Merchants with Standalone, IP-Connected PTS Point- of-Interaction (POI) Terminals ± No Electronic Cardholder Data Storage

For use with PCI DSS version 3.2

Version 1.1
January 2017

Document Changes iAQ DSS0 gj 1 0 1-8

Date	PCI DSS Version	SAQ Revision	Description
N/A	1.0		Not used.
N/A	2.0		Not used.
February 2014	3.0		New SAQ to address requirements applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction devices with an IP connection to the payment processor. Content aligns with PCI DSS v3.0 requirements and testing procedures.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1*.
July 2015	3.1	1.1	June 30, 2015.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2.* Requirements added from PCI DSS v3.2 Appendix A2.
January 2017	3.2	1.1	Updated Document Changes to clarify requirements add in the April 2016 update.
			Updated Before You Begin section to and intent of SCR

Table of Contents

Before You Begin

SAQ B-IP has been developed to address requirements applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices with an IP connection to the payment processor. An exception applies for POI devices classified as Secure Card Readers (SCR); merchants using SCRs are not eligible for this SAQ.

SAQ B-IP merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B-IP merchants confirm that, for this payment channel:

Completing the Self-Assessment Questionnaire

status regarding that requirement. ***Only one response should be selected for each question.***

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.
No	

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information			
Part 1a. Merchant Organization Information			
Company Name:		DBA (doing business as):	
Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:	Country:		Zip5/F

Section 2: Self-Assessment Questionnaire B-IP

Note: *The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the* PCI DSS Requirements and Security Assessment Procedures *document.*

Self-assessment completion date:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
1.1.2	(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	Review current network diagram Examine network configurations	☐	☐	☐	☐
	(b) Is there a process to ensure the diagram is kept current?	Interview responsible personnel	☐	☐	☐	☐
1.1.4	(a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	Review firewall configuration standards Observe network configurations to verify that a firewall(s) is in place	☐	☐	☐	☐
	(b) Is the current network diagram consistent with the firewall configuration standards?	Compare firewall configuration standards to current network diagram	☐	☐	☐	☐
1.1.6	(a) Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?	Review firewall and router configuration standards	☐	☐	☐	☐

PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
		Yes	Yes with CCW	No	N/A
(b) Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?					

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
		Yes	Yes with CCW	No	N/A
3.2.2					

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
4.1.1	Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?	Review documented standards Review wireless networks Examine system configuration settings	☐	☐	☐	☐
4.2	(b) Are policies in p 1 0 0 1ic s					

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
	(b) Are critical security patches installed within one month of release? ***Note**: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	Review policies and procedures Examine system components Compare list of security patches installed to recent vendor patch lists	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	Review policies and procedures for distribution of media	☐	☐	☐	☐
	(b) Do controls include the following:					
9.6.1	Is media classified so the sensitivity of the data can be determined?	Review policies and procedures for media classification Interview security personnel	☐	☐	☐	☐
9.6.2	Is media sent by secured co126.74 416325(Is)-8(m)4(e)-3					

PCI DSS Question	Expected Testing	Response

PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
		Yes	Yes with CCW	No	N/A
(b) Have personnel at point-of-sale locations					

Regularly Monitor and Test Networks

Requirement 11: Regularly test security systems and processes

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
11.2.2	(a) Are quarterly external vulnerability scans performed? ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	Review results from the four most recent quarters of external vulnerability scans	☐	☐	☐	☐

PCI DSS Question	Expected Testing	

PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
		Yes	Yes with CCW	No	N/A
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent cardholder data environment? ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being proe two p18 3079 666.12 44*				

Appendix C: Explanation of Non-Applicability

If the "N / (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example:	
3.4	Cardholder data is never stored electronically

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ B-IP (Section 2), dated *(SAQ completion date).*

Based on the results documented in the SAQ B-IP noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status

Part 3a. Acknowledgement of Status (continued)