | Each individual is identified and authenticated before being granted access to the 3DS data centers. These controls provide assurance that the identity of every individual in the data center is known at any given time. |
| **P2** | 7.1.6 A physical intrusion-detection system that is connected to the alarm system is in place. | - Interview personnel.<br>- Observe intrusion-detection controls. | To be effective, an intrusion-detection system should be activated whenever the 3DS environment is intended to be unoccupied. The intrusion-detection system may be activated automatically or via manual process. |
| **P2** | 7.1.7 Physical connection points leading into the 3DE are controlled at all times. | - Observe physical connection points. | Securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources. |
| **P2-7.2 CCTV** | | | |
| **P2** | 7.2.1 CCTV cameras are located at all entrances and emergency exit points and capture identifiable images, at all times of the day and night. | - Observe all entrances and emergency exit points.<br>- Examine CCTV footage. | The cameras need to be able to identify individuals physically entering and exiting the area, even during dark periods, as this provides valuable information in the event of an investigation. |
| **P2** | 7.2.2 CCTV recordings are time stamped. | - Examine CCTV records. | Clocks need to be properly synchronized to ensure the captured images can be correlated to create an accurate record of the sequence of events. Synchronization may use automated or manual mechanisms. |

# Appendix A-1: Compensating Controls

Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to meet a PCI 3DS requirement.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI 3DS requirement.
2. Provide a similar level of defense as the original PCI 3DS requirement, such that the compensating control sufficiently offsets the risk that the original PCI 3DS requirement was designed to defend against.
3. Be “above and beyond” other PCI 3DS requirements. (Simply being in compliance with other PCI 3DS requirements is not a compensating control.)

   When evaluating “above and beyond” for compensating controls, consider the following:

   (a) Existing PCI 3DS requirements CANNOT be considered as compensating controls if they are already required for the item under review.

   (b) Existing PCI 3DS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review.

   (c) Existing PCI 3DS requirements may be combined with new controls to become a compensating control.

   ***Note:*** *The items at a) through c) above are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI 3DS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a particular compensating control will not be effective in all environments.*

4. Be commensurate with the additional risk imposed by not adhering to the PCI 3DS requirement.

The assessor is required to thoroughly evaluate all compensating controls during the PCI 3DS assessment and validate that each compensating control adequately addresses the risk the original PCI 3DS requirement was designed to address. Processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

# Appendix A-2: Compensating Controls Worksheet

Use this worksheet to document any compensating controls used to meet a PCI 3DS requirement. Compensating controls should also be documented with the corresponding PCI 3DS requirement in the 3DS Report on Compliance.

| | |
|---|---|
| **3DS Requirement Number and Description:** | |

| Information Required | Description | Explanation |
|---|---|---|
| **1. Constraints** | List constraints precluding compliance with the original requirement. | |
| **2. Objective** | Define the objective of the original requirement; identify the objective met by the compensating control. | |
| **3. Identified Risk** | Identify any additional risk posed by the lack of the original control. | |
| **4. Definition of Compensating Controls** | Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any. | |
| **5. Validation of Compensating Controls** | Define how the compensating controls were validated and tested. | |
| **6. Maintenance** | Define processes and controls in place to monitor and maintain the effectiveness of the compensating controls. | |

# Appendix B: Alignment between PCI 3DS and PCI DSS Requirements

The PCI 3DS Part 1 Baseline Security Requirements cover many of the security objectives required by PCI DSS. Where PCI DSS has been applied to the 3DS environment as described below, the implementation of additional controls may not be needed to meet the PCI 3DS Part 1 Requirements:

1. The 3DE is contained within a CDE, and all 3DS system components—including supporting infrastructure and systems—are included in scope for the applicable PCI DSS requirements. See Table 2 "Mapping of PCI 3DS Part 1: Baseline Security Requirements to PCI DSS Requirements" later in this section for details of applicable PCI DSS requirements; ***and***
2. The applicable PCI DSS requirements are confirmed to be "In Place" through a PCI DSS assessment performed no more than 12 months prior to the 3DS assessment.

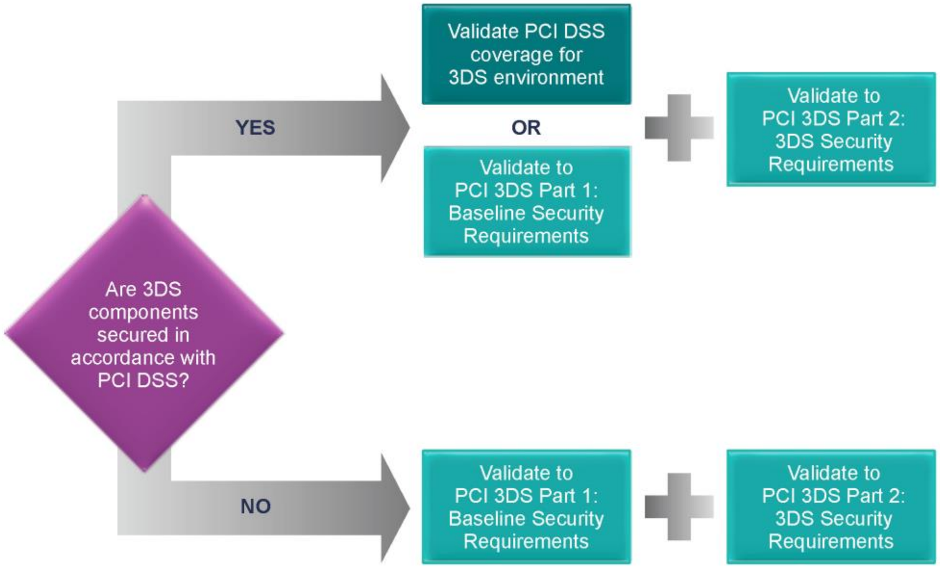
A 3DE that is not within the security boundary of a PCI DSS-compliant (as defined by applicable payment brand compliance programs) CDE, or does not store, process, or transmit any cardholder data (CHD) or sensitive authentication data (SAD), may be subject to PCI 3DS Part 1 Requirements, based on payment brand compliance programs.

The applicability of PCI 3DS Part 2: 3DS Security Requirements is not impacted by a PCI DSS implementation. The PCI 3DS Part 2 Requirements apply whether or not PCI DSS is also implemented.

***Note:*** *The individual payment brand compliance programs define whether an entity is required to validate to PCI 3DS, PCI DSS, or both.*

The following diagram provides an illustration of how PCI DSS may impact applicability of 3DS Requirements.

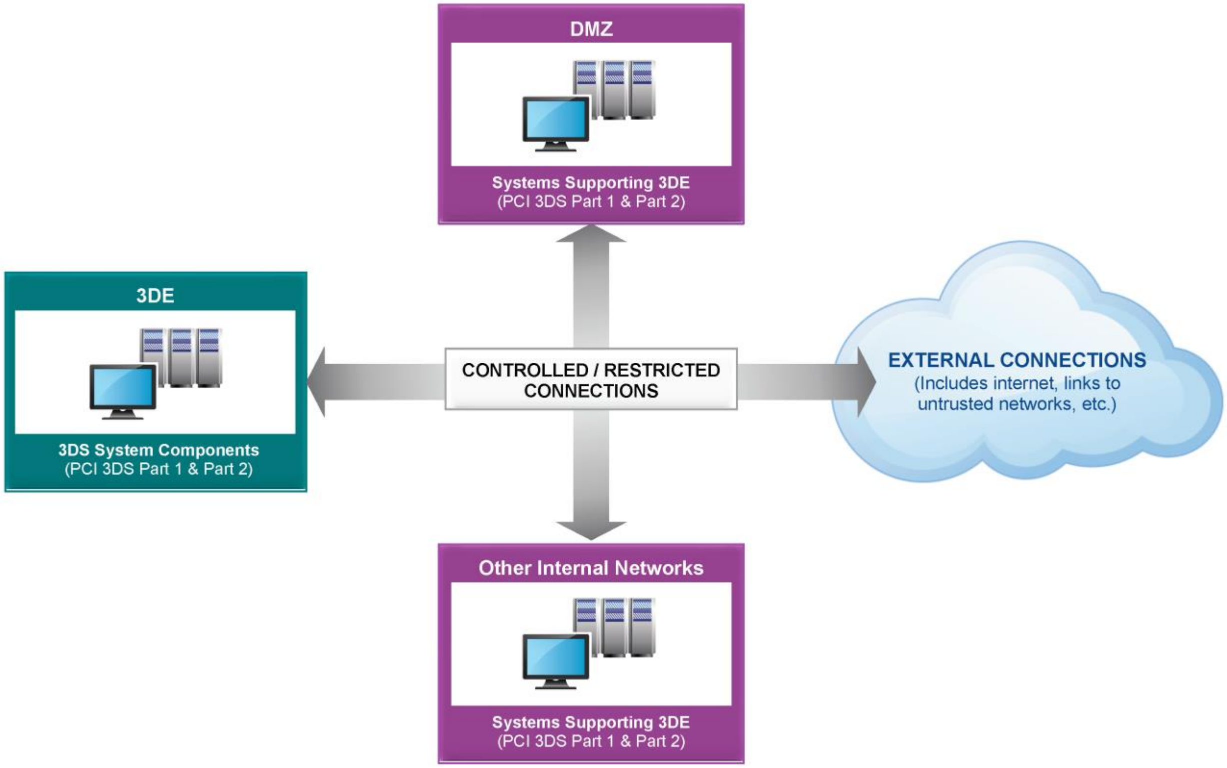
**Diagram 1: Relationship between PCI 3DS Requirements and PCI DSS**


Are 3DS components secured in accordance with PCI DSS?
YES
Validate PCI DSS coverage for 3DS environment
OR
Validate to PCI 3DS Part 1: Baseline Security Requirements
Validate to PCI 3DS Part 2: 3DS Security Requirements
NO
Validate to PCI 3DS Part 1: Baseline Security Requirements
Validate to PCI 3DS Part 2: 3DS Security Requirements

A 3DS entity that has applied PCI DSS in accordance with Table 2 “Mapping of PCI 3DS Part 1: Baseline Security Requirements to PCI DSS Requirements” may either confirm that its PCI DSS validation covers the systems and environments in scope for PCI 3DS, or complete validation to the 3DS Part 1 Requirements. A 3DS entity that does not store, process, or transmit any account data (CHD and/or SAD), and therefore has not applied PCI DSS, should complete both 3DS Part 1 and 3DS Part 2 Requirements.

The following diagrams conceptually illustrate how a 3DE could be separate to or within a CDE, and the corresponding applicability of requirements.

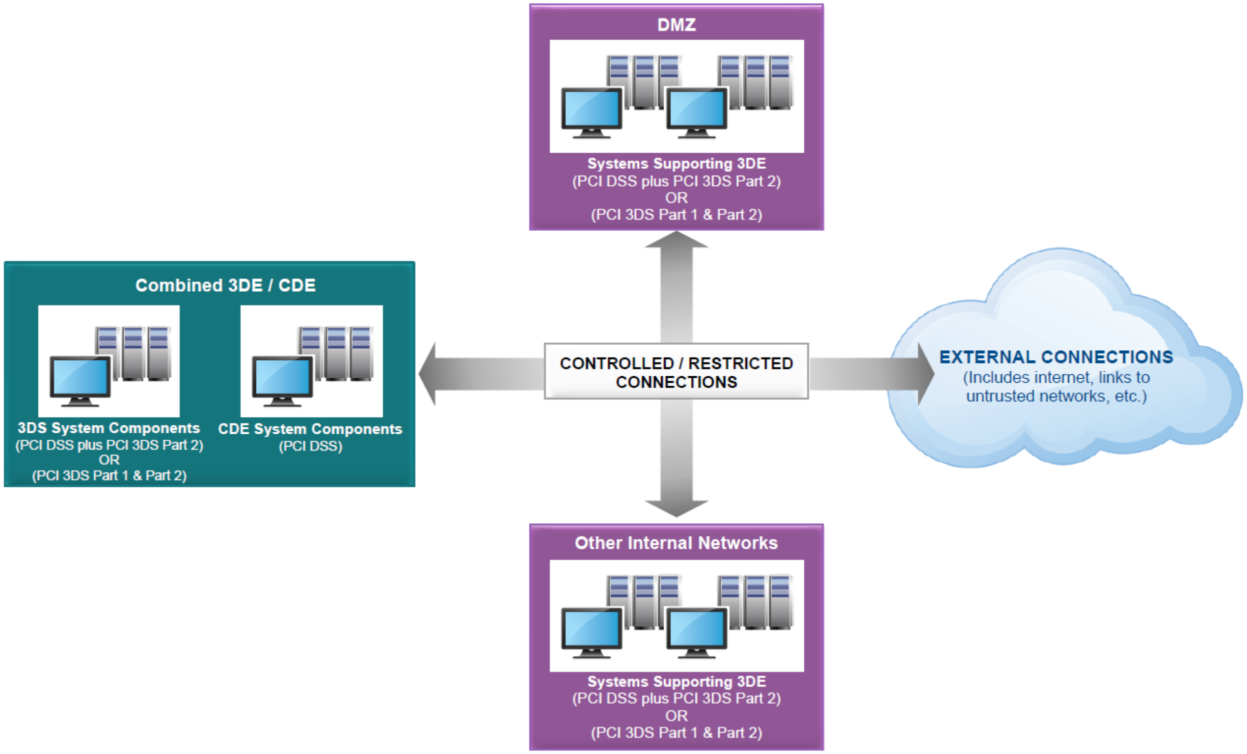
**Diagram 2: Scenario with Standalone 3DE**


DMZ
Systems Supporting 3DE
(PCI 3DS Part 1 & Part 2)
3DE
3DS System Components
(PCI 3DS Part 1 & Part 2)
CONTROLLED / RESTRICTED CONNECTIONS
EXTERNAL CONNECTIONS
(Includes internet, links to untrusted networks, etc.)
Other Internal Networks
Systems Supporting 3DE
(PCI 3DS Part 1 & Part 2)

In Diagram 2 above, the 3DS entity does not store, process, or transmit any account data (CHD or SAD) as part of the 3DS transaction process. This entity’s 3DE is therefore not part of any CDE and is not protected by PCI DSS. In this scenario, the 3DS systems in the 3DE are subject to 3DS Part 1 and Part 2 Requirements.

Systems that are outside of the 3DE and that connect to or otherwise support 3DS system components in the 3DE would also be subject to 3DS Part 1 and Part 2 Requirements.

**Diagram 3: Scenario with Combined 3DE/CDE**


DMZ
Systems Supporting 3DE
(PCI DSS plus PCI 3DS Part 2)
OR
(PCI 3DS Part 1 & Part 2)
Combined 3DE / CDE
3DS System Components
(PCI DSS plus PCI 3DS Part 2)
OR
(PCI 3DS Part 1 & Part 2)
CDE System Components
(PCI DSS)
CONTROLLED / RESTRICTED CONNECTIONS
EXTERNAL CONNECTIONS
(Includes internet, links to untrusted networks, etc.)
Other Internal Networks
Systems Supporting 3DE
(PCI DSS plus PCI 3DS Part 2)
OR
(PCI 3DS Part 1 & Part 2)

In Diagram 3 above, the entity's 3DE is contained within or is the same as its CDE, and all 3DE system components (including ACS, DS, and/or 3DSS) are already protected by PCI DSS. In this scenario, the 3DS systems in the 3DE may be validated to either PCI DSS or 3DS Part 1 Requirements. The 3DS Part 2 Requirements also apply to these system components.

System components that are outside the combined 3DE/CDE and that connect to or otherwise support 3DS system components in the 3DE also need to be protected. If all connected-to and supporting systems are protected by the appropriate PCI DSS controls, these system components could also be validated to either PCI DSS or 3DS Part 1 Requirements. In all cases, these system components would be subject to 3DS Part 2 Requirements.

## Leveraging PCI DSS for PCI 3DS Part 1: Baseline Security Requirements

A mapping of PCI 3DS Part 1 Requirements to the applicable PCI DSS requirements is provided in Table 2 on the following page. The intent of this mapping is to assist 3DS entities that have implemented PCI DSS to protect their 3DS environment in confirming that the PCI DSS controls they have implemented are appropriate to meet the objectives of the 3DS Part 1 Requirements.

- **All identified PCI DSS requirements in place** – 3DS entities that *have all* the identified PCI DSS requirements in place for their 3DS environment could either:

  (a) Confirm PCI DSS coverage for the scope of their 3DS environment, ***or***

  (b) Validate to 3DS Part 1 Requirements

- **Some but not all identified PCI DSS requirements in place** – 3DS entities that *have some but not all* the identified PCI DSS requirements in place for their 3DS environment could either:

  (a) Implement and validate the applicable PCI DSS requirements in order to confirm PCI DSS coverage, ***or***

  (b) Validate to 3DS Part 1 Requirements.

- **One or more PCI DSS requirements identified as N/A** – If any PCI DSS requirements were identified as being “Not Applicable” during the PCI DSS assessment, the 3DS entity could either:

  (a) Provide verification that all “N/A” PCI DSS requirement(s) are also not applicable to the 3DS environment, ***or***

  (b) Implement and validate the applicable PCI DSS requirements in order to confirm PCI DSS coverage, ***or***

  (c) Complete the 3DS Part 1 Requirements.

- **PCI DSS has not been implemented** – Entities that have not implemented PCI DSS should complete the 3DS Part 1 Requirements in their entirety.

**Table 2: Mapping of PCI 3DS Part 1: Baseline Security Requirements to PCI DSS Requirements**

| 3DS Part 1: Baseline Security Requirements | PCI DSS Requirements |
|---|---|
| **1. Maintain security policies for all personnel** | ▪ Requirement 12: Maintain a policy that addresses information security for all personnel |
| **2. Secure network connectivity** | ▪ Requirement 1: Install and maintain a firewall configuration to protect cardholder data<br>▪ Requirement 10: Track and monitor all access to network resources and cardholder data<br>▪ Requirement 11: Regularly test security systems and processes |
| **3. Develop and maintain secure systems** | ▪ Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters<br>▪ Requirement 6: Develop and maintain secure systems and applications |
| **4. Vulnerability management** | ▪ Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs<br>▪ Requirement 6: Develop and maintain secure systems and applications<br>▪ Requirement 11: Regularly test security systems and processes |
| **5. Manage access** | ▪ Requirement 7: Restrict access to cardholder data by business need to know<br>▪ Requirement 8: Identify and authenticate access to system components |
| **6. Physical security** | ▪ Requirement 9: Restrict physical access to cardholder data |
| **7. Incident response preparedness** | ▪ Requirement 10: Track and monitor all access to network resources and cardholder data<br>▪ Requirement 12: Maintain a policy that addresses information security for all personnel |

***Note:*** *The applicability of 3DS Part 2: 3DS Security Requirements is not impacted by a PCI DSS implementation.*