SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI DSS v4.0.1 Self-Assessment Questionnaire P2PE and Attestation of Compliance

SAQ P2PE is the PCI DSS v4.0.1 self-assessment for merchants whose only payment systems are terminals from a validated, PCI-listed P2PE solution; it covers Requirements 3, 9 and 12 only.



What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire P2PE (SAQ P2PE) is the shortest card-present validation form the PCI Security Standards Council (PCI SSC) publishes: it may be used by merchants whose only systems that store, process or transmit account data are payment terminals from a validated, PCI-listed point-to-point encryption (P2PE) solution, and it validates against PCI DSS v4.0.1 . The October 2024 edition is the current one; the Council issued the v4.0.1 SAQs on October 15, 2024, and they have been the only SAQs accepted since January 1, 2025, after PCI DSS v4.0 retired on December 31, 2024. The SAQ is a reporting form with an Attestation of Compliance (AOC), not a standard of its own.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Assessment / Maturity Model

VERSION
v4.0.1 SAQ P2PE (October 2024)

EFFECTIVE
January 1, 2025 (the only SAQs accepted after PCI DSS v4.0 retired on December 31, 2024)

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
Global

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
Low

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

Why it matters

- **Five eligibility criteria** All payment processing via a validated PCI-listed P2PE solution; the listed terminals are the only systems touching account data; no other electronic receipt, transmission or storage; any retained account data on paper and not received electronically; all PIM controls implemented (Merchant Eligibility Criteria and AOC Part 2h).
- **Three requirements instead of twelve** Section 2 contains Requirements 3, 9 and 12 only, and Part 2g of the AOC summarizes responses for those three; Requirement 3 applies only to merchants with paper records that include account data.
- **Terminal controls spelled out** Requirement 9.5.1 asks for a list of POI devices with make, model, location and serial number (9.5.1.1), periodic inspection of device surfaces (9.5.1.2) and training to spot tampering or substitution (9.5.1.3); the SAQ notes these apply to the POI devices used as part of the P2PE solution.
- **Guidance sized for small merchants** The SAQ Completion Guidance under 12.1.1 and 12.1.2 says the security policy can be a simple document on protecting the store and payment devices per the solution provider's instructions and whom to call in an emergency; under 12.6.1 an awareness program can be a flyer in the back office or a periodic e-mail.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports PCI DSS 4.0.1 SAQ P2PE

Eligibility and Solution Record (Parts 2e and 2h)

Record the solution provider, solution name, listing reference, listed POI devices and reassessment date next to the five eligibility statements, with a reminder before the reassessment date.

PIM Control Checklist

Hold each control from the P2PE Instruction Manual as a record with owner, status and evidence, so the fifth eligibility criterion can be shown as met.

POI Device Inventory (9.5.1.1)

Use IT Asset Management (ITAM) for the terminal list with make, model, location and serial number, and link each device to its inspection history.

Inspection and Training Log (9.5.1.2, 9.5.1.3)

Schedule periodic surface inspections per device, record findings and suspected substitution, and keep training records for personnel in POI environments.

Policy, Awareness and Incident Plan (Requirement 12)

Store the security policy with its 12-month review date, the awareness program materials and the incident response plan with who to call, as the SAQ Completion Guidance describes.

TPSP Register and AOC Pack (12.8, Section 3)

Use Third Party Risk Management for the TPSP list, agreements and annual status checks, and assemble the SAQ, Appendix C explanations and signed AOC for the acquirer.

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

Which merchants are eligible for SAQ P2PE?

Merchants whose payment channel runs entirely through a validated PCI-listed P2PE solution, where the terminals of that solution are the only systems that store, process or transmit account data, the merchant does not otherwise receive, transmit or store account data electronically, any retained account data is on paper and not received electronically, and all controls in the P2PE Instruction Manual have been implemented. The Merchant Eligibility Criteria allow brick-and-mortar and mail or telephone order merchants; e-commerce channels and service providers are excluded.

Which PCI DSS requirements does SAQ P2PE include?

Only Requirements 3, 9 and 12. Requirement 3 applies solely to merchants with paper records containing account data (3.1.1, 3.2.1, 3.3.1.2); Requirement 9 covers paper media (9.4.1 to 9.4.6) and the POI device list, inspections and training (9.5.1 to 9.5.1.3); Requirement 12 covers the security policy (12.1.1 to 12.1.3), awareness (12.6.1), third-party service providers (12.8.1 to 12.8.5) and the incident response plan (12.10.1). Part 2g of the AOC and the Part 4 action plan list the same three requirements.

What happens if the P2PE solution's validation has expired?

The SAQ's footnote states that solutions on the PCI list of Point-to-Point Solutions with Expired Validations are no longer considered validated under the P2PE Program Guide. A merchant using an expired solution should check with its acquirer or the individual payment brands about whether SAQ P2PE is still acceptable. Part 2e of the AOC records the solution's reassessment date so the merchant can see when the listing is due to lapse.

What is the P2PE Instruction Manual and why does it matter for SAQ P2PE?

The P2PE Instruction Manual (PIM) is the document the P2PE Solution Provider gives the merchant, setting out the controls the merchant must apply to the terminals and their use. Implementing all PIM controls is the fifth eligibility criterion, certified in Part 2h of the AOC. The Document Changes table records that Requirements 3.3 and 4.2 were removed from this SAQ in April 2016 because the P2PE solution and the PIM already cover them.

What does a merchant complete and sign in the SAQ P2PE Attestation of Compliance?

Section 1 (AOC Parts 1 and 2) records contacts, payment channels, the environment, the validated solution in Part 2e, third-party service providers in Part 2f, the summary of responses in Part 2g and the eligibility certification in Part 2h. Section 3 (Parts 3 and 4) records the compliance status (Compliant, Non-Compliant or Compliant but with Legal exception), the acknowledgement that SAQ P2PE Version 4.0.1 was completed per its instructions, the signature of a merchant executive officer, any QSA or ISA involvement and, if the acquirer requests it after a Non-Compliant result, an action plan for Requirements 3, 9 and 12. The SAQ and AOC are then submitted to the acquirer or payment brand with any other requested documentation.

License included / downloadable: Yes The PCI Security Standards Council publishes SAQ P2PE in its Document Library, where it can be downloaded free of charge after accepting the Council's license agreement.

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