Payment Card Industry (PCI)

# Payment Application Data Security Standard

## Summary of Changes from PA-DSS Version 2.0 to 3.0

**November 2013**

# Introduction

This document provides a summary of changes from PA-DSS v2.0 to PA-DSS v3.0. Table 1 provides an overview of the types of changes included in PA-DSS v3.0. Table 2 on the following pages provides a summary of material changes to be found in PA-DSS v3.0.

**Table 1: Change Types**

| Change Type | Definition |
|---|---|
| Clarification | Clarifies intent of requirement. Ensures that concise wording in the standard portrays the desired intent of requirements. |
| Additional guidance | Explanation, definition and/or instruction to increase understanding or provide further information or guidance on a particular topic. |
| Evolving Requirement | Changes to ensure that the standards are up to date with emerging threats and changes in the market. |

**Table 2: Summary of Changes**

| Section | | Change | Type |
|---|---|---|---|
| **PA-DSS v2.0** | **PA-DSS v3.0** | | |
| Introduction | Introduction | **Purpose of This Document**<br>Clarified purpose and use of the document and included reference to PA-DSS ROV Reporting Template. | Clarification |
| | | **Relationship between PCI DSS and PA-DSS**<br>Added clarification that PA-DSS applications are in scope for an organization's PCI DSS assessment. | Clarification |
| PCI DSS Applicability Information | PCI DSS Applicability Information | Relocated section and updated to align with changes to PCI DSS. Removed some PCI DSS language that is not applicable to PA-DSS. | Clarification |
| Scope of PA-DSS | Scope of PA-DSS | Removed information about which payment applications are eligible for PA-DSS. Information on PA-DSS eligibility can be found in the *PA-DSS Program Guide*. | Clarification |
| Roles and Responsibilities | | Information regarding relevant stakeholders and their PA-DSS roles and responsibilities has been removed as it is included in the *PA-DSS Program Guide*. | Clarification |
| PA-DSS Implementation Guide | PA-DSS Implementation Guide | Provided more guidance on the *PA-DSS Implementation Guide* and clarified the PA-QSA's role. | Additional Guidance |
| Instructions and Content for Report on Validation | Instructions and Content for Report on Validation | Content relocated to separate *ROV Reporting Template*. | Clarification |
| PA-DSS Completion Steps | PA-DSS Completion Steps | Updated section to focus on assessment process rather than documentation (documentation details moved to *ROV Reporting Template)*. | Clarification |
| PA-DSS Program Guide | PA-DSS Program Guide | Removed reference to PABP transition, since there is no longer a transition process. | Clarification |
| PA-DSS Requirements and Security Assessment Procedures | PA-DSS Requirements and Security Assessment Procedures | Added language to define the column headings in this section, and removed references to "In Place," "Not In Place," and "Target Date/Comments" columns. | Clarification |

| General changes implemented throughout the PA-DSS requirements | Type |
|---|---|
| New "Guidance" column to describe the intent or security objective of each requirement. The guidance in this column is intended to assist understanding of the requirements and does not replace or extend the PA-DSS Requirements and Testing Procedures. | Additional Guidance |
| Updated requirements and/or testing procedures to reflect PCI DSS changes, where a PA-DSS requirement aligns with a PCI DSS requirement. | As defined in PCI DSS |
| Updated language in requirements and/or corresponding testing procedures for alignment and consistency. | Clarification |
| Separated complex requirements / testing procedures for clarity and removed redundant / overlapping testing procedures. | Clarification |
| Enhanced testing procedures to clarify level of validation expected for each requirement, including:<br>▪ Required PA-DSS Implementation Guide information.<br>▪ Installing the application per the *PA-DSS Implementation Guide* to verify accuracy of *Implementation Guide* instructions. | Clarification |
| Other general editing changes include:<br>▪ Removed the following columns: "In Place," "Not in Place," and "Target Date/Comments."<br>▪ Renumbered requirements and testing procedures to accommodate changes.<br>▪ Reformatted requirements and testing procedures for readability—e.g., content from paragraph reformatted to bullet points, etc.<br>▪ Made minor wording changes throughout for readability.<br>▪ Corrected typographical errors. | Clarification |

| Requirement | | Change | Type |
|---|---|---|---|
| **PA-DSS v2.0** | **PA-DSS v3.0** | | |
| **Requirement 1** | | | |
| Requirement 1 – General | | Title updated for consistency, to replace "magnetic stripe" with "track data." | Clarification |
| 1.1.c | 1.1.1 – 1.1.3 | Removed Testing Procedure 1.1.c and added instruction to related testing procedures for Requirements 1.1.1 through 1.1.3. | Clarification |
| **Requirement 2** | | | |
| 2.x | 2.x | Added *PA-DSS Implementation Guide* components to the testing procedures throughout this section. | Evolving Requirement |

| Requirement | | Change | Type |
|---|---|---|---|
| **PA-DSS v2.0** | **PA-DSS v3.0** | | |
| 2.1 | 2.1 | Changed language to refer to secure deletion of data rather than purging. | Clarification |
| 2.2 | 2.2 | Enhanced testing procedures to require validation of PAN-masking features. | Clarification |
| 2.4 | | Removed requirement regarding the use of full disk encryption solutions.<br>Subsequent requirements renumbered accordingly. | Evolving Requirement |
| 2.6.x | 2.5.x | Updated testing procedures to clarify key-management techniques must be properly tested. | Clarification |
| 2.7 | 2.6 | Updated to clarify that application vendor should provide a mechanism for removing cryptographic key material, if the current or previous versions used cryptographic key materials or cryptograms. | Clarification |
| **Requirement 3** | | | |
| 3.1 | 3.1 | Moved note from former Testing Procedure 3.1.d to Requirement 3.1. | Clarification |
| 3.1.b – 3.1.c | 3.1.1 – 3.1.2 | New requirements created from former Testing Procedures 3.1.b – 3.1.c to ensure that changing of default passwords is enforced by the application and appropriately validated. | Clarification |
| 3.1.4 | 3.1.7 | Moved requirement to 3.1.7 for better organization of requirements. | Clarification |
| 3.1.6 – 3.1.7 | 3.1.6 | Combined password complexity requirements to align with PCI DSS v3.0 and provide flexibility for other password-composition alternatives that meet the minimum strength requirement. | Clarification |
| 3.3 | 3.3.1 – 3.3.2 | Split requirement 3.3 into two requirements to focus separately on *transmitted* passwords (3.3.1) and *stored* passwords (3.3.2).<br>Updated 3.3.2 to require use of a strong one-way cryptographic algorithm with a unique input variable to render passwords unreadable. | Evolving Requirement |
| | 3.4 | New requirement for applications to limit access to required functions/resources and enforce least privilege for built-in application accounts. | Evolving Requirement |
| **Requirement 4** | | | |
| 4.2.5 | 4.2.5 | Updated requirement to clarify types of identification and authentication mechanisms that must be logged, including creation of new accounts. | Clarification |

| Requirement | | Change | Type |
|---|---|---|---|
| **PA-DSS v2.0** | **PA-DSS v3.0** | | |
| **Requirement 5** | | | |
| 5.1 | 5.1 | Enhanced requirement to include security reviews in development processes. | Evolving Requirement |
| | 5.1.5 | New requirement for payment application developers to verify integrity of source code during the development process. | Evolving Requirement |
| | 5.1.6 | New requirement for payment applications to be developed according to industry best practices for secure coding techniques, including:<br>▪ Developing with least privilege for the environment.<br>▪ Developing with fail-safe defaults—i.e., all execution is by default denied unless specified within initial design.<br>▪ Developing for all access-point considerations, including input variances such as multi-channel input to the application.<br>▪ Documentation of how PAN and/or SAD are handled in memory. | Evolving Requirement |
| | 5.1.7 | New requirement created from former Testing Procedures 5.2.a and 5.2.b for payment application developers to be trained in secure development practices. | Clarification |
| 5.2 | 5.2 | Updated requirement to focus on preventing common coding vulnerabilities. | Clarification |
| | 5.2.10 | New requirement to address “Broken authentication and session management.” | Evolving Requirement |
| 5.4 | 8.2 | Moved requirement to 8.2 to align with other requirements that facilitate a secure PCI DSS environment, and keep requirement 5.x focused on software development practices. | Clarification |
| | 5.4 | New requirements for the payment application vendor to define and implement a versioning methodology in accordance with *PA-DSS Program Guide*. | Evolving Requirement |
| | 5.5 | New requirement for payment application vendors to incorporate risk assessment techniques into their software development process. | Evolving Requirement |
| | 5.6 | New requirement for payment application vendors to implement a formal authorization process prior to final release. | Evolving Requirement |

| Requirement | | Change | Type |
|---|---|---|---|
| **PA-DSS v2.0** | **PA-DSS v3.0** | | |
| **Requirement 6** | | | |
| 6.1 – 6.2 | 6.1 – 6.3 | Reorganized requirements to clarify controls that apply to all applications and controls that apply only where wireless is provided or intended for use with the payment application.<br>New Requirement 6.3 created from former Testing Procedure 6.2.b. | Clarification |
| **Requirement 7** | | | |
| Requirement 7 – General | | Title updated to reflect intent of requirement (to address vulnerabilities *and maintain application updates).* | Clarification |
| 7.1 | 7.1.1 – 7.1.3 | Split into separate requirements and required use of "reputable" sources for security vulnerability information. | Clarification |
| 7.2 | 7.2.1 – 7.2.2 | Split into separate requirements. | Clarification |
| | 7.3 | New requirement for the application vendor to provide release notes for all application updates. | Evolving Requirement |
| **Requirement 8** | | | |
| 8.1 | 8.1 | Expanded example to clarify intent of requirement. | Clarification |
| 5.4 | 8.2 | Moved requirement from 5.4 to align with other requirements that facilitate a secure PCI DSS environment. | Clarification |
| 10.1 | 8.3 | Moved requirement from 10.1 to align with other requirements that facilitate a secure PCI DSS environment. | Clarification |
| **Requirement 9** | | | |
| 9.1 | 9.1 | Added language to clarify the intent of requirement that web servers and cardholder data storage components are not required to be in the same network zone, with databases now an example of a cardholder data storage component and DMZ an example of a network zone. | Clarification |
| **Requirement 10** | | | |
| 10.1 | 8.3 | Moved requirement to 8.3 to align with other requirements that facilitate a secure PCI DSS environment.<br>Renumbered subsequent requirements. | Clarification |

| Requirement | | Change | Type |
|---|---|---|---|
| **PA-DSS v2.0** | **PA-DSS v3.0** | | |
| 10.2 | 10.1 | Clarified requirement applies to remote access originating from outside the customer's network. | Clarification |
| | 10.2.2 | New requirement for vendors who provide support/maintenance services to customers to maintain unique authentication credentials for each customer. | Evolving Requirement |
| 10.3.2 | 10.2.3 | Updated to clarify that requirement applies to all types of remote access. | Clarification |
| **Requirement 11** | | | |
| 11.1 | 11.1 | Minor updates to provide additional clarity and align with PCI DSS. | Clarification |
| **Requirement 12** | | | |
| 12.1 | 12.1<br>12.2 | Reorganized requirements to clarify controls that apply to all applications and controls that apply only where the payment application facilitates non-console administrative access. | Clarification |
| **Requirement 13** | | | |
| Requirement 13 – General | | Title changed to focus on requirements for the *PA-DSS Implementation Guide*. Requirements for instructional documentation and training programs moved to new Requirement 14. | Clarification |
| | 13.1.1 | New requirement to validate that the *PA-DSS Implementation Guide* is specific to the application and version(s) being assessed. | Clarification |
| 13.1.3 | 13.1.3 | Clarified intent that the *PA-DSS Implementation Guide* should be reviewed and updated whenever the application or PA-DSS requirements change. | Clarification |
| **Requirement 14** | | | |
| Requirement 14 – General | | See "General – 13 above." New requirement to focus on instructional documentation and training programs, including internal training for vendor personnel with PA-DSS responsibilities. | Clarification |
| | 14.1 | New requirement for providing information security and PA-DSS training for vendor personnel with PA-DSS responsibility at least annually. | Evolving Requirement |
| | 14.2 | New requirement for assignment of PA-DSS responsibilities to vendor personnel. | Evolving Requirement |

| Requirement | | Change | Type |
|---|---|---|---|
| **PA-DSS v2.0** | **PA-DSS v3.0** | | |
| 13.2 | 14.3 | Enhanced requirements formerly included in 13 for integrator/reseller training programs. Clarified intent that the training materials should be reviewed and updated whenever the application or PA-DSS requirements change. | Clarification |
| **Appendix B** | | | |
| Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment | Testing Laboratory Configuration for PA-DSS Assessments | Refocused Appendix to provide information about expectations and capabilities of the laboratory used to conduct PA-DSS assessments.<br>Details and template for documenting the testing laboratory configuration moved to separate *PA-DSS ROV Reporting Template*. | Clarification |