SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI DSS v4.0.1 – SAQ P2PE

PCI DSS SAQ P2PE provides self-assessment controls for merchants using validated point-to-point encryption to protect cardholder data.

What it is

The PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ P2PE) is a compliance tool that helps merchants confirm the implementation of security controls for protecting cardholder data using validated Point-to-Point Encryption (P2PE) solutions. This self-assessment supports organizations in evaluating whether their processes and systems securely manage payment card data, reducing the risk of data breaches and supporting regulatory compliance.

Published by the Payment Card Industry Security Standards Council (PCI SSC), the SAQ P2PE is used by merchants who process payment cards and have implemented PCI-validated P2PE solutions. The questionnaire focuses on specific cybersecurity requirements such as encryption, device management, and the secure handling of cardholder data, offering a streamlined scope compared to broader PCI DSS requirements.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Assessment / Maturity Model

VERSION
v4.0.1

EFFECTIVE
June 11, 2024

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
Payment Card Industry Security Standards Council, LLC This is the governing authority that issues the PCI DSS Self-Assessment Questionnaire (SAQ P2PE) and related documents. It is headquartered in Wakefield, Massachusetts, United States ([en.wikipedia.org](https://en.wikipedia.org/wiki/Payment_Card_Industry_Security_Standards_Council?utm_source=openai)).

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: https://www.pcisecuritystandards.org/document_library/?category=saqs

Why it matters

- **Strengthen payment data protection** Reduce the risk of cardholder data compromise by leveraging validated point-to-point encryption solutions to minimize data exposure.
- **Simplify compliance scope** Narrow the PCI DSS assessment scope for merchants using validated P2PE solutions, reducing compliance burden and associated costs.
- **Improve security oversight** Establish clear accountability and control ownership over payment systems and third-party

How SmartSuite supports PCI DSS 4.0 SAQ P2PE

Service Provider Control Library

Structure PCI DSS SAQ D requirements with mapped controls, owners, and implementation responsibilities.

Service Provider Scope Documentation

Document systems, infrastructure, and data flows supporting services that process or store cardholder data.

Security Monitoring and Incident Response

Track logging, monitoring alerts, and response workflows protecting payment processing environments.

Access and Privileged Account Governance

Manage authentication policies, privileged access reviews, and system access approvals.

Third-Party Service Provider Oversight

Track third-party service providers, customer responsibilities, and compliance documentation.

PCI DSS Service Provider Compliance Reporting

Provide dashboards showing requirement coverage, remediation status, and readiness for PCI DSS service provider assessments.

Common framework mappings

ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

PCI DSS v4.0.1 Self-Assessment Questionnaire P2PE

Provides guidelines for merchants using validated Point-to-Point Encryption solutions.

pcisecuritystandards.org/document_library/?category=saqs

PCI DSS v4.0.1 Documentation Library

Provides comprehensive PCI DSS v4.0.1 standards and supporting documents for compliance.

pcisecuritystandards.org/document_library

PCI Point-to-Point Encryption (P2PE) Standard

Outlines requirements for merchants implementing PCI P2PE solutions.

pcisecuritystandards.org/document_library/?category=p2pe

P2PE Implementation Guide

Defines implementation best practices for Point-to-Point Encryption standards.

pcisecuritystandards.org/document_library/?category=p2pe

Frequently asked questions

What is the PCI DSS v4.0.1 SAQ P2PE used for?

The PCI DSS v4.0.1 SAQ P2PE is designed for merchants who process cardholder data exclusively through payment terminals that are part of a PCI-validated Point-to-Point Encryption (P2PE) solution. Its primary purpose is to validate that appropriate security controls are in place for protecting cardholder data during payment transactions. The SAQ helps merchants ensure compliance with PCI requirements and reduce their overall risk profile.

Is compliance with the PCI DSS SAQ P2PE mandatory for merchants?

Compliance with PCI DSS, including the SAQ P2PE, is not a legal requirement but is mandatory for businesses that accept payment cards under their contractual obligations with payment card brands and acquiring banks. Merchants using a PCI-listed P2PE solution may be eligible to complete the SAQ P2PE instead of other, more extensive assessment types.

Who can use the PCI DSS SAQ P2PE?

The SAQ P2PE is applicable only to merchants that use a validated P2PE solution for all their card-present transactions and do not electronically store, process, or transmit any cardholder data outside of the P2PE solution. Merchants must confirm that all payment devices and relevant processes are fully encompassed by an approved P2PE solution before using this SAQ.

 © 2026 SmartSuite Inc. All rights reserved.

What are the key controls and requirements of the PCI DSS SAQ P2PE?

Key controls include securing devices, restricting physical and logical access to payment terminals, maintaining an accurate inventory of devices, and ensuring staff are properly trained on P2PE procedures. The SAQ also requires that merchants follow P2PE solution provider guidance, do not store cardholder data, and regularly inspect equipment for signs of tampering.

How does a merchant implement the SAQ P2PE in practice?

Implementation involves identifying all payment terminals, confirming they are covered by a PCI P2PE solution, following the documented processes of the solution provider, and completing the SAQ based on implemented controls. Merchants must develop and maintain supporting evidence, such as device inventories and training records, to demonstrate compliance.

How does PCI DSS SAQ P2PE relate to other PCI DSS Self-Assessment Questionnaires?

The SAQ P2PE is one of several SAQs tailored to different merchant environments; it offers a reduced set of requirements when compared to other SAQs because cardholder data is encrypted at the point of interaction. Merchants not using validated P2PE solutions may need to complete other SAQ types with broader or more stringent requirements.

What are the ongoing compliance requirements for PCI DSS SAQ P2PE merchants?

Ongoing compliance includes annual completion of the SAQ, continuous adherence to P2PE solution provider instructions, regular staff training, and prompt response to potential device tampering or security incidents. Merchants should update inventories, document procedural changes, and maintain open communication with their acquirer and service providers.

How would SmartSuite support PCI DSS v4.0.1 SAQ P2PE compliance?

SmartSuite can help organizations manage PCI DSS SAQ P2PE compliance by centralizing risk assessments, control implementation, and evidence collection for audit readiness. Users can track device inventories, assign responsibility for control activities, store supporting documentation, and automate reminders for annual compliance tasks. SmartSuite also facilitates comprehensive reporting to demonstrate ongoing adherence and supports collaboration across compliance and IT teams.

License included / downloadable: Yes PCI Security Standards Council publishes PCI DSS v4.0.1 and SAQ P2PE; the official SAQ and related guidance are publicly available on the PCI SSC website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/pci-dss-4-0-1-saq-p2pe