Payment Card Industry (PCI)

Payment Application Data Security Standard

Summary of Changes from PA-DSS Version 3.0 to 3.1

May 2015

Introduction

This document provides a summary of changes from PA-DSS v3.0 to PA-DSS v3.1. Table 1 provides an overview of the types of changes. Table 2 summarizes the material changes found in PA-DSS v3.1.

Table 1: Change Types

[1]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[1]
PA-DSS v3.0	PA-DSS v3.1		
All	All	Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	Clarification
All	All	Changed references from “merchant” to “customer” when referring to entities that use payment applications.	Clarification
PCI DSS Applicability Information	PCI DSS Applicability Information	Changed reference from “financial institutions” to “acquirers, issuers”. Clarified that PCI DSS applies to any entity that stores, processes or transmits account data.	Clarification
2.3	2.3	Clarified in requirement “Note” that additional controls are required if hashed and truncated versions of the same PAN are generated by the payment application. Added Testing Procedure 2.3.c for validation of the Note, and renumbered subsequent testing procedures.	Clarification
2.4	2.4	Updated guidance to clarify key-encrypting keys are not required to be encrypted. However, they must be protected in accordance with Requirement 2.4.	Additional Guidance
2.5	2.5	Changed “encryption” to “cryptographic” in testing procedure to align with the requirement.	Clarification

3.1.a	3.1.a	Updated testing procedure to clarify that guidance in the *PA-DSS Implementation Guide* includes assigning secure authentication to all default accounts in the environment, and that any default accounts that won't be used should also be disabled or not used.	Clarification
3.1.7	3.1.7	Clarified that passwords must be changed at least *once* every 90 days.	Clarification
5.1.d	5.1.d	Updated testing procedure to align with the requirement.	Clarification
5.3.3.a 5.4.1.c	5.3.3.a 5.4.1.c	Updated language in testing procedures for consistency.	Clarification
5.4.3.a	5.4.3.a	Combined bullets in testing procedures to remove redundancy	Clarification
5.4.5.b	5.4.5.b	Updated testing procedure to align with requirement.	Clarification
6.3	6.3	Removed redundant language in testing procedure.	Clarification
8.2	8.2	Removed SSL as an example of a secure technology. Added a note that SSL and early TLS are not considered strong cryptography and payment applications must not use, or support the use of, SSL or early TLS. Also impacts Requirements 11.1 and 12.1 – 12.2.	Evolving Requirement
8.3	8.3	Updated for consistency with PCI DSS.	Clarification
10.2.2	10.2.2	Clarified that a unique authentication credential must be used for each customer.	Clarification
11.1	11.1	Removed SSL as an example of a secure technology and added a note to the requirement. See explanation above at 8.2.	Evolving Requirement
12.1 – 12.2	12.1 – 12.2	Removed SSL as an example of a secure technology and added a note to the requirement. See explanation above at 8.2.	Evolving Requirement
Appendix A: Summary of Contents for the PA-DSS Implementation Guide	Appendix A: Summary of Contents for the PA-DSS Implementation Guide	Updated to reflect changes made to requirements, as applicable.	Clarification