PCI PA - DSS

Point iPOS Implementation Guide

Hypercom – P2100 using the Point iPOS Payment Core
Hypercom – H2210/K1200 using the Point iPOS Payment Core

Version 1.02

POINT TRANSACTION SYSTEMS AB
Box 92031, 120 06 Stockholm, Tel. +46 8 566 287 00
www.point.se

Revision History

Version	Name	Date	Comments
1.00	Mats Oscarsson	2011-03-25	Initial version
1.01	Mats Oscarsson	2011-04-28	Changed front page to indicate that the Point iPOS Payment Core is used for both P2100 and H2210/K1200. Changed to cover the case when H2210/K1200 is used and connected to a vending machine or similar. Chapter 3.3 Protect wireless transmissions is updated.
1.02	Mats Oscarsson	2011-04-29	A new chapter “Back-out or product de-installation procedures” is added.

References

Nbr.	Title	Version
1	Payment Card Industry – Payment Application Data Security Standard	1.2.1
2	Payment Card Industry – Data Security Standard	1.2.1

Table of contents

1. Introduction

The Payment Card Industry Data Security Standard (PCI-DSS) defines a set of requirements for the configuration, operation, and security of payment card transactions in your business. If you use Point iPOS in your business to store, process, or transmit payment card information, this standard and this guide apply to you.

The requirements are designed for use by assessors conducting onsite reviews and for merchants who must validate compliance with the PCI DSS.

Failure to comply with these standards can result in significant fines if a security breach should occur. For more details about PCI DSS, please see the following link:

http://www.pcisecuritystandards.org

This guide is updated whenever there are changes in Point iPOS software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in the Point iPOS as well as the PCI standards. You can download the latest version of this document from

http://www.point.se/

The Payment Card Industry has also set the requirements for software applications that store, process or transmit cardholder data. These requirements are defined by the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS). In order to facilitate for you to get a PCI DSS assessment the Point iPOS software application has been approved by PCI to comply with the PCI PA-DSS requirements.

Note: This guide refers to Point iPOS terminals using the Point iPos Payment Core. The version of the Point iPos Payment Core is listed on the PCI web site "List of Validated Payment Applications" that have been validated in accordance with PCI PA-DSS. If you cannot find the version of the Point iPos Payment Core running on your Point iPOS on that list please contact our helpdesk in order to upgrade your terminal.

http://www.pcisecuritystandards.org/

Document Use

This PA-DSS Implementation Guide contains information for proper use of the Point iPOS application. Point Transaction Systems AB does not possess the authority to state that a merchant may be deemed "PCI Compliant" if information contained within this document is followed. Each merchant is responsible for creating a PCI-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the Point iPOS application in a manner that will support a merchant's PCI DSS compliance efforts.

Note 1: Both the System Installer and the controlling merchant must read this document.

Note 2: This document must also be used when training ECR/vending machine integrators/resellers at initial workshops.

2. Summary of PCI DSS requirements

This summary provides a basic overview of the PCI DSS requirements and how they apply to your business and the Point iPOS terminal.

2.1 Build and Maintain a Secure Network

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

a. What the requirement says

“Firewalls are computer devices that control computer traffic allowed between a company’s network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company’s internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.
A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce,employees’ Internet access through desktop browsers, employees’ e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.”. Reference 2.

b. How your Point iPOS helps you meet this requirement

Point iPOS is designed to operate in a network behind a firewall.

c. What this means to you

If you are using wireless technology you must install and maintain a firewall to protect your Point iPOS from someone hacking the wireless environment. Also, if your network connection allows inbound traffic you should use a firewall.
For more information about setting up your firewall to work with Point iPOS, please refer to the manual supplied by your firewall vendor.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

a. *What the requirement says*

“Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information. ”. Reference 2.

b. *How your Point iPOS helps you meet this requirement*

Point iPOS does not allow users to access any card holder data or sensitive authentication data. IP addresses for processors, terminal management systems and software download servers are protected by unique passwords per terminal and these passwords are changed on a daily basis. For more information about the level of passwords protection for Point iPOS maintenance menus please refer to “*Point Transaction Systems AB – Point iPos User’s Guide”, reference 3*

c. *What this means to you*

Since the password protection for the Point iPOS is handled entirely within the unit there is no need for you to take any action.

2.2 Protect Cardholder Data

Requirement 3: Protect stored cardholder data

a. *What the requirement says*

“Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails”. Reference 2.

b. *How your Point iPOS helps you meet this requirement*

Point iPOS never stores full magnetic stripe data from the card. For offline transactions PAN and expiry date are stored encrypted using a unique key per transaction

At transaction time PAN is truncated before it is stored, only the first 6 and last 4 digits are stored. For printout of receipts and reports the truncated PAN is sent to the ECR/vending machine.

c. *What this means to you*

For cards read by the Point iPOS magnetic stripe reader or chip card reader you do not have to take any action.

For voice referrals it is never allowed to write down or otherwise store PAN, expiration date or CVV2.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

a. What the requirement says

“Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments. ”. Reference 2.

b. How your Point iPOS helps you meet this requirement

The Point iPOS encrypts card holder data using triple DES with a unique key per transaction.

c. What this means to you

If you are using a wireless network, WLAN, you must set up your wireless network to use WPA/WPA2 encryption for new installations. **N.B. WEP must not be used after June 30 2010.** The WLAN encryption is applied on top of the triple DES encryption.

If you connect to an external network without using WLAN you do not need to take any action.

2.3 Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

a. What the requirement says

“Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business approved activities including employees’ e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. ”. Reference 2.

b. How your Point iPOS helps you meet this requirement

The Point iPOS cannot be used for e-mails or internet activities. All software downloaded to the terminal is controlled by Point, protected by a digital signature (MAC). These security measures prevent malicious software being installed onto your Point iPOS terminal.

c. What this means to you

You should install and maintain antivirus software which helps to protect your system. Make sure that this software is up to date as security threats change.

For the Point iPOS you do not need to take any action regarding antivirus software.

Requirement 6: Develop and maintain secure systems and applications

a. What the requirement says

“Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendorprovided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software. ”. Reference 2.

b. How your Point iPOS helps you meet this requirement

Point Transaction Systems constantly works with the latest security findings and requirements throughout the life cycle of your Point iPOS. This includes automatic SW updates whenever necessary.

c. What this means to you

You should keep your system up to date with software updates, operating system updates, and any other security patches.

For the Point iPOS you do not need to take any action.

2.4 Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

a. What the requirement says

“To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. ”. Reference 2.

b. How your Point iPOS helps you meet this requirement

The Point iPOS does not disclose any cardholder data. Sensitive authentication data is always encrypted when sent for authorization and never stored. PAN is always truncated when stored, thus only truncated PANs are sent to the ECR/vending machine for printouts of reports, logs or receipts.

c. What this means to you

In case you have to do voice referrals you must never keep written copies or otherwise store copies of cardholder data. Also, you must never e-mail, fax etc card holder data.

For cards read by the Point iPOS magnetic stripe reader or chip card reader you do not need to take any additional security measures.

Requirement 8: Assign a unique ID to each person with computer access

a. What the requirement says

“Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. ”. Reference 2.

Requirement 8.3: “ Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.” Reference 2.

b. How your Point iPOS helps you meet this requirement

The Point iPOS does not allow access to critical data.

Requirement 8.3: The Point iPOS does not allow direct remote access to the system. But for remote updates via Terminal Management Systems the authentication used as part of an authenticated remote software distribution framework for the PED, should be evaluated by a QSA as part of any PCI DSS assessment.

c. What this means to you

Since the Point iPOS does not allow access to critical data you do not need to take any action.

Requirement 8.3: Ask your QSA to include the remote update process in the PCI DSS assessment.

Requirement 9: Restrict physical access to cardholder data

a. *What the requirement says*

“Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. ”. Reference 2.

b. *How your Point iPOS helps you meet this requirement*

The Point iPOS physically prevents by encryption and truncation users to access cardholder data.

c. *What this means to you*

For your Point iPOS you do not need to take any action.

2.5 Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

a. *What the requirement says*

“Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs. ”. Reference 2.

b. *How your Point iPOS helps you meet this requirement*

The Point iPOS keeps a log for the 500 latest transactions. This log contains truncated PANs. No cardholder data is accessible from the Point iPOS.

The Point iPOS also keeps an Audit Trail to track changes to system level objects.

c. *What this means to you*

For the transaction log you do not need to take any action since no cardholder data is accessible.

For the Audit Trail there are no settings you need to do. The Audit Trail is created automatically and cannot be disabled. The Audit Trail could be retreived and stored to a file by using the PC-tool IposConf, for further details please refer to the user’s manual.

Requirement 11: Regularly test security systems and processes

a. What the requirement says

“Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment. ”. Reference 2.

b. How your Point iPOS helps you meet this requirement

Your Point iPOS has mechanisms to ensure that software and parameters can be downloaded from trusted sources only. These mechanisms are based on cryptographic signatures and MAC protection (Message Authentication Code).

c. What this means to you

You should test your network connections (including wireless networks) periodically for vulnerabilities, and make use of network vulnerability scans. If you make any significant changes to your network, you should also test for vulnerabilities.

2.6 Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

a. What the requirement says

“A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, “employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site. ”. Reference 2.

b. How your Point iPOS helps you meet this requirement

----

c. What this means to you

----

3. How to set up your Point iPOS to ensure PCI DSS compliance

3.1 Do not retain full magnetic stripe or card validation code

When upgrading the payment application in your Point iPOS to comply with the PCI PA-DSS requirements this could be done two ways.

1. Your old unit is physically replaced by a new Point iPOS loaded with software that complies with the PCI PA-DSS requirements. Since the old unit may contain historical magnetic stripe data, PANs, and CVV2s the unit must be returned to Point.
2. Your existing Point iPOS is downloaded remotely with new software that complies with the PCI PA-DSS requirements. After download your Point iPOS software is designed to remove all historical magnetic stripe data, PANs and CVV2s stored by previous versions of the software.

In both cases you must make sure that the software version of the Point iPos Payment Core that runs on your Point iPOS is listed on the PCI web site “List of Validated Payment Applications” that have been validated in accordance with PCI PA-DSS.

http://www.pcisecuritystandards.org

In order for your organization to comply with PCI DSS requirements it is absolutely necessary to remove historical data stored prior to installing your PCI PA-DSS compliant Point iPOS terminal. Therefore you must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) are removed from all storage devices used in your system, ECRs, vending machines, PCs, servers etc. For further details please refer to your vendor.

No specific setup of your Point iPOS PCI PA-DSS compliant terminal is required. PAN is stored either truncated or encrypted. Full magnetic stripe data is deleted immediately after authorization and never stored. CVV2 is never used in the terminal since manual entry of PAN is not implemented.

However, if you need to do a voice referral you should never write down or otherwise store PAN, expiration date or CVV2. Collect this type of data only when absolutely necessary.

3.2 Protect stored card holder data

PAN and expiration date are encrypted and stored in your Point iPOS for offline transactions. For this encryption a unique key per transaction is used. Once your Point iPOS goes online any stored transactions are sent to the processor and securely deleted from the Point iPOS memory.

To comply with the PCI DSS requirements all cryptographic material must be removed. The removal of this material is handled within the Point iPOS and you do not need to take any action.

3.3 Protect wireless transmissions

If you are using wireless network within your business you must make sure that firewalls are installed that deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Point iPOS environment. Please refer to your firewall manual.

In case you are using a wireless network you must also make sure that:

- Encryption keys were changed from vendor defaults at installation.
- Passwords to access the wireless router/access point were changed from vendor defaults.
- Strong encryption (https or SSH) are used for authentication, i.e. entry of user identity and password, to access the wireless router/ access point.
- Encryption keys are changed anytime someone with knowledge of the keys leaves the company or changes position.
- Default SNMP community strings on wireless devices are changed
- Firmware on wireless devices is updated to support strong encryption, WPA/WPA2. Please note that WEP must not be used for new installations and is not allowed after June 30, 2010.
- Strong encryption (WPA/WPA2) are used for all transmission over the wireless network.
- Other security related vendor defaults are changed.

3.4 Facilitate secure remote software updates

The software of your Point iPOS could be updated remotely and automatically. For connection to external networks it is recommended to use firewall protection as per ”2.1 Build and Maintain a Secure Network” in this document.

3.5 Encrypt sensitive traffic over public networks

Your Point iPOS allows transmission over public networks, e.g. public internet. To protect sensitive data your Point iPOS uses triple DES encryption with a unique key per transaction. To connect your Point iPOS to public networks you do not need to take any further action regarding encryption.

4. Back-out or product de-installation procedures

The software of your Point iPOS could be updated remotely either automatically or manually triggered. In the unlikely event that your newly downloaded software fails or malfunctions please contact your TMS operator in order to allow you to download an older version of the software.

5. Terminology and abbreviations

PCI DSS: Payment Card Industry Data Security Standard, the subject of this document. Retailers that use applications to store, process or transmit payment card data are subject to the PCI DSS standard.

PA DSS: Payment Application Data Security Standard is a standard for validation of payment applications that store, process or transmit payment card data. Applications that comply with PA DSS have built in protection of card data and hereby facilitates for retailers to comply with PCI DSS.

Cardholder Data: PAN, Expiration Date, Cardholder Name (not used by Point iPOS) and Service Code.

Service Code: A three digit code from the magnetic stripe data defining (1) Interchange and technology, (2) Authorization processing and (3) Range of services and PIN requirements.

PAN: Primary Account Number. PAN, also called card number, is part of the magnetic stripe data and is also printed or embossed on the card. PAN can also be stored in the chip of the card.

SSL: Secure Sockets Layer is a commonly used method to protect transmission across public networks. SSL includes strong encryption.

ECR: Electronic Cash Register

CVV2: Card Verification Value, also called CVC2, is a three or four digit value printed on the back of the card but not encoded on the magnetic stripe or the chip. Supplying this code in a transaction is intended to verify that the card is present at the point of sale.

SNMP: Simple Network Management Protocol, is a network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

WPA and **WPA2:** Wi-Fi Protected Access, is a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks.

WEP: Wired Equivalent Privacy, a wireless network security standard. Sometimes erroneously called "Wireless Encryption Protocol"

Magnetic Stripe Data: Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.

Sensitive Authentication Data: Magnetic Stripe Data, CVV2 and PIN.

TMS: Terminal Management System