PA DSS Implementation Guide

For Verifone terminals e355 and Vx690
using the
VEPP NB application version 1.2.1.x

Version 1.6

Date: **2017-05-04**

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 1.2.1.x 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 VEPP software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in VEPP payment application 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.com

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 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 application running on your payment environment in the list on the website below, please contact our 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 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 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. Hence, the Implementation Guide should be distributed to all relevant payment application users (customers, resellers and integrators)

Note 2: This document must also be used when training integrators/resellers at initial workshops.

1.3 References

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

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.

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 Application	Terminal Payment Application for use on Verifone hardware payment environment.
VEPP Terminal	Terminal with installed VEPP 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.

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 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 application meets this requirement	No specific setup for VEPP application is required. New version of VEPP application does not use any cardholder's sensitive historical data collected by previous version of the application. On installation, VEPP application performs secure wipe for all terminal's memory, which is available for custom application files.
merchant/reseller 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 absolutely necessary for PCI DSS compliance.

Aligns with PCI DSS Requirement 3.2

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

Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	
How VEPP application meets this requirement	No any sensitive cardholder's data are retrieving by VEPP application in Verifone production terminals. In case when sensitive cardholder's data need to be present in the logs for troubleshooting is only done at Verifone lab/test environment using test terminals.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

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 application meets this requirement	All cardholder data is automatically erased during the nightly batch sending or if manual batch sending is done. See the list of files in the Annex *A1 Terminal files*
merchant/reseller actions required	All cardholder data is automatically erased once a transaction advice is sent to the host. If you want to do this operation manually it is possible. Please refer to the VEPP NB User Guide on how to send the batch manually. This will also erase all stored cardholder data. Full PAN is never sent to ECR

Aligns with PCI DSS Requirement 3.1

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

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) so only personnel with a business need can see the full PAN.	
How VEPP 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.
merchant/reseller actions required	If the terminal prints full PAN on merchant ticket please securely protect the receipts in accordance with PCI DSS Requirement 3.3 and ensure that the data available only to personnel with a legitimate business need can see the full PAN.

Aligns with PCI DSS Requirement 3.3

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

Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). The PAN must be rendered unreadable anywhere it is stored, even outside the payment application (for example, log files output by the application for storage in the customer environment)	
How VEPP 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 *A3 Instances where PAN is displayed*
merchant/reseller actions required	The customer is responsible for rendering PAN unreadable in all instances where a PAN could be stored in outside of VEPP application.

Aligns with PCI DSS Requirement 3.4

2.6 PA-DSS Req. 2.4: Protect keys

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

Aligns with PCI DSS Requirement 3.5

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

Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	
How VEPP application meets this requirement	VEPP terminal uses the following keys: TPK (Terminal PIN encryption Key) – for online PIN encryption; TEK (Terminal data Encryption Key) – SRED key for cardholder data encryption. There is no any possibility to manage the keys directly on the terminal. If a new key has to be injected the key will be wrapped by terminal unique RSA key in Verifone secure room and transferred to the terminal over TMS. All key generation and delivery implemented according to PCI requirement. Chapter *5 VEPP application key management* gives short introduction into VEPP key management.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.6

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

Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.	
How VEPP application meets this requirement	Cardholder data stored in terminal memory is encrypted by key that is periodically updated by the application without any user intervention. There is no any possibility to manage the keys directly on the terminal. If a new key has to be injected the key will be wrapped by terminal unique RSA key in Verifone secure room and transferred to the terminal over TMS. All key generation and delivery implemented according to PCI requirement. Chapter *5 VEPP application key management* gives short introduction into VEPP key management.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.6

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

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

Aligns with PCI DSS Requirement 8.1 and 8.2

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

Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	
How VEPP application meets this requirement	The VEPP application does not provide functionality and does not maintain user accounts for administrative access or individual access to cardholder data.

merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.1 and 8.2

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

Implement automated audit trails.	
How VEPP application meets this requirement	VEPP application supports syslogs. This log contains masked PANs. No cardholder data is accessible from the VEPP terminal. The application also keeps an Audit Trail to track changes to system level objects.
merchant/reseller actions required	For the Audit Trail there are no settings you need to do. The Audit Trail is created automatically and cannot be disabled. The Audit Trail could be sent manually to a centralized server. The address to the centralized log server is already set when you receive the terminal and normally there is no need to change that address in the terminal. However, if for some reason this address needs to be changed please contact the representative of your service provider. Chapter *"Audit Trail log"* also gives you guidance on how to correctly setup the centralized log server.

Aligns with PCI DSS Requirement 10.1

2.12 PA-DSS Req. 4.4: Facilitate centralized logging

Facilitate centralized logging.	
How VEPP application meets this requirement	VEPP application provides SYSLOG for audit trails delivery.
merchant/reseller actions required	The merchant/reseller needs to setup a 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

2.13 PA-DSS Req. 5.4.4: Application versioning methodology

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

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

Securely implement wireless technology. For payment applications using wireless technology, the wireless technology must be implemented securely.	
How VEPP application meets this requirement	If wireless is used VEPP application supports strong encryption (WPA) and Bluetooth 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/reseller 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

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

Secure transmissions of cardholder data over wireless networks. For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	
How VEPP application meets this requirement	If wireless is used VEPP application supports strong encryption (WPA). 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/reseller actions required	For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. For other actions please refer to *2.14* part of the implementation guide.

Aligns with PCI DSS Requirement 4.1.1

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

Provide instructions for secure use of wireless technology.	
How VEPP application meets this requirement	If wireless is used VEPP application supports strong encryption (WPA). 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/reseller 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

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

Provide instructions for customers about secure installation of patches and updates.	
How VEPP application meets this requirement	VEPP 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 application released by Verifone our Product Manager notifies responsible person of the integrator/reseller and provides all necessary material for VEP terminal update.
merchant/reseller actions required	The merchant is not required to take any action in relation to this requirement.

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

Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	
How VEPP application meets this requirement	VEPP application does not employ unnecessary or insecure services or functionality. Full list of application components and dependent components / protocols described in Annex *A3 Instances where PAN is displayed*
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.2.3

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

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

Aligns with PCI DSS Requirement 1.3.7

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

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

Aligns with PCI DSS Requirement 8.3

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

Securely deliver remote payment application updates. If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always-on" connections	
How VEPP application meets this requirement	VEPP 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/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 1 and 12.3.9

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

Securely implement remote-access software.	
How VEPP application meets this requirement	VEPP application does not provide remote access functionality and does not maintain user accounts for any remote access to the application.

merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 2, 8 and 10

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

Secure transmissions of cardholder data over public networks.	
How VEPP 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/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.1

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

Encrypt cardholder data sent over end-user messaging technologies. If the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs.	
How VEPP application meets this requirement	VEPP application doesn't use any end-user messaging technologies to send cardholder data.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.2

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

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

Aligns with PCI DSS Requirement 2.3

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

The terminal serial number is registered in TMS and WEPP application assigned to the serial number. VEPP 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.

1. Your old unit is physically replaced by a new VEPP loaded with software that complies with the PCI PA-DSS requirements.
2. Your existing VEPP 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 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

In order for your organization to comply with PCI DSS requirements it is absolutely necessary to remove historical data stored prior to installing your PCI PA-DSS compliant 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: Using the PCI PA-DSS compliant VEPP terminal you will never be prompted to enter CVV2.

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

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.

For the E355 PTS POI device used with VEPP NB the supported firmware has a built in algorithm to calculate the required PIN automatically. This increases the security as it blocks other devices from connecting with the device. The device is provided with the appropriate Bluetooth drivers and no additional configuration is required.

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.

Also the security part of the software that resides in the PED (PIN Entry Device) part of the terminal could be updated remotely. The Terminal Management System that is used for distribution of the PED software should be evaluated by a QSA as part of any PCI DSS assessment.

3.5 Encrypt sensitive traffic over public networks

Your VEPP application allows transmission over public networks, e.g. public internet. To protect sensitive data your VEPP 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. To connect your VEPP terminal to public networks you do not need to take any further action regarding encryption.

4. Back-out or product de-installation procedures

The software of your 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.

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

5.3 Key Generation

Only strong encryption keys are to be used. Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm. Depending on the encryption scheme in question, the following are minimum length requirements for the encryption keys:

Triple-DES – 112 bits

AES – 128 bits

RSA – 2048 bits

Industry recommendations/best practices for other encryption methodologies

Cryptographic keys or key components must be generated by one of the following:

An approved key-generation function of a PCI-approved HSM or POI;

An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM; or

An approved random number generator that has been certified by an independent laboratory to comply with NIST SP800-22.

Generating encryption keys is accomplished by a minimum of two custodians authorised by the [Information Security Department]. Each custodian will generate one random clear text piece (key component) that will be used to create the encryption key.

To prevent unauthorised substitution of keys, physical and logical access to the key generating procedures and mechanisms are secured. Security controls include inspection of the devices that are used in the key generation processes for any signs of tampering.

Finally, all key generation events are logged and documented with acknowledgement by all parties that all security controls have been adhered to.

6. Audit Trail log

6.1 How to change the address to the centralized log server

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

On VEPP Terminal:

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

Once A-LOG in SYSLOG format is activated, 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

The format of the terminal log file needed to meet the PCI DSS requirement 10, "Track and monitor all access to network resources and cardholder data", described in PCI Requirements and Security Assessment Procedures Version 3.

6.2.1 File size

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

6.2.2 File format

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

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

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

Event Type	Content	Description
Download	file = [filename downloaded]([download location])	Result of file download from remote host. Indicates file name downloaded and ip+port of remote host from which file was downloaded
Validate	file = [filename validated]	Validation result of file
Install	file = [filename installed]	Installation result of file
Configuration	[parameter name] old = [Old paramete value] new = [New parameter value]	Terminal configuration change affecting host IP configuration, terminal Identifiers, rescheduling of operations, change of terminal identifiers or user password change.
Audit send	ip:port = [destination ip:port]	Result of audit log sending. Indicates destination server which the log was sent to.
RT Audit Start	ip:port = [syslog server ip:port]	Start of Real-Time audit log sending to SysLog server. Indicates IP&Port of destination syslog server.
RT Audit Stop	reason = [reason for stop]	Interruption of Real-Type audit log sending to syslog server. Optionally indicates reason for stopping: e.g. technical failure, customer interruption, etc.
Startup	app[veppnb] running: 1 launch_app[veppnb] running[1] active[1] Set Application::APPLICATION_NAME = veppnb Set Application::APPLICATION_VERSION = 1.2.0.0-3 Set Application::APPLICATION_COMMIT_HASH = 131c6f7 Set Application::APPLICATION_COMMIT_DATE = 2016-08-24T07:43:31+02:00	Indicates application startup. Indicates application version as well as versions and checksums of external modules.

6.2.3 File sample

Below is an example of log entries from a terminal:

```
<67>1 2016-08-26T08:05:38.734Z - MAC 14 - - (src/mac/file.cpp:222) binary name[VEPPNB.OUT]
```

```
<71>1 2016-08-26T08:05:38.743Z - MAC 45 - - (src/mac/comm.cpp:392) Com interface successfull!
present interface[16282688]
<71>1 2016-08-26T08:05:38.753Z - MAC 14 - - (src/mac/file.cpp:446) env
file[I:1/_VEPPNB.OUT_.ENV]
<71>1 2016-08-26T08:05:38.758Z - MAC 45 - - (src/mac/comm.cpp:403) getting COM interfaces[0]
<71>1 2016-08-26T08:05:38.762Z - MAC 14 - - (src/mac/file.cpp:467) writing  env
file[I:1/_VEPPNB.OUT_.ENV]
<71>1 2016-08-26T08:05:38.766Z - MAC 45 - - (src/mac/comm.cpp:487) Present interface: WIFI
<71>1 2016-08-26T08:05:38.786Z - MAC 14 - - (src/mac/file.cpp:475) env[GUIPRT_APPNAME]=[]
<71>1 2016-08-26T08:05:38.792Z - MAC 45 - - (src/mac/comm.cpp:505) Present interface: BT
<71>1 2016-08-26T08:05:38.797Z - MAC 14 - - (src/mac/file.cpp:475) env[GUI_REGION]=[4]
<71>1 2016-08-26T08:05:43.857Z - MAC 45 - - (src/mac/comm.cpp:509) Init com values[0]
interface[16282688]
<71>1 2016-08-26T08:05:44.076Z - MAC 14 - - (src/mac/file.cpp:269) start_app[F:1/veppnb.out]
pid[64] args[] errno[2]
<71>1 2016-08-26T08:05:44.113Z - MAC 45 - - (src/libcom.cpp:1206) libcom: API
com_SetDevicePropertyInt called
<71>1 2016-08-26T08:05:44.533Z - veppnb - - - (app/main.cpp:46) Application [veppnb v1.2.0.0-
3] starting. Commit 131c6f7 2016-08-24T07:43:31+02:00
<71>1 2016-08-26T08:05:44.189Z - MAC 14 - - (src/mac/launcher.cpp:877) autolaunch app[veppnb]
region[4] pid[64] status[0]
<71>1 2016-08-26T08:05:44.792Z - veppnb - - - (src/libcom.cpp:1515) libcom: API com_GetVersion
called
<71>1 2016-08-26T08:05:44.808Z - veppnb - - - (src/libcom.cpp:431) libcom: API com_Init
called, library version: 2.7.1-154
<71>1 2016-08-26T08:05:44.711Z - MAC 45 - - (src/libcom_util.cpp:28) libcom: prv_sendCommand
send command {"command":3,"interface":200,"property":29,"property_value":10}
<71>1 2016-08-26T08:05:45.215Z - MAC 14 - - (src/mac/launcher.cpp:195) Appid[vipa]
type[service]
<71>1 2016-08-26T08:05:45.242Z - MAC 14 - - (src/mac/launcher.cpp:1143) pid[58]
cmd[F:1/mapp.vsa] running[1]
<71>1 2016-08-26T08:05:45.266Z - MAC 14 - - (src/mac/launcher.cpp:1143) pid[58] cmd[]
running[0]
<71>1 2016-08-26T08:05:45.285Z - MAC 14 - - (src/mac/launcher.cpp:1091) app[vipa] running: 1
<71>1 2016-08-26T08:05:45.454Z - veppnb - - - (src/libcom_net.cpp:531) libcom: Created network
thread
<71>1 2016-08-26T08:05:45.456Z - veppnb - - - (src/libcom.cpp:1520) libcom: API
com_GetSvcVersion called
<71>1 2016-08-26T08:05:45.295Z - MAC 45 - - (src/libcom_util.cpp:81) libcom: prv_sendCommand
received {"command":3,"error":0,"interface":13,"property":29,"property_value":10,"result":0}
from daemon
<71>1 2016-08-26T08:05:45.306Z - MAC 14 - - (src/mac/launcher.cpp:777) autolaunch[vipa]
running[1]
<71>1 2016-08-26T08:05:45.312Z - MAC 45 - - (src/libcom_util.cpp:107) libcom: prv_sendCommand
daemon has accepted

<71>1 2016-08-26T08:05:45.617Z - veppnb - - - (src/libcom_util.cpp:107) libcom:
prv_sendCommand daemon has accepted
<71>1 2016-08-26T08:05:45.621Z - veppnb - - - (application/application.cpp:83) Set
Application::APPLICATION_NAME = veppnb
<71>1 2016-08-26T08:05:45.456Z - MAC 14 - - (src/mac/region.cpp:900) appid[veppnb]
statusbar[1]
<71>1 2016-08-26T08:05:45.457Z - MAC 14 - - (src/mac/layout.cpp:97) Getting application last
statusbar state[0]
<71>1 2016-08-26T08:05:45.642Z - veppnb - - - (application/application.cpp:92) Set
Application::APPLICATION_VERSION = 1.2.0.0-3
<71>1 2016-08-26T08:05:45.644Z - veppnb - - - (application/application.cpp:101) Set
Application::APPLICATION_COMMIT_HASH = 131c6f7
<71>1 2016-08-26T08:05:45.477Z - MAC 14 - - (src/mac/region.cpp:1312) layout[mac-app-sb]
statusbar[1] keyboard[0] status[0]
<71>1 2016-08-26T08:05:45.646Z - veppnb - - - (application/application.cpp:110) Set
Application::APPLICATION_COMMIT_DATE = 2016-08-24T07:43:31+02:00
```

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	Encrypted by SRED
SYSLOG.LOGx	Application log data. Used for monitoring.	PAN	Masked (6 first + 4 last)

A2 Application Version Numbering policy

The following convention should be used for all applications:

APPNAME-a.b.S.c<-bldno|-RCn|-<D> where

M or O	Letter	Description	Example Version	Example Description
Mandatory	a	**Major Application Architecture Change** - This means that you cannot upgrade from 4 to 5 or 5 to 6 for example without either changing the hardware or changing the OS (eg. Verix to Verix EVO) or installing from scratch. NOTE: From version 6, for VIPA will be OS independent across VOS and Verix EVO.	1.2.0.0 to 2.0.0.0	VOS2 to VOS3
Mandatory	b	**Major Functionality Change** - This means a new feature has been introduced	1.2.0.0 to 1.3.0.0	CTLS PayPass 3.0 support, new GUI support, etc
Mandatory	S	SRED/P2P2 Application Certified - check PCI web site for Validated P2PE Applications either ▪ 0 if not P2PE Certified ▪ 1 if it has **NOTE: numbers 2 and above are reserved for future use, and should never be used for any customer specific indications.**	• 6.0.0.0 • 6.0.1.0 • 6.0.1.1 • 6.2.1.1	• Not P2PE Certified/Listed • Is P2PE Certified/Listed • Bugfix to P2PE Certified release which is NOT security impacting. • Bugfix which is security impact, represents new major functionality.
Mandatory	c	**Patch Release** - This is used to indicate the bugfix patch level to that release. (No new functionality will be added)	6.0.0.0 to 6.0.0.1	A bug has been found in an existing feature which doesn't impact certification.

Optional	bldno	**Build Number** - 0,1,2 etc. - This is only for a Development & QA tracking purpose to distribute builds internally only between releases. QA should certify a build to be good, at which point this get's renamed by removing the build number. Builds should never go to the customer as they cannot be consider as QA tested until QA make it available (see RC)	MYAPP-6.0.0.0-1 MYAPP-6.0.0.0-2 etc.	
Optional	RCn	**Release Candidate** - This is a release that can go to the customer, but can only be certified as customer available by the QA team. Release Candidate versions means that the functionality has known issues but has been through a QA test cycle, and thus a test exit report together with a set of release notes with known issues can be provided to the customer. n - should indicate a number number increasing from 1.	MYAPP-6.0.0.0-RC1	Release candidate done for customer X for pilot testing.
Optional	D	**Debug Version** - If a release with all the debug symbols compiled/enabled is in.	MYAPP-6.0.0.0-D	

A3 Instances where PAN is displayed

Below represented instances where VEPP application can show cardholders data:

Instance	Description	Protection
CARDHOLDERS RECEIPT (terminal printer and/or ECR protocol)		Masked
DISPLAY of VEPP Terminal	Approved transaction	Masked
	Declined transaction	Masked
ECR protocol: transaction result message	Regular transaction	Masked
	Offline transaction	Masked

A4 Application components and used protocols

Hardware platform supported:

Vx690 (PCI PTS approval Number: 4-30128)
e355 (PCI PTS approval Number: 4-30168)

OS Requirements:

Verix eVo

Terminal to Host protocol in use:

ISO 8583 - POS 03001

Terminal to ECR protocol in use:

EPAS 2.0

A5 Installation and Setup

Instructions about installation, setup and use can be found in the document "Cobra_QuickStartupGuide"