Verifone

®

Verifone Finland PA-DSS

Implementation Guide

Atos Worldline Yomani & Yomani ML 3.00.xxxx.xxxx

Verifone Vx520, Vx520C, Vx680, Vx690, Vx820 & Ux300 VPFIPA0401.xx.xx

Contents

1 Revision history

Version	Author	Date	Comments
0.1	Pekka Ylitalo	1.2.2010	Initial draft
0.2	Pekka Ylitalo	5.2.2010	Review by Martin Gutekunst
0.3	Pekka Ylitalo	26.2.2010	Updated after review by Acertigo
0.4	Lauri Mäkinen	27.4.2010	Made YOMANI related changes to req. 1.1.5 and chapter 5
1.0	Lauri Mäkinen	4.5.2010	Updated version number to 1.0
1.1	Pekka Ylitalo	25.8.2010	Made changes to req. 1.1.4 and chapter 6
1.2	Pekka Ylitalo	8.12.2011	Verifone application firewall requirement changes to chapter 4.3 req. 6 and chapter 4.4 req. 9 and 10
1.3	Kimmo Heiskanen	10.5.2013	Added multiple requirement definitions to meet PA-DSS v2.0 audit requirements
1.4	Pekka Ylitalo	16.9.2013	Implementation guide updated and finalized according to PA-DSS v2.0 implementation guide requirements
1.5	Pekka Ylitalo	15.10.2013	Minor updates after review by TÜV SÜD
1.6	Pekka Ylitalo	4.2.2014	Added Verifone terminal models to the title page
1.7	Pekka Ylitalo	2.7.2014	Implementation guide updated according to PA-DSS v3.0 implementation guide requirements
1.8	Pekka Ylitalo	21.10.2014	Updates after review by Adsigo
1.9	Pekka Ylitalo	10.03.2015	Yomani ML and Vx690 added to terminal models. TLS is now used for all terminal models instead of SSL.
2.0	Pekka Ylitalo	19.11.2015	Company name and information changed from Point to Verifone
2.1	Pekka Ylitalo	28.11.2016	Implementation guide updated according to PA-DSS v3.2 implementation guide requirements. Removed Vx670 from terminal models. Added Vx520C to terminal models.
2.2	Pekka Ylitalo	22.12.2016	Application methodology updated for Verifone terminals. Reviewed by Adsigo.

2.2	Pekka Ylitalo	1.1.2017	Annual review. No changes needed.
2.2	Pekka Ylitalo	1.1.2018	Annual review. No changes needed.

2   Introduction

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

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

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

http://www.pcisecuritystandards.org

3   Document use

This PA-DSS Implementation Guide contains information about the Verifone application. Verifone Finland Oy does not possess the authority to state that a merchant may be deemed "PCI Compliant". 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 Verifone application in a manner that will support a merchant's PCI DSS compliance efforts.

3.1   Important notes

• This guide refers to Verifone application 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 running on your Verifone terminal on that list please contact our helpdesk at Verifone in order to upgrade your terminal

• Both the System Installer and the controlling merchant must read this document

• This document must also be used when training ECR integrators/resellers at initial workshops

4   Summary of requirements

This summary covers shortly the PCI DSS/PA-DSS requirements that have a related PA-DSS Implementation Guide topic. It also explains how the requirement is handled in the Verifone application and also explains the requirement from your aspect.

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

http://www.pcisecuritystandards.org

4.1   Do not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data

Requirement 1.1.4: Delete sensitive authentication data stored by previous payment application versions.

1. What the requirement says

Securely delete any track data (from the magnetic stripe or equivalent data contained on a chip), card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.

2. How the Verifone application meets this requirement

No specific setup for the Verifone application is required. The Verifone application does not store any historical data so removal of historical data is not needed.

3. What this means to you

You must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) is removed from all other storage devices used in your systems, ECRs, PCs, servers etc. For further details please refer to the appropriate vendor. Removal of historical data is absolutely necessary for PCI DSS compliance.

Requirement 1.1.5: Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.

1. What the requirement says

Do not store sensitive authentication data on vendor systems. If any sensitive authentication data (pre-authorization data) must be used for debugging or troubleshooting purposes, ensure the following:

• Sensitive authentication data is collected only when needed to solve a specific problem.

• Such data is stored in a specific, known location with limited access.

• The minimum amount of data is collected as needed to solve a specific problem.

• Sensitive authentication data is encrypted with strong cryptography while stored.

• Data is securely deleted immediately after use, including from:

- Log files

- Debugging files

- Other data sources received from customers

2. How the Verifone application meets this requirement

Generally troubleshooting is not done on production terminals. However, if logs are written, no sensitive data is included in them.

Terminal logging level may be raised to a higher level from the application. If the logging level is for any reason raised to a higher level PAN's are stored in truncated format.

Logs can only be sent from terminal to a Verifone backend and thus be examined only by Verifone personnel.

Troubleshooting logs storage time is 20 days.

3. What this means to you

No actions needed.

4.2   Protect stored cardholder data

Requirement 2.1: Securely delete cardholder data after customer-defined retention period.

1. What the requirement says

Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period.

2. How the Verifone application meets this requirement

All cardholder data is automatically erased during the nightly batch sending or if manual batch sending is done.

Below is a list of all the locations where the payment application stores cardholder data:

- Verifone terminals:

    o FILETRANSLIST.LST, PAYMENTS.BLS, EcrTrnBackup.LST, TrmLog.log, FILESETUP.CFG, paymentapplog.txt and paymentapplog.zip

- Atos Worldline Yomani terminals:

    o /usr/paymentapp/logs, /usr/paymentapp/store/pending, /usr/paymentapp/store/sent, /usr/paymentapp/store/lastFailed,

/usr/paymentapp/blacklist_ranges.bin and

/usr/paymentapp/blacklist_singles.bin

No activity is necessary to prevent inadvertent capture or retention of cardholder data. For example, system backup or restore points.

3. What this means to you

All cardholder data is automatically erased during the nightly batch sending. If you want to do this operation manually it is possible. Please refer to the Verifone application user manual on how to send the batch manually. This will erase all cardholder data.

Requirement 2.2: Mask PAN when displayed so only personnel with a business need can see more than the first six/last four digits of the PAN.

1. What the requirement says

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

2. How the Verifone application meets this requirement

PAN is always automatically masked as described above. PAN can be shown in the following instances:

- Receipt

- Terminal screen

- Troubleshooting logs

3. What this means to you

No actions needed.

Requirement 2.3: Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs).

1.What the requirement says

Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)

- Truncation (hashing cannot be used to replace the truncated segment of PAN)

- Index tokens and pads (pads must be securely stored)

- Strong cryptography with associated key-management processes and procedures.

2.How the Verifone application meets this requirement

PAN is always automatically rendered unreadable anywhere it is stored.

3.What this means to you

No actions needed.

Requirement 2.4: Protect keys used to secure cardholder data against disclosure and misuse.

1.What the requirement says

Payment application must protect any keys used to secure cardholder data against disclosure and misuse.

2.How the Verifone application meets this requirement

Access to the encryption keys is prevented. Keys are stored in special safe memory.

3.What this means to you

No actions needed.

Requirement 2.5: Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

1. What the requirement says

Payment application must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

2. How the Verifone application meets this requirement

The KEY management process is automatic and controlled only by the Verifone application.

See chapter 5 for detailed information about key management and cryptographic material removal.

3. What this means to you

No actions needed.

Requirement 2.5.1 – 2.5.7: Implement secure key-management functions.

1.What the requirement says

Generation of strong cryptographic keys. Secure cryptographic key distribution. Secure cryptographic key storage.

Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher-

text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines.

Retirement or replacement of keys (for example: by archiving, destruction, and/or revocation as applicable) as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component, etc.) or keys are suspected of being compromised.

If the payment application supports manual clear-text cryptographic key-management operations, these operations must enforce split knowledge and dual control.

Prevention of unauthorized substitution of cryptographic keys.

2.How the Verifone application meets this requirement

The KEY management process is automatic and controlled only by the Verifone application.

See chapter 5 for detailed information about key management and cryptographic material removal.

3.What this means to you

No actions needed.

Requirement 2.6: Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.

1. What the requirement says

Provide a mechanism to render irretrievable any cryptographic key material or cryptogram stored by the payment application, in accordance with industry-accepted standards.

These are cryptographic keys used to encrypt or verify cardholder data.

2. How the Verifone application meets this requirement

All cryptographic material must be removed and it is absolutely necessary for PCI DSS compliance. The removal of this material is automatically handled by the Verifone application so you do not need to take any action.

See chapter 5 for detailed information about key management and cryptographic material removal.

3. What this means to you

No actions needed.

4.3 Provide secure authentication features

Requirement 3.1: Use unique user IDs and secure authentication for administrative access and access to cardholder data.

1. What the requirement says

The payment application must support and enforce the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication must be enforced to all accounts generated or managed by the application by the completion of installation and for subsequent changes after installation.

2. How the Verifone application meets this requirement

No administrative access to the Verifone application is possible.

3. What this means to you

No actions needed.

Requirement 3.2: Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.

1. What the requirement says

Software vendor must provide guidance to customers that all access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication.

2. How the Verifone application meets this requirement

The Verifone application does not provide any accounts or access to critical data.

3. What this means to you

No actions needed.

4.4 Log payment application activity

Requirement 4.1: Implement automated audit trails.

1. What the requirement says

At the completion of the installation process, the "out of the box" default installation of the payment application must log all user access and be able to link all activities to individual users.

2. How the Verifone application meets this requirement

The Verifone application does not allow making any changes relevant to the payment functionality. Because of this no activity can be performed which would need logging/auditing.

3. What this means to you

No actions needed.

Requirement 4.4: Facilitate centralized logging.

1. What the requirement says

Payment application must facilitate centralized logging

2. How the Verifone application meets this requirement

The Verifone application provides a functionality that it sends logs into an arbitrary log server, in general a log server maintained by the merchant. This functionality is always on by default and it cannot be changed or turned off. Disabling logs would result in non-compliance with PCI DSS so therefore it cannot be done.

Troubleshooting logs are sent separately from the payment terminal if requested by Verifone backend system, or by activating troubleshooting log sending from the terminal.

3. What this means to you

If you want to receive the logs you need to setup an arbitrary log server. Logs are sent in syslog format, so any system that can assimilate syslog format messages will work as an arbitrary log server.

Please refer to the Verifone application user manual on how to enter the arbitrary log server's IP-address onto the terminal or contact Verifone customer service. Below is the relevant section from the user's manual:

2.10 Audit log IP

With the audit log IP-function, your payment terminal sends log information to a desired IP-address. The terminal logs include error and update information etc. from the payment terminal.

To input your desired IP-address, select the Settings icon from the screen and press enter. Choose Edit, and navigate down with the arrow icon and select Audit log IP. Input the IP-address; to get a dot, press 1 repeatedly until the correct character is on the display.

If you are using a Yomani terminal please contact Verifone customer service.

4.5 Develop secure payment applications

Requirement 5.4.4: Implement and communicate application versioning methodology.

1.What the requirement says

The vendor's published versioning methodology must be communicated to customers and integrators/resellers.

2.How the Verifone application meets this requirement

The Verifone application uses the following version methodologies in all releases:

For Verifone terminals the version number has three parts: XXYY.RR.SS		
Version number component:	Description:	Changes if:
XX	Major Version	• Major changes to payment process, change that impacts security functionality • Major OS update case, operating system is dramatically changed • New terminal model a new PTS approval addition to the application • Existing terminal model has got a new PTS approval
YY	Minor version	• Large feature additions • Terminal model addition where PTS approval already is within applications PA-DSS approval, but requiring application changes to implement • OS update what requires application changes
RR	Wildcard / Revision	• Changes that have impact on application functionality but no impact on security or PA-DSS requirements • Changes have no impact on functionality of application or it's dependencies - cosmetic changes for instance • Patch into OS and no change into PTS approval • Terminal model addition where PTS approval already is within applications PA-DSS approval and not requiring application changes to implement

		• Additions that don't touch PA-DSS, revision exists for internal use • Wildcard number resets on Major & Minor updates, otherwise increases continuously
SS	Wildcard / Revision incremental	• Incremental identifier for a version, for instance a small patch to application

For Yomani terminals the version number has four parts: X.YY.RRRR.SSSS		
Version number component:	Description:	Changes if:
X	Major Version	• Major changes to payment process, change that impacts security functionality. Requires a full PA-DSS assessment. • Major OS update case, operating systems is dramatically changed • New terminal model a new PTS approval addition to the application • Existing terminal model has got a new PTS approval
YY	Minor version	• Large feature additions • Terminal model addition where PTS approval already is within applications PA-DSS approval, but requiring application changes to implement • OS update what requires application changes
RRRR	Wildcard / Revision	• Changes that have impact on application functionality but no impact on security or PA-DSS requirements • Changes have no impact on functionality of application or it's dependencies - cosmetic changes for instance

		• Patch into OS and no change into PTS approval • Terminal model addition where PTS approval already is within applications PA-DSS approval and not requiring application changes to implement • Additions that don't touch PA-DSS, revision exists for internal use • Wildcard number resets on Major & Minor updates, otherwise increases continuously
SSSS	Sprint	• The development sprint to what code base the application is based at, used for easier application version identfication • Sprint is consisting of month & year. mmyy

3.What this means to you

No actions needed.

4.6 Protect wireless transmissions

Requirement 6.1: Securely implement wireless technology.

1. What the requirement says

For payment applications using wireless technology, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The wireless technology must be implemented securely.

2. How the Verifone application meets this requirement

The Verifone application operates in a network behind a firewall or in a network without a firewall. The Verifone application supports strong encryption for wireless, WPA and WPA2. Also all data sent to and from the Verifone application is always protected using TLS.

For ECR integrations TLS is not used when the terminal is communicating with the ECR using serial port or WiFi connection. Also for log sending TLS is not used. These connections never contain any cardholder sensitive data.

See requirement 8.2 for the communication protocols and ports used by the Verifone application on wireless networks.

3. What this means to you

If you are using wireless network within your business you must make sure that firewalls are installed and configured to deny or (if such traffic is necessary for business purposes) permit only authorized traffic betyoun the wireless environment and the Verifone application environment and any system that stores cardholder data. Please refer to your firewall manual.

In case you are using a wireless network you must also make sure that the following requirements are met:

• Encryption keys and passwords are changed from vendor defaults at installation

• Encryption keys and passwords are changed anytime someone with knowledge of them leaves the company or changes position

• Default SNMP community strings on wireless devices are changed

• SNMP community strings on wireless devices are changed anytime someone with knowledge of them leaves the company or changes position

• Firmware on wireless devices is updated to support strong encryption, WPA/WPA2. Please note that the use of WEP as a security control was prohibited as of 30 June 2010.

• Other security related vendor defaults like passwords and logins are changed

Requirement 6.2: Secure transmissions of cardholder data over wireless networks.

1. What the requirement says

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. Please note that the use of WEP as a security control was prohibited as of 30 June 2010.

2. How the Verifone application meets this requirement

The Verifone application supports strong encryption for wireless, WPA and WPA2. Also all data sent to and from the Verifone application is always protected using TLS.

For ECR integrations TLS is not used when the terminal is communicating with the ECR using serial port or WiFi connection. Also for log sending TLS is not used. These connections never contain any cardholder sensitive data.

3. What this means to you

Please refer to the Verifone application user manual on how to configure the application to use strong encryption for wireless. Below is the relevant section from the user's manual:

2.11 WIFI settings

NOTE! To change the WIFI information you need the terminal's daily password. To get the password go to Point reporting or contact Point's customer service.

Press the SETTINGS icon and input the daily password.
Press enter and choose EDIT
Choose WLAN PARAMS

SSID = Network's name
WEP KEY = Network's password
WEP MODE = WPA or WPA2 **NOTE! The terminal doesn't support other encryptions!**
CHANNEL = Number for the channel in use

Requirement 6.3: Provide instructions for secure use of wireless technology.

See requirement 6.1.

4.7 Test payment applications to address vulnerabilities and maintain payment application updates

Requirement 7.2.3: Provide instructions for customers about secure installation of patches and updates.

1. What the requirement says

Provide instructions for customers about secure installation of patches and updates.

2. How the Verifone application meets this requirement

All Verifone application updates and patches are downloaded from Verifone's terminal management system by the Verifone application and are automatically installed after download.

All applications and patches are signed by Verifone. The signature in the applications and patches ensure that the applications and patches are verified by Verifone and cannot be replaced with any other applications or patches.

3. What this means to you

No actions needed.

4.8 Facilitate secure network implementation

Requirement 8.2: Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.

1. What the requirement says

The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application.

SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that use or support TLS must not allow fallback to SSL.

2. How the Verifone application meets this requirement

The Verifone application and terminals use TLS-secured communication by default. Below is a list of all the communication protocols and ports used.

Connection type	Protocols used	Port numbers
Cable / Ethernet	TCP/IP TLS for host Serial, TCP for ECR TCP, UDP for audit logs	Host: 443 ECR: Port defined on ECR side Audit logs: Port defined on audit log server side
WiFi	WiFi TLS for host TCP for ECR TCP for audit logs	Host: 443 ECR: Port defined on ECR side Audit logs: Port defined on audit log server side
Bluetooth	TCP/IP TLS for host Serial, TCP for ECR TCP for audit logs	Host: 443 ECR: Port defined on ECR side Audit logs: Port defined on audit log server side
GPRS / 3G	GPRS TLS for host TCP for audit logs	Host: 443 Audit logs: Port defined on audit log server side

For ECR integrations TLS is not used when the terminal is communicating with the ECR using serial port, TCP or WiFi connection. Also for log sending TLS is not used. These connections never contain any cardholder sensitive data.

3. What this means to you

No actions needed.

4.9 Cardholder data must never be stored on a server connected to the Internet

Requirement 9.1: Store cardholder data only on servers not connected to the Internet.

1. What the requirement says

The payment application must be developed such that any web server and any cardholder data storage component (for example, a database server) are not required to be on the same server, nor is the data storage component required to be on the same network zone (such as a DMZ) with the web server.

2. How the Verifone application meets this requirement

The Verifone application does not store any cardholder data in a server connected to the internet.

3. What this means to you

No actions needed.

4.10 Facilitate secure remote access to payment application

Requirement 10.1: Implement multi-factor authentication for all remote access to payment application that originates from outside the customer environment.

1. What the requirement says

Multi-factor authentication must be used for all remote access to the payment application that originates from outside the customer environment.

2. How the Verifone application meets this requirement

The Verifone application cannot be accessed remotely.

3. What this means to you

No actions needed.

Requirement 10.2.1: Securely deliver remote payment application updates.

1. What the requirement says

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 virtual private network (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.

2. How the Verifone application meets this requirement

The Verifone application is not delivered remotely to the customer's systems. Application updates are downloaded from Verifone's terminal management system. The Verifone application cannot be accessed remotely.

3. What this means to you

No actions needed.

Requirement 10.2.3: Securely implement remote-access software.

1. What the requirement says

If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely.

2. How the Verifone application meets this requirement

The Verifone application cannot be accessed remotely.

3. What this means to you

No actions needed.

4.11 Encrypt sensitive traffic over public networks

Requirement 11.1: Secure transmissions of cardholder data over public networks.

1. What the requirement says

If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

2. How the Verifone application meets this requirement

All data sent to and from the Verifone application is always protected using TLS. Only trusted keys and/or certificates are accepted and used by the Verifone application.

For ECR integrations TLS is not used when the terminal is communicating with the ECR using serial port or WiFi connection. Also for log sending TLS is not used. These connections never contain any cardholder sensitive data.

3. What this means to you

No actions needed.

Requirement 11.2: Encrypt cardholder data sent over end-user messaging technologies.

1.   What the requirement says

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.

2.   How the Verifone application meets this requirement

The Verifone application is not able to send any cardholder data using end-user messaging technologies

3.   What this means to you

No actions needed.

4.12 Secure all non-console administrative access

Requirement 12.1 – 12.2: Encrypt non-console administrative access.

1.   What the requirement says

If the payment application facilitates non-console administrative access, encrypt all such access with strong cryptography.

2.   How the Verifone application meets this requirement

The Verifone application cannot be accessed remotely and no non-console access is possible.

3.   What this means to you

Any applicable terminal management systems used as part of an authenticated remote software distribution framework for the PED, should be evaluated by a QSA as part of any PCI DSS assessment.

5   Verifone application key management

The main idea is that the KEY management process is automatic and controlled only by the Verifone application. It does not require any key injections from outside. A 3DES key is used for encryption. The key is generated and stored in the POS TRM and never goes outside.

• The 3DES encryption key is generated by the terminal's operating system.

• The encryption key is stored in tamper evident memory by the terminal's operating system.

• Key transmission is not required.

• Non-YOMANI terminals: New key is generated when terminal starts for the 1st time, after terminal software update, after every batch sending (at least once per 24 hours) and after manual transaction deletion operation. If the key generation process was not successful then

the application doesn't allow making any payment transactions, only service functions are allowed. Before new key generation the old key is destroyed and cryptographic material is removed.

• Non-YOMANI terminals: If for some reason the application/terminal is not able to send the batch for a time longer than 30 days, then the application doesn't allow making any payment transactions.

• YOMANI terminals: Each encrypted file will use a unique encryption key. When a single encryption is more than one year old, it is regenerated and the file is re-encrypted using the new key.

6   Implementation Guide reviews and updates

The Verifone PA-DSS Implementation Guide is reviewed on an annual basis and updated as needed to document all major and minor changes to the Verifone application and PA-DSS standard changes. When a new implementation guide is released there will be a notification about this in the news section on the Verifone website.

The latest Verifone PA-DSS Implementation Guide can be found at:

http://www.verifone.fi

7   Terminology

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.

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.

Cardholder Data: PAN, Expiration Date, Cardholder Name and Service Code.

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.

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.

SSL: Secure Sockets Layer is a commonly used method to protect transmission across public networks. SSL includes strong encryption.

TLS: Acronym for "Transport Layer Security." Designed with the goal of providing data secrecy and data integrity between two communicating applications. TLS is the successor of SSL.

ECR: Electronic Cash Register

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.

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.

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.

WEP: Wired Equivalent Privacy, a wireless network security standard. Sometimes erroneously called "Wireless Encryption Protocol"

Magnetic Stripe Data: Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.

Sensitive Authentication Data: Magnetic Stripe Data, CVV2 and PIN.

POS: Point of sale

TRM: Tamper resistant module

3DES: Triple DES common name for the Triple Data Encryption Algorithm

8   References

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

2. Payment Card Industry – Data Security Standard v3.2