Point PA-DSS

Implementation Guide

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	Update 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

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 Protecting sensitive- cardholder data

Requirement 1: Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2), or PIN block data

1. What the requirement says

Do not store sensitive authentication data after authorization. Only those data elements needed for business should be stored.

2. How the Point application meets this requirement

No specific setup for the Point application is required. PAN is always stored encrypted. Full magnetic stripe data and CVV2 is deleted immediately after authorization and never stored.

3. What this means to You

If You need to enter PAN, expiration date and CVV2 manually or 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 to perform manual entry or voice referral.

Requirement 1.1.4: Historical data deletion

1. What the requirement says

Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the payment application

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 necessary for PCI-DSS compliance.

Requirement 1.1.5: Securely delete any sensitive data used for debugging or troubleshooting

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

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.

3. What this means to You

No actions needed.

Requirement 2: Protect stored cardholder data

1. 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.

2. How the Point application meets this requirement

Point application never stores full magnetic stripe data from the card. For transactions PAN and expiry date are stored encrypted. A 3DES key is used for encryption. The key is generated and stored in the POS TRM and never goes outside.

3. What this means to You

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

For manually entered PAN and for voice referrals it is never allowed to write down or otherwise store the PAN, expiration date or CVV2.

Requirement 2.1: Purging cardholder data

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.

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 2.7: Cryptographic material removal

1. What the requirement says

Securely delete any cryptographic key material or cryptogram stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion. 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. 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.

4.2 User IDs, secure authentication and user access logging

Requirement 3: Provide secure authentication features

1. 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.

2. How the Point application meets this requirement

The Point application does not allow access to critical data.

3. What this means to You

No actions needed.

Requirement 3.1: Unique user IDs and secure authentication for administrative access

1. What the requirement says

The “out of the box” installation of the payment application in place at the completion of the installation process, must facilitate use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data.

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: Unique user IDs and secure authentication for access to servers etc

1. What the requirement says

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.

Requirement 4: Log payment application activity

1. 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.

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

Review Your systems logs if any periodically to see which users are accessing Your systems.

Requirement 4.2: Implement automated audit trails

1. What the requirement says

Payment application must implement an automated audit trail to track and monitor access.

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.

4.3 Wireless technology

Requirement 6: Protect wireless transmissions

1. What the requirement says

Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

2. How the Point application meets this requirement

Point application operates in a network behind a firewall or in a network without a firewall. If wireless is used the Point application supports strong encryption, WPA.

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:

- Encryption keys were 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 WEP must not be used for new installations and is not allowed after June 30, 2010
- Other security related vendor defaults are changed

Requirement 6.1: Securely implement wireless technology

1. What the requirement says

For payment applications using wireless technology, the wireless technology must be implemented securely.

2. How the Point application meets this requirement

If wireless is used the Point application supports strong encryption, WPA. The wireless encryption is applied on top of the 3DES encryption. Also all data sent to and from the Point application is always protected using SSL.

3. What this means to You

No actions needed.

Requirement 6.2: Secure transmission 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.

2. How the Point application meets this requirement

If wireless is used the Point application supports strong encryption, WPA. The wireless encryption is applied on top of the 3DES encryption. Also all data sent to and from the Point application is always protected using SSL.

3. What this means to You

No actions needed.

4.4 Data storage and remote access/updates

Requirement 9: Cardholder data must never be stored on a server connected to the Internet

1. What the requirement says

Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment. Limit inbound Internet traffic to IP addresses within the DMZ. Do not allow internal addresses to pass from the Internet into the DMZ.

2. How the Point application meets this requirement

Point application operates in a network behind a firewall or in a network without a firewall. Point application also allows the use of DMZs.

3. What this means to You

No actions needed.

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.

Requirement 10: Facilitate secure remote software updates

1. 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.

Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use.

2. How the Point application meets this requirement

Point application operates in a network behind a firewall or in a network without a firewall.

3. What this means to You

You must install and maintain a firewall for all computers used in Your business to block any unauthorized traffic/remote access. For more information about setting up Your firewall to work with Point application, please refer to the manual supplied by Your firewall vendor.

Requirement 10.1: 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 highspeed 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

No remote access to Point production terminals or the application is possible.

3. What this means to You

No actions needed.

Requirement 11: Facilitate secure remote access to payment terminal

1. What the requirement says

Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

2. How the Point application meets this requirement

No remote access to Point production terminals or the application is possible.

3. What this means to You

No actions needed.

Requirement 11.2: 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 twofactor authentication mechanism.

2. How the Point application meets this requirement

No remote access to Point production terminals or the application is possible.

3. What this means to You

No actions needed.

Requirement 11.3: Securely implement remote access software

1. What the requirement says

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

2. How the Point application meets this requirement

No remote access to Point production terminals or the application is possible.

3. What this means to You

No actions needed

4.5 Sensitive traffic/access encryption

Requirement 12: Encrypt sensitive traffic over public networks

1. 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.

Use strong cryptography and security protocols such as SSL/TLS or IPSEC 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.

3. What this means to You

No actions needed.

Requirement 12.1: 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 such as SSL/TLS and Internet protocol security (IPSEC) 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.

3. What this means to You

No actions needed.

Requirement 12.2: Encrypt cardholder data sent over end-user messaging technologies

1. What the requirement says

The payment application must never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).

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.

Requirement 13: Encrypt all non-console administrative access

1. What the requirement says

Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for webbased management and other non-console administrative access.

2. How the Point application meets this requirement

No remote access to Point production terminals or the application is possible.

3. What this means to You

No actions needed.

Requirement 13.1: Encrypt non-console administrative access

1. What the requirement says

Instruct customers to encrypt all non-console administrative access 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

No remote access to Point production terminals or the application is possible.

3. What this means to You

No actions needed.

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 v1.2.1
2. Payment Card Industry – Data Security Standard v1.2.1