PCI PA DSS Implementation Guide

MultiPOINT 03.20.072.xxxxx,
05.20.074.xxxxx,
06.20.075.xxxxx.

Version 3.6(Release)

Date: **2019-09-06**

Contents

1. Introduction

1.1. Purpose

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 Verifone MultiPOINT payment application in your business to store, process, or transmit payment card information, this standard and this guide apply to you.

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

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

http://www.pcisecuritystandards.org

This guide is updated whenever there are changes in MultiPOINT software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in the MultiPOINT 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.lv/

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

Note: This guide refers to MultiPOINT software versions on the PCI SSC 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 MultiPOINT application on that list, please contact our helpdesk at Verifone Baltic in order to upgrade your terminal.

http://www.pcisecuritystandards.org/

1.2. Document Use

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

Note 1: Both the System Installer and the 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 the ECR integrators/resellers at initial workshops.

1.3. References

(1) Payment Card Industry – Payment Application Data Security Standard v3.2
(2) Payment Card Industry – Data Security Standard v3.2.1
(3) Terminal Audit Log v1.8
(4) Verifone Baltic – Terminal Software Version Numbering Specification v1.4.1

1.4. Update History

Ver.	Name	Date	Comments
1.00	Sergejs Melnikovs	2010-04-08	Original version
1.01	Janis Grikis	2010-04-09	Reviewed
1.3	Sergejs Melnikovs	2010-06-09	Corrected according to GAP Analysis Report on April 27, 2010
1.4	Sergejs Melnikovs	2010-07-28	Correction according to GAP Analysis Report on July 23, 2010
1.5	Sergejs Melnikovs	2011-01-20	Correction according PA-DSS v1.2 requirement 4.2
1.6	Sergejs Melnikovs	2013-06-19	Annual review and update the document according to PA DSS version 2.0 requirements
1.7	Sergejs Melnikovs	2013-07-09	Added application version on title page
1.8	Sergejs Melnikovs	2013-07-17	Added notes about TMS in chapter 2
1.9	Sergejs Melnikovs	2014-07-18	Minor rework of the document according to MultiPOINT version 02.20.071. Added annex about version methodology
2.0	Sergejs Melnikovs	2015-06-15	Document rebranding. Updated according to PCI DSS & PCI PA DSS version 3.1 requirements
2.1	Sergejs Melnikovs	2015-07-09	Added description of connection initiation for integrated mode.
3.0	Sergejs Melnikovs	2016-01-09	Updated according to PCI DSS & PCI PA DSS version 3.2 requirements. Redesign content of the document to improve usability. Small minor editor changes.
3.1	Sergejs Melnikovs	2017-04-07	Added clarification related to PA DSS requirements 2.3.a, 3.1.a & 7.2.3
3.2	Sergejs Melnikovs	2018-07-06	- Added support for MultiPOINT version 05.20.074.xxxxx; - Added more clarification about key management; - Other minor editor changes.
3.3	Sergejs Melnikovs	2018-07-12	Added version of TLS used by applications, PAN masking scheme, updated list of terminal files (annex A1)
3.4	Sergejs Melnikovs	2018-07-16	Extended explanation about wireless communication supported by the applications.
3.5	Sergejs Melnikovs	2019-07-09	Added support for MultiPOINT version 06.20.075.xxxxx
3.6	Sergejs Melnikovs	2019-09-06	Updated according to QSA recommendations.

1.5. Terminology and abbreviations

3DES	Triple DES common name for the Triple Data Encryption Algorithm
AES	Advances encryption standard
Cardholder Data	PAN, Expiration Date, Cardholder Name and Service Code.
Security codes	F. ex. Card Verification Value, also called CVV2, 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.
ECR	Electronic Cash Register
HSM	Hardware security module
Magnetic Stripe Data	Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.
MultiPOINT Application	Terminal Payment Application for use in Baltic States (Estonia, Latvia, Lithuania)
MultiPOINT Terminal	Terminal with installed MultiPOINT Application
PCI 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.
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. Retailers that use applications to store, process or transmit payment card data are subject to the PCI DSS standard.
PCI PTS	Payment Card Industry PIN Transaction Security
PED	PIN Entry Device
POS	Point of sale
Sensitive Authentication Data	Magnetic Stripe Data, Security Codes, PINs/PIN-block.
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.
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. In this document TLS refers on TLS version 1.2
TMS	Terminal management system
TRSM	Tamper resistant security module
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"
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.

2. SUMMARY OF PCI DSS REQUIREMENTS

This summary provides basic overview of the PCI PA-DSS requirements that have a related to Implementation Guide topic. It also explains how each requirement is handled on the MultiPOINT application side and required actions for you (as a customer).

The complete PCI DSS and PA-DSS documentation can be found at:

http://www.pcisecuritystandards.org

Note: If TMS is used as part of an authenticated remote software distribution framework for the PED, it should be evaluated by a QSA as part of any PCI DSS assessment.

2.1. PA-DSS Req. 1.1.4: Historical data deletion

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	
How MultiPOINT application meets this requirement	No specific setup for MultiPOINT application is required. New version of MultiPOINT application does not use any cardholder's sensitive historical data collected by previous version of the application. On installation, MultiPOINT application performs secure wipe for all terminal's NVRAM memory, which is available for custom application files.
merchant/reseller actions required	You must make sure that historical data (track or track equivalent data, cardholder data or Security codes) are removed from all other storage devices used in your systems, ECRs, PCs, servers etc. For further details please refer to your vendor. Removal of sensitive authentication data is absolutely necessary for PCI DSS compliance.

Aligns with PCI DSS Requirement 3.2

2.2. PA-DSS Req. 1.1.5: Securely delete any sensitive authentication data used for debugging or troubleshooting

Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	
How MultiPOINT application meets this requirement	No any sensitive cardholder's data are retrieving by MultiPOINT application in Verifone 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.
merchant/reseller actions required	As the application doesn't provide capability to collect sensitive authentication data the merchant/reseller is not required to take any action in relation to this requirement. If by some unexpected case the sensitive authentication data become in possession of merchant/reseller than they should follow this instruction: • Collect sensitive authentication only when needed to solve a specific problem. • Store such data only in specific, known locations with limited access. • Collect only the limited amount of data needed to solve a specific problem. • Encrypt sensitive authentication data while stored. • Securely delete such data immediately after use.

Aligns with PCI DSS Requirement 3.2

2.3. PA-DSS Req. 2.1: Purging cardholder data

Securely delete cardholder data after customer-defined retention period.	
How MultiPOINT application meets this requirement	All cardholder data is automatically erased during the nightly batch sending or if manual batch sending is done. See the list of files in the Annex *A1 Terminal files*
merchant/reseller actions required	All cardholder data is automatically erased according to batch sending configuration on MultiPOINT terminal. If you want, you can send batch manually. If the terminal prints full PAN on merchant ticket, please securely protect the merchant receipts/data and securely delete them after retention period in accordance with PCI DSS Requirements. Such protection is absolutely necessary for PCI DSS compliance.

Aligns with PCI DSS Requirement 3.1

2.4. PA-DSS Req. 2.2: Mask PAN when displayed

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) so only personnel with a business need can see the full PAN.	
How MultiPOINT application meets this requirement	Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts are available in Annex *A3 Instances where PAN is displayed*.
merchant/reseller actions required	If the terminal prints full PAN on merchant ticket, please securely protect the receipts in accordance with PCI DSS Requirement 3.3 and ensure that the data available only to personnel with a legitimate business need can see the full PAN.

Aligns with PCI DSS Requirement 3.3

2.5. PA-DSS Req. 2.3: Render PAN unreadable anywhere it is stored

Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). The PAN must be rendered unreadable anywhere it is stored, even outside the payment application (for example, log files output by the application for storage in the customer environment)	
How MultiPOINT application meets this requirement	PAN is stored encrypted of truncated. The list of such files and the method of protection can be found in Annex 1. Truncation is First 6, Last 4. Not configurable. Encryption is AES 128-bit. Not configurable.
merchant/reseller actions required	The customer is responsible for rendering PAN unreadable in all instances where a PAN could be stored in outside of MultiPOINT application.

Aligns with PCI DSS Requirement 3.4

2.6. PA-DSS Req. 2.4: Protect keys

Protect keys used to secure cardholder data against disclosure and misuse. Access to keys used for cardholder data encryption must be restricted to the fewest possible number of key custodians. Keys should be stored securely.	
How MultiPOINT application meets this requirement	Cryptographic keys used to encrypt cardholder data stored inside tamper-protected memory area of terminals. Tamper protected memory area protection implemented according to PCI PTS requirements.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.5

2.7. PA-DSS Req. 2.5: Implement key management processes and procedures

Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	
How MultiPOINT application meets this requirement	There is no any possibility to manage the keys directly on the terminal. All key generation and delivery implemented according to PCI requirements. MultiPOINT application is designed to use TLS 1.2 or TLS 1.1 (secure configuration in accordance with NIST SP 800-52 rev 1) communication channel encryption. Cardholder data stored in terminal memory is encrypted by key that is automatically generated and periodically updated by the application without any user intervention. Key management is briefly described in chapter *MultiPOINT application key management* of this document.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.6

2.8. PA-DSS Req. 2.6: Provide a mechanism to render irretrievable any cryptographic key material

Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.	
How MultiPOINT application meets this requirement	MultiPOINT application is designed to use TLS 1.2 or TLS 1.1 (secure configuration in accordance with NIST SP 800-52) communication channel encryption. Cardholder Data or Sensitive Authentication Data that are sent to host during authorization are encrypted by key residing only within authorization systems HSM and protected memory of a terminal. Cardholder Data stored in terminal memory is encrypted by key that is automatically generated and periodically updated by the application without any user intervention. All cryptographic material must be removed before new version of payment application deployed into the terminal. The removal of this material is automatically handled by the MultiPOINT application, so you do not need to take any action. New version of MultiPOINT application does not use any encrypted historical data collected by previous version of the application Key management is briefly described in chapter *MultiPOINT application key management* of this document.
merchant/reseller actions required	Please be sure that you use valid TLS certificate of the acquirer. When the certificate close to be expired replace it by new one according to acquirer policy.

Aligns with PCI DSS Requirement 3.6

2.9. PA-DSS Req. 3.1: Unique user IDs and secure authentication

Use unique user IDs and secure authentication for administrative access and access to cardholder data.	
How MultiPOINT application meets this requirement	This requirement cannot be applied to the payment MultiPOINT application because there is no user login for the payment application itself. It runs on a Hardware terminal without requiring an operator or admin login.
merchant/reseller actions required	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 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.

Aligns with PCI DSS Requirement 8.1 and 8.2

2.10. PA-DSS Req. 3.2: Unique user IDs and secure authentication for access to servers etc.

Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	
How MultiPOINT application meets this requirement	MultiPOINT application does not provide functionality and does not maintain user accounts for administrative access or individual access to cardholder data.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.1 and 8.2

2.11. PA-DSS Req. 4.1: Implement automated audit trails

Implement automated audit trails.	
How MultiPOINT application meets this requirement	MultiPOINT application has an Audit Trail logging functionality. This log may contain truncated PANs. No cardholder data is accessible from the MultiPOINT terminal. The application also keeps an Audit Trail to track changes to system level objects.
merchant/reseller actions required	The application uses syslog protocol for audit trails. If you need to receive this data on your syslog server too please follow description in *(3)Terminal Audit Log v1.8.*

Aligns with PCI DSS Requirement 10.1

2.12. PA-DSS Req. 4.4: Facilitate centralized logging

Facilitate centralized logging.	
How MultiPOINT application meets this requirement	The MultiPOINT application provides ability to collect/analyze logging information by sending log files to remote host. The log file has syslog format and described in separate document *(3)Terminal Audit Log v1.8*.
merchant/reseller actions required	The application uses syslog protocol for audit trails. If you need to receive this data on your syslog server too please follow description in *(3)Terminal Audit Log v1.8.*

Aligns with PCI DSS Requirement 10.5.3

2.13. PA-DSS Req. 5.4.4: Application versioning methodology

Implement and communicate application versioning methodology.	
How MultiPOINT application meets this requirement	Detailed description of version numbering methodology available in Annex *A2 Application Version Numbering policy* of the implementation guide.
merchant/reseller actions required	The merchant/reseller needs to understand which version of the payment application they are using, and ensure validated versions are in use.

2.14. PA-DSS Req. 6.1: Securely implement wireless technology

Securely implement wireless technology. For payment applications using wireless technology, the wireless technology must be implemented securely.	
How MultiPOINT application meets this requirement	MultiPOINT application is designed to operate in a network behind a firewall. If wireless is used the MultiPOINT application supports only strong encryption (WPA/WPA2).
merchant/reseller actions required	If you are using wireless network within your business, you must make sure, that firewalls are installed, what deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the MultiPOINT application environment. Please refer to your firewall manual.

Aligns with PCI DSS Requirements 1.2.3 & 2.1.1

2.15. PA-DSS Req. 6.2: Secure transmission of cardholder data over wireless networks

Secure transmissions of cardholder data over wireless networks. 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.	
How MultiPOINT application meets this requirement	If wireless is used the MultiPOINT application supports only strong encryption (WPA/WPA2). First time setup wireless parameters according to description in chapter *4 MultiPOINT application wireless configuration.* After initial setup, type of wireless encryption could be changed only through TMS. It is no possible to assign PCI DSS non-compatible wireless connection type.
merchant/reseller actions required	For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. For other actions please refer to action required part of chapter *2.16 PA-DSS Req. 6.3: Provide instructions for secure use of wireless technology.*

Aligns with PCI DSS Requirement 4.1.1

2.16. PA-DSS Req. 6.3: Provide instructions for secure use of wireless technology

Provide instructions for secure use of wireless technology.	
How MultiPOINT application meets this requirement	MultiPOINT application is designed to operate in a network behind a firewall. If cases where wireless is used the MultiPOINT application supports only strong encryption (WPA/WPA2).
merchant/reseller actions required	If you are using wireless network within your business, you must make sure, that firewalls are installed, what deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the MultiPOINT 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 Initial setup of wireless parameters for MultiPOINT application described in chapter *4 MultiPOINT application wireless configuration.*

Aligns with PCI DSS Requirements 1.2.3, 2.1.1, & 4.1.1

2.17. PA-DSS Req. 7.2.3: Instructions for customers about secure installation and updates

Provide instructions for customers about secure installation of patches and updates.	
How MultiPOINT application meets this requirement	MultiPOINT application facilitates secure update functionality by downloading updates directly from the management server, verifying integrity and authenticity of the update through digital signatures and applying updates to the terminal when it's not in use. Once a security patch or an update of MultiPOINT application released by Verifone, our Product Manager notifies by email (or via phone call) the 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 agreed on in advance with the integrator/reseller.
merchant/reseller actions required	The merchant is not required to take any action in relation to this requirement because MultiPOINT once per 24h connects to management server and downloads a new version of the application if that command received from the server. There is also possibility to initiate application update from the terminal menu: **Service→Parameters→Download→Programs→Phone→Full** The integrator/reseller which provides management server service to the customer should configure the management server to deliver patches and updates to MultiPOINT terminal once it's received from Verifone according to PCI DSS required timeframe.

2.18. PA-DSS Req. 8.2: Must only use secure services, protocols and other components

Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	
How MultiPOINT application meets this requirement	MultiPOINT application does not employ unnecessary or insecure services or functionality. Full list of application components and dependent components / protocols described in Annex *A4 Application components and used protocols*
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.2.3

2.19. PA-DSS Req. 9.1: Store cardholder data only on servers not connected to the Internet

Store cardholder data only on servers not connected to the Internet.	
How MultiPOINT application meets this requirement	MultiPOINT does not have any server component.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 1.3.7

2.20. PA-DSS Req. 10.1: Implement two-factor authentication for remote access to payment application

Implement two-factor authentication for all remote access to payment application that originates from outside the customer environment.	
How MultiPOINT application meets this requirement	MultiPOINT application does not provide the functionality and does not maintain user accounts for any remote access to the application.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.3

2.21. PA-DSS Req. 10.2.1: Securely deliver remote payment application updates

Securely deliver remote payment application updates. 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	
How MultiPOINT application meets this requirement	MultiPOINT application facilitates secure update functionality by downloading updates directly from the management server, verifying integrity and authenticity of the update through digital signatures and applying updates to the terminal when it's not in use. Connection to the management server initiated by the MultiPOINT terminal according to configuration.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 1 and 12.3.9

2.22. PA-DSS Req. 10.2.3: Securely implement remote access software

Securely implement remote-access software.	
How MultiPOINT application meets this requirement	MultiPOINT application does not provide remote access functionality and does not maintain user accounts for any remote access to the application.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 2, 8 and 10

2.23. PA-DSS Req. 11.1: Secure transmissions of cardholder data over public networks

Secure transmissions of cardholder data over public networks.	
How MultiPOINT application meets this requirement	All Cardholders Data and Sensitive Authentication Data sent to and from the MultiPOINT application over public networks always protected using TLS v1.1 or TLS v1.2 encryption protocol.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.1

2.24. PA-DSS Req. 11.2: Encrypt cardholder data sent over end-user messaging technologies

Encrypt cardholder data sent over end-user messaging technologies. 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.	
How MultiPOINT application meets this requirement	MultiPOINT application doesn't use any end-user messaging technologies to send cardholder data.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.2

2.25. PA-DSS Req. 12.1, 12.1.1 and 12.2: Secure all non-console administrative access

Encrypt non-console administrative access. Use multi-factor authentication for all personnel with non-console administrative access.	
How MultiPOINT application meets this requirement	MultiPOINT application does not provide non-console access functionality and does not maintain user accounts for any administrative access to the application.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.3

3. MultiPOINT application key management

3.1. Stored CHD protection

Key management is performed automatically by the MultiPOINT application without any user interaction. MultoPOINT doesn't require any key injection operations from the outside. A 3DES or AES key is used for encryption. The key is generated and stored in the POS TRSM and never leaves the POI.

- The key is generated by the terminal's operating system.
- The encryption key is stored in tamper resistant secure module's memory of the terminal.
- MultiPOINT 03.20.072.xxxxx uses double length 3DES(112 bit) key.
- MultiPOINT 05.20.074.xxxxx and version 06.20.075.xxxxx use AES-128 for CHD encryption on the terminal.
- Key transmission is not required.
- 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 to make any payment transaction, only service functions are allowed. Before a new key generation, the old key is destroyed and cryptographic material is removed.
- If for some reason the application or terminal is not able to send the batch for a time longer than 30 days, then the application doesn't allow to make a new payment transaction without sending the batch.

3.2. Online PIN key management

Name	Type	Purpose
TPK	DUKPT (2TDES) 112bit	**Terminal PIN Key.** The key used for Online PIN encryption on the terminal. Terminal sends encrypted data to authorization host.

Each MultiPOINT terminal equipped by unique TPK.

3.2.1. Key distribution process

TPK derived from BDK in Verifone secure room, wrapped by terminal unique RSA key and as a payload delivered to the terminal over Terminal Management System. Once the terminal receives the payload, decrypts and verifies the signatures of the keys and only after successful verification installs the new key into the secure memory. Secure memory is protected by PCI PTS certified TRSM hardware module of the terminal.

Cryptographic keys should never be conveyed in the following ways:

- Dictating verbally keys or components
- Recording key or component values on voicemail
- Faxing, e-mailing, or otherwise conveying clear-text secret or private keys or components over end-user messaging technologies
- Conveying clear-text private or secret keys or their components without containing them within tamper-evident, authenticable packaging
- Writing key or component values into start-up instructions
- Taping key or component values to or inside devices
- Writing key or component values in procedure manuals

All key-encryption keys used to encrypt for transmittal or conveyance of other cryptographic keys must be at least as strong as the key being sent. The table below defines keys of equivalent strengths:

Algorithm	TDEA	RSA	Elliptic Curve	DSA/D-H	AES
Minimum key size in number of bits:	112	1024	160	1024/160	-
	168	2048	224	2048/224	-
	-	3072	256	3072/256	128
	-	7680	384	7680/384	192
	-	15360	512	15360/512	256

4. MultiPOINT application wireless configuration

MultiPOINT application supports the following wireless configurations:

MultiPOINT version	Terminal models	Wireless communication types
03.20.072.xxxxx	Vx675, Vx680	Wi-Fi, Mobile (GPRS)
05.20.074.xxxxx	V240m, V400m	Wi-Fi, Mobile (GPRS/3G/4G)
06.20.075.xxxxx	V200c, V200t, V240m, V400m	Wi-Fi, Mobile (GPRS/3G/4G)

Note: SNMP community string isn't supported by MultiPOINT application.

4.1. Wi-Fi configuration

On the terminal enter into "**Service**" menu and go to **Parameters / Edit / TCP/IP Parameters / WiFi parameters**. There you have possibility to configure the following parameters:

Parameter	Description
Print	Print Wi-Fi configuration on the paper.
SYSID	Setup Service Set Identifier, setup according to Wi-Fi network you are going to connect the terminal.
WPA Mode(*)	5 – WPA, 8 – WPA2
WPA Key	Setup Pre-Shared Key for SYSID of the network.

(*) – this parameter configurable in MultiPOINT 03.20.072.xxxxx. MultiPOINT 05.20.074.xxxxx & 06.20.075.xxxxx supports only WPA2 security algorithms.

4.2. GPRS/3G/4G configuration

On the terminal enter into "**Service**" menu and go to **Parameters / Edit / GSM parameters**. There you have possibility to configure the following parameters:

Parameter	Description
GSM card's PIN	PIN code of SIM card
Operator selection	Under this item you have two choices: Manual or Automatic setup mobile network provider.
APN	Setup the Access Point Name according to mobile network you are going to connect the terminal to.

Annexes

A1 Terminal files

In a table below represented list of files on the terminal what can contains any cardholder data or logs of important events from the terminal.

File Name	Description	Cardholders data	Protection
FILEREVERSALLIST.LST	Payment list queue for cancellation	PAN & Expiry date	AES 128-bit
FILETRANSSETUP.CFG	Last payment data and batch counters	PAN & Expiry date	AES 128-bit
FILETRANSSETUP.CPY	Last payment data and batch counters, backup copy	PAN & Expiry date	AES 128-bit
FILETRANSLIST.LST	24h Payment list	PAN & Expiry date	AES 128-bit
FILETRANSLIST.CPY	24h Payment list, backup copy	PAN & Expiry date	AES 128-bit
FILEPREAUTHLIST.LST	Pre-authorization list	PAN & Expiry date	AES 128-bit
FILEGOODSLIST.LST	Payment details for goods payments	PAN	AES 128-bit
FILELASTTRANS.DAT	Last transaction record	PAN & Expiry date	AES 128-bit
FILETMPTRANS.DAT	Information about unfinished transactions (for ECR requests processing)	PAN & Expiry date	AES 128-bit
TRANS_.....TXT	Payment statistics	Truncated(*) PAN & Expiry date	
DEBUG.LOG	Application debug information	Truncated(*) PAN & Expiry date	
TRACE.LOG	Transaction errors and speed measurement log	Truncated(*) PAN & Expiry date	
STATS.LOG	Communication statistics log		
ERROR.LOG	Application Error event log		
SYS.LOG	Audit log		
*.TRACE	Transaction errors and speed measurement logs. Compressed	Truncated(*) PAN & Expiry date	
*.SRZ	Archive for sending to terminal management system, contains compressed log files	Truncated(*) PAN & Expiry date	
PRINTCOPYDEALOYAL.LST	“Dealoyal” receipt copy (loyalty bonus points)	Truncated(*) PAN	
BATCH_MON_x.TXT	List of unsent transactions, where “x” is acquirer index (0-6)	Truncated(*) PAN	

(*) Truncation method: First 6, last 4.

A2 Application Version Numbering policy

Below represented MultiPOINT application version numbering methodology what is based on common Verifone Baltic version numbering policy for terminal payment applications (reference *(4) Verifone Baltic – Terminal Software Version Numbering Specification v1.4.1*)

Application version numbering format:

<NNNNNNNNNN> <XX>.<YY>.<ZZZ> .<BBBBB>, where :

Format	Subject	Description
NNNNNNNNNN	Software Name;	Name of the application
XX	Major application version number	This version number indicates the major version of the payment application. It is increased every time, when major changes are done, according to PA-DSS rules. Number is never restarted within the application life cycle
YY	Payment application identifier	Number is attached to a combination of particular payment application and “major” (from PA-DSS prospective) payment functionality. For current application it has fixed value: 20 - MultiPOINT payment application, main configuration;
ZZZ	Minor application version number	This number is increased every time some changes to the functionality of the application are done, which are not considered “major” by PA-DSS rules for payment application. Number can be (but not mandatory should be) restarted, when “Payment application major version number” or “Payment application identifier” is changed. In cases, when changes contain only bug fixes of existing functionality, but functionality itself isn’t changed, minor application number should not be increased
BBBBB	build number	Increased every time, when new software package is created, even on minor bug fixes, when no changes to neither version numbers are made. Number is never restarted during the application life cycle. Should mandatory present, but should not be mandatory presented to external parties, when indicating application version. If a new package contains changes what could be classified as Low-impact or High-impact from PA-DSS prospective than together with build number other relevant part of version number MUST be changed

Example: let’s look on MultiPOINT 03.20.072.00390:

MultiPOINT	Software Name;
03	Major application version number
20	Payment application identifier
072	Minor application version number
00390	build number

A3 Instances where PAN is displayed

Below represented instances where MultiPOINT application can show cardholders data:

Instance	Description	Protection
DISPLAY	Manual PAN entry dialog	none
	Voice authorization dialog	none
CARDHOLDERS RECEIPT (terminal printer and/or ECR protocol)		Masked(*)
MERCHANT RECEIPT (terminal printer and/or ECR protocol)	Regular transaction	Masked(*)
	Offline transaction(**)	none
	Pre-authorization(**)	none
Preauthorization's list receipt (terminal printer and/or ECR protocol)		Masked(*)
Last EMV transaction parameters receipt (terminal printer and/or ECR protocol)		Masked(*)
ECR protocol: transaction result message	Regular transaction	Masked(*)
	Offline transaction	none
	Pre-authorization	none

(*) - the first six and last four digits are the maximum number of digits to be displayed

(**) – due to an acquirer requirement and only when configured by a terminal service provider over TMS for particular merchant.

A4 Application components and used protocols

Hardware platform and OS supported:

MultiPOINT 03.20.072.xxxxx

Model Name	PCI PTS Approval #	OS Required
Vx805	4-10106	QT850240, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx
Vx675	4-10116	QT650240, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx
Vx680	4-20146, 4-30053	QT680240, QT6G0240, QT6B0240, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx
Vx820	4-40053, 4-40054	QT820240, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx
Vx520	4-30050, 4-30052	QT520240, QT5G0240, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx
Ux300 + Ux100 + Ux400	4-20259	30070600
Vx700 + SCR710	4-20095, 4-20077, 4-20096	QH0011A1
Vx510	4-30014	QA0012A2
Vx570	4-10004	QC0011A2
Vx610	4-30015	QB0111A2
Vx670	4-40005	QD0012A5
Vx810	4-30019	QG0012A2

MultiPOINT 05.20.074.xxxxx

Model Name	PCI PTS Approval #	OS Required
V200c, V200c Plus, V200c CTLS	4-30182, 4-30323	VAULT: 7.x.x AppM: 11.x.x VFSRED: 7.x.x VFOP: 1.x.x
V240m, V240m Plus 3GBWC	4-80023	
V400m	4-30260	
P200/P200 Plus	4-10196, 4-10238	
P400/P400 Plus	4-10191, 4-10239	

MultiPOINT 06.20.075.xxxxx

Model Name	PCI PTS Approval #	OS Required
V200c, V200c Plus, V200c CTLS	4-30323	VAULT: 8.x.x AppM: 12.x.x VFSRED: 9.x.x VFOP: 1.x.x
V200t	4-10227	
V240m, V240m Plus 3GBWC	4-80023	
V400m	4-30260	
P200/P200 Plus	4-10196, 4-10238	
P400/P400 Plus	4-10239	
Ux300 (Ux100&Ux400)	4-20299	VAULT: 14.x.x AppM: 10.x.x VFSRED: 7.x.x VFOP: 7.x.x
Ux410	4-20297	

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.