Implementation Guide

paypoint version 5.08.xx, 5.11.xx, 5.15.xx, 5.16.xx

1 Introduction

This PA-DSS Implementation Guide contains information for proper use of the paypoint application. Verifone Norway AS 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-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the paypoint application in a manner that will support a merchant's PCI DSS compliance efforts.

1.1 Audience

The PA-DSS implementation guide must be read and understood by terminal operators including resellers, ECR integrators, support organizations and the merchant controlling the terminal. The guide should be used by assessors conducting onsite reviews and for merchants who must validate their compliance with the PCI DSS requirements.

This implementation guide is reviewed annually and updated if needed due to changes in paypoint or the PCI requirements. Latest version is always made available on www.verifone.no and information about updates are sent in the release notes.

1.2 Payment Card Industry (PCI) Security Standard Council

The PCI Security Standards Council is an open global forum, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

1.3 PCI DSS

Secure payment applications such as paypoint must be run in a secure environment. An environment may be deemed secure if it runs PCI approved system, network and firewall configurations. Payment Card Industry Data Security Standard (PCI DSS) provides a set of requirements to enhance security in the merchant environment. It ensures secure system configuration, operation, and security of systems supporting card payment transactions in your business or operating environment. If you use paypoint in your business to store, process, or transmit payment card information, the PCI DSS standard and this guide apply to you. Failure to comply with the PCI DSS standard and requirements can result in significant fines if a security breach should occur.

1.4 PCI PA-DSS

PCI payment application data security standard (PA-DSS) is a software security standard provided by the PCI council to ensure that payment applications store, process or transmit payment transactions securely. In order to meet this requirements paypoint undergoes regular security audit and certification led by PCI approved qualified security assessor (QSA) . The outcome of the PA-DSS audit and certification is listed on the PCI "List of Validated Applications" site. Contact Verifone Norway AS support in order to upgrade if you cannot find the paypoint version running on your terminals on this list.

1.5 Cardholder Data and Sensitive Authentication Data

PCI defines cardholder data and sensitive authentication data in the table below.

Account Data	
Cardholder Data (CHD)	**Sensitive Authentication Data (SAD)**
Primary Account Number (PAN)	Full track data (Magnetic-stripe data or equivalent on a chip)
Cardholder Name	CAV2/CVC2/CVV2/CID
Expiration Data	PINs/PIN block
Service Code	

Table 1: Account Data

According to this PCI sensitive authentication data cannot be stored. Primary Account Number (PAN) must be protected when stored. Protection includes strong encryption or masking.

1.6 Dependencies

All required paypoint dependencies and configurations are stated in section 3 and 4.

2 Content of Implementation Guide

The Table 2. below shows PCI requirements and instructions for merchants who operate paypoint in their PCI DSS approved environment. **Column 1** is the row number, **Column 2** states the PCI requirements**, column 3** documents paypoint implementation of those requirements and **column 4** states what **YOU** the merchants should do to become compliant.

Row	PA-DSS Requirement	paypoint Implementation	Instruction for Merchant (YOU)
1	1.1.4 Delete sensitive authentication data stored by previous payment application versions. Such removal is absolutely necessary for PCI DSS compliance.	paypoint automatically and securely delete all historical sensitive authentication data. paypoint does not store sensitive authentication data prior or after authorisation.	No action required by merchant to delete historical data. You are not allowed to collect from your customers or store sensitive authentication data after authorization
2	1.1.5 Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application	paypoint does not require sensitive authentication data for troubleshooting	You are not allowed to collect from your customers or store sensitive authentication data in order to troubleshoot any problem.
3	2.1 Securely delete cardholder data after customer-defined retention period	Your paypoint terminal will not store any PANs in scope for PCI without protection. The PAN is either encrypted, masked or truncated when stored and is deleted when not needed. Cardholder data are only stored inside the terminal (in the paypoint directory) and are encrypted and inaccessible for the merchant.	You must have a quarterly process for identifying and securely deleting stored cardholder data including BankAxept offline receipts that exceeds defined retention. (PCI DSS 3.1)

Row	PA-DSS Requirement	paypoint Implementation	Instruction for Merchant (YOU)
		Encrypted cardholder data needed for online processing are securely deleted after online transmission, this includes cardholder data stored offline. Since the payment application handles all deletion and re-encryption of cardholder data the merchant does not need to take any action to delete cardholder data transactions and pre-authorisation data needed for capture. Encrypted cardholder data stored for reversal purpose are deleted after 90 minutes. Historical data exceeding the retention period of one year is automatically re-encrypted with new keys by paypoint. Since the payment application handles all deletion and re-encryption of cardholder data the merchant does not need to take any action to delete cardholder data	
4	2.2 Mask PAN when displayed so only personnel with a business need can see the full PAN.	paypoint application does not disclose full PAN in scope for PCI on display or on the receipt, neither in any data sent to ECR nor log files. Only the last 4 credit card digits of the PAN are available on the receipts. **Exception**: BankAxept PAN has to be printed on the merchant part of the offline-(reserveløsning)receipts. paypoint terminals will not accept any cardholder data from any external device	**No action required except when BankAxept cards are involved** The Norwegian regulator (BSK) mandates the printing of PAN of BankAxept cards, (the Norwegian debit card), on merchant copy of offline backup solution (reserveløsning) receipts. You are therefore required to handle these BankAxept receipts in a secure way. You are not supposed to store them longer than necessary. BankAxept cards are technically out of scope of PCI-DSS, but Bits and

Row	PA-DSS Requirement	paypoint Implementation	Instruction for Merchant (YOU)
			BankAxept require that such receipts are handled according to the PCI DSS requirements. You must have a quarterly process for identifying and securely deleting stored cardholder data including, BankAxept offline receipts that exceeds defined retention.
5	2.3 Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs)	paypoint does not store any PAN in scope for PCI outside the payment terminals. PANs are encrypted when stored in the payment terminals and are deleted when not needed. This is not configurable. **Exception**: BankAxept PAN has to be printed on the merchant part of the offline-(reserveløsning)receipts. It is not possible to activate any logging that includes full PAN.	You must have a quarterly process for identifying and securely deleting stored cardholder data including BankAxept offline receipts (reserveløsning) that exceeds defined retention. (PCI DSS 3.1)
6	2.4-2.6 Key generation and management	Keys needed to encrypt cardholder and sensitive authentication data are generated and managed by Verifone and the POS terminal (PTS device) in a secure and approved way in accordance with PCI and local regulations. Historic data stored in the POS terminal are automatically re-encrypted by paypoint.	No action required as long as you do not store cardholder data in your local environment. But if you decide to do so then it must be encrypted according to PCI and you should manage your keys according to the PCI requirements.
7	3.1 Use unique user IDs and secure authentication for administrative access and access to cardholder data.	paypoint does not allow customers access to cardholder data stored in a paypoint terminal	No action required
8	3.2 Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	paypoint is only installed on terminals and has no database support	No action required
9	4.1 Implement automated audit trails.	paypoint terminals are configured automatically to	No action required

Row	PA-DSS Requirement	paypoint Implementation	Instruction for Merchant (YOU)
		send audit log to Verifone's central server	
10	4.4 Facilitate centralized logging.	paypoint can be configured to send centralized log messages to a syslog server operated by the merchant. The messages can be monitored or reviewed by the merchant. The logging can't be turned off since this will result in non-compliance with PCI requirements	**See section 3** for information on how to configure the terminal to send syslog messages to the your syslog server.
11	5.4.4 Implement and communicate application versioning methodology.	See section 6	Read the versioning methodology in **Section 6**
12	6.1 and 6.3 Securely implement wireless technology.	Secure wireless implementation can be configured in paypoint menu	You must change wireless vendor default settings of any supporting wireless device or component. For example default SSID, default encryption keys, password and the SNMP community strings if wireless connection is used. You must change the above parameters if anyone with the knowledge leaves the company or changes position You must configure firewall to permit only authorized traffic between the wireless environment and cardholder data environment **(Please see your wireless router manual)** **See installation guide for terminal configuration**
13	6.2 Secure transmissions of cardholder data over wireless networks.	paypoint does not allow WEP encryption paypoint protects transmission of card holder data by strong encryption.	If you are using a wireless network, WLAN, you must set up your wireless network to use WPA/WPA2 encryption. **(Please see your wireless router manual)** **See installation guide for terminal configuration**
14	8.2 Use only necessary and secure services, protocols, components,	paypoint is configured to work on only trusted hardware (PTS approved) and software	No action required

Row	PA-DSS Requirement	paypoint Implementation	Instruction for Merchant (YOU)
	and dependent software and hardware, including those provided by third parties.	components using strong encryption and protocols including secure services. See hardware dependencies **Section 5** below	
15	9.1 Store cardholder data only on servers not connected to the Internet.	No card data is stored outside the paypoint terminal	You are not allowed to store cardholder data without strong encryption and on a server connected to the internet
16	10.1 Implement two-factor authentication for all remote access to payment application that originates from outside the customer environment.	paypoint does not allow remote access	No action required
17	10.2.1 Securely deliver remote payment application updates. 7.2.3 Provide instructions for customers about secure installation of patches and updates.	paypoint terminals automatically check for updates and paypoint ensures secure installation of authenticated patches and updates. Only Verifone signed software will be accepted	No action required
18	10.2.3 Securely implement remote-access software.	paypoint does not allow remote access	No action required
19	11.1 Secure transmissions of cardholder data over public networks.	paypoint always use DUKPT field encryption over TLS 1.2 to transmit card and sensitive data over public networks. paypoint will not allow fallback to insecure protocols like SSL.	No action required. Open firewall ports to allow secure connections (**See section 4**)
20	11.2 Encrypt cardholder data sent over end-user messaging technologies.	paypoint encrypt all cardholder data	No action required
21	12.1 Encrypt non-console administrative access. 12.2 Multi-factor authentication is provided with the application	No non-console administrative access in paypoint and consequently no need for multi-factor authentication	No action required
22	13.1. Provides relevant information specific to the application for customers, resellers, and integrators to use.	Paypoint is always delivered with the dependencies required and is always configured in a PCI DSS compliant way.	Verify that your application version is listed in the header first in this implementation guide. No further action needed since

Row	PA-DSS Requirement	paypoint Implementation	Instruction for Merchant (YOU)
			paypoint can only be configured in a PCI DSS compliant way.
23	DFE1: Clear text cardholder data and sensitive auth data shall only be available at the point of encryption and at the point of decryption	Paypoint does not transmit plain-text PAN or SAD outside the POS terminal, and only uses secure and approved communication methods included in the PCI PTS evaluation. Paypoint does not have any configuration options to make cardholder data accessible outside of the terminal. paypoint terminals will not accept any cardholder data from any external device	No action required.
24	DFE3.2/DFE4.3 Cardholder data in settlement reports and clearing	Clearing, settlement and reconciliation messages and reports sent by paypoint do not contain any cardholder data.	No action required

Table 2: Details of implementation guide

References:

- PA-DSS_v3-2
- PCI_DSS_v3-2 17-342-5
- Visa Data Field Encryption Best Practices V1.0
- PNC E2EE Evaluation Form - POI - Ver E Final
- BankAxept POS - Security Requirements v2p1

3 Configure Syslog Server

You must activate syslog server in the terminal menu to receive syslog messages on your own server.

- Activate syslog server:
  - Menu + Administration + Change settings + Communication + System log + Yes
- Configure the IP address for the syslog server:
  - Menu + Administration + Change settings + Communication + TCP/IP innst + TCP / IP log
- Configure the port the syslog server:
  - Menu + Administration + Change settings + Communication + TCP/IP innst + TCP / IP log port

Syslog logs all parameter changes and administrative connections from a terminal, and sends it to the syslog server at the first opportunity.

For more details about syslog and a description of the message format, contact Verifone Norway AS.

4 Configuring communication

The following TCP/IP-addresses and ports in the Table 3 below need to be opened in the firewall configuration to enable paypoint to function.

NETS		
TCP/IP prim	193.214.020.211	
TCP/IP prim port	9100	
TCP/IP back	193.214.020.211	
TCP/IP back port	9100	
Sales Connector	Configuration 1 (*)	Configuration 2 (*)
TCP/IP prim	91.207.36.107	88.80.164.126
TCP/IP prim port	443	443
TCP/IP back	88.80.164.107	91.207.36.128
TCP/IP back port	443	443
Other settings		
TCP/IP prog	062.092.014.217	
TCP/IP prog port	5214 (Atos) / 10760 (Vx)	
TCP/IP admin	195.088.107.033	
TCP/IP admin port	2610	
TCP/IP ECR port (default port for ECR IP-integrated terminals)	9500 / 9550	

Table 3: Configurations

For the payment terminal to be operational, it must connect to admin-center and register BAX. In addition, it must have made a successful connection to host. To make this happen, the communication needs to be correctly configured. The default IP addresses and port numbers in the Table above are already configured in the terminal. For more information on configurations see the installation guide.

4.1 TCP/IP Settings

TCP / IP settings are located in the menu below
Administration → Change settings → Communication → TCP/IP param.

If a backup-address is not specified, the terminal will enter the primary address as the backup address. See installation guide for more configuration information.

4.2 TCP/IP prog port

Verifone terminals use 10760 TCP/IP for prog port.
Atos Worldline (Banksys) terminals use 5214 for TCP/IP prog port

4.3 Sales Connector

(*) Terminals that use configuration 1 are: Vx680, Vx690, Vx820, Vx520c and Xenteo.
(*) Terminals that use configuration 2 are: Yomani, Yomani XR and Xenteo Eco. These will also need access to 212.213.189.139:443.

5 Hardware Dependencies

paypoint version	Hardware Dependency	PTS Approval ID
5.08.xx	Atos Worldline, Xenteo	4-30011
5.11.xx	Verifone Inc, Vx690	4-30128
	Verifone Inc, Vx520c	4-30052
	Verifone Inc, Vx820	4-40054
	Verifone Inc, Vx680	4-30053
	Atos Worldline, Yomani	4-30046
	Atos Worldline, YomaniXR	4-30092
	Atos Worldline, Xenteo ECO Atos Worldline, Xenteo ECO reader	4-30104 4-30096
	Atos Worldline, Yoximo	4-30094
5.15.xx	Verifone Inc, Vx690	4-30128
	Verifone Inc, Vx520c	4-30052
	Verifone Inc, Vx820	4-40054
	Verifone Inc, Vx680	4-30053
	Atos Worldline, Yomani	4-30046
	Atos Worldline, YomaniXR	4-30092
	Atos Worldline, Xenteo ECO Atos Worldline, Xenteo ECO reader Atos Worldline, Yoneo reader	4-30104 4-30096 4-30119
	Atos Worldline, Yoximo	4-30094

Table 4: Hardware Dependencies

6 Versioning Methodology

The version number has three parts; X.YY.ZZ:

X = High impact security changes affecting either payment application security or PA-DSS requirement. High Impact changes requires a full PA-DSS assessment

YY = A functionality or low impact security changes affecting either payment application security, PA-DSS requirement or internal application dependencies. Such changes are eligible for partial or "delta" PA-DSS assessment.

ZZ = Minor functionality changes that have no impact on payment application security or PA-DSS requirements. The changes have minor impact on the functionality of the application or its dependencies. For example, bug fixes or minor adjustment of existing functionality. No Impact changes may be eligible for partial or "delta" PA-DSS assessment. This change will be represented by wildcards in the PCI PA-DSS listing.

Change Rules

- Change in X will reset all of the right elements (YY,ZZ) to zero
- Change in YY will reset ZZ to zero
- Change in ZZ will not affect any of the elements

7 PCI DSS Skimming Prevention Requirements

It is obligatory for the merchant to ensure their operating environment prevents skimming. You are therefore advised to implement the PCI DSS requirement 9.9.x in your environment in order to prevent skimming. For self-checkout points, please see "BankAxept Security Requirements for Self-Checkout Points".

The summary of the requirements are as follows:

- Merchants are to keep an up-to-date list of all POI devices in use. This list must be continually updated (substitutions, new acquisitions, relocation of POI etc.) and must contain, as a minimum, the following information:
  - Model and description of the POI device (e.g. Verifone Vx820, Yomani XR)
  - A clear identification of the POI device, e.g., by the serial number
  - Precise information as to where the POI device is installed (e.g., the address of the branch or company or, in the case of mobile devices, the responsible person that has possession of the device).
  - This list can be maintained manually or automatically, for example, using a terminal management system.
- Merchants are responsible for regular checks for fraudulent devices, manipulation or substitution of device. This shall be done at least daily. Self-Checkout Terminals must be checked at least every sixth hour during opening hours, starting with the first check when the merchant opens.
- There must be written instructions specifying how a device is to be checked, who is responsible for this, and at what intervals the checks should be carried out. The method for checking for compromises will depend on the type of device in question and can be carried out, for example, in the following ways:
  - Checking the seal (frequently already attached by the manufacturer, or else by individual merchants using their own seals or labels)
  - Comparing the POI device to a photo of the original POI to reveal any differences in its construction (e.g., caused by substitution) or any attached skimming components
  - Comparing the serial numbers
  - Looking for cameras
- It is the responsibility of the merchant to specify the intervals between inspections. This must be done as part of their yearly risk assessment in accordance with PCI DSS Requirement 12.2, also taking into account, amongst other things, factors such as the location of the device and whether it is an attended/unattended POI.
- Merchants are required to train staff on skimming prevention. Appropriate training materials and training sessions should be used to raise staff awareness and make any manipulation or substituting of devices more difficult. At the very least, the following should be included in the training:
  - Identification of third parties (e.g., maintenance engineers) that wish to service POI devices or substitute them before any such person is given access to the POI
  - Installation, substitution or return of a device only after checking that this has been planned and approved
  - Suspicious actions by strangers near to or directly at the device

7.1 Self-checkout points / Semi-attended terminals

Please see BankAxept Security Requirements for Self-Checkout Points for a complete list of BankAxept requirements. Below we have included some of them that are related to protection, location and inspection.

- The Self-Checkout Point must be placed within the merchant's facilities.
- The Self-Checkout Point must be located indoor.
- The merchant must perform a check for fraudulent devices at Self-Checkout Terminals at least every sixth hour during opening hours, starting with the first check when the merchant opens. The check shall be based on security guidance received from the Terminal Manufacturer and/or Terminal Vendor.
- The Self-Checkout Terminal must be locked or in other way attached to the Self-Checkout Point, or alarmed, to avoid theft and unauthorised replacement.
- Each merchant or retailer must answer the Self-Checkout Point Self-Assessment Questionnaire (SAQ) and send it to Bits at terminalsert@bits.no, before Self-Checkout Points are implemented. Bits will review the SAQ and archive it. The SAQ form may be obtained by contacting post@bits.no.

8 Updates and patches

Notification of new updates and patches are done via the external release notes that are sent out by the production/operation department. It is also communicated in the news section on www.verifone.no when it is released for full production.

Updates and patches are delivered in a secure manner with a known chain of trust where both the terminal and the SW-center identities are checked. The integrity of the patch and updates are automatically checked for both the Wordline and Verifone terminals.

Software distribution certificates are installed in the POS terminal as part of the initial deployment process together with initial software version and encryption keys. The terminal will only accept to install patches and updates which are signed with the corresponding key and will check the integrity of the software before installation.

Patches and updates are securely signed and made available for download on Verifone Norway's SW center. The updates can only be downloaded by a legitimate POS terminal delivered by Verifone Norway from Verifone SW center. The POS terminal will regularly check for new downloads, at least every 10th day. The merchant can also download the updates by manually selecting Contact Program center on the POS terminal. For automatic download the merchant doesn't need to do anything.

9 Privacy shield requirements

Ref: BankAxept – POS Security Requirements BAX-SEC-REQ, Ver: 2.1, 25/1 2018

A PIN pad must be equipped with privacy shield in accordance with [PCI PTS] DTR A7 (Visual Observation Deterrents) and Appendix A (Criteria for the Privacy Screen Design).

> **Exception**: Handheld devices as defined in [PCI PTS] and operated in its intended manner, handheld by the cardholder when entering PIN. Requirement SEC-HW-03 must then be met.
>
> A handheld terminal/device must by weight, size and shape encourage its handheld operation. If the standing and/or mounting support indicate that the PIN entry device is to be installed on a swivel arm or a similar apparatus, it will not be considered as a handheld terminal, but a desktop device.

10 Contactless mandates

Contactless Payments Acceptance Mandate for Visa Europe

Based on Member Letter: VE 94/14

On 31 October 2014, the Visa Europe Board approved a resolution to mandate the acceptance of contactless payments at all face-to-face, semi-attended and unattended Visa terminals, including Mobile Acceptance Terminals (otherwise known as mobile point-of-sale or 'mPOS' terminals) where they are installed in a fixed merchant location.

- With effect from **31 December 2015**, any terminal installation with a new Visa merchant, or any terminal infrastructure upgrade programme with an existing Visa merchant, must accept contactless payments.
- With effect from **31 December 2019**, all Visa terminals deployed must accept contactless payments.

BankAxept mandates

Ref: 161114 mandatebrev til terminaloperatører og kortpersonaliserere mandate.pdf

From January 1st 2017

- All new POS terminals must have HW and SW supporting BankAxept contactless (CTLS) payment. The merchant can decide when to activate CTLS payment.
- If a POS terminal accept BankAxept and CTLS payment for a different brand, the terminal must also accept BankAxept CTLS payment.

Unattended Payment Terminal

A POS device where the transaction is initiated by the cardholder, and there is no immediate merchant support available. These include terminals such as: Automated fuel dispensers, Kiosks and Self-service devices, such as ticketing/ vending or car parking terminals.

MasterCard mandates

Ref: Transaction Processing Rules (18 December 2018)
https://www.mastercard.us/content/dam/mccom/global/documents/transaction-processing-rules.pdf

Contactless Enablement in the Europe Region:
The Acquirer of a Merchant located in the Europe Region (excluding countries where a country-specific mandate is set out below) must ensure that:

- All new and all upgraded POS Terminals (including MPOS Terminals) deployed on or after 1 January 2016 are contactless-enabled; and
- Effective 1 January 2020, all existing POS Terminals (including MPOS Terminals) are contactless-enabled

What is included in the definition of POS terminals?
The term POS terminals refers to both attended point-of-sale (POS) and unattended point-of-sale (cardholder-activated terminals [CAT]) terminals. It does not include ATMs or financial institution (bank) branch terminals.

MasterCard : Effective 1 January 2020, all newly-deployed contactless-enabled terminals must only support EMV mode contactless transactions and must not support magstripe mode contactless transactions.

11 Manual key entry

Paypoint does only support manual key entry for technical fallback (i.e. when the chip can't be read). Paypoint can't be used for MOTO (Mail Order – Telephone Order) transactions when the cardholder and card are not present.