YourIT!
Your Logo Goes Here

PCI DSS - SAQ P2PE

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

Purpose

The intended audience for this SAQ includes merchants that utilize validated P2PE solutions for processing cardholder data, specifically in card-present and mail/telephone-order environments. This SAQ should be used when merchants do not store, process, or transmit account data electronically outside of the validated P2PE solution. Unique compliance requirements include adherence to the P2PE Instruction Manual and the absence of access to clear-text data. Merchants must ensure all relevant personnel are aware of their responsibilities regarding data security as outlined in the SAQ.

Scope

This Self-Assessment Questionnaire (SAQ) P2PE applies exclusively to merchants that process account data solely through a validated PCI-listed Point-to-Point Encryption (P2PE) solution. It encompasses all systems, personnel, and processes involved in the handling of cardholder data via approved payment terminals. Merchants must not have access to clear-text account data and should only enter data through these terminals. Segmentation considerations are critical; any systems outside the validated P2PE solution are excluded from this SAQ. This SAQ differs from others by focusing specifically on environments that do not electronically store or transmit cardholder data.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Requirement 3 - Protect Stored Account Data

PCI DSS - SAQ P2PE	Other Requirements
Requirement 3 Protect Stored Account Data	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

3.1 Processes and mechanisms for protecting stored account data are defined and understood.
3.2 Storage of account data is kept to a minimum.
3.3 Sensitive authentication data (SAD) is not stored after authorization.

Guidance
Overview
Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk-mitigation opportunities. For example, methods for minimizing risk include not storing account data unless necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies such as e-mail and instant messaging.

If account data is present in non-persistent memory (for example, RAM, volatile memory), encryption of PAN is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. Data should be removed from volatile memory once the business purpose (for example, the associated transaction) is complete. In the case that data storage becomes persistent, all applicable PCI DSS Requirements will apply including encryption of stored data.

Requirement 3 applies to protection of stored account data unless specifically called out in an individual requirement.

Refer to Appendix G for definitions of strong cryptography and other PCI DSS terms.

SAQ Completion Guidance for SAQ P2PE - Requirement 3

Requirement 3.1.1
If the merchant has paper storage of account data, having policies and procedures in place ensures that personnel are aware of and follow security policies and documented operational procedures for managing the secure storage of any paper records with account data. If the merchant does not store paper records with account data, this requirement is not applicable.

Requirement 3.2.1
Having data disposal policies in place means that if the merchant stores any paper containing account data, it is stored according to those policies and destroyed when no longer needed. If the merchant never prints or stores any paper containing account data, this requirement is not applicable.

Requirement 3.3.1.2
If the merchant writes down the card verification code during a transaction, it must be securely destroyed immediately after the transaction or obscured before storage. If the merchant never requests the card verification code, this requirement is not applicable.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- PCI-3.1.1 - Requirement 3.1.1:
  Processes and mechanisms for protecting stored account data are defined and understood.

  3.1.1 All security policies and operational procedures that are identified in Requirement 3 are:
  • Documented.
  • Kept up to date.
  • In use.
  • Known to all affected parties.

  Procedure
  - Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 3 are managed in accordance with all elements specified in this requirement.

- PCI-3.2.1 - Requirement 3.2.1:
  Storage of account data is kept to a minimum.

  3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:
  • Coverage for all locations of stored account data.
  • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
  • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
  • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
  • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
  • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

  Procedure
  - Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement.
  - Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy.
  - Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.

- PCI-3.3.1.2-v4.0.1 - Requirement 3.3.1.2:
  Sensitive authentication data (SAD) is not stored after authorization.

  3.3.1.2 The card verification code is not stored upon completion of the authorization process.

  Procedure
  - Examine data sources, to verify that the card verification code is not stored upon completion of the authorization process.

References

- PCI Security Standards Council Document Library - https://www.pcisecuritystandards.org/document_library/
- PCI Security Standards Council - https://www.pcisecuritystandards.org/
- PCI DSS v4.0 At a Glance - https://www.pcisecuritystandards.org/document_library?category=pcidss&document=dss4aag
- PCI DSS Requirements & Testing Procedure - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Requirement 9 - Restrict Physical Access to Cardholder Data

PCI DSS - SAQ P2PE	Other Requirements
Requirement 9 Restrict Physical Access to Cardholder Data	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.
9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

Note:
Control PCI-9.5.1.2.1 is intentionally left blank for the SAQ.

Guidance
Overview
Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.

There are three different areas mentioned in Requirement 9:
1. Requirements that specifically refer to sensitive areas are intended to apply to those areas only. Each entity should identify the sensitive areas in its environments to ensure the appropriate physical controls are implemented.
2. Requirements that specifically refer to the cardholder data environment (CDE) are intended to apply to the entire CDE, including any sensitive areas residing within the CDE.
3. Requirements that specifically refer to the facility are referencing the types of controls that may be managed more broadly at the physical boundary of a business premise (such as a building) within which CDEs and sensitive areas reside. These controls often exist outside a CDE or sensitive area, for example a guard desk that identifies, badges, and logs visitors. The term facility is used to recognize that these controls may exist at different places within a facility, for instance, at building entry or at an internal entrance to a data center or office space.

Refer to Appendix G for definitions of media, personnel, sensitive areas, visitors, and other PCI DSS terms.

SAQ Completion Guidance for SAQ P2PE - Requirement 9

Requirement 9.1.1
Having policies and procedures in place means that the merchant governs activities related to securing any paper media with cardholder data and protecting POI devices.

Requirement 9.4

If the merchant securely stores any paper media with account data, it must be done in a manner such as using locked storage, and the merchant must destroy such paper when no longer needed for business purposes. If the merchant never stores any paper with account data, this requirement is not applicable.

Requirement 9.5
Having policies and procedures in place means that the merchant maintains a current list of devices, conducts periodic inspections, and trains employees to detect tampered or substituted devices.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- PCI-9.1.1 - Requirement 9.1.1:
  Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

  9.1.1 All security policies and operational procedures that are identified in Requirement 9 are:
  • Documented.
  • Kept up to date.
  • In use.
  • Known to all affected parties.

  Procedure
  - Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 9 are managed in accordance with all elements specified in this requirement.

- PCI-9.4.1 - Requirement 9.4.1:
  Media with cardholder data is securely stored, accessed, distributed, and destroyed.

  9.4.1 All media with cardholder data is physically secured.

  Procedure
  - Examine documentation to verify that the procedures defined for protecting cardholder data include controls for physically securing all media.

- PCI-9.4.1.1 - Requirement 9.4.1.1:
  Media with cardholder data is securely stored, accessed, distributed, and destroyed.

  9.4.1.1 Offline media backups with cardholder data are stored in a secure location.

  Procedure
  - Examine documentation to verify that procedures are defined for physically securing offline media backups with cardholder data in a secure location.
  - Examine logs or other documentation and interview responsible personnel at the storage location to verify that offline media backups are stored in a secure location.

- PCI-9.4.6 - Requirement 9.4.6:
  Media with cardholder data is securely stored, accessed, distributed, and destroyed.

  9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:
  • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
  • Materials are stored in secure storage containers prior to destruction.

Procedure
- Examine the periodic media destruction policy to verify that procedures are defined to destroy hard-copy media with cardholder data when no longer needed for business or legal reasons in accordance with all elements specified in this requirement.
- Observe processes and interview personnel to verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that cardholder data cannot be reconstructed.
- Observe storage containers used for materials that contain information to be destroyed to verify that the containers are secure.

- PCI-9.5.1.1 - Requirement 9.5.1.1:
  Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

  9.5.1.1 An up-to-date list of POI devices is maintained, including:
  • Make and model of the device.
  • Location of device.
  • Device serial number or other methods of unique identification.

  Procedure
  - Examine the list of POI devices to verify it includes all elements specified in this requirement.
  - Observe POI devices and device locations and compare to devices in the list to verify that the list is accurate and up to date.
  - Interview personnel to verify the list of POI devices is updated when devices are added, Customized Approach Objective relocated, decommissioned, etc.

- PCI-9.5.1.2 - Requirement 9.5.1.2:
  Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

  9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.

  Procedure
  - Examine documented procedures to verify processes are defined for periodic inspections of POI device surfaces to detect tampering and unauthorized substitution.
  - Interview responsible personnel and observe inspection processes to verify: • Personnel are aware of procedures for inspecting devices. • All devices are periodically inspected for evidence of tampering and unauthorized substitution.

- PCI-9.5.1.2.1 - Requirement 9.5.1.2.1:
  Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

  9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

  Procedure
  - Examine the entity's targeted risk analysis for the frequency of periodic POI device inspections and type of inspections performed to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.

- Examine documented results of periodic device inspections and interview personnel to verify that the frequency and type of POI device inspections performed match what is defined in the entity's targeted risk analysis conducted for this requirement.

- PCI-9.5.1.3 - Requirement 9.5.1.3:
  Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

  9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:
  • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
  • Procedures to ensure devices are not installed, replaced, or returned without verification.
  • Being aware of suspicious behavior around devices.
  • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

  Procedure
  - Review training materials for personnel in POI environments to verify they include all elements specified in this requirement.
  - Interview personnel in POI environments to verify they have received training and know the procedures for all elements specified in this requirement.

- PCI-9.5.1-v4.0.1 - Requirement 9.5.1:
  Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

  9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:
  • Maintaining a list of POI devices.
  • Periodically inspecting POI devices to look for tampering or unauthorized substitution.
  • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

  Procedure
  - Examine documented policies and procedures to verify that processes are defined that include all elements specified in this requirement.

References

- PCI Security Standards Council Document Library - https://www.pcisecuritystandards.org/document_library/
- PCI Security Standards Council - https://www.pcisecuritystandards.org/
- PCI DSS v4.0 At a Glance - https://www.pcisecuritystandards.org/document_library?category=pcidss&document=dss4aag
- PCI DSS Requirements & Testing Procedure - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Truncated Sample Document