Verifone

PCI PA DSS Implementation Guide

For
Atos Worldline Banksys YOMANI XR
terminals using the
SAPC Y02.01.xxx Payment Core
(Stand Alone)

Version 2.1

Date: **01-Aug-2016**

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 SAPC payment core application in your business to store, process, or transmit payment card information, this standard and this guide apply to you.

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

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

http://www.pcisecuritystandards.org

This guide is updated whenever there are changes in SAPC software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in the software 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.se/

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 Atos terminals using SAPC Payment Core. The version of SAPC Payment Core is listed 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 your SAPC application on that list 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 SAPC 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 SAPC 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, Version 3.2
(2) Payment Card Industry – Data Security Standard, Version 3.2
(3) Babs & CEKAB Security Requirements for an EFTPOS Terminal, Version 3.0

1.4 Update History

Ver.	Name	Date	Comments
1.00	Mats Oscarsson	18-Sep-2013	Initial Revision
1.10	Mats Oscarsson	26-Feb-2014	Changed to also cover the YOMANI XR HW plat-form.
2.0	Sergejs Melnikovs	12-Jun-2016	Major update: - Document rebranding; - Changes according to PCI 3.2; - Rewording with focus on PCI PA DSS requirements; - SAPC version Y02.01.xxx only supported starting from this version of implementation guide
2.1	Sergejs Melnikovs	01-Aug-2016	Changes according to PA QSA recommendations.

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.
SAPC Application	Terminal Payment Application for use on Verifone hardware payment environment.
SAPC Terminal	Terminal with installed SAPC 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 provides basic overview of the PCI PA-DSS requirements that have a related to Implementation Guide topic. It also explains how the requirement is handled on the SAPC application side and required actions for your (as a customer).

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

http://www.pcisecuritystandards.org

Note: If a Terminal Management Systems is used as part of an authenticated remote software distribution framework for the PED, it should be evaluated by a QSA as part of any PCI DSS assessment.

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 SAPC application meets this requirement	No specific setup for SAPC application is required. New version of SAPC application does not use any cardholder's sensitive historical data collected by previous version of the application. On installation, SAPC 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 SAPC application meets this requirement	No any sensitive cardholder's data are retrieving by SAPC 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 SAPC 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 according to batch sending configuration on SAPC terminal. If you want you can send batch manually Please securely protect the merchant receipts/data and securely delete them after retention period in accordance with PCI DSS Requirements. Such protection is absolutely necessary for PCI DSS compliance.

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 SAPC 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 SAPC 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 SAPC 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 SAPC 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 SAPC application meets this requirement	There is no any possibility to manage the keys directly on the terminal. All key generation and delivery implemented according to PCI requirements and *(3) Babs & CEKAB Security Requirements for an EFTPOS Terminal, Version 3.0*
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 SAPC 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. All key generation and delivery implemented according to PCI requirements and *(3) Babs & CEKAB Security Requirements for an EFTPOS Terminal, Version 3.0*
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 SAPC application meets this requirement	SAPC 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 SAPC application meets this requirement	SAPC 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 SAPC application meets this requirement	SAPC application keeps a log for the 1000 latest transactions. This log contains truncated PANs. No cardholder data is accessible from the SAPC 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 SAPC application meets this requirement	SAPC 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 SAPC 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 SAPC application meets this requirement	SAPC application does not support wireless communication type.
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 SAPC application meets this requirement	SAPC application does not support wireless communication type.
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 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 SAPC application meets this requirement	SAPC application does not support wireless communication type.
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 SAPC application meets this requirement	SAPC 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 SAPC application released by Verifone our Product Manager notifies responsible person of the integrator/reseller and provides (in according with Software Release Distribution process) all necessary material for SAPC terminal update.
merchant/reseller actions required	The merchant is not required to take any action in relation to this requirement. The integrator/reseller which provides management server service to the customer should configure the management server to deliver patches and updates to SAPC terminal once it's received from Verifone.

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 SAPC application meets this requirement	SAPC application does not employ unnecessary or insecure services or functionality. Full list of application components and dependent components / protocols described in Annex *A4 Application components and used protocols*
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 SAPC application meets this requirement	SAPC 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 SAPC application meets this requirement	SAPC 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 SAPC application meets this requirement	SAPC 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.
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 SAPC application meets this requirement	SAPC 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 SAPC application meets this requirement	SAPC application encrypts cardholder data using triple DES with a unique key per transaction (field encryption) according to *(3) Babs & CEKAB Security Requirements for an EFTPOS Terminal, Version 3.0*. On top of that the entire messages sent to and from the SAPC Terminal are protected using SSL/TLS, if the processor supports SSL/TLS protocol.
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 SAPC application meets this requirement	SAPC 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: Secure all non-console administrative access

Encrypt non-console administrative access. Use multi-factor authentication for all personnel with non-console administrative access.	
How SAPC application meets this requirement	SAPC 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 SAPC terminal to ensure PCI DSS compliance

3.1 Do not retain full magnetic stripe or card validation code

When upgrading the payment application in your SAPC 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 SAPC loaded with software that complies with the PCI PA-DSS requirements.
2. Your existing SAPC 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 SAPC 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 SAPC 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 SAPC 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.

However, if you need to enter PAN, expiration date and CVV2 manually or do a voice referral you should never write down or otherwise store PAN, expiration date or CVV2. Collect this type of data only when absolutely necessary to perform manual entry or voice referral.

Note: Using the PCI PA-DSS compliant SAPC terminal you will never be prompted to enter CVV2.

No any sensitive authentication data are retrieving by SAPC 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 SAPC terminal for offline transactions. For this encryption a unique key per transaction is used. Once your SAPC terminal goes online any stored transactions are sent to the processor and securely deleted from the SAPC 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 SAPC 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 SAPC 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.

3.4 Facilitate secure remote software updates

The software of your SAPC 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 SAPC application allows transmission over public networks, e.g. public internet. To protect sensitive data your SAPC application uses field encryption technology based on triple DES encryption with a unique key per transaction according to *(3) Babs & CEKAB Security Requirements for an EFTPOS Terminal, Version 3.0*. On top of that all data sent to and from the SAPC terminal is protected under SSL/TLS. To connect your SAPC 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 SAPC terminal could be updated remotely either automatically or manually triggered. In the unlikely event that your newly downloaded software fails or malfunctions please contact your TMS operator in order to allow you to download an older version of the software.

5. Audit Trail log

5.1 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 SAPC Terminal:

1. Select "ADMIN"
2. Select (3) "LOGGMENY"
3. Select (1) "INSTÄLLNINGAR"
4. Select (1) "KOMMUNIKATION"
5. Enter IP address
6. Enter port number

However, if you want to use another server and receive the Audit Trail in SYSLOG format then do as follows.

On SAPC Terminal:

1. Select "ADMIN"
2. Select (3) "LOGGMENY"
3. Select (2) "A-LOG" (Audit Trail)
4. Select (2) "SKICKA TCP SYSLOGG"
5. Select (2) "REAL-TIME SKICKA"
6. Enter IP address for Syslog Server
7. Enter PORT number
8. Select (1) "On"

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 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.

5.2 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.

5.2.1 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.

5.2.2 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	YYMMDDhhmmss
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
Config	[parameter name] <separator:’ ’> old = [Old paramete value] <separator:’!’> 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	Audit log started – A-LOG STARTED APP.VERS: [value] BUILD: [value] Paymentcore: [value] Key version: [value] Samoa version: [value] SHA1: [value] /mp1.img SHA1: [value] /linux SHA1: [value] /emv_eng/EmvEng SHA1: [value] /EmvEng MD5: [value] /ePoint MD5: [value] /ppEng MD5: [value] /pwEng	Indicates application startup. Indicates application version as well as versions and checksums of external modules.

5.2.3 File format

Below is an example of log entries from a terminal:

```
DCAPP;Config;160615170600;OK;Man;Erase all TspFiles
DCAPP;Validate;160615170605;NOK;Auto;file=BINPAR
DCAPP;Download;160615170611;OK;Man;file=9370000100002705(88.131.71.147:443)
DCAPP;Validate;160615170611;OK;Man;file=9370000100002705
DCAPP;Download;160615170612;OK;Man;file=BINPAR__160615151349
DCAPP;Download;160615170614;OK;Man;file=CAPUB___130320115017
DCAPP;Download;160615170614;OK;Man;file=DCPAR___160615151347
DCAPP;Download;160615170615;OK;Man;file=MASPAR__160615151347
DCAPP;Download;160615170615;OK;Man;file=SRVCA___121030140000
DCAPP;Download;160615170616;OK;Man;file=SRVCRL__121030140000
DCAPP;Download;160615170617;OK;Man;file=CTLSPAR_160615151349(88.131.71.147:443)
DCAPP;Download;160615170618;OK;Man;file=CTLSPARH160615151350(88.131.71.147:443)
DCAPP;Validate;160615170620;OK;Man;file=BINPAR__160615151349
DCAPP;Validate;160615170621;OK;Man;file=CAPUB___130320115017
DCAPP;Validate;160615170621;OK;Man;file=DCPAR___160615151347
DCAPP;Validate;160615170621;OK;Man;file=MASPAR__160615151347
DCAPP;Validate;160615170621;OK;Man;file=CTLSPAR_160615151349
DCAPP;Validate;160615170621;OK;Man;file=CTLSPARH160615151350
DCAPP;Install;160615170621;OK;Man;file=BINPAR__160615151349
DCAPP;Install;160615170621;OK;Man;file=CAPUB___130320115017
DCAPP;Install;160615170621;OK;Man;file=DCPAR___160615151347
DCAPP;Install;160615170621;OK;Man;file=MASPAR__160615151347
DCAPP;Install;160615170621;OK;Man;file=CTLSPAR_160615151349
DCAPP;Install;160615170621;OK;Man;file=CTLSPARH160615151350
DCAPP;Download;160616085256;OK;Auto;file=9370000100002705(88.131.71.147:443)
DCAPP;Validate;160616085257;OK;Auto;file=9370000100002705
DCAPP;Download;160627084443;OK;Auto;file=9370000100002705(88.131.71.147:443)
DCAPP;Validate;160627084443;OK;Auto;file=9370000100002705
DCAPP;Download;160627084444;OK;Auto;file=BINPAR__160620120617
DCAPP;Validate;160627084447;OK;Auto;file=BINPAR__160620120617
DCAPP;Install;160627084448;OK;Auto;file=BINPAR__160620120617
DCAPP;Download;160629020203;OK;Auto;file=9370000100002705(88.131.71.147:443)
DCAPP;Validate;160629020203;OK;Auto;file=9370000100002705
DCAPP;Config;160704104619;OK;Man;B24Ip1 old=194.137.75.24:445    !new=194.137.75.24:445
DCAPP;Config;160704104620;OK;Man;B24Ip2 old=194.137.75.24:445    !new=194.137.75.24:445
DCAPP;Config;160704104621;OK;Man;TspIpPort old=88.131.71.147:443    !new=88.131.71.147:443
DCAPP;Audit Send;160704105119;OK;Man;(88.131.71.141:8000)
```

6. 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
fallback	Transaction information pending to be sent to Authorization host	PAN, Expiry Date	Encrypted by DUKPT method
SLOG.txt	File of offline stored transactions for sending to log server	PAN, Expiry Date	Encrypted by DUKPT method
P000000.PDB	Temporary file which is used for sending offline stored transactions to log server (slog)	PAN, Expiry Date	Encrypted by DUKPT method
P000001.PDB	Merchant receipt copy of the last transaction	PAN, Expiry Date	PAN and Expiry Date are Encrypted by DUKPT method PAN is masked (6 first + 4 last)
P000002.PDB	Cardholder receipt copy of the last transaction	PAN	Masked (4 last)
elog.elog	Application activity trace.	PAN	Masked (6 first + 4 last)
TXN_RECORD.PDB	Transaction log of the last performed transaction	PAN	Masked (6 first + 4 last)
TxnDT.PDB	Transaction log data. Used for printing report of last transactions. Stores last 1000 transaction data as maximum.	PAN	Masked (6 first + 4 last)

A2 Application Version Numbering policy

Version number consists of 4 elements. Non-static elements are separated by '.' (dot) symbol.

The format is **Yxx.yy.zzz** where

Y: Static letter, does not change.

xx: Major version (numeric values 01-99) Initial value is 01 The value is never reset within application lifecycle.
The major version number is incremented in case of major changes to payment process, change that impacts security functionality. Requires a full PA-DSS assessment.

yy: Minor version: (numeric values 01-99) Initial value is 01. The value is reset to '01' if major version number is changed.
The minor version number is incremented in case of large feature additions, terminal model additions, any cause of delta-assessment, partial audit, re-audit due to expiration etc.

zzz: Wildcard / Revision. (numeric values 001 – 999). Initial value is 001. The value is reset if minor or major version number is changed.
Revision number is incremented in case of minor change which has impact on the application functionality but no impact on security or PA-DSS Requirements.

A3 Instances where PAN is displayed

Below represented instances where SAPC application can show cardholders data:

Instance	Description	Protection
DISPLAY	Manual PAN entry dialog	none
CARDHOLDER RECEIPT (terminal printer)		Masked
MERCHANT RECEIPT (terminal printer)	Regular transaction	Masked
	Offline transaction	Encrypted by DUKPT method
S&F Report (terminal printer)	Report which contains information regarding stored offline transactions	Encrypted by DUKPT method
Transaction list report (terminal printer)	Report which contains information regarding performed transactions	Masked
Last EMV transaction report (terminal printer)	EMV detailed receipt of the last performed EMV transaction	Masked

A4 Application components and used protocols

Hardware platform supported:

Model name: YOMANI XR/ML
PCI PTS Approval Number: 4-30092

OS Requirements:

Linux samoa 3.6.0 / Busybox v1.00
MP1: 24.43 and 23.44

Terminal to Host protocol in use:

SPDH version 3.1

Terminal to TMS protocol in use:

PPL version 3.1