Point PA-DSS

Implementation Guide

Banksys Yomani 1.04

VeriFone & PAX VPFIPA0201

Point Transaction Systems Oy | Vanha Nurmijärventie 62 | FI-01670 VANTAA | www.point.fi

Contents

1 Revision history

Version	Author	Date	Comments
0.1	Pekka Ylitalo	1.2.2010	Initial draft
0.2	Pekka Ylitalo	5.2.2010	Review by Martin Gutekunst
0.3	Pekka Ylitalo	26.2.2010	Updated after review by Acertigo
0.4	Lauri Mäkinen	27.4.2010	Made YOMANI related changes to req. 1.1.5 and chapter 5
1.0	Lauri Mäkinen	4.5.2010	Updated version number to 1.0
1.1	Pekka Ylitalo	25.8.2010	Made changes to req. 1.1.4 and chapter 6
1.2	Pekka Ylitalo	8.12.2011	Point application firewall requirement changes to chapter 4.3 req. 6 and chapter 4.4 req. 9 and 10
1.3	Kimmo Heiskanen	10.5.2013	Added multiple requirement definitions to meet PA-DSS v2.0 audit requirements
1.4	Pekka Ylitalo	16.9.2013	Implementation guide updated and finalized according to PA-DSS v2.0 implementation guide requirements
1.5	Pekka Ylitalo	15.10.2013	Minor updates after review by TÜV SÜD

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

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 application has been approved by PCI to comply with the PCI PA-DSS requirements.

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

http://www.pcisecuritystandards.org

3 Document use

This PA-DSS Implementation Guide contains information about the Point application. Point Transaction Systems Oy does not possess the authority to state that a merchant may be deemed “PCI Compliant”. 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 application in a manner that will support a merchant’s PCI DSS compliance efforts.

3.1 Important notes

• This guide refers to Point application versions 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 running on Your Point terminal on that list please contact our helpdesk at Point in order to upgrade Your terminal

• Both the System Installer and the controlling merchant must read this document

• This document must also be used when training ECR integrators/resellers at initial workshops

4 Summary of requirements

This summary covers shortly the PCI DSS/PA-DSS requirements that have a related PA-DSS Implementation Guide topic. It also explains how the requirement is handled in the Point application and also explains the requirement from Your aspect.

The complete PCI DSS and PA-DSS documentation can be found at:
http://www.pcisecuritystandards.org

4.1 Do not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data

Requirement 1.1.4: Delete sensitive authentication data stored by previous payment application versions.

1. What the requirement says

Securely delete any magnetic stripe data, card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.

2. How the Point application meets this requirement

No specific setup for the Point application is required. The Point application does not store any historical data so removal of historical data is not needed.

3. What this means to You

You must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) is removed from all other storage devices used in Your systems, ECRs, PCs, servers etc. For further details please refer to the appropriate vendor. Removal of historical data is absolutely necessary for PCI DSS compliance.

Requirement 1.1.5: Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.

1. What the requirement says

Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card verification codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.

2. How the Point application meets this requirement

Generally troubleshooting is not done on production terminals. However, if logs are written, no sensitive data is included in them.

For the Yomani terminal logging level may be raised to a higher level from the application. If the logging level is for any reason raised to a higher level PAN's are stored in truncated format.

Logs can only be sent from terminal to a Point backend and thus be examined only by Point personnel.

Troubleshooting logs storage time is 20 days.

3. What this means to You

No actions needed.

4.2 Protect stored cardholder data

Requirement 2.1: Purge cardholder data after customer-defined retention period.

1. What the requirement says

Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period.

2. How the Point application meets this requirement

All cardholder data is automatically erased during the nightly batch sending or if manual batch sending is done.

Below is a list of all the locations where the payment application stores cardholder data:

- VeriFone terminals:
    - FILETRANSLIST.LST, PAYMENTS.BLS and EcrTrnBackup.LST
- PAX:
    - FILETRANSLIST.LST and PAYMENTS.BLS
- Banksys Yomani:
    - /usr/paymentapp/logs, /usr/paymentapp/store/pending, /usr/paymentapp/store/sent, /usr/paymentapp/store/lastFailed, /usr/paymentapp/blacklist_ranges.bin and /usr/paymentapp/blacklist_singles.bin

No activity is necessary to prevent inadvertent capture or retention of cardholder data. For example, system backup or restore points.

3. What this means to You

All cardholder data is automatically erased during the nightly batch sending. If You want to do this operation manually it is possible. Please refer to the Point application user manual on how to send the batch manually. This will erase all cardholder data.

Requirement 2.5: Protect keys used to secure cardholder data against disclosure and misuse.

1. What the requirement says

Payment application must protect any keys used to secure cardholder data against disclosure and misuse.

2. How the Point application meets this requirement

Access to the encryption keys is prevented. Keys are stored in special safe memory.

3. What this means to You

No actions needed.

Requirement 2.6: Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

1. What the requirement says

Payment application must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

2. How the Point application meets this requirement

The KEY management process is automatic and controlled only by the Point application.

See chapter 5 for detailed information about key management and cryptographic material removal.

3. What this means to You

No actions needed.

Requirement 2.7: Render irretrievable cryptographic key material or cryptograms stored by previous payment application versions.

1. What the requirement says

Render irretrievable any cryptographic key material or cryptogram stored by previous versions of the payment application, in accordance with industry-accepted standards. These are cryptographic keys used to encrypt or verify cardholder data

2. How the Point application meets this requirement

All cryptographic material must be removed and it is absolutely necessary for PCI DSS compliance. The removal of this material is automatically handled by the Point application so You do not need to take any action.

See chapter 5 for detailed information about key management and cryptographic material removal.

3. What this means to You

No actions needed.

4.3 Provide secure authentication features

Requirement 3.1: Use unique user IDs and secure authentication for administrative access and access to cardholder data

1. What the requirement says

The payment application must support and enforce the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication must be enforced to all accounts, generated or managed by the application, by the completion of installation and for subsequent changes after installation.

2. How the Point application meets this requirement

No administrative access to the Point application is possible.

3. What this means to You

No actions needed.

Requirement 3.2: Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications

1. What the requirement says

Software vendor must provide guidance to customers that all access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication.

2. How the Point application meets this requirement

The Point application does not provide any accounts or access to critical data.

3. What this means to You

No actions needed.

4.4 Log payment application activity

Requirement 4.1: Implement automated audit trails

1. What the requirement says

At the completion of the installation process, the “out of the box” default installation of the payment application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users.

2. How the Point application meets this requirement

The Point application does not allow making any changes relevant to the payment functionality. Because of this no activity can be performed which would need logging/auditing.

3. What this means to You

No actions needed.

Requirement 4.4: Facilitate centralized logging

1. What the requirement says

Payment application must facilitate centralized logging

2. How the Point application meets this requirement

The Point application provides a functionality to send logs into an arbitrary log server, in general a log server maintained by the merchant.

For the Yomani terminal troubleshooting logs are sent separately from the payment terminal if requested by Point backend system, or by activating troubleshooting log sending from the terminal.

3. What this means to You

If You want to setup an arbitrary log server, please refer to the Point application user manual on how to do this. If You are using a Yomani terminal please contact Point customer service.

4.5 Develop secure payment applications

Requirement 5.4: Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties

1. What the requirement says

The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application (for example, if NetBIOS, filesharing, Telnet, FTP, etc., are required by the application, they are secured via SSH, S-FTP, SSL, IPSec, or other technology).

2. How the Point application meets this requirement

The Point application and terminals use SSL-secured communication by default. Below is a list of all the communication protocols and ports used.

Connection type	Protocols used	Port numbers
Cable / Ethernet	TCP/IP SSL for host Serial for ECR TCP, UDP for audit logs	Host: 443 ECR: Port defined on ECR side Audit logs: Port defined on audit log server side
WiFi	WiFi SSL for host TCP for ECR TCP for audit logs	Host: 443 ECR: Port defined on ECR side Audit logs: Port defined on audit log server side
GPRS / 3G	GPRS SSL for host TCP for audit logs	Host: 443 Audit logs: Port defined on audit log server side

For ECR integrations SSL is not used when the terminal is communicating with the ECR using serial port or WiFi connection. Also for log sending SSL is not used. These connections never contain any cardholder sensitive data.

3. What this means to You

No actions needed.

4.6 Protect wireless transmissions

Requirement 6.1: Securely implement wireless technology

1. What the requirement says

For payment applications using wireless technology, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The wireless technology must be implemented securely.

2. How the Point application meets this requirement

Point application operates in a network behind a firewall or in a network without a firewall. The Point application supports strong encryption for wireless, WPA and WPA2. Also all data sent to and from the Point application is always protected using SSL v3.

For ECR integrations SSL is not used when the terminal is communicating with the ECR using serial port or WiFi connection. Also for log sending SSL is not used. These connections never contain any cardholder sensitive data.

3. What this means to You

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 application environment. Please refer to Your firewall manual.

In case You are using a wireless network You must also make sure that the following requirements are met:

• Encryption keys are changed from vendor defaults at installation

• 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 the use of WEP as a security control was prohibited as of 30 June 2010.

• Other security related vendor defaults like passwords and logins are changed

Requirement 6.2: Secure transmissions of cardholder data over wireless networks

1. What the requirement says

For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Please note that the use of WEP as a security control was prohibited as of 30 June 2010.

2. How the Point application meets this requirement

The Point application supports strong encryption for wireless, WPA and WPA2. Also all data sent to and from the Point application is always protected using SSL v3.

For ECR integrations SSL is not used when the terminal is communicating with the ECR using serial port or WiFi connection. Also for log sending SSL is not used. These connections never contain any cardholder sensitive data.

3. What this means to You

No actions needed.

4.7 Cardholder data must never be stored on a server connected to the Internet

Requirement 9.1: Store cardholder data only on servers not connected to the Internet

1. What the requirement says

The payment application must be developed such that the database server and web server are not required to be on the same server, nor is the database server required to be in the DMZ with the web server.

2. How the Point application meets this requirement

Point application does not store any cardholder data in a server connected to the internet.

3. What this means to You

No actions needed.

4.8 Facilitate secure remote access to payment application

Requirement 10.2: Implement two-factor authentication for remote access to payment application

1. What the requirement says

If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism.

2. How the Point application meets this requirement

The Point application cannot be accessed remotely.

3. What this means to You

No actions needed.

Requirement 10.3.1: Securely deliver remote payment application updates

1. What the requirement says

If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes.

Alternatively, if delivered via VPN or other high speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always on" connections.

2. How the Point application meets this requirement

The Point Payment application is not delivered remotely to the customer's systems. Application updates are downloaded from Point's terminal management system. The Point application cannot be accessed remotely.

3. What this means to You

No actions needed.

Requirement 10.3.2: Securely implement remote access software

1. What the requirement says

If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely.

2. How the Point application meets this requirement

The Point application cannot be accessed remotely.

3. What this means to You

No actions needed.

4.9 Encrypt sensitive traffic over public networks

Requirement 11.1: Secure transmissions of cardholder data over public networks

1. What the requirement says

If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols (for example, SSL/TLS, Internet protocol security (IPSEC), SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.

2. How the Point application meets this requirement

All data sent to and from the Point application is always protected using SSL v3.

For ECR integrations SSL is not used when the terminal is communicating with the ECR using serial port or WiFi connection. Also for log sending SSL is not used. These connections never contain any cardholder sensitive data.

3. What this means to You

No actions needed.

Requirement 11.2: Encrypt cardholder data sent over end-user messaging technologies

1. What the requirement says

If the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs.

2. How the Point application meets this requirement

Point application is not able to send any cardholder data using end-user messaging technologies

3. What this means to You

No actions needed.

4.10 Encrypt all non-console administrative access

Requirement 12.1: Encrypt non-console administrative access

1. What the requirement says

Instruct customers to encrypt all non-console administrative access with strong cryptography, using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

2. How the Point application meets this requirement

The Point application cannot be accessed remotely and no non-console access is possible.

3. What this means to You

Any applicable terminal management systems 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.

5 Point application key management

The main idea is that the KEY management process is automatic and controlled only by the Point application. It does not require any key injections from outside. A 3DES key is used for encryption. The key is generated and stored in the POS TRM and never goes outside.

• The 3DES encryption key is generated by the terminal's operating system.

• The encryption key is stored in tamper evident memory by the terminal's operating system.

• Key transmission is not required.

• Non-YOMANI terminals: New key is generated when terminal starts for the 1st time, after terminal software update, after every batch sending (at least once per 24 hours) and after manual transaction deletion operation. If the key generation process was not successful then the application doesn't allow making any payment transactions, only service functions are allowed. Before new key generation the old key is destroyed and cryptographic material is removed.

• Non-YOMANI terminals: If for some reason the application/terminal is not able to send the batch for a time longer than 30 days, then the application doesn't allow making any payment transactions.

• YOMANI terminal: Each encrypted file will use a unique encryption key. When a single encryption is more than one year old, it is regenerated and the file is re-encrypted using the new key.

6 Implementation Guide reviews and updates

The Point PA-DSS Implementation Guide is reviewed on an annual basis and updated as needed to document all major and minor changes to the Point application and PA-DSS standard changes.

The latest Point PA-DSS Implementation Guide can be found at:

http://www.point.fi

7 Terminology

PCI DSS: Payment Card Industry Data Security Standard. 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 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 when PAN is entered manually or when a voice referral is performed.

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.

POS: Point of sale

TRM: Tamper resistant module

3DES: Triple DES common name for the Triple Data Encryption Algorithm

8 References

1. Payment Card Industry – Payment Application Data Security Standard v2.0
2. Payment Card Industry – Data Security Standard v2.0