Implementation Guide

MultiPOINT 07.20.076

Version 1.0
Date: **2022-09-15**

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 Secure Software Standard (PCI SSS). In order to facilitate a PCI DSS assessment, the Verifone software application has been approved by PCI to comply with the PCI SSS requirements.

Note: This guide refers to MultiPOINT software versions on the PCI SSC web site “List of Validated Payment Software” that have been validated in accordance with PCI SSS. If you cannot find the version of your MultiPOINT application on that list, please contact Verifone helpdesk in order to upgrade your terminal.

http://www.pcisecuritystandards.org/

1.2. Document Use

This Implementation Guide contains information for proper use of the Verifone MultiPOINT payment application. Verifone 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 integrators/resellers at initial workshops.

1.3. References

(1) Payment Card Industry – Software Security Framework
(2) Payment Card Industry – Secure Software Standard
(3) Payment Card Industry – Data Security Standard
(4) Terminal Vendor PCI PTS POI Security Policy
(5) Terminal Audit Log
(6) PKI MANAGEMENT PROTOCOL FOR PKK

1.4. Update History

Ver.	Name	Date	Comments
1.0	Sergejs Melnikovs	2022-09-15	First version

1.5. Terminology and abbreviations

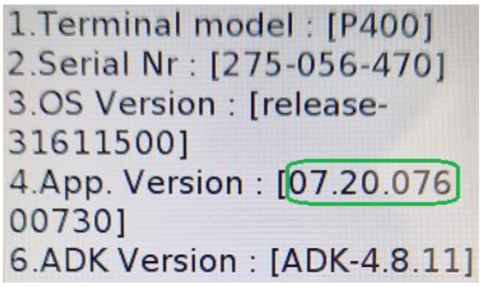
3DES	Triple DES common name for the Triple Data Encryption Algorithm
AES	Advances encryption standard
Cardholder Data	PAN, Expiration Date, Cardholder Name and Service Code.
Security codes	Card Verification Value, also called CVV2, is a three or four digit value printed on the back of the card but not 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 SSF	Payment Card Industry Software Security Framework. A collection of software security standards that leverage a common validation and certification model.
PCI SSS	Payment Card Industry Secure Software Standard ensure that payment software is designed, engineered, developed, and maintained in a manner that protects payment transactions and data, minimizes vulnerabilities, and defends itself from attacks.
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 and other in according to PCI standards.
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. How to verify MultiPOINT PCI compliance

Please visit https://www.pcisecuritystandards.org, go to "Validated Payment Software" (you can find it under "Products & Solutions Listings") or use direct link:

https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_software?agree=true

Find MultiPOINT application in the list and compare published version number with version of the application on your terminal. On the terminal press key combination: *** 0 #** and you will see application's details like on picture below:



```
1.Terminal model : [P400]
2.Serial Nr : [275-056-470]
3.OS Version : [release-
31611500]
4.App. Version : [07.20.076
00730]
6.ADK Version : [ADK-4.8.11]
```

Please also follow Hardware Identification steps of ***Terminal Vendor PCI PTS POI Security Policy (4)*** to validate PCI PTS compliance of the hardware product.

3. What should you know about MultiPOINT application

MultiPOINT terminal is not providing any option to the user to pause or disable security settings or parameters within the installed environment. Users are also not able to configure retention periods of sensitive data transient or otherwise. This storage is governed by the application in terms of the transaction processing requirements.

MultiPOINT application has implemented security controls to mitigate software attacks. The application registers any suspicious activity into an audit log. Details about the audit log functionality can be found in the configuration chapter of this document.
Additionally, please follow *Error! Reference source not found.* in this document and ***Terminal Vendor PCI PTS POI Security Policy (4)***

MultiPOINT application works on isolated user space of the terminal with sufficient privileges to serve all necessary functionality and doesn't provide any possibility to change the privileges for the application on the terminal.

Initial software loading to the terminal must be done by an authorized TSP engineer. Future software releases and updates are delivered automatically over TMS in a secure manner and fully controlled from the TMS.

MultiPOINT terminal doesn't support the installation of any third-party software. All payment functionality is provided by MultiPOINT application.

MultiPOINT application doesn't provide a non-console access to the POI. Only channel for processing data is the transaction processing to the host which takes place over a TLS encrypted channel or over other communication protocol described in Annex *A3 Application components and used protocols*

Access to MultiPOINT terminal user space is password protected by POI firmware. The firmware is PCI PTS approved and has brute force protection in place. Default password is changed by Verifone. If you are TSP who should have access to the POI user space, it's strongly recommended to use maximally allowed length for the password. The password must be kept secure and be shared only to authorized individuals.

Under certain circumstances, MultiPOINT application can be configured to print clear-text PAN if required. This configuration can only be performed by Verifone via the TMS and requests should be made formerly to the Verifone representative in order to perform such a configuration. The printing of clear-text PAN can only be done on POI devices that have an integrated printer as the MultiPOINT application cannot share clear-text PAN via its logical interfaces with other software. In such cases, the customer should secure the paper receipts containing clear-text PAN in accordance with PCI DSS requirements and a retention period should be clearly defined and implemented based on solid business requirements.

4. MultiPOINT application configuration

MultiPOINT application does not need any specific configuration on the terminal. All necessary configurations are provided over TMS and controlled by the TMS. All that is needed is:

- keep terminal installed behind of firewall (where it's possible)
- configure network to provide outgoing traffic from the terminal to external host needed by the configuration. Contact your Verifone representative to get all necessary details (IP/Port etc.) for the network setup.

4.1. Wireless configuration

MultiPOINT application supports the following wireless configurations:

MultiPOINT version	Terminal models	Wireless communication types
07.20.076	V200c, V200t, V240m, V400m	Wi-Fi, Mobile (GPRS/3G/4G)

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

4.1.1. 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	8 – WPA2
WPA Key	Setup Pre-Shared Key for SYSID of the network.

4.1.2. 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.

4.2. Activity logs configuration

MultiPOINT application automatically logs activity of accessing and using of sensitive data on the terminal without disclosure of the data. There is no sensitive data in the log. PTS firmware protects the integrity of log data internally in the firmware while it's present on the terminal. The log is regularly uploaded to the TMS. Contact Verifone Helpdesk If you need the logs.

Also, there is an option to collect the audit logs from MultiPOINT terminal on your environment. MultiPOINT utilizes syslog protocol RFC3164. Events and information collected by the terminal audit log is described in ***Terminal Audit Log (5)***

4.2.1. How to configure Syslog

Enter "Batch menu" -> Log sending -> Sys Log -> Edit

Terminal will prompt to confirm/enter several parameters one-by-one, if parameter is correct press Enter and next parameter will be displayed.

If parameter needs to be corrected press Cancel and enter correct value.

Parameters can be entered for two different hosts for main and for backup. if connection to main host fails then the terminal will try to connect the backup host.

Parameters to configure:

- **Phone ID** - host ID (0 - main host, 1 **-** backup host)
- **Number** - IP address and port separated with "," (eg:"192.168.1.7,1468")
- **X25 Address** – must be empty
- **Format** - choose TCPIP
- **Timer A** - send timeout (seconds)
- **Timer C** - receive timeout (seconds)
- **Dial time** - connection timeout (seconds)
- **ConxProtocol** - choose "Sys Log"

4.2.2. How to send Syslog

Enter "Batch menu" -> Log sending -> Sys Log -> Send Log

5. MultiPOINT application key management

5.1. Stored sensitive data protection

For stored sensitive data on the terminal, DEK is used.

Name	Type	Purpose
DEK	AES 128bit	**Data Encryption Key.** The key used for encryption sensitive data stored on MultiPOINT terminal.

Key management is performed automatically by the MultiPOINT application without any user interaction. MultiPOINT doesn't require any key injection operations from the outside. AES-128 key is used for encryption. The key is generated and stored in the Terminal TRSM (Which is a certified PCI PTS device) and never leaves the device.

Additional keys can m be used by the application when implemented with specific protocols and details of how these keys are managed can be found in the following documentation *PKI MANAGEMENT PROTOCOL FOR PKK (6)*

- 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.
- AES-128 is used for sensitive data encryption stored 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 and only service functions are allowed. Before a new key generation, the old key is destroyed and cryptographic materials are removed automatically by the MultiPOINT application.
- 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 a new payment transaction to be made without sending the batch.

5.2. 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.

5.2.1. Key distribution process

Key Loading is the process where keys are injected into terminals. A KLD (Key Loading Device) is used to securely inject a unique RSA key pair to a Key Receiving Device (KRD). Key load is performed at a secure site or remotely from a secure site by using Verifone's VeriShield Remote Key (VRK) product.

Unique RSA key pair is injected into the Terminal by using PCI compliant environment. All keys residing on the terminal are VeriShield Retain signed. The loading of the terminal RSA specific signed key pair is performed in secure room and is intended to be a one-time operation. However, if the Terminal is sent to the repair center a new terminal RSA specific signed key pair is performed in secure room The RSA key is static and fixed for terminal life. The RSA Key update requires loading in a secure room under the secure key loading procedure.

TPK derived from BDK in Verifone secure room, wrapped by the terminal unique RSA key and as a file delivered to the terminal over Terminal Management System.

Once the terminal receives the file, 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. The public key infrastructure supporting this key exchange is maintained by the Verifone Certificate Authority(CA). The CA infrastructure involves the secure injection of key pairs into the POI device withing a Key Injection Facility and allows for the secure authentication of keys aligned with PCI Security Standards such as PCI P2PE and PCI PIN Security.

5.3. TLS keys and certificates

Any connection from MultiPOINT terminal to an external host is TLS protected.
Initially terminal receives TMS related unique TLS key pair and certificates from Certificate Management System. On the next step the terminal connects to TMS and receives other TLS keys and certificates according for external host which is configured to this terminal on TMS database.

6. MultiPOINT application update

Before upgrading/downgrading the software on a terminal, the new software is bundled into a single TGZ/TAR file. The TGZ/TAR file can contain multiple files. Each of the files is signed by Verifone Sponsor Certificate and additionally has a signature file with the same name and extension p7s. MultiPOINT application package is always signed by Verifone authorized security officers under dual control.
Signed package can be delivered to the terminal remotely via TMS or TSP authorized engineer can load the software via cable connected to the terminal using software loading application running on local machine.
Terminal authenticates the application package and any configuration files received using the Verifone terminal Cert chain provided by the POI device firmware. If there is no signature or the signature validation fails, the package will be rejected by the terminal.

Annexes

A1 Application Version Numbering policy

Below represented MultiPOINT application version numbering methodology

Application version numbering format:

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

Format	Subject	Description
NNNNNNNNNN	Software Name;	Name item of version naming and numbering is self-explaining of the software.
XX	Major application version number	This version number indicates the major version of the payment application. It is increased every time a major change that triggers High-impact Change PCI SSF criteria. 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 PCI SSF perspective) 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 don't trigger High-impact Change PCI SSF criteria for the payment application. Number can be (but not mandatory should be) restarted, when “Payment application major version number” or “Payment application identifier” is changed. These changes can be considered as Low or No Impact.

Example: let’s look on MultiPOINT 07.20.076:

MultiPOINT	Software Name;
07	Major application version number
20	Payment application identifier
076	Minor application version number

A2 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)	Regular transaction	Masked(*)
	Offline transaction	Masked(**)
	Pre-authorization	Masked(**)
MERCHANT RECEIPT (ECR protocol)		Masked(*)
Preauthorization's list receipt (terminal printer and/or ECR protocol)		Masked(*)
Last EMV transaction parameters receipt (terminal printer and/or ECR protocol) **ECR protocol: transaction result message**		Masked(*)

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

(**) – by default, the first six and last four digits are displayed. Could be configured to print clear-text full PAN

A3 Application components and used protocols

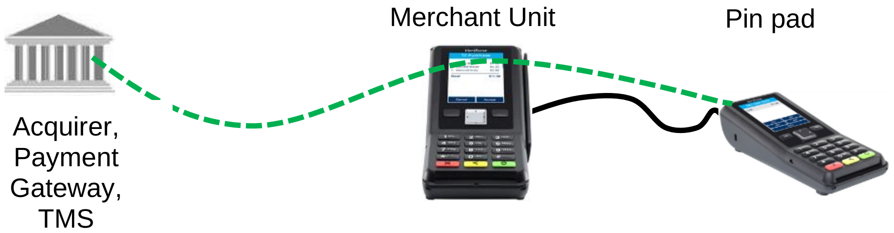
Hardware platform and OS supported:

MultiPOINT 07.20.076

Model Name	PCI PTS Approval #	OS Required
V200c, V200c Plus, V200c CTLS	4-30323	Vault 11.1.6.16106 AppM 15.2.16.16116 VFSRED 12.1.1.16101 OP 2.0.1
V200t	4-10227	
V240m, V240m Plus 3GBWC	4-80023	
V400m	4-30260	
P200/P200 Plus	4-10238	
P400/P400 Plus	4-10239	
Ux300 (Ux100&Ux400)	4-20353	Vault 19.1.2.16102 AppM 12.2.9.16109 SRED 12.0.03 OP 8.0.1
Ux410	4-20353	

Optional Component

MultiPOINT has an optional Merchant Unit component to work in integrated mode. In this mode the MultiPOINT terminal works as a pin pad on the customer side and to the merchant faced Merchant Unit device which allows to start a transaction, shows operation progress to the merchant, print a receipt. Also, Merchant Unit used as card entry mode for manual card entry and magnetic swipe transaction.



These two devices are RS232 cable connected and utilize ECR protocol for the communication. MultiPOINT terminal plays a master role in the payment solution, controls Merchant Unit's screens, interacts with external systems. In communication to an external host Merchant Unit device provides TCP/IP connection and on top of that MultiPOINT application applies data protection (TLS, data encryption, etc.), that way the Merchant Unit plays a "router" role without possibility to impact on the data transferred in between the pin pad and the host.

As a Merchant Unit could be used one of the following devices:

Model Name	PCI PTS Approval #	OS Required
V200c, V200c Plus, V200c CTLS	4-30323	Vault 11.1.6.16106 AppM 15.2.16.16116 VFSRED 12.1.1.16101 OP 2.0.1
V200t	4-10227	

The Merchant Unit software couldn't work independently from MultiPOINT terminal.

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.

Terminal to Merchant Unit protocol in use:

List of supported protocols available in application release notes.