Verifone

PA DSS Implementation Guide

For Verifone terminals E285, P400, M400, V400M, V400C, X10(Carbon 8, Carbon 10) using the VEPP NB application version 3.x.x.x.x

Version 3.2

Date: **2019-09-10**

Table of 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 VEPP NB payment application version 3.x.x.x.x in your business to store, process, or transmit payment card information, this standard and this guide apply to you.

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

The PA-DSS implementation 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 VEPP NB application or the PCI requirements. Latest version is always made available on www.verifone.com and information about updates are sent in the release notes. It's merchant's responsibility to periodically verify that version they are using complies to the latest version of the implementation guide available on the webpage.

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 VEPP NB software versions on the PCI web site "List of Validated Payment Applications" that have been validated in accordance with PCI PA-DSS. If you cannot find the version of the VEPP NB application running on your payment environment in the list on the website below, please contact Terminal Service Providers' helpdesk 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 VEPP NB 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-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the VEPP NB payment application in a manner that will support a merchant's PCI DSS compliance efforts.

Note 1: Both the System Installer and the controlling merchant must read this document.

1.3 References

(1) *Payment Card Industry – Payment Application Data Security Standard v3.2*
(2) *Payment Card Industry – Data Security Standard v3.2.1*

1.4 Update History

Ver.	Name	Date	Comments
0.1	Sergejs Melnikovs	01-Jun-2016	Initial draft version, without technical info about the application.
0.2	Gudmundur Jonsson	08-Aug-2016	Updated with VEPP specifics
1.1	Gudmundur Jonsson	23-Aug-2016	Log information added and A3 updated.
1.2	Sergejs Melnikovs	26-Aug-2016	Updated in according to PA DSS QSA recommendations.
1.3	Jan Warming	22-Nov-2016	Domain changed from .se to .com
1.4	Jan Warming	30-Nov-2016	Annex A5 added
1.5	Jan Warming	14-Feb-2017	Updated in according to PA DSS QSA recommendations.
1.6	Jan Warming	04-May-2017	Included guidance and information regarding Bluetooth.
2.0	Sergejs Melnikovs	15-Sep-2017	Updated according to VEPP NB 2.2.0.x applications functionality for P400 & M400 terminals
2.1	Sergejs Melnikovs	10-Oct-2017	Updated in according to PA DSS QSA recommendations.
2.2	Sergejs Melnikovs	11-Dec-2017	Updated according to VEPP NB 2.3.0.x.x applications functionality and new version numbering policy
2.3	Sivakumar Subramanian	21-May-2018	Updated according to VEPP NB 2.4.0.x.x applications functionality and new version numbering policy
2.4	Sergejs Melnikovs	25-May-2018	Added anti-skimming requirements
2.5	Sivakumar Subramanian	02-Nov-2018	Reviewed and Updated according to VEPP NB 2.5.0.x.x applications functionality
2.6	Sergejs Melnikovs	12-Nov-2018	Remove eVo terminal models and add e285 Update data in Annex A1
2.7	Sergejs Melnikovs	29-Mar-2019	Updated according to VEPP NB 2.6.0.x.x applications functionality. Introduce new representation of application summary information.
2.8	Sergejs Melnikovs	10-Apr-2019	Update Annex A1
2.9	Sergejs Melnikovs	20-May-2019	Updated chapter 2.1 (Req. 1.1.4)
3.0	Sivakumar Subramanian	19-Aug-2019	Updated according to 3.x.x.x.x functionality
3.1	Sergejs Melnikovs	27-Aug-2019	Updated in according to PA DSS QSA recommendations.
3.2	Sergejs Melnikovs	10-Sep-2019	Added explanation to new version numbering methodology

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.
VEPP NB Application	Terminal Payment Application for use on Verifone hardware payment environment.
VEPP Terminal	Terminal with installed VEPP NB Application
CVV2	Card Verification Value, also called CVC2, is a three or four digit value printed on the back of the card but not encoded on the magnetic stripe or the chip. Supplying this code in a transaction is intended to verify that the card is present at the point of sale when PAN is entered manually or when a voice referral is performed.
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.
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 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.
PCI PTS	Payment Card Industry PIN Transaction Security
PED	PIN Entry Device
POS	Point of Sale
PSP	Payment Service Provider offers merchants online services for accepting electronic payments.
Sensitive Authentication Data	Magnetic Stripe Data, CAV2/CVC2/CVV2/CID, 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.
SSL	Secure Sockets Layer is a commonly used method to protect transmission across public networks.
SYSLOG	Syslog is a standard for computer data logging.
TCP	Transmission Control Protocol is one of the core protocols of the Internet protocol suite.
TLS	Acronym for “Transport Layer Security.” Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
TMS	Terminal management system
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.

1.6 Application Summary

Payment Application Name	**VEPP NB**	**Payment Application Version**	**3.x.x.x.x**
Application Description	The Verifone VEPP NB PA-DSS application provides an interface which easily integrates with 3rd party software and host architecture that customer choices. Application runs on PTS approved devices and performs a variety of payment functionalities with a single supported gateway		
Typical Role of Application	Application runs on PTS approved devices and performs a variety of payment functionalities with a single supported gateway		
Target Market for Payment Application	**Target Market for Payment Application (check all that apply)**: X Retail | Processors | Gas/Oil e-Commerce | Small/medium merchants Others (please specify):		
Stored Cardholder Data	The following is a brief description of files and tables that store cardholder data:		
	See Annex A1 for details of where Cardholder's Data is stored.		
	Individual access to cardholder data is logged as follows: *N/A. Cardholder Data is encrypted using SRED functionality of the PTS approved device therefore there is no access to clear text card data.*		
Components of the Payment Application	The following are the application-vendor-developed components which comprise the payment application:		
	VEPP NB is a single application that doesn't have subcomponents.		
Required Third Party Payment Application Software and Hardware	VEPP NB can be deployed on a number of Verifone terminals such as e285 (Bluetooth, WiFi), M400 (WiFi, Ethernet), P400 (WiFi, Ethernet), V400M (WiFi, 4G/2G), V400C (WiFi, Ethernet), X10 Carbon8/Carbon10 (WiFi, Ethernet)		
Database Software Supported	The following are database management systems supported by the payment application:		
	Not applicable. No database software supported		
Other Required Third Party Software	The following are other required third party software components required by the payment application:		
	none		
	The following are Operating Systems supported or required by the payment application:		

<table>
<tr><td>Operating System(s) Supported</td><td>VEPP NB Application runs on Verifone proprietary Operating system VOS/2.

P400/P400 Plus: PCI PTS 5.x (4-10239)
M400: PCI PTS 5.x (4-10231)
V400m: PCI PTS 5.x (4-30260)
V400c, V400c Plus: PCI PTS 5.x (4-30306)
X10, Carbon 8, Carbon 10: PCI PTS 4.x (4-10209), PCI PTS 5.x (4-10241)
e285 PCI PTS 5.x (4-30276)</td></tr>
<tr><td>Application Authentication</td><td>N/A. VEPP NB doesn’t provide authentication functionality.</td></tr>
<tr><td>Application Encryption</td><td>N/A. Application relies on a SRED functionality of PTS approved device.</td></tr>
<tr><td>Application Functionality Supported</td><td>Payment Application Functionality (check only one):
<table>
<tr><td></td><td>Automated Fuel Dispenser</td><td></td><td>POS Kiosk</td><td></td><td>Payment Gateway/Switch</td></tr>
<tr><td></td><td>Card-Not-Present</td><td></td><td>POS Specialized</td><td></td><td>Payment Middleware</td></tr>
<tr><td></td><td>POS Admin</td><td></td><td>POS Suite/General</td><td></td><td>Payment Module</td></tr>
<tr><td>X</td><td>POS Face-to-Face/POI</td><td></td><td>Payment Back Office</td><td></td><td>Shopping Cart & Store Front</td></tr>
</table></td></tr>
<tr><td>Payment Processing Connections:</td><td>TLS 1.2 is the only protocol supported by the application to protect data transmitted over public network. All transaction data is sent to single supported payment gateway</td></tr>
</table>

2. SUMMARY OF PCI PA DSS REQUIREMENTS

This summary covers shortly PA-DSS requirements that have a related to Implementation Guide topic. It also explains how the requirement is handled in the VEPP NB application and requirement from your (as a customer) aspect.

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

http://www.pcisecuritystandards.org

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 VEPP NB application meets this requirement	No specific setup for the VEPP NB application is required. VEPP NB application doesn't store any sensitive authentication data after authorization – hence there is no previous magnetic stripe data, card validation values or codes, and PINs or PIN block data available from previous versions of application, it is automatically deleted after authorization..
merchant actions required	You must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) 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 necessary for PCI DSS compliance.

Aligns with PCI DSS Requirement 3.2

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

Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	
How VEPP NB application meets this requirement	Sensitive authentication data is never stored by the VEPP NB application either encrypted or in the clear (even when needed to solve a specific problem) in production terminals.
merchant actions required	Verifone does not store Sensitive Authentication Data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with Sensitive Authentication Data used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data): • Collect sensitive authentication data 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 VEPP NB application meets this requirement	All cardholder data is automatically erased from VEPP NB terminal after successful connection with authorization system. See the list of files in the Annex *A1 Terminal files*
merchant actions required	VEPP NB terminal does store cardholder data using a SRED functionality of PTS approved device. The merchant is not required to take any action in relation to this requirement. Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will securely delete (render irretrievable) the stored cardholder data. When defining a retention period, you must take into account legal, regulatory, or business purpose. All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN.

Aligns with PCI DSS Requirement 3.1

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 VEPP NB 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* The application by default mask PAN according to PCI requirements and has no configurable options to change this. The application doesn't have an ability to display or export full PAN.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.3

2.4 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 VEPP NB application meets this requirement	PAN is rendered unreadable by default in the application. The application has no configurable options to change this. Details of rendering method and all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts are available in Annex *A1 Terminal files*
merchant actions required	The merchant is responsible for rendering PAN unreadable in all instances where a PAN could be stored in outside of VEPP NB application.

Aligns with PCI DSS Requirement 3.4

2.5 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 VEPP NB application meets this requirement	N/A The payment application doesn't have access to the keys. All key management is handled by a SRED functionality of PTS approved device.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.5

2.6 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 VEPP NB application meets this requirement	N/A The payment application doesn't have access to the keys. All key management is handled by a SRED functionality of PTS approved device.
Merchant actions required	The merchant is not required to take any action related to key management on VEPP NB terminal. If by some reason VEPP NB terminal displays message "**SRED key is missed**" please immediately contact terminal service provider for future instructions. In this state the terminal will not permit to start any transaction. Most of the problems could be solved remotely except a case when the terminal is tampered. Tampered terminal must be: • physically replaced; • returned to Terminal Service Provider for investigation.

Aligns with PCI DSS Requirement 3.6

2.7 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 VEPP NB application meets this requirement	N/A The payment application doesn't have access to the keys. All key management is handled by a SRED functionality of PTS approved device.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.6

2.8 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 VEPP NB application meets this requirement	The VEPP NB application does not provide functionality and does not maintain user accounts for administrative access or individual access to cardholder data.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.1 and 8.2

2.9 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 VEPP NB application meets this requirement	The VEPP NB application does not provide functionality and does not maintain user accounts for administrative access or individual access to cardholder data.
Merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.1 and 8.2

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

Implement automated audit trails.

How VEPP NB application meets this requirement	VEPP NB application supports Syslog. This log contains masked PANs. This may also contain SRED encrypted PAN if log level is set to LOG_TRACE. No cardholder data is accessible from the VEPP terminal. The application also keeps an Audit Trail to track changes to system level objects.
merchant actions required	For the Audit Trail there are no settings you need to do. The Audit Trail is created automatically. The Audit Trail could be sent manually to a centralized server. Although typically not possible, but merchant should be aware that application and TMS logs should not be disabled and doing so will result in non-compliance with PCI DSS.

Aligns with PCI DSS Requirement 10.1

2.11 PA-DSS Req. 4.4: Facilitate centralized logging

Facilitate centralized logging.	
How VEPP NB application meets this requirement	VEPP NB application provides SYSLOG for audit trails delivery.
Merchant actions required	The merchant may choose to setup a local SYSLOG server and configure the SYSLOG server IP address in the terminal settings. Chapter *"Audit Trail log"* gives you guidance on how to correctly setup the centralized log server.

Aligns with PCI DSS Requirement 10.5.3

2.12 PA-DSS Req. 5.4.4: Application versioning methodology

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

2.13 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 VEPP NB application meets this requirement	If wireless is used VEPP NB application supports strong encryption (WPA, WPA2) functionality aligned to industry best practices. The wireless encryption is applied on top of SRED technology used to transmit Cardholder Data and Sensitive Authentication Data. Also, all data sent to and from the application by default protected using TLS 1.2 with strong ciphers.
merchant actions required	If you are using wireless network within your business please follow recommendations in chapter *3.3 Protect wireless transmissions* of the implementation guide.

Aligns with PCI DSS Requirements 1.2.3 & 2.1.1

2.14 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 VEPP NB application meets this requirement	If wireless is used VEPP NB application supports strong encryption (WPA, WPA2). The wireless encryption is applied on top of SRED technology used to transmit Cardholders Data and Sensitive

	Authentication Data. Also, all data sent to and from the application by default always protected using TLS 1.2 using strong ciphers.
merchant 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 chapter 2.13 PA-DSS Req. 6.1: Securely implement wireless technology of the implementation guide.

Aligns with PCI DSS Requirement 4.1.1

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

Provide instructions for secure use of wireless technology.	
How VEPP NB application meets this requirement	If wireless is used VEPP NB application supports strong encryption (WPA, WPA2). The wireless encryption is applied on top of SRED technology used to transmit Cardholders Data and Sensitive Authentication Data. Also, all data sent to and from the application by default always protected using TLS using strong ciphers.
merchant actions required	If you are using wireless network within your business please follow recommendations in chapter *3.3 Protect wireless transmissions* of the implementation guide.

Aligns with PCI DSS Requirements 1.2.3, 2.1.1, & 4.1.1

2.16 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 VEPP NB application meets this requirement	VEPP NB 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 update of VEPP NB application is released by Verifone, customers will be notified by their account manager.
Merchant actions required	The merchant is not required to take any action in relation to this requirement.

2.17 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 VEPP NB application meets this requirement	VEPP NB application does not employ unnecessary or insecure services or functionality. Full list of application components and dependent components / protocols described in chapter *1.6* Application Summary
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.2.3

2.18 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 VEPP NB application meets this requirement	VEPP NB application does not store any cardholder data in a server connected to the internet.

merchant actions required	Never store cardholder data on internet accessible systems.

Aligns with PCI DSS Requirement 1.3.7

2.19 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 VEPP NB application meets this requirement	VEPP NB application does not provide functionality and does not maintain user accounts for any remote access to the application.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.3

2.20 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 VEPP NB application meets this requirement	VEPP NB 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 is not in use.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 1 and 12.3.9

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

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

Aligns with PCI DSS Requirements 2, 8 and 10

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

Secure transmissions of cardholder data over public networks.	
How VEPP NB application meets this requirement	By default, configured to use TLS 1.2 with strong ciphers encryption is applied on top of SRED encryption used to transmit Cardholders Data and Sensitive Authentication Data from VEPP terminal to the authorization host over public networks.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.1

2.23 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 VEPP NB application meets this requirement	VEPP NB application doesn't use any end-user messaging technologies to send cardholder data.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.2

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

Encrypt non-console administrative access.	
How VEPP NB application meets this requirement	VEPP NB application does not provide non-console access functionality and does not maintain user accounts for any administrative access to the application.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.3

3. How to set up your VEPP terminal to ensure PCI DSS compliance

The terminal serial number is registered in TMS and VEPP NB application assigned to the serial number. VEPP NB application bundle is then downloaded to terminal with TMS agent.

3.1 Do not retain full magnetic stripe or card validation code

When upgrading the payment application in your VEPP terminal to comply with the PCI PA-DSS requirements this could be done two ways.

- Your old unit is physically replaced by a new VEPP NB loaded with software that complies with the PCI PA-DSS requirements.
- Your existing VEPP NB application is downloaded remotely with new software that also complies with the PCI PA-DSS requirement.

In both cases you must make sure that the software version of the VEPP NB Application that runs on your terminal is listed on the PCI web site “List of Validated Payment Applications” that have been validated in accordance with PCI PA-DSS.

http://www.pcisecuritystandards.org

For your organization to comply with PCI DSS requirements it is necessary to remove historical data stored prior to installing your PCI PA-DSS compliant VEPP terminal. Therefore, you must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) are removed from all storage devices used in your system, ECRs, PCs, servers etc. For further details please refer to your vendor.

No specific setup of your VEPP PCI PA-DSS compliant terminal is required. PAN is stored either truncated or encrypted. Full magnetic stripe data and other Sensitive Authentication Data deleted immediately after authorization and never stored.

Note: When using the PCI PA-DSS compliant VEPP terminal, you will never be prompted to enter CVV2.

Sensitive authentication data is never stored by the VEPP NB application in the clear (even when needed to solve a specific problem) in production terminals. If a case arises when Sensitive Authentication Data is needed for troubleshooting, this will only be done in a Verifone lab/test environment using test terminals and test data.

3.2 Protect stored card holder data

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

To comply with the PCI DSS requirements all cryptographic material must be rendered irretrievable. The removal of this material is handled within the VEPP terminal and you do not need to take any action.

3.3 Protect wireless transmissions

If you are using wireless network within your business, you must make sure that firewalls are installed that deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the VEPP 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 were changed

- Default passwords/passphrases on access points were changed
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks, for example IEEE 802.11i. Please note that the use if WEP as a security control was prohibited as of 30 June 2010.
- Other security related wireless vendor defaults were changed.

Bluetooth:
When using Bluetooth (BT) the default PIN must not be used. Change the PIN from the default.

3.4 Facilitate secure remote software updates

The software of your VEPP terminal could be updated remotely and automatically. For connection to external networks it is recommended to use firewall protection.

VEPP NB application bundle signed by Verifone production signing certificate and VEPP terminal will reject an application if it is signed by any other certificate. VEPP NB application bundle could be downloaded to terminal remotely from TMS server. TMS agent requires certain certificates to be installed in order to properly communicate with the TMS server. Three certificate files in use for the communication:

- **Protocol Certificate** – This certificate is used during the key exchange to send encrypted key data to the server;
- **SSL Certificate Tree** – This is the certificate tree that the agent can use to verify the cert exchanged during SSL communication all the way back to its issuer CA;
- **Download SSL Certificate Tree** - This is the certificate tree that the agent can use to verify the cert exchanged during SSL downloads all the way back to its issuer CA.

When talking to VeriFone Hosted TMS, the correct certificates are included in the FULL version of the TMS Agent. TMS Agent is included into VEPP NB application bundle. So, for VeriFone Hosted TMS customers, just use the FULL VEPP NB application package then everything should work.

3.5 Encrypt sensitive traffic over public networks

Your VEPP NB application allows transmission over public networks, e.g. public internet. To protect sensitive data your VEPP NB application uses SRED technology based on triple DES encryption with a unique key per transaction. On top of that all data sent to and from the VEPP terminal is protected under TLS 1.2. To connect your VEPP terminal to public networks you do not need to take any further action regarding encryption.

3.6 PCI DSS Skimming Prevention Requirements

It is obligatory for the merchant to ensure their operating environment prevents skimming. Merchants are therefore advised to implement the PCI DSS requirement 9.9.x in their environment to prevent skimming. 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 M400, Verifone P400)
  - 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 manipulation or substitution of device. This shall be done at least daily.
- 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 considering, 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

4. Back-out or product de-installation procedures

The software of your VEPP terminal could be updated remotely either automatically or manually triggered. In the unlikely event that your newly downloaded software fails or malfunctions please contact customer support in order to allow you to download an older version of the software.

5. VEPP application key management

5.1 Keyset description

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 Gateway.
TEK	DUKPT (2TDES) 112bit	**Terminal Encryption Key**. Another name for the key is SRED Key. Used in one-way Cardholders Data and Sensitive Authentication Data encryption on the terminal. The data could be decrypted only by the Gateway's HSM.

Each VEPP terminal equipped by unique set of the keys.

5.2 Key distribution process

TPK and TEK 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 verify signature of the keys and only after successful verification install new keys into secure memory. Secure memory 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	-
Minimum key size in number of bits:	168	2048	224	2048/224	-
Minimum key size in number of bits:	-	3072	256	3072/256	128
Minimum key size in number of bits:	-	7680	384	7680/384	192
Minimum key size in number of bits:	-	15360	512	15360/512	256

6. Audit Trail log

6.1 How to change the address to the centralized log server

By default, the audit trail is stored locally on the device. It can be retrieved by the terminal management system by your PSP or extracted by a technician. if the Audit Trail destination is set to UDP, Audit Trail is sent to a centralized log server automatically.

To achieve automatic audit trail sending on VEPP Terminal:

1. Select (2) “Administration Menu”
2. Select (1) “Settings”
3. Select (3) “Application logs”
4. Select (1) “Set destination”
5. Select UDP
6. Select (5) “Set UDP host”
7. Enter IP address
8. Page down and select (2) “Set UDP port”
9. Enter port number

Once audit trail is set to be sent over UDP, all information of major events will be transferred to your designated server. Terminal will keep theses settings even after power loss or reboot.

Important:

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

6.2 Data Contents of Audit Trail

Depending on the destination of the audit trail, different actions will be logged. UDP audit trail only transfers the application log which can be considered a high-level log. This log is very important for troubleshooting so make sure to always use the appropriate application and syslog log level that matches your needs.
Additionally, low-level operating log can be extracted from the device by a technician locally or remotely by your PSP.

The following logging levels are available for configuration:

Level	Description
0 – LOG_EMERG	Emergency / system is unusable. Performance logs are also printed with this level so performance would always be visible.
1 – LOG_ALERT	An immediate action must be taken.
2 – LOG_CRIT	Critical conditions.
3 – LOG_ERR	Error has occurred.
4 – LOG_WARNING	Warning reporting. Indicates that there has been a situation, that requires attention.
5 – LOG_NOTICE	Normal, but significant condition.
6 – LOG_INFO	Regular info message about the actions being performed.
7 – LOG_TRACE	High verbosity messages to give additional information about the application flows and results.

F. ex. if configured level 3 then events from level 0,1 and 2 also will be logged.
For PA-DSS purposes, log level should be enabled at least at Emergency level (enabled by the default).
The log level configuration only affects the application and syslog log levels, but not the low-level operating system log.

6.2.1 File size

When log destination is set to file, the lifetime of the log file will be determined by how actively the terminal is used and what log levels are set. These limits can be changed by your PSP.
If you find a need to increase these limits, please contact your PSP.

6.2.2 File format

The terminal audit log file is a readable ASCII text file with one entry on each line.

6.2.3 File sample

Below is an example of log entries from a terminal:

```
<13>Sep 18 17:05:13 veppnb: (app/main.cpp:64) Application [veppnb v2.2.0.0-4] starting. Commit
f79cfe8 2017-09-13T02:26:09-07:00
<13>Sep 18 17:05:13 veppnb: (app/main.cpp:65) Build time: 2017-09-15T14:32:31.932920
<15>Sep 18 17:05:13 veppnb: (src/libcom.cpp:1606) libcom: API com_GetVersion called
<15>Sep 18 17:05:13 veppnb: (src/libcom.cpp:430) libcom: API com_Init called, library version:
2.9.9-231
<15>Sep 18 17:05:13 veppnb: (src/libcom_net.cpp:531) libcom: Created network thread
<15>Sep 18 17:05:13 veppnb: (src/libcom.cpp:1611) libcom: API com_GetSvcVersion called
<15>Sep 18 17:05:13 veppnb: (src/libcom_util.cpp:28) libcom: prv_sendCommand send command
{"command":20,"interface":200}
<15>Sep 18 17:05:13 veppnb: (src/libcom_net.cpp:354) libcom: readNetworkEvent start
<15>Sep 18 17:05:13 veppnb: (src/libcom_util.cpp:81) libcom: prv_sendCommand received
{"command":20,"error":0,"interface":200,"version":"2.9.9-231"} from daemon
<15>Sep 18 17:05:13 veppnb: (src/libcom_util.cpp:108) libcom: prv_sendCommand daemon has
accepted
<15>Sep 18 17:05:13 veppnb: (src/libcom.cpp:465) libcom: Remote comdaemon is version: 2.9.9-
231
<15>Sep 18 17:05:13 veppnb: (src/libcom.cpp:1289) libcom: API com_SetDevicePropertyInt called
<15>Sep 18 17:05:13 veppnb: (src/libcom_util.cpp:28) libcom: prv_sendCommand send command
{"command":3,"interface":200,"property":13,"property_value":1}
<15>Sep 18 17:05:13 veppnb: (src/libcom_util.cpp:81) libcom: prv_sendCommand received
{"command":3,"error":0,"interface":200,"property":13,"property_value":1} from daemon
<15>Sep 18 17:05:13 veppnb: (src/libcom_util.cpp:108) libcom: prv_sendCommand daemon has
accepted
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:69) Set Application::APPLICATION_NAME
= veppnb
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:78) Set
Application::APPLICATION_VERSION = 2.2.0.0-4
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:87) Set
Application::APPLICATION_COMMIT_HASH = f79cfe8
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:96) Set
Application::APPLICATION_COMMIT_DATE = 2017-09-13T02:26:09-07:00
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:181) Application::Application [veppnb
2.2.0.0-4 f79cfe8 2017-09-13T02:26:09-07:00]
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:101) Application::checkForIPC veppnb
<14>Sep 18 17:05:13 veppnb: (ipc.cpp:366) ipc_init name=veppnb tid=2830929920
<13>Sep 18 17:05:13 veppnb: (app/application/cobra_application.cpp:38) Application created:
veppnb version: 2.2.0.0-4 f79cfe8 2017-09-13T02:26:09-07:00
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:202) Application::Run
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:142) Application::addDependencies
<15>Sep 18 17:05:13 veppnb: (gui_worker.cpp:151) Setting GUI resource and default path to:
/home/usr1/flash/www/veppnb
<15>Sep 18 17:05:13 veppnb: (gui_worker.cpp:156) uiLayout(): 0
<15>Sep 18 17:05:13 veppnb: (vipa/vipa_client.cpp:149) VipaClient::VipaClient() !!!!!!!!!!!!
<15>Sep 18 17:05:13 veppnb: (app/epas/com/epas_com_manager.cpp:19)
EpasComManager::EpasComManager()
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:332) initMAC::ipcSetAppID [ veppnb ]
<15>Sep 18 17:05:13 veppnb: (application/application.cpp:195) sysToForground veppnb
starting...
<15>Sep 18 17:05:13 veppnb: (src/libmac/libmac.cpp:490)
SendAndWaitForReturn[{"libmac_appid":"veppnb","libmac_cmd":"libmac_foreground","libmac_from":"
veppnb","libmac_version":"3.26.3-8"}]
<15>Sep 18 17:05:13 veppnb: (src/libmac/libmac.cpp:496) Sending notification to MAC...
<15>Sep 18 17:05:13 veppnb: (src/libmac/libmac.cpp:519) Waiting for return notification from
MAC

Mon Feb 25 14:32:02 2019: Installing pkg.ccp_rsc.tgz
Mon Feb 25 14:32:02 2019: Installed package pkg.ccp.tgz - ccp: 1.4.27-352
Mon Feb 25 14:32:03 2019: Installed package pkg.ccp_rsc.tgz - ccp_rsc: 1.4.27-352
Mon Feb 25 14:32:03 2019: Installed bundle: ccp.tgz: ccp: 1.4.27-352
Mon Feb 25 14:32:03 2019: Installing Bundle File cloudproxy-3.0.5.tgz
Mon Feb 25 14:32:03 2019: Installed Certificate: Certif.crt
Mon Feb 25 14:32:03 2019: Installed Certificate: SponsorCertif.crt
Mon Feb 25 14:32:03 2019: Installing pkg.cloudproxy.tgz
Mon Feb 25 14:32:03 2019: Installed package pkg.cloudproxy.tgz - cloudproxy: 3.0.5
```

```
Mon Feb 25 14:32:03 2019: Installed bundle: cloudproxy-3.0.5.tgz: cloudproxy: 3.0.5
Mon Feb 25 14:32:03 2019: Installing Bundle File com.tgz
Mon Feb 25 14:32:03 2019: Installed Certificate: Certif.crt
Mon Feb 25 14:32:03 2019: Installed Certificate: SponsorCertif.crt
Mon Feb 25 14:32:03 2019: Installing pkg.comdaemon.tgz
Mon Feb 25 14:32:04 2019: Installing pkg.comlib.tgz
Mon Feb 25 14:32:04 2019: Installed package pkg.comdaemon.tgz - comdaemon: 2.35.26-352
Mon Feb 25 14:32:04 2019: Installed package pkg.comlib.tgz - comlib: 2.35.26-352
Mon Feb 25 14:32:04 2019: Installed bundle: com.tgz: com: 2.35.26-352
Mon Feb 25 14:32:04 2019: Installing Bundle File lcp.tgz
Mon Feb 25 14:32:04 2019: Installed Certificate: Certif.crt
Mon Feb 25 14:32:04 2019: Installed Certificate: SponsorCertif.crt
Mon Feb 25 14:32:04 2019: Installing pkg.lcp.tgz
Mon Feb 25 14:32:04 2019: Installed package pkg.lcp.tgz - lcp: 2.16.9
Mon Feb 25 14:32:04 2019: Installed bundle: lcp.tgz: lcp: 2.16.9
Mon Feb 25 14:32:04 2019: Installing Bundle File libEMV_CTLS_AK-2.2.7+VEL2.0.5.tgz
Mon Feb 25 14:32:04 2019: ERROR: addCertificate: -506
Mon Feb 25 14:32:04 2019: Failed to install Certificate: Certif.crt
Mon Feb 25 14:32:04 2019: /mnt/flash/install/bundles/libEMV_CTLS_AK-2.2.7+VEL2.0.5.tgz auth
error: -213
Mon Feb 25 14:32:04 2019: Failed to install bundle: /mnt/flash/install/bundles/libEMV_CTLS_AK-
2.2.7+VEL2.0.5.tgz (228): Certificate not found
Mon Feb 25 14:32:09 2019: Failed to install Download file:
/mnt/flash/install/dl/vos2_load_solutions_dl.cobra-ADK44_REGIONS-nightly-230-vos2-p400-
prod.tgz
```

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
payment.db	Transaction information pending to be sent to Sales Connector	PAN, Expiry Date	• PAN Encrypted by SRED • PAN Truncated (6 first + 4 last)
Backup.db	Local backup of payment.db file	PAN, Expiry Date	• PAN Encrypted by SRED • PAN Truncated (6 first + 4 last)

A2 Application Version Numbering policy

The following convention should be used for all applications:

VEPP NB V.w.x.y.z where

Release Number segment	Mandatory or Optional?	Description	Used in Production Release?
V	Mandatory	**PCI** - Major Application Architecture Change or Compliance Impacting change - Indication for either a High Impact change as defined in the PCI PA DSS program guide which meet any of the following criteria: 1. Four or more PA-DSS Requirements are affected, not including Requirements 13 and 14; 2. Half or more of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14; 3. Half or more of the Payment Application's functionality or half or more of its code-base is changed; or 4. Addition of tested platform/operating system to include on the List of Validated Payment Applications. Or a Low Impact Changes as defined in the PCI PA DSS program guide which meets all of the following criteria: 1. Three or fewer PA-DSS Requirements are affected, not including Requirements 13 and 14; 2. Less than half of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14; and 3. Less than half the Payment Application's functionality is affected and less than half the Payment Application's code-base is changed.	Yes
w (Wildcard)	Mandatory	**EMV - Indicator for EMV kernel changes** - This means a new EMV firmware or kernel has been introduced that would have no impact on PA-DSS or security of the application as defined in 'V'. If an 'EMV' change is identified as having an impact of PA DSS requirements or meeting either the criteria for High Impact Change or Low Impact Change in accordance to the PCI PA-DSS program guide, then the first digit, 'V', which is the PCI version digit will be incremented.	Yes
x (Wildcard)	Mandatory	**Functionality - Major Functionality Change** - This means a new feature which is large in size or multiple features have been introduced that would have no impact on PA-DSS or security of the application. If a 'functionality' change is identified as having an impact of PA DSS requirements or meeting either the criteria for High Impact Change or Low Impact Change in accordance to the PCI PA-DSS program guide, then the first digit, 'V', which is the PCI version digit will be incremented.	Yes
y (Wildcard)	Mandatory	**Maintenance - Minor enhancements and bug fixes** - This means minor enhancements or maintenance bug fixes are included without impacting the overall functionality. If a "Maintenance" change is identify as having an impact of PA DSS requirements or security of the application, then the First digit "V", which is the PCI version digit will be incremented.	Yes
z (Wildcard)	Mandatory	**Patch - Patch Release Indicator** - This is used to indicate the bug fix patch level on a previously released version to customer. Only bug fixes are included at this level.	Yes

A3 Instances where PAN is displayed

Below represented instances where VEPP NB application can show cardholders data:

Instance	Cardholder Data
CARDHOLDERS RECEIPT (Paper or ECR protocol)	PAN Masked (last 4 digits)
DISPLAY of VEPP Terminal	PAN Masked (6 first + 4 last)
MERCHANT RECEIPT (Paper or ECR protocol)	PAN Masked (6 first + 4 last)

A4 Installation and Setup

When merchant receives the terminal from Verifone, the VEPP NB application will already be preinstalled on the device. Parameters will be handled by the Terminal Management System (TMS). However, the network setup still needs to be performed on the terminal in order for it to communicate with the external systems. To achieve that, several steps need to be followed:

- Setup the communication interfaces. For doing that, enter the terminal menu by pressing the 4+6 keys together, enter the password, then navigate to Administration -> Settings -> Communications -> Configuration and configure the interfaces to use. Usable interfaces will differ from one model to another.
- Choose the network interface priorities. Since several network interfaces can be used in the same time, ensure that the interfaces are selected correctly in the network interface menu -> Administration -> Settings -> Network interface -> Default. Be sure to select the configured network as the default one. If required, networks that will be used if the default fails can be selected as fallback interfaces.