Payment Card Industry (PCI)

Point-to-Point Encryption

Solution Requirements and Testing Procedures version 1.1

Summary of Changes from

P2PE Solution Requirements Initial Release v1.0

April 2012

Section or Requirement		Change
Old	**New**	
Preface	Introduction	Updated and restructured introduction sections to incorporate testing procedures and additional program information.
Definition of Account data	N/A	Removed section as covered in PCI DSS.
N/A	Merchants Using P2PE Solutions	New section added to incorporate merchant-focused guidance and information about P2PE into one section.
N/A	Relationship between P2PE and other PCI standards	New section added to clarify how P2PE complements other PCI standards (PCI DSS, PA-DSS, PTS, and PIN).
P2PE Roles and Responsibilities	P2PE Roles and Responsibilities	This section streamlined to provide summary of roles and responsibilities specifically related to P2PE assessments. Additional roles and responsibilities moved to P2PE Program Guide.
N/A	Scope of Assessment for P2PE Solutions	New section added to provide information and guidance for scoping P2PE solution assessments.
N/A	Network Segmentation	New section added to provide information regarding network segmentation for the P2PE solution provider environment.
N/A	Third Parties/ Outsourcing	New section added to provide information regarding P2PE solution provider management of third parties.
N/A	Sampling of System Components	New section added to provide information for P2PE assessors regarding use of sampling in a P2PE solution assessment.
N/A	Multiple Acquirers	New section added to provide information and guidance for situations where multiple acquirers or multiple solution providers manage one or more P2PE solutions on the same POI device.
N/A	P2PE Program Guide	New section added to provide reference to the P2PE Program Guide.
P2PE At-a-Glance	P2PE At-a-Glance	Tables and graphics updated to clarify the characteristics of each P2PE domain and how they fit together to produce the overall P2PE solution. Clarified validation process for the different stakeholders involved in the P2PE solution.
All Domains	All Domains	Testing Procedures added for all requirements for Domains 1, 2, 3, 5, and 6
All Domains	All Domains	Introductions for each domain updated to provide additional guidance and clarification.

Section or Requirement		Change
Old	**New**	
All Domains	All Domains	Requirements reorganized and restructured for clarity across all domains, including: • Separated complex or multi-part requirements into sub-requirements • Consolidated overlapping requirements and removed duplicate requirements • Multiple "notes" added and clarified to provide guidance for specific requirements • Most requirements renumbered due to reorganization and restructure of domains.
Domain 1: Encryption Device	Domain 1: Encryption Device Management	Domain 1 renamed to more accurately reflect the scope of these requirements.
Domain 2: Application Security	Domain 2: Application Security	Two sets of Testing Procedures added – one set for assessment of the application vendor and a separate set for assessment of the solution provider.
N/A	Domain 2 Annex: Summary of Contents for the Implementation Guide for P2PE Applications	New Annex added to Domain 2 to summarize required content for the application vendor's *Implementation Guide* for applicable P2PE applications.
N/A	Requirement 3B-2.2	Requirements added for solution provider to implement an opt-out process for merchants in the event that P2PE device encryption fails.
N/A	Requirement 3C: Maintain P2PE Instruction Manual for merchants	New section to incorporate requirements for the solution provider's *P2PE Instruction Manual (PIM)*.
N/A	Domain 3 Annex: Summary of Contents for the P2PE Instruction Manual (PIM)	New Annex added to Domain 3 to summarize required content for the solution provider's *P2PE Instruction Manual (PIM).*
Domain 4: Transmissions between Encryption and Decryption Environments	Domain 4: Segmentation between Encryption and Decryption Environments	Domain 4 renamed to more accurately reflect the intent that future P2PE scenarios will address segregation of duties and functions between encryption and decryption environments. Clarification that Domain 4 has no applicable requirements for the P2PE hardware/hardware scenario.
Domain 5: Decryption Environment	Domain 5: Decryption Environment and Device Management	Domain 5 renamed to more accurately reflect the scope of these requirements.
N/A	Requirement 5A: Use approved decryption devices	Requirements addressing the use of approved decryption devices moved to the first requirement in Domain 5.

Section or Requirement		Change
Old	**New**	
Domain 6: Cryptographic Key Operations	Domain 6: P2PE Cryptographic Key Operations	Domain 6 renamed to more accurately reflect the scope of these requirements.
Domain 6 Annex A: Symmetric Key Distribution using Asymmetric Techniques	Domain 6 Annex A: Symmetric Key Distribution using Asymmetric Techniques	Introduction to Physical Security Requirements for CAs and RAs integrated into requirements for consistency.
Domain 6 Annex B: Cryptographic Key Operations – Annex B: Key-Injection Facilities	Domain 6 Annex B: Cryptographic Key Operations – Annex B: Key-Injection Facilities	New set of requirements added (as indicated in initial release) to address physical protection of key-injection facilities. Requirements aligned with updates to the PCI PIN Security Requirements Version 1.0, released in September 2011.
Appendix A: PCI DSS Validation for P2PE Merchants	N/A	Applicable merchant-focused guidance moved to Introduction section. Information on merchant compliance validation to be separately documented.
Appendix B: Glossary	N/A	Glossary provided as separate, standalone document.
Appendix C: Minimum Key Sizes and Equivalent Key Strengths	Appendix A: Minimum Key Sizes and Equivalent Key Strengths	Appendix renumbered.