



PA DSS Implementation Guide

For Verifone terminals Vx680, Vx680WiFi,
Vx6803G, Vx520C, Vx820, Vx690
using the
POSICC application version 7.7.x.x

Version 1.04

Date: **2021-08-09**



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 2 (24)
Phone +354 5445060		

Table of Contents

1. INTRODUCTION	4
1.1 PURPOSE	4
1.2 DOCUMENT USE	4
1.3 REFERENCES	5
1.4 UPDATE HISTORY	5
1.5 TERMINOLOGY AND ABBREVIATIONS	6
1.6 APPLICATION SUMMARY	7
2. SUMMARY OF PCI PA DSS REQUIREMENTS	9
2.1 PA-DSS REQ. 1.1.4: HISTORICAL DATA DELETION	9
2.2 PA-DSS REQ. 1.1.5: SECURELY DELETE ANY SENSITIVE DATA USED FOR DEBUGGING OR TROUBLESHOOTING	9
2.3 PA-DSS REQ. 2.1: PURGING CARDHOLDER DATA	9
PA-DSS REQ. 2.2: MASK PAN WHEN DISPLAYED	10
2.4 PA-DSS REQ. 2.3: RENDER PAN UNREADABLE ANYWHERE IT IS STORED	10
2.5 PA-DSS REQ. 2.4: PROTECT KEYS	10
2.6 PA-DSS REQ. 2.5: IMPLEMENT KEY MANAGEMENT PROCESSES AND PROCEDURES	10
2.7 PA-DSS REQ. 2.6: PROVIDE A MECHANISM TO RENDER IRRETRIEVABLE ANY CRYPTOGRAPHIC KEY MATERIAL	11
2.8 PA-DSS REQ. 3.1: UNIQUE USER IDs AND SECURE AUTHENTICATION	11
2.9 PA-DSS REQ. 3.2: UNIQUE USER IDs AND SECURE AUTHENTICATION FOR ACCESS TO SERVERS ETC.	11
2.10 PA-DSS REQ. 4.1: IMPLEMENT AUTOMATED AUDIT TRAILS	11
2.11 PA-DSS REQ. 4.4: FACILITATE CENTRALIZED LOGGING	12
2.12 PA-DSS REQ. 5.4.4: APPLICATION VERSIONING METHODOLOGY	12
2.13 PA-DSS REQ. 6.1: SECURELY IMPLEMENT WIRELESS TECHNOLOGY	12
2.14 PA-DSS REQ. 6.2: SECURE TRANSMISSION OF CARDHOLDER DATA OVER WIRELESS NETWORKS	12
2.15 PA-DSS REQ. 6.3: PROVIDE INSTRUCTIONS FOR SECURE USE OF WIRELESS TECHNOLOGY	13
2.16 PA-DSS REQ. 7.2.3: INSTRUCTIONS FOR CUSTOMERS ABOUT SECURE INSTALLATION AND UPDATES	13
2.17 PA-DSS REQ. 8.2: MUST ONLY USE SECURE SERVICES, PROTOCOLS AND OTHER COMPONENTS	13
2.18 PA-DSS REQ. 9.1: STORE CARDHOLDER DATA ONLY ON SERVERS NOT CONNECTED TO THE INTERNET	13
2.19 PA-DSS REQ. 9.1.C: OPEN ONLY THE PORTS NEEDED FOR OPERATION	13
2.20 PA-DSS REQ. 10.1: IMPLEMENT MULTI-FACTOR AUTHENTICATION FOR REMOTE ACCESS TO PAYMENT APPLICATION	14
2.21 PA-DSS REQ. 10.2.1: SECURELY DELIVER REMOTE PAYMENT APPLICATION UPDATES	14
2.22 PA-DSS REQ. 10.2.3: SECURELY IMPLEMENT REMOTE ACCESS SOFTWARE	14
2.23 PA-DSS REQ. 11.1: SECURE TRANSMISSIONS OF CARDHOLDER DATA OVER PUBLIC NETWORKS	14
2.24 PA-DSS REQ. 11.2: ENCRYPT CARDHOLDER DATA SENT OVER END-USER MESSAGING TECHNOLOGIES	15
2.25 PA-DSS REQ. 12.1, 12.1.1 AND 12.2: ENCRYPT ALL NON-CONSOLE ADMINISTRATIVE ACCESS	15
3. HOW TO SET UP YOUR POSICC TERMINAL TO ENSURE PCI DSS COMPLIANCE	16
3.1 DO NOT RETAIN FULL MAGNETIC STRIPE OR CARD VALIDATION CODE	16
3.2 PROTECT STORED CARD HOLDER DATA	16
3.3 PROTECT WIRELESS TRANSMISSIONS	16
3.4 FACILITATE SECURE REMOTE SOFTWARE UPDATES	17
3.5 ENCRYPT SENSITIVE TRAFFIC OVER PUBLIC NETWORKS	17
3.6 PCI DSS SKIMMING PREVENTION REQUIREMENTS	17
4. BACK-OUT OR PRODUCT DE-INSTALLATION PROCEDURES	18
5. POSICC APPLICATION KEY MANAGEMENT	18
5.1 KEYSSET DESCRIPTION	18
5.2 KEY DISTRIBUTION PROCESS	18
6. AUDIT TRAIL LOG	19
6.1 HOW TO CHANGE THE ADDRESS TO THE CENTRALIZED LOG SERVER	19
6.2 DATA CONTENTS OF AUDIT TRAIL	19



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 3 (24)
Phone +354 5445060		

6.2.1 *File size*..... 19

6.2.2 *File format*..... 21

6.2.3 *File sample* 21

ANNEXES **22**

A1 TERMINAL FILES 22

A2 APPLICATION VERSION NUMBERING POLICY 23

A3 INSTANCES WHERE PAN IS DISPLAYED 24

A4 INSTALLATION AND SETUP 24



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 4 (24)
Phone +354 5445060		

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 POSICC payment application version 7.7.x.x in your business to store, process, or transmit payment card information, this standard and this guide apply to you.

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

<http://www.pcisecuritystandards.org>

The PA-DSS implementation guide should be used by assessors conducting onsite reviews and for merchants who must validate their compliance with the PCI DSS requirements.

This implementation guide is reviewed annually and updated if needed due to changes in POSICC application or the PCI requirements. Latest version is always made available on www.verifone.com and information about updates are sent in the release notes. It's merchant's responsibility to periodically verify that version they are using complies to the latest version of the implementation guide available on the webpage.

The Payment Card Industry has also set the requirements for software applications that store, process or transmit cardholder data. These requirements are defined by the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS). In order to facilitate for you to get a PCI DSS assessment the Verifone software application has been approved by PCI to comply with the PCI PA-DSS requirements.

Note: This guide refers to POSICC 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 POSICC application running on your payment environment in the list on the website below, please contact Terminal Service Providers' helpdesk in order to upgrade your terminal.

<http://www.pcisecuritystandards.org/>

1.2 Document Use

This PA-DSS Implementation Guide contains information for proper use of the Verifone POSICC 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 POSICC 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.

PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 5 (24)
Phone +354 5445060		

1.3 References

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

1.4 Update History

Ver.	Name	Date	Comments
0.1	Sergejs Melnikovs	01-Jun-2016	Initial draft version, without technical info about the application.
1.0	Bjarni Valsson	14-sep-2020	Updated with POSICC specifics
1.01	Bjarni Valsson	13-Nov-2020	Updated version info.
1.02	Gudmundur Jonsson	07-Dec-2020	Update OS version and encryption method
1.03	Bjarni Valsson	30-Apr-2021	Updated version info and ports and protocols used.
1.04	Bjarni Valsson	09-Aug-2021	Updated clerical errors.



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 6 (24)
Phone +354 5445060		

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



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 7 (24)
Phone +354 5445060		

1.6 Application Summary

Payment Application Name	POSICC	Payment Application Version	7.7.x.x																
Application Description	The Verifone POSICC PA-DSS application provides an interface which easily integrates with 3 rd party software and host architecture that customer chooses. Application runs on PTS approved devices and performs a variety of payment functionalities with a single supported gateway																		
Typical Role of Application	Application runs on PTS approved devices and performs a variety of payment functionalities with a single supported gateway																		
Target Market for Payment Application	<table border="1"> <tr> <td colspan="4">Target Market for Payment Application (check all that apply):</td> </tr> <tr> <td>X</td> <td>Retail</td> <td>Processors</td> <td>Gas/Oil</td> </tr> <tr> <td></td> <td>e-Commerce</td> <td>Small/medium merchants</td> <td></td> </tr> <tr> <td></td> <td colspan="3">Others (please specify):</td> </tr> </table>			Target Market for Payment Application (check all that apply):				X	Retail	Processors	Gas/Oil		e-Commerce	Small/medium merchants			Others (please specify):		
Target Market for Payment Application (check all that apply):																			
X	Retail	Processors	Gas/Oil																
	e-Commerce	Small/medium merchants																	
	Others (please specify):																		
Stored Cardholder Data	<p>The following is a brief description of files and tables that store cardholder data:</p> <p>See Annex A1 for details of where Cardholder's Data is stored.</p> <p>Individual access to cardholder data is logged as follows:</p> <p><i>N/A. Cardholder Data is encrypted using 3DES functionality of the PTS approved device therefore there is no access to clear text card data.</i></p>																		
Components of the Payment Application	<p>The following are the application-vendor-developed components which comprise the payment application:</p> <p>POSICC is a single application that doesn't have subcomponents.</p>																		
Required Third Party Payment Application Software and Hardware	POSICC can be deployed on a number of Verifone terminals such as Vx680BTWIFI (Bluetooth, WiFi), Vx820 (Ethernet), Vx520C (Ethernet), Vx690 (WiFi, 3G/2G), Vx6803G (3G/2G), Vx680 (2G)																		
Database Software Supported	<p>The following are database management systems supported by the payment application:</p> <p>Not applicable. No database software supported</p>																		
Other Required Third Party Software	<p>The following are other required third party software components required by the payment application:</p> <p>none</p>																		
	The following are Operating Systems supported or required by the payment application:																		



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 8 (24)
Phone +354 5445060		

Operating System(s) Supported	<p>POSICC Application runs on Verifone proprietary Operating system Verix Evo.</p> <p>Vx680: QT000500 Vx6803g: QT000500 Vx680BTWIFI: QT000500 Vx690: QT000500 Vx820: QT000500 Vx520C: QT000500</p>																								
Application Authentication	N/A. POSICC doesn't provide authentication functionality.																								
Application Encryption	N/A. Application relies on a 3DES functionality of PTS approved device.																								
Application Functionality Supported	<p>Payment Application Functionality (check only one):</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;"><input type="checkbox"/></td> <td style="width: 33%;">Automated Fuel Dispenser</td> <td style="width: 33%;"><input type="checkbox"/></td> <td>POS Kiosk</td> <td style="width: 33%;"><input type="checkbox"/></td> <td>Payment Gateway/Switch</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Card-Not-Present</td> <td><input type="checkbox"/></td> <td>POS Specialized</td> <td><input type="checkbox"/></td> <td>Payment Middleware</td> </tr> <tr> <td><input type="checkbox"/></td> <td>POS Admin</td> <td><input type="checkbox"/></td> <td>POS Suite/General</td> <td><input type="checkbox"/></td> <td>Payment Module</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>POS Face-to-Face/POI</td> <td><input type="checkbox"/></td> <td>Payment Back Office</td> <td><input type="checkbox"/></td> <td>Shopping Cart & Store Front</td> </tr> </table>	<input type="checkbox"/>	Automated Fuel Dispenser	<input type="checkbox"/>	POS Kiosk	<input type="checkbox"/>	Payment Gateway/Switch	<input type="checkbox"/>	Card-Not-Present	<input type="checkbox"/>	POS Specialized	<input type="checkbox"/>	Payment Middleware	<input type="checkbox"/>	POS Admin	<input type="checkbox"/>	POS Suite/General	<input type="checkbox"/>	Payment Module	<input checked="" type="checkbox"/>	POS Face-to-Face/POI	<input type="checkbox"/>	Payment Back Office	<input type="checkbox"/>	Shopping Cart & Store Front
<input type="checkbox"/>	Automated Fuel Dispenser	<input type="checkbox"/>	POS Kiosk	<input type="checkbox"/>	Payment Gateway/Switch																				
<input type="checkbox"/>	Card-Not-Present	<input type="checkbox"/>	POS Specialized	<input type="checkbox"/>	Payment Middleware																				
<input type="checkbox"/>	POS Admin	<input type="checkbox"/>	POS Suite/General	<input type="checkbox"/>	Payment Module																				
<input checked="" type="checkbox"/>	POS Face-to-Face/POI	<input type="checkbox"/>	Payment Back Office	<input type="checkbox"/>	Shopping Cart & Store Front																				
Payment Processing Connections:	TLS 1.2 is the only protocol supported by the application to protect data transmitted over public network. All transaction data is sent to single supported payment gateway																								

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 POSICC 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 POSICC application meets this requirement	No specific setup for the POSICC application is required. POSICC application doesn't store any sensitive authentication data after authorization is completed.
merchant actions required	You must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) are removed from all other storage devices used in your systems, ECRs, PCs, servers etc. For further details please refer to your vendor. <u>Removal of sensitive authentication data is necessary for PCI DSS compliance.</u>

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 POSICC application meets this requirement	Sensitive authentication data is never stored by the POSICC application either encrypted or in the clear (even when needed to solve a specific problem) in production terminals.
merchant actions required	Verifone does not store Sensitive Authentication Data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with Sensitive Authentication Data used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data): <ul style="list-style-type: none"> • Collect sensitive authentication data only when needed to solve a specific problem • Store such data only in specific, known locations with limited access • Collect only the limited amount of data needed to solve a specific problem • Encrypt sensitive authentication data while stored • Securely delete such data immediately after use

Aligns with PCI DSS Requirement 3.2

2.3 PA-DSS Req. 2.1: Purging cardholder data

Securely delete cardholder data after customer-defined retention period.	
How POSICC application meets this requirement	All cardholder data is automatically erased from POSICC terminal after batch is successfully sent from terminal. See the list of files in the <i>Annex A1 Terminal files</i>
merchant actions required	POSICC terminal does store cardholder data using a 3DES functionality of PTS approved device.

	<p>The merchant is not required to take any action in relation to this requirement.</p> <p>Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will securely delete (render irretrievable) the stored cardholder data. When defining a retention period, you must take into account legal, regulatory, or business purpose.</p> <p>All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN.</p>
--	---

Aligns with PCI DSS Requirement 3.1

PA-DSS Req. 2.2: Mask PAN when displayed

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) so only personnel with a business need can see the full PAN.	
How POSICC application meets this requirement	<p>Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts are available in Annex A3 <i>Instances where PAN is displayed</i> The application by default mask PAN according to PCI requirements and has no configurable options to change this.</p> <p>The application doesn't have an ability to display or export full PAN.</p>
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.3

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

Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). The PAN must be rendered unreadable anywhere it is stored, even outside the payment application (for example, log files output by the application for storage in the customer environment)	
How POSICC application meets this requirement	<p>PAN is rendered unreadable by default in the application. The application has no configurable options to change this. Details of rendering method and all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts are available in Annex A1 <i>Terminal files</i></p>
merchant actions required	The merchant is responsible for rendering PAN unreadable in all instances where a PAN could be stored in outside of POSICC application.

Aligns with PCI DSS Requirement 3.4

2.5 PA-DSS Req. 2.4: Protect keys

Protect keys used to secure cardholder data against disclosure and misuse. Access to keys used for cardholder data encryption must be restricted to the fewest possible number of key custodians. Keys should be stored securely.	
How POSICC application meets this requirement	N/A The payment application doesn't have access to the keys. All key management is handled by a 3DES functionality of PTS approved device.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.5

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

Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.
--

How POSICC application meets this requirement	N/A The payment application doesn't have access to the keys. All key management is handled by a 3DES functionality of PTS approved device.
Merchant actions required	The merchant is not required to take any action related to key management on POSICC terminal. If by some reason POSICC terminal displays message " Tamper " please immediately contact terminal service provider for future instructions. In this state the terminal will not be able to start any transaction. Tampered terminal must be: <ul style="list-style-type: none"> physically replaced; returned to Terminal Service Provider for investigation.

Aligns with PCI DSS Requirement 3.6

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

Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.	
How POSICC application meets this requirement	N/A The payment application doesn't have access to the keys. All key management is handled by a 3DES functionality of PTS approved device.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.6

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

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

Aligns with PCI DSS Requirement 8.1 and 8.2

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

Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	
How POSICC application meets this requirement	The POSICC application does not provide functionality and does not maintain user accounts for administrative access or individual access to cardholder data.
Merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.1 and 8.2

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

Implement automated audit trails.	
How POSICC application meets this requirement	POSICC application supports Syslog. This log contains masked PANs. This may also contain 3DES encrypted PAN if log level is set to LOG_TRACE. No cardholder data is accessible from the POSICC terminal. The application also keeps an Audit Trail to track changes to system level objects.
merchant actions required	For the Audit Trail there are no settings you need to do. The Audit Trail is created automatically. The Audit Trail could be sent manually to a

	centralized server. Although typically not possible, but merchant should be aware that application and TMS logs should not be disabled and doing so will result in non-compliance with PCI DSS.
--	---

Aligns with PCI DSS Requirement 10.1

2.11 PA-DSS Req. 4.4: Facilitate centralized logging

Facilitate centralized logging.	
How POSICC application meets this requirement	POSICC application provides SYSLOG for audit trails delivery.
Merchant actions required	The merchant may choose to setup a local SYSLOG server and configure the terminal to send logs to that server. Chapter “ <i>Audit Trail log</i> ” gives you guidance on how to correctly setup the centralized log server.

Aligns with PCI DSS Requirement 10.5.3

2.12 PA-DSS Req. 5.4.4: Application versioning methodology

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

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

Securely implement wireless technology. For payment applications using wireless technology, the wireless technology must be implemented securely.	
How POSICC application meets this requirement	If wireless is used POSICC application supports strong encryption (WPA, WPA2) functionality aligned to industry best practices. Also, all data sent to and from the application by default protected using TLS 1.2 with strong ciphers.
merchant actions required	If you are using wireless network within your business please follow recommendations in chapter 3.3 <i>Protect wireless transmissions</i> of the implementation guide.

Aligns with PCI DSS Requirements 1.2.3 & 2.1.1

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

Secure transmissions of cardholder data over wireless networks. For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	
How POSICC application meets this requirement	If wireless is used POSICC application supports strong encryption (WPA, WPA2). All data sent to and from the application by default always protected using TLS 1.2 using strong ciphers.
merchant actions required	For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. For other actions please refer to 0chapter 2.13 PA-DSS Req. 6.1: Securely implement wireless technology of the implementation guide.

Aligns with PCI DSS Requirement 4.1.1

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

Provide instructions for secure use of wireless technology.	
How POSICC application meets this requirement	If wireless is used POSICC application supports strong encryption (WPA, WPA2). The wireless encryption is applied on top of 3DES technology used to transmit Cardholders Data and Sensitive Authentication Data. Also, all data sent to and from the application by default always protected using TLS using strong ciphers.
merchant actions required	If you are using wireless network within your business please follow recommendations in chapter 3.3 <i>Protect wireless transmissions</i> of the implementation guide.

Aligns with PCI DSS Requirements 1.2.3, 2.1.1, & 4.1.1

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

Provide instructions for customers about secure installation of patches and updates.	
How POSICC application meets this requirement	POSICC 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 POSICC application is released by Verifone, Verifone will update the terminals automatically for customer via central management.
Merchant actions required	The merchant is not required to take any action in relation to this requirement.

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

Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	
How POSICC application meets this requirement	POSICC application does not employ unnecessary or insecure services or functionality. Full list of application components and dependent components / protocols described in chapter 1.6 Application Summary
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.2.3

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

Store cardholder data only on servers not connected to the Internet.	
How POSICC application meets this requirement	POSICC application does not store any cardholder data in a server connected to the internet.
merchant actions required	Never store cardholder data on internet accessible systems.

Aligns with PCI DSS Requirement 1.3.7

2.19 PA-DSS Req. 9.1.C: Open only the ports needed for operation

Firewalls should only be opened for ports needed to ensure the operation of the terminal
--



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 14 (24)
Phone +354 5445060		

How POSICC application meets this requirement	POSICC application needs to connect to the following hosts:			
	Address	Port	Protocol	
	global.verifone.is	443	TCP	
	t01.verifone.is	443	TCP	
	apim-tax-prod.azure-api.net	443	TCP	
	fintrax.auth0.com	443	TCP	
	212.213.189.132	443	TCP	
	91.207.36.131	443	TCP	
	193.4.61.195	443	TCP	
x.x.x.x	514	UDP	(Syslog, configurable host).	
localhost	10676	TCP	ECR communication.	
merchant actions required	Open only the listed ports.			

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

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

Aligns with PCI DSS Requirement 8.3

2.21 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 POSICC application meets this requirement	POSICC application facilitates secure update functionality by downloading updates directly from the management server, verifying integrity and authenticity of the update through digital signatures and applying updates to the terminal when is not in use.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 1 and 12.3.9

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

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

Aligns with PCI DSS Requirements 2, 8 and 10

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

Secure transmissions of cardholder data over public networks.



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 15 (24)
Phone +354 5445060		

How POSICC application meets this requirement	By default, configured to use TLS 1.2 with strong ciphers encryption.
merchant actions required	The merchant is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.1

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

Aligns with PCI DSS Requirement 4.2

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

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

Aligns with PCI DSS Requirement 2.3

PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 16 (24)
Phone +354 5445060		

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

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

3.1 Do not retain full magnetic stripe or card validation code

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

- Your old unit is physically replaced by a new POSICC loaded with software that complies with the PCI PA-DSS requirements.
- Your existing POSICC 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 POSICC Application that runs on your terminal is listed on the PCI web site “List of Validated Payment Applications” that have been validated in accordance with PCI PA-DSS.

<http://www.pcisecuritystandards.org>

For your organization to comply with PCI DSS requirements it is necessary to remove historical data stored prior to installing your PCI PA-DSS compliant POSICC 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 POSICC 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.

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

3.2 Protect stored card holder data

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

PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 17 (24)
Phone +354 5445060		

- 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 of WEP as a security control was prohibited as of 30 June 2010.
- Other security related wireless vendor defaults were changed.

Bluetooth:

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

3.4 Facilitate secure remote software updates

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

POSICC application bundle signed by Verifone production signing certificate and POSICC terminal will reject an application if it is signed by any other certificate. POSICC application bundle could be downloaded to terminal remotely from TMS server. POSICC requires certain certificate to be installed in order to properly communicate with the TMS server. It comes bundled with the software.

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

3.5 Encrypt sensitive traffic over public networks

Your POSICC application allows transmission over public networks, e.g. public internet. To protect sensitive data your POSICC application uses TLS 1.2. To connect your POSICC terminal to public networks you do not need to take any further action regarding encryption.

3.6 PCI DSS Skimming Prevention Requirements

It is obligatory for the merchant to ensure their operating environment prevents skimming. Merchants are therefore advised to implement the PCI DSS requirement 9.9.x in their environment to prevent skimming. The summary of the requirements are as follows:

- Merchants are to keep an up-to-date list of all POI devices in use. This list must be continually updated (substitutions, new acquisitions, relocation of POI etc.) and must contain, as a minimum, the following information:
 - Model and description of the POI device (e.g. Verifone Vx820, Verifone Vx520C)
 - A clear identification of the POI device, e.g., by the serial number or PTID number.
 - Precise information as to where the POI device is installed (e.g., the address of the branch or company or, in the case of mobile devices, the responsible person that has possession of the device).
 - This list can be maintained manually or automatically, for example, using a terminal management system.
- Merchants are responsible for regular checks for manipulation or substitution of device. This shall be done at least daily.
- There must be written instructions specifying how a device is to be checked, who is responsible for this, and at what intervals the checks should be carried out. The method for checking for compromises will depend on the type of device in question and can be carried out, for example, in the following ways:
 - Checking the seal (frequently already attached by the manufacturer, or else by individual merchants using their own seals or labels)
 - Comparing the POI device to a photo of the original POI to reveal any differences in its construction (e.g., caused by substitution) or any attached skimming components
 - Comparing the serial numbers
 - Looking for cameras



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 18 (24)
Phone +354 5445060		

- It is the responsibility of the merchant to specify the intervals between inspections. This must be done as part of their yearly risk assessment in accordance with PCI DSS Requirement 12.2, also considering, amongst other things, factors such as the location of the device and whether it is an attended/unattended POI.
- Merchants are required to train staff on skimming prevention. Appropriate training materials and training sessions should be used to raise staff awareness and make any manipulation or substituting of devices more difficult. At the very least, the following should be included in the training:
 - Identification of third parties (e.g., maintenance engineers) that wish to service POI devices or substitute them before any such person is given access to the POI
 - Installation, substitution or return of a device only after checking that this has been planned and approved
 - Suspicious actions by strangers near to or directly at the device

4. Back-out or product de-installation procedures

The software of your POSICC 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. POSICC application key management

5.1 Keypad description

Name	Type	Purpose
IPEK	DUKPT (2TDES) 112bit	Terminal PIN Key. The key used for Online PIN encryption on the terminal. Terminal sends encrypted data to Gateway.

Each POSICC terminal is equipped by unique set of the keys.

5.2 Key distribution process

IPEK is 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	-



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 19 (24)
Phone +354 5445060		

Minimum key size in number of bits:	-	3072	256	3072/256	128
Minimum key size in number of bits:	-	7680	384	7680/384	192
Minimum key size in number of bits:	-	15360	512	15360/512	256

6. Audit Trail log

6.1 How to change the address to the centralized log server

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

To achieve automatic audit trail sending on POSICC Terminal contact Verifone and ask for the logs to be sent to your host by giving information about what host settings to use.

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

Important:

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

6.2 Data Contents of Audit Trail

Depending on the destination of the audit trail, different actions will be logged. UDP audit trail only transfers the application log which can be considered a high level log. This log is very important for troubleshooting so make sure to always use the appropriate application and syslog log level that matches your needs.

Additionally, low level operating log can be extracted from the device by a technician locally.

The following logging levels are available for configuration:

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

F. ex. if configured level 3 then events from level 0,1 and 2 also will be logged.

For PA-DSS purposes, log level should be enabled at least at Emergency level (enabled by the default). The log level configuration only affects the application and syslog log levels, but not the low level operating system log.

6.2.1 File size

When log destination is set to file, the lifetime of the log file will be determined by how actively the terminal is used and what log levels are set.



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author	Verifone	Created: 2016-05-30
E-mail	verifone@verifone.is	Updated: 2021-08-09
Phone	+354 5445060	Version 1.04 Page 20 (24)



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 21 (24)
Phone +354 5445060		

6.2.2 File format

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

6.2.3 File sample

Below is an example of log entries from a terminal:

```
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.797Z vf72253518.terminals.verifone.is POSICC 21 Posicc:ProcessNetworkEvent -
Network event detected: NWhandle[0] event[18] eventData[0] CE_EVT_PROCESSING_NET_UP
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.798Z vf72253518.terminals.verifone.is POSICC 21 Posicc:ProcessNetworkEvent -
Network event detected: NWhandle[0] event[1] eventData[0] CE_EVT_NET_UP
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.803Z vf72253518.terminals.verifone.is POSICC 21 Startup - Message type 0
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.805Z vf72253518.terminals.verifone.is POSICC 21 Startup - Handshake
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.811Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - InitIPP(checkKey
== false)
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.813Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - Init()
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.814Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - SendRcvMsg(msgId
18, iTimeout 15)
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.817Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - Check IPP7 key
management mode: 0F31383441330E
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.818Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - SendRcvMsg(msgId
17, iTimeout 15)
213.167.140.122      Sep 10 10:59:28      1      local1 debug          2020-09-
10T10:59:09.820Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - ReceiveData()
IPP_E_CANCEL
213.167.140.122      Sep 10 10:59:29      1      local1 debug          2020-09-
10T10:59:09.822Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - Set 3DES DUKPT
mode: 0F31373041330E
213.167.140.122      Sep 10 10:59:29      1      local1 debug          2020-09-
10T10:59:09.823Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - SendRcvMsg(msgId
15, iTimeout 15)
213.167.140.122      Sep 10 10:59:29      1      local1 debug          2020-09-
10T10:59:09.824Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - ReceiveData()
IPP_E_CANCEL
213.167.140.122      Sep 10 10:59:29      1      local1 debug          2020-09-
10T10:59:09.826Z vf72253518.terminals.verifone.is POSICC 21 InternalPinPad - Set IPP key
management mode 'VISA': 0F3135564953410E
213.167.140.122      Sep 10 10:59:29      1      local1 debug          2020-09-
10T10:59:09.827Z vf72253518.terminals.verifone.is POSICC 21 InitializeNoNW - Online PIN
should be supported
213.167.140.122      Sep 10 10:59:29      1      local1 debug          2020-09-
10T10:59:09.828Z vf72253518.terminals.verifone.is POSICC 21 InitializeNoNW - Online PIN
encryption key is installed
213.167.140.122      Sep 10 10:59:29      1      local1 info           2020-09-
10T10:59:09.833Z vf72253518.terminals.verifone.is POSICC 21 CopyMVTtoRAM - Terminal
capabilities: 'E0B0C8'
213.167.140.122      Sep 10 10:59:29      1      local1 info           2020-09-
10T10:59:09.836Z vf72253518.terminals.verifone.is POSICC 21 CopyMVTtoRAM - Terminal
capabilities: 'E0F0C8'
213.167.140.122      Sep 10 10:59:29      1      local1 info           2020-09-
10T10:59:09.839Z vf72253518.terminals.verifone.is POSICC 21 CopyMVTtoRAM - Terminal
capabilities: 'E0F0C8'
213.167.140.122      Sep 10 10:59:29      1      local1 debug          2020-09-
10T10:59:09.846Z vf72253518.terminals.verifone.is POSICC 21 Startup - RFU1 2 (2)
213.167.140.122      Sep 10 10:59:29      1      local1 crit           2020-09-
10T10:59:09.996Z vf72253518.terminals.verifone.is POSICC 21 POSICCServer - Incorrect EMV lib.
Use version Vx 8.1.0.01 Found version Vx 8.1.0
213.167.140.122      Sep 10 10:59:29      1      local1 info           2020-09-
10T10:59:09.998Z vf72253518.terminals.verifone.is POSICC 21 POSICCServer - ICC initialized
```



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 22 (24)
Phone +354 5445060		

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
BATCH-M1-TRN	Transaction information pending to be sent to Sales Connector	PAN, Expiry Date	<ul style="list-style-type: none">PAN Encrypted by 3DES
OfflineList.dat	List of PAN's that have been used in transactions that have been approved offline.	PAN	<ul style="list-style-type: none">PAN SHA-256
DeclineList.dat	List of PAN's that have been used in declined transactions.	PAN	<ul style="list-style-type: none">PAN SHA-256 PAN



PA DSS Implementation Guide: POSICC application version 7.7.x.x		
Author Verifone	Created: 2016-05-30	Version 1.04
E-mail verifone@verifone.is	Updated: 2021-08-09	Page 23 (24)
Phone +354 5445060		

A2 Application Version Numbering policy

The following convention should be used for all applications:

POSICC Major.Minor/Security.Maintenance.Patch_bIno where

Release Number segment	Mandatory or Optional?	Description	Used in Production Release?
Architecture	Mandatory	<p>Application Architecture Change</p> <p>This means new Application Architecture has been introduced.</p> <p>This means that upgrade from previous release cannot be made without either changing the hardware or changing the Operating System (OS) e.g. Verix to VOS or installing from scratch. Current architecture version is 7.x.x.x</p>	Yes
Major Security	Mandatory	<p>The second numeric value represents the major version number. This value is only incremented between versions if changes with impact on any security functionality or PA-DSS requirement are present. Such changes are marked as having “High” or “Low” PA-DSS Impact in the Jira system and correspond to changes that impact the PA-DSS v3 standard. Examples of this are any kind of change in how sensitive cardholder data is handled, the security features (encryption, network connectivity) of the application or a major redesign on some part of the application.</p>	Yes
Minor	Mandatory	<p>The third numeric value represents the minor version number. This value is incremented if the new version contains changes with impact on application functionality but no impact on security or PA-DSS requirements. Such changes are marked as having “No” PA-DSS Impact in the Jira system and correspond to having no Impact on changes in the PA-DSS v3 standard.</p>	Yes
Patch	Mandatory	<p>Changes with no impact on functionality of the application or its dependencies are marked as having “None” PA-DSS Impact in the Jira system and correspond to No Impact changes in the PA-DSS v3 standard. This class of changes results in an increase in the fourth digit of the version number (wildcard).</p>	Yes

A3 Instances where PAN is displayed

Below represented instances where POSICC application can show cardholders data:

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

A4 Installation and Setup

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

- Setup the communication interfaces. For Vx690 and Vx680BTWIFI the communication interface needs to be selected (other types have only one interface). To configure that select "More" -> "More" -> "Net" on the screen there it is possible select the interface to use.
- Configure network settings. By default the terminal will use DHCP but it is possible to configure static IP address for the terminal. To configure select "More" -> "More" -> TCP/IP.
- Configure WIFI: To configure the terminal for WIFI the terminal must scan available networks select More" -> "More" -> "Net" -> Enter merchant password -> WIFI -> Scan. Then select the network to connect to and enter the network password.