Verifone

VeriFone Payment Core

Implementation Guide

For VeriFone Vx520, Vx675, Vx680, Vx690, Vx820, Vx825 terminals using the

Point VxPC F02.01.xxx Software

(Vx Payment Core)

Version 1.2

Date: **09-Feb-2018**

Revision History

Version	Name	Date	Comments
0.01	Mats Oscarsson	2012-12-19	Draft version
0.02	Karlis Balcers	2012-12-21	Chapters "2.1 Build and Maintain a Secure Network" and "6. Appendix A – Configuration of Audit Trail" updated.
0.03	Mats Oscarsson	2013-01-04	1. Editorial changes. 2. "6. Appendix A – Configuration of Audit Trail" Updated to specify the data contents of the Audit Trail log file.
0.04	Mats Oscarsson	2013-01-10	List of abbreviations updated. Editorial changes Terminal identity is added when Audit Trail is sent to centralized server. Version of SW changed to F01.01 Front page is changed to include Vx675 Instructions on how to find out what ports are used for outbound traffic is updated.
0.05	Mats Oscarsson	2013-02-08	FinECR protocol mentioned in section "2.1 Build and Maintain a Secure Network"
0.06	Jevgenijs Smirnovs	2014-10-24	Updated implementation guide as per VxPC F02.01. Added Version Numbering Policy
0.07	Jevgenijs Smirnovs	2014-10-30	Updated description of major and minor version number in Version Numbering Policy
0.08	Sergejs Melnikovs	2014-12-12	Document update according to PCI DSS & PCI PA DSS version 3.0 requirements
0.10	Jevgenijs Smirnovs	2014-12-19	Updated Appendix B with list of files containing Cardholder Data and Appendix C with instances of PAN occurrences. Added menu path to access Audit Logs in integrated mode; Added possible entries to Audit Logs
0.11	Jevgenijs Smirnovs	2015-04-29	Document rebranding
0.12	Sergejs Melnikovs	2015-06-05	Corrected download location of Implementation Guide
1.0	Sergejs Melnikovs	2015-06-12	Minor editor changes and document release
1.1	Sergejs Melnikovs	2017-12-20	Added clarifications and guidelines to chapters 2.2 & 2.4 according to PCI DSS & PCI PA DSS version 3.2 requirements; Added appendix D with supported HW & protocols.
1.2	Sergejs Mlnikovs	2018-02-09	Added more explanation about application update process

References

Nbr.	Title	Version
1	Payment Card Industry – Payment Application Data Security Standard	3.2
2	Payment Card Industry – Data Security Standard	3.2

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 the VeriFone Vx terminal 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.

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 VxPC software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in the software as well as the PCI standards. Guidelines how to download the latest version of this document could be found on the following web site

http://www.verifone.se

The Payment Card Industry (PCI) 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 VxPC (Point Vx Payment Core) software has been validated by PCI to comply with the PCI PA-DSS requirements.

Note: This guide refers to VeriFone Vx terminals using the Point VxPC (Point Vx Payment Core) SW. The version of the Point VxPC 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 your Point VxPC on that list please contact your helpdesk in order to upgrade your terminal.

http://www.pcisecuritystandards.org/

Document Use

This PA-DSS Implementation Guide contains information for proper use of VeriFone Vx terminals using the Point VxPC. Verifone does not possess the authority to state that a merchant may be deemed "PCI DSS Compliant" if information contained within this document is followed. Each merchant is responsible for creating a PCI DSS compliant environment. The purpose of this guide is to provide information needed during installation and operation of terminals using the Point VxPC 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. Hence, the Implementation Guide should be distributed to all relevant payment application users (customers, resellers and integrators)

Note 2: This document must also be used when training 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 when using the VeriFone Vx terminal with Point VxPC.

In this chapter Point Vx refers to Verifone Vx terminals using the Point VxPC SW.

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 devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. 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, employee Internet access through desktop browsers, employee e-mail access, dedicated connections 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. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.", reference 2.

Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

b. How your Point Vx helps you meet this requirement

Point VxPC 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 Vx from someone hacking the wireless environment. Also, if your network connection allows inbound traffic you should use a firewall. The terminal should not be placed in an Internet accessible network zone ("DMZ").

In case the terminal is connected to an ECR and a firewall is connected between the terminal and the ECR the TCP port used must be opened to enable communication between the two.

Protocol	TCP port
LPP	2000
PayPoint	9500
AirPay	5000
Restaurant	45001

For ports used for outbound traffic please refer to the information menu of the terminal as described below.

- Stand Alone Vx520 terminals or equivalent monochrome terminals with functional keys:
  1. Press the F3 key.
  2. Press the F3 key ”TERMINAL INFO”
  3. Press “ENTER” for Terminal Info List
  4. Select “HOST Parameters” to print the information.

- Stand Alone Vx680 terminals or equivalent terminal with touchscreen:
  1. Press “MENU” on the touch screen.
  2. Press “MAINTENANCE”
  3. Press “TERMINAL INFO”
  4. Press “PRINT REPORTS”
  5. Press “Host Parameters” to print the information

- Vx820 or Vx825 terminals connected to an ECR or equivalent.
  1. Press “MENU” on the touch screen
  2. Press “GENERAL MENU”
  3. Press “INFORMATION”
  4. Press “HOST INFO”
  5. Then scroll up or down to display the information

- Stand Alone Vx675 or Vx520C terminals:
  1. Press the “MENU” key.
  2. Scroll down and select “MAINTENANCE”
  3. Select ”TERMINAL INFO”
  4. Press “Enter” for “Print Reports”
  5. Scroll down and select “HOST Parameters” to print the information.

For more information about setting up your firewall to work with Point Vx, 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 an entity) 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.

Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

b. How your Point Vx helps you meet this requirement

Point Vx does not allow users to access any cardholder data or sensitive authentication data. The application also doesn't facilitate any non-console administrative access to the network. 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.

c. What this means to you

Since the password protection for the Point Vx is handled entirely within the unit and no any non-console administrative access provided 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 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 also 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 unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of "strong cryptography" and other PCI DSS terms.", reference 2.

b. How your Point Vx helps you meet this requirement

Point Vx 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 or (in case of ISO8583) generated 3DES double-length key, which is retained until file exists in terminal. The file is deleted once all content is sent and confirmed by host.

Point Vx never displays full PAN of the card on the screen (except manual PAN entry dialogue). Full list of instances where PAN could be output to store outside of the application control represented in "Appendix C".

At transaction time PAN is truncated before it is stored, only the first 6 and last 4 digits are stored, or encrypted in case of ISO8583. For printout of receipts and reports the truncated PAN is sent to the ECR.

Point Vx application does not allow plaintext PAN output even for debugging/troubleshooting purposes.

Point Vx never uses end-user messaging technologies for cardholder data sending.

c. What this means to you

For cards read by the Point Vx magnetic stripe reader, chip card reader or NFC 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 PAN, expiration date or CVV2.

If you store (as needed for business) cardholder data please don't use a public-facing systems (for example, web server and database server must not be on same server).

Do not utilize end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.) to send unprotected PAN unless they are configured to provide strong encryption.

Note: Sending of unprotected PANs via end-user messaging technologies strictly prohibited.

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 continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.", reference 2.

b. How your Point Vx helps you meet this requirement

The Point Vx encrypts cardholder data using triple DES with a unique key per transaction. On top of that the entire messages sent to and from the Point Vx are protected using SSL/TLS, if the processor supports SSL/TLS.

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 installations. **N.B. WEP must not be used after June 30, 2010.** The WLAN encryption is applied on top of the triple DES encryption and SSL/TLS (if SSL/TLS is supported by the processor) implemented in the terminal.

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

2.3. Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware 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 employee 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. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.", reference 2.

b. How your Point Vx helps you meet this requirement

The Point Vx cannot be used for e-mails or internet activities. All software downloaded to the terminal is controlled by Verifone, protected by a digital signature (MAC) and sent over an SSL/TLS connection (if the processor supports SSL/TLS). These security measures prevent malicious software being installed onto your Point Vx 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 Vx 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 vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.", reference 2.

b. How your Point Vx helps you meet this requirement

Verifone Inc. constantly works with the latest security findings and requirements throughout the life cycle of your Point Vx. 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 Vx 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. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.", reference 2.

b. How your Point Vx helps you meet this requirement

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

c. What this means to you

In case you need to enter card numbers manually or if 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. cardholder data.

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

Requirement 8: Identify and authenticate access to system components

a. What the requirement says

"Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their 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 and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system — particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.", reference 2.

b. How your Point Vx helps you meet this requirement

The Point Vx does not allow access to critical data.

Requirement 8.3: The Point Vx 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

All other systems in the cardholder data should be protected by PCI-compliant authentication methods. That means:

- Each user account must be assigned a unique ID.
- The authentication must be performed at least either by a password, a token, or some biometric.
- No group accounts or generic accounts may be used.
- User passwords must be changed at least once every 90 days.
- A password must be at least seven characters long.
- The password must consist of numeric and alphabetic characters.
- The password history must be saved and a password must be different from the last four passwords used.
- The account must be locked after no more than six invalid login attempts.
- A lock must last at least 30 seconds.
- After 15 minutes of inactivity, the user must authenticate again.
- Assigning secure authentication to all default accounts in use

Any default accounts which are not required must be disabled or removed.

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. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.”, reference 2.

b. How your Point Vx helps you meet this requirement

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

c. What this means to you

For your Point Vx 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, if not impossible, without system activity logs.”, reference 2.

b. How your Point Vx helps you meet this requirement

The Point Vx keeps a log for the 1000 latest transactions. This log contains truncated PANs. No cardholder data is accessible from the Point Vx. The log file is deleted at software update

The Point Vx 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 sent manually to a centralized server by entering the Point Vx "LOG MENU", for further details please refer to the user's manual.

The address to the centralized log server is already set when you receive the terminal and normally there is no need to change that address in the terminal. However, if for some reason this address needs to be changed please contact the representative of your service provider. Chapter "5 Audit Trail log" also gives you guidance on how to change the address of the centralized log server.

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 Vx helps you meet this requirement

Your Point Vx 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

"All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.", reference 2.

b. How your Point Vx helps you meet this requirement

----

c. What this means to you

---

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

In this chapter Point Vx refers to terminals using the Point VxPC.

3.1. Do not retain full magnetic stripe or card validation code

When upgrading the payment application in your Point Vx 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 Vx loaded with software that complies with the PCI PA-DSS requirements. If the old unit is not PCI PA-DSS compliant it could contain historical magnetic stripe data, PANs, and CVV2s. Therefore the non PCI PA-DSS compliant unit must be returned to Verifone.
2. Your existing Point Vx is upgraded remotely with new software that complies with the PCI PA-DSS requirements. After download your Point Vx 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 VxPC that runs on your Point Vx 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 Vx 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, PCs, servers etc. For further details please refer to your vendor.

No specific setup of your Point Vx 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.

However, if you need to enter PAN and expiration date 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.

Note: Using the PCI PA-DSS compliant Point Vx terminal you will never be prompted to enter CVV2.

No any sensitive cardholder’s data are retrieving by Point VxPC application (even when needed to solve a specific problem) in production terminals. In case when sensitive cardholder’s data need to be present in the logs for troubleshooting is only done at Verifone lab/test environment using test terminals.

Note: Removal of sensitive authentication data is absolutely necessary for PCI DSS compliance.

3.2. Protect stored cardholder data

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

To comply with the PCI DSS requirements all cryptographic material must be rendered irretrievable. This is handled within the Point Vx 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 Vx 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 for authentication and transmission over wireless networks, for example IEEE 802.11i. Please note that the use if WEP as a security control was prohibited as of June 30, 2010.
- Other security related vendor defaults are changed.

3.4. Facilitate secure remote software updates

The software of your Point Vx 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. The terminal should not be placed in an Internet accessible network zone (“DMZ”).

Also the security part of the software that resides in the PED (PIN Entry Device) part of the terminal could be updated remotely. The merchant is not required to take any action in relation to terminal update because the application periodically connects to terminal management system and verify is a pathed version available for downloading. Once a new version downloaded the terminal upgrades the application and only after successful integrity verification through digital signatures installs new version of the application. There is also possibility to initiate application update manually from the terminal menu: **Menu→ Functions → load parameter**s

Once a security patch or update of payment application released by Verifone a Product Manager notifies by email (or via phone call) responsible person of the integrator/reseller and provides encrypted package by corresponding integrator/reseller’s public PGP key, signs it with his own private PGP key and provides it to the integrator/reseller’s contact person via email or other communication channel which is agree in advance with the integrator/reseller.

The integrator/reseller which provides management server service to the customer should configure the management server to deliver patches and updates to the terminal once it's received from Verifone according to PCI DSS required timeframe.

The Terminal Management System that is used for distribution of the PED software should be evaluated by a QSA as part of any PCI DSS assessment.

3.5. Encrypt sensitive traffic over public networks

Your Point Vx allows transmission over public networks, e.g. public internet. To protect sensitive data your Point Vx uses triple DES encryption with a unique key per transaction. On top of that all data sent to and from the Point Vx is protected under SSL/TLS, if the processor supports SSL/TLS. To connect your Point Vx 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 Vx 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. Audit Trail log

5.1. How to change the address to the centralized log server

By default the Audit Trail is sent to a centralized log server hosted by your PSP. If you want to continue to use that log server you don't have to take any action.

However, if you want to use another server and receive the Audit Trail in SYSLOG format then do as follows.

On the Point Vx terminal Stand Alone mode

1. Select "MENU"
2. Select "Maintenance"
3. Scroll down to "LOG MENU"
4. Select "A-LOG" (Audit Trail)
5. Select "Send TCP SYSLOG"
6. Select "Real-Time send"
7. Enter IP address for Audit Trail Log Server
8. Enter PORT number
9. Verify if terminal succeeds to connect and send by selecting "Send once"

On Integrated Solution:

1. Select MENU
2. Enter Menu Access Password
3. Select 'Functions'
4. Select 'Log Menu'

5. Select ‘A-Log’ (Audit Trail)
6. Select “Send TCP SYSLOG”
7. Select “Real-Time send”
8. Enter IP address for Audit Trail Log Server
9. Enter PORT number
10. Verify if terminal succeeds to connect and send by selecting “Send once”

Once A-LOG in SYSLOG format is activated, all information of major events will be transferred to your designated server as soon as terminal will go out in IDLE (NEW CUSTOMER screen). Terminal will keep theses settings even after power loss or reboot.

Important:

- SysLog is sent in TCP message instead of UDP. Make sure your SysLog server supports it.
- SysLog is based on standard internet protocols as specified by RFC 3164 and RFC 3195.

5.2. Data Contents of Audit Trail

The format of the terminal log file needed to meet the PCI DSS requirement 10, “Track and monitor all access to network resources and cardholder data”, described in PCI Requirements and Security Assessment Procedures Version 3.0.

5.2.1. File size

The size of the file has to be decided for each application/platform. According to PCI DSS requirement 10.7 audit trails must be retained for at least three months online (ready for immediate forensic analysis) and for a total of one year.

5.2.2. File format

The terminal audit log file should be a readable ascii text file with one entry on each line. The log entries should consist of data according to table below with each value separated by semi-colon “;” last data element is also padded with ‘;’ character. This makes it possible to import the file to a number of existing database programs.

Requirement	Name	Value
10.3.1	User ID	Full name of process or script depending on application/platform.
10.3.2	Type of event	See table below
10.3.3	Date & Time	YYMMDDhhmmss
10.3.4	Success	OK / NOK
10.3.5	Origination	Auto / Man / Timer
10.3.6	Content data	Depending on type of event. See table below. In case of several data entries in single event separator “!” is used to split data entries.
	Trailer	Newline characters indicating end of log entry: ‘\n’ (0x0A)

SysLog is sent in TCP message instead of UDP. Make sure your SysLog server supports it.

SysLog is based on standard internet protocols as specified by RFC 3164 and RFC 3195.

Event Type	Content	Description
Download	file = [filename downloaded]([download location])	Result of file download from remote host. Indicates file name downloaded and ip+port of remote host from which file was downlaoded
Validate	file = [filename validated]	Validation result of file
Install	file = [filename installed]	Installation result of file
Configuration	[parameter name] old = [Old paramete value] new = [New parameter value]	Terminal configuration change affecting host IP configuration, terminal Identifiers, rescheduling of operations, change of terminal identifiers or user password change.
Audit send	ip:port = [destination ip:port]	Result of audit log sending. Indicates destination server which the log was sent to.
RT Audit Start	ip:port = [syslog server ip:port]	Start of Real-Time audit log sending to SysLog server. Indicates IP&Port of destination syslog server.
RT Audit Stop	reason = [reason for stop]	Interruption of Real-Type audit log sending to syslog server. Optionally indicates reason for stopping: e.g. technical failure, customer interruption, etc.
Startup	app = [PaymentCore version] os = [OS version] eos = [EOS version] emv = [EMV Kernel version] script = [Secure Script version]	Indicates application startup. Indicates application version as well as versions of external modules used during handling of sensitive data.

5.2.3.Example

Below is an example of log entries from a terminal.

PPL;Download;20141023173821;NOK;Man;file=9170060000001981(:);
PPL;Download;20141023170024;OK;Man;file=9170060000001981(:);
PPL;Validate;20141023170024;OK;Auto;file=9170060000001981.dld;
PPL;Download;20141023170024;OK;Man;file=MASPAR__140814094410(:);
PPL;Validate;20141023170024;OK;Auto;file=MASPAR__140814094410.dld;
PPL;Download;20141023170025;OK;Man;file=DCPAR___140814094410(:);
PPL;Validate;20141023170025;OK;Auto;file=DCPAR___140814094410.dld;
PPL;Download;20141023170027;OK;Man;file=BINPAR__140814101442(:);
PPL;Validate;20141023170027;OK;Auto;file=BINPAR__140814101442.dld;
PPL;Download;20141023170029;OK;Man;file=CAPUB___130417154000(:);
PPL;Validate;20141023170029;OK;Auto;file=CAPUB___130417154000.dld;
FA;Configuration;20141023170029;OK;Auto;[Next_Social_call] old=20141028030800![Next_Social_call] new=20140906;
PPL;Install;20141023170029;OK;Auto;file=MASPAR__;
PPL;Install;20141023170030;OK;Auto;file=DCPAR___;
PPL;Install;20141023170030;OK;Auto;file=NEWBINPAR__;
PPL;Install;20141023170031;OK;Auto;file=CAPUB___;

6. Terminology and abbreviations

Cardholder Data	PAN, Expiration Date, Cardholder Name (not used by Point Vx) and Service Code.
CVV2	Card Verification Value, also called CVC2 (Card Verification Code), is a three or four digit value printed on the back of the card but not encoded on the magnetic stripe or the chip.
ECR	Electronic Cash Register
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification.
Magnetic Stripe Data	Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.
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.
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.
PCI PA-DSS	Payment Card Industry 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.
PED	PIN Entry Device.
PIN	Personal Identification Number. Secret numeric password known only to the user and a system to authenticate the user to the system.
Point VxPC	The Payment Core used by Point Vx terminals. The Point VxPC is the part of the Point Vx software that stores, processes and transmits cardholder data. The Point VxPC is validated in accordance with the requirements of PCI PA-DSS.
PSP	Payment Service Provider offers merchants online services for accepting electronic payments.
Sensitive Authentication Data	Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
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.
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.
SSH	Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
SSL	Secure Sockets Layer is a commonly used method to protect transmission across public networks. SSL includes strong encryption.
SYSLOG	Syslog is a standard for computer data logging.

TCP	Transmission Control Protocol is one of the core protocols of the Internet protocol suite.
TLS	Acronym for “Transport Layer Security.” Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
TMS	Terminal Management System.
UDP	User Datagram Protocol is one of the core protocols of the Internet protocol suite.
WEP	Wired Equivalent Privacy, a wireless network security standard. Sometimes erroneously called "Wireless Encryption Protocol". Weak algorithm used to encrypt wireless networks. Several serious weaknesses have been identified by industry experts such that a WEP connection can be cracked with readily available software within minutes. See WPA
WPA and **WPA2**	Acronym for “Wi-Fi Protected Access.” Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA.

Appendix A: Version Numbering Policy

Version number consists of 4 elements. Non-static elements are separated by ‘.’ (dot) symbol

The format is Fxx.yy.zzz where

- **F**: Static letter, does not change.
- **xx**: Major version (numeric values 01-99) Initial value is 01 The value is never reset within application lifecycle.
  The major version number is incremented in case of major changes to payment process, change that impacts security functionality. Requires a full PA-DSS assessment.
- **yy**: Minor version: (numeric values 01-99) Initial value is 01. The value is reset to ‘01’ if major version number is changed.
  The minor version number is incremented in case of large feature additions, terminal model additions, any cause of delta-assessment, partial audit, re-audit due to expiration etc.
- **zzz**: Wildcard / Revision. (numeric values 001 – 999). Initial value is 001. The value is reset if minor or major version number is changed.
  incremented in case of minor change which has impact on the application functionality but no impact on security or PA-DSS Requirements.

Appendix B: Terminal files

In table below represented list of files on the terminal what can contains any cardholder data

File Name	Description	Cardholders data	Protection
#STOREFWD	Transaction information pending to be sent to Authorization host	PAN, Expiry Date	Encrypted by terminal storage key
***.LOG**	Application activity trace. File name has format <Module_Name>.LOG	PAN	Masked (6 first + 4 last)
CURRTRANS	Current transaction data file. Used to track store transaction data at pre-defined checkpoints. Used for transaction recovery.	PAN, Expiry Date, Masked PAN	Encrypted by terminal storage key and/or DUKPT
LAST_RECEIPT	Last transaction receipt data. Used to print copy of last transaction receipt in PayPoint ECR Protocol the file contains all data required to build both merchant and cardholder receipts	PAN	Masked (6 first + 4 last) and/or Encrypted with DUKPT
LASTEMVTRAN	File used to generate last emv transaction report.	PAN	Truncation 6 and last 4 digits of
LASTTRAN	Last transaction data. Removed at successful completion of sequent transaction or successful close batch.	PAN, Expiry Date	Encrypted by terminal storage key and/or DUKPT
LOSTREC	File containing copy of transaction receipt data used to print lost receipt in LPP ECR protocol the file contains all data required to build both merchant and cardholder receipts	PAN	Masked (6 first + 4 last) and/or encrypted with DUKPT
TRANSLOG_V2	Transaction log data. Used for printing report of last transactions. Stores last 1000 transaction data as maximum. Wiped after software update.	PAN	Masked (6 first + 4 last)

Appendix C: Instances where PAN is displayed

Instance	Description	Protection
DISPLAY	Only during manual PAN entry dialogue.	none
CARDHOLDERS RECEIPT		Masked
MERCHANT RECEIPT		Masked
MERCHANT RECEIPT		Encrypted
Transaction Result Message to ECR	Only for PayPoint ECR Protocol (contained in Local Mode message)	Masked

Appendix D: Application components and used protocols

Hardware platform and OS supported:

Model Name	PCI PTS Approval #	OS required
Vx520	4-30052, 4-30050	QT520240, QTyy0500.xxxxxxxx
Vx675	4-10116	QT650253, QT650240, QTyy0500.xxxxxxxx
Vx680	4-20146, 4-30053	QT680240, QT6B0240, QTyy0500.xxxxxxxx
Vx690	4-30128	QT690263, QTyy0500.xxxxxxxx
Vx820	4-40053, 4-40054	QT820244, QT820240, QTyy0500.xxxxxxxx
Vx825	4-10107	QT830240, QTyy0500.xxxxxxxx

Terminal to Host protocol in use:

List of supported protocols available in application release notes.

Terminal to TMS protocol in use:

List of supported protocols available in application release notes.

Terminal to ECR protocol in use:

List of supported protocols available in application release notes.