PCI DSS - SAQ SPoC

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

1 - Purpose

2 - Scope

3 - Sanctions/Compliance

4 - Requirement 3 - Protect Stored Account Data

5 - Requirement 8 - Identify Users and Authenticate Access to System Components

6 - Requirement 9 - Restrict Physical Access to Cardholder Data

7 - Requirement 12 - Support Information Security with Organizational Policies and Programs

Purpose

The intended audience for this SAQ includes merchants who process card-present transactions using validated SPoC solutions. This SAQ should be utilized when merchants do not store, process, or transmit cardholder data outside of the specified SPoC environment. It outlines compliance requirements tailored to this specific payment channel, ensuring that merchants understand their obligations regarding data security and access control. Unique validation requirements include adherence to the controls outlined in the SPoC user guide and maintaining compliance with PCI DSS standards relevant to their operational scope.

Scope

This Self-Assessment Questionnaire (SAQ) SPoC applies to merchants utilizing Software-based PIN entry on Commercial Off-The-Shelf (COTS) devices, specifically for card-present transactions. It encompasses all system components, personnel, and processes involved in the secure handling of cardholder data via validated Secure Card Reader-PIN (SCRP) devices. Merchants must ensure that their payment environment is isolated from other systems and that no clear-text account data is stored electronically. This SAQ is distinct from others as it specifically addresses the unique requirements for merchants using SPoC solutions, excluding unattended transactions and service providers.

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 SPoC	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 SPoC - Requirement 3

Requirement 3.1.1
If the merchant retains account data on paper, they must have documented policies and procedures in place to ensure personnel are aware of and adhere to security requirements for handling and storing such records. If no paper records containing account data are stored, this requirement does not apply.

Requirement 3.2.1
Merchants must implement data disposal policies governing the retention of account data. If storing paper records with account data, these policies must define retention periods based on business, legal, or

regulatory needs and specify secure destruction methods once the data is no longer required. If the merchant does not store paper records containing account data, this requirement does not apply.

Requirement 3.3.1.2
If the merchant collects the card verification code during a transaction, it must be securely destroyed immediately after use or obscured before storage. If the merchant does not collect this code, this requirement does not apply.

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 8 - Identify Users and Authenticate Access to System Components

PCI DSS - SAQ SPoC	Other Requirements
Requirement 8 Identify Users and Authenticate Access to System Components	N/A

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

8.3 Strong authentication for users and administrators is established and managed.

Guidance
Overview
Two fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity is who the user claims to be. Identification of an individual or process on a computer system is conducted by associating an identity with a person or process through an identifier, such as a user, system, or application ID. These IDs (also referred to as accounts) fundamentally establish the identity of an individual or process by assigning unique identification to each person or process to distinguish one user or process from another. When each user or process can be uniquely identified, it ensures there is accountability for actions performed by that identity. When such accountability is in place, actions taken can be traced to known and authorized users and processes. The element used to prove or verify the identity is known as the authentication factor. Authentication factors are 1) something you know, such as a password or passphrase, 2) something you have, such as a token device or smart card, or 3) something you are, such as a biometric element. The ID and the authentication factor together are considered authentication credentials and are used to gain access to the rights and privileges associated with a user, application, system, or service accounts. These requirements for identity and authentication are based on industry-accepted security principles and best practices to support the payment ecosystem. NIST Special Publication 800-63, Digital Identity Guidelines provides additional information on acceptable frameworks for digital identity and authentication factors. It is important to note that the NIST Digital Identity Guidelines is intended for US Federal Agencies and should be viewed in its entirety. Many of the concepts and approaches defined in these guidelines are expected to work with each other and not as standalone parameters.

Note: Unless otherwise stated in the requirement, these requirements apply to all accounts on all system components, unless specifically called out in an individual requirement, including but not limited to:
- Point-of-sale accounts
- Accounts with administrative capabilities
- System and application accounts
- All accounts used to view or access cardholder data or to access systems with cardholder data.

This includes accounts used by employees, contractors, consultants, internal and external vendors, and other third parties (for example, for providing support or maintenance services). Certain requirements are not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. When items do not apply, they are noted directly within the specific requirement.

These requirements do not apply to accounts used by consumers (cardholders).

Refer to Appendix G for definitions of PCI DSS terms.

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

Related Internal Controls

- PCI-8.3.1 - Requirement 8.3.1:
  Strong authentication for users and administrators is established and managed.

  8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
  • Something you know, such as a password or passphrase.
  • Something you have, such as a token device or smart card.
  • Something you are, such as a biometric element.

  Procedure
  - Examine documentation describing the authentication factor(s) used to verify that user access to system components is authenticated via at least one authentication factor specified in this requirement.
  - For each type of authentication factor used with each type of system component, observe an authentication to verify that authentication is functioning consistently with documented authentication factor(s).

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