



VX 690

PCI PTS POI v4.x Security Policy



VX 690 PCI PTS POI V4.X SECURITY POLICY

Contents

PREFACE	3
Audience	3
Organization	3
CHAPTER 1	4
Introduction	4
SCOPE 4	4
ROLES AND RESPONSIBILITIES	4
PRODUCT IDENTIFICATION AND INSPECTION	4
CHAPTER 2	10
FIRMWARE AND APPLICATION MAINTENANCE	10
LOCAL OPERATIONS	10
REMOTE OPERATIONS	10
CHAPTER 3	11
Security Policy	11
ENVIRONMENT	11
KEY MANAGEMENT	13
KEY LOADING	15
For ADE: ADE keys are loaded and managed as the IPP keys.	16
ADMINISTRATION SECURITY	16
DEVICE DIAGNOSTICS	17
DEVICE SECURITY	18
CODERS/DEVELOPERS (Firmware and Application)	19
COMMUNICATION METHODS AND PROTOCOLS	20
CRYPTOGRAPHY	21
PATCHING AND UPDATING	22
FIRMWARE UPDATES	22
DECOMMISSIONING/REMOVAL FROM SERVICE	22
CHAPTER 4	23
REFERENCES	23
ACRONYMS.....	23



VX 690 PCI PTS POI V4.X SECURITY POLICY

PREFACE

AUDIENCE

This guide is useful for the following users:

- **Entities deploying VX 690 terminals to end user sites**

Perform specific tasks required to deploy new VX 690 terminals into the field, such as:

- Terminal configuration
- Application software download
- Testing of the terminal prior to deployment

- **Administrators or Site Managers**

Perform administrative and on-site duties, such as:

- Change passwords
- Perform routine tests and terminal maintenance
- Configure terminals for remote diagnostics and downloads

ORGANIZATION

This guide is organized as follows:

Chapter 1, Introduction. Provides an overview of the current security policy document.

Chapter 2, Firmware and Application Maintenance. Provides information on System Mode and Application Download procedures.

Chapter 3, Security Policy. Provides information on how to securely deploy VX 690 terminals.



VX 690 PCI PTS POI V4.X SECURITY POLICY

CHAPTER 1

INTRODUCTION

This Security Policy provides guidance for the proper and secure usage of Payment Card Industry (PCI) Payment Terminal Security (PTS) Approved Point of Interaction version 4.x devices, such as the VX 690.

SCOPE

The security policy applies to the VX 690 terminal, which is PCI PTS version 4.x POI approved. Failure to use the terminal in accordance with this security policy will cause the terminal to not be in compliance with the PCI PTS POI Modular Security Requirements version 4.x.

ROLES AND RESPONSIBILITIES

Broadly speaking, the device has two modes of operation:

- Normal Operational Mode: Power On to Booting the System, and running.
- Key Injection Mode: Authorized terminal administrators can perform local key injection operations under dual control. They can also perform local downloading operations using the System Mode.

PRODUCT IDENTIFICATION AND INSPECTION

Carefully inspect the shipping carton and its contents for possible tampering or damage.

1. Validate the authenticity of the sender by verifying the shipping tracking number and other information located on the product order paperwork.
2. Remove the VX 690 unit from the shipping box or carton.
3. Remove all plastic wrapping from the unit and other components.
4. Remove the clear protective film from the display.
5. Save the shipping carton and packing material for future repacking or moving the device.
6. Thoroughly inspect the device for any sign of tampering or damage of the external integrity of the plastic. Conduct a periodic check, as directed in the Chapter-3 “Security Policy”, section “Environment”.

The name of the device is on a sticker on the back. This sticker must be visible at all times and should never be covered.

The minimum features of the product include an LCD screen, a smartcard reader, a magnetic stripe reader, a numeric keypad.

To verify if your VX 690 product is PCI approved as a PED (PIN Entry Device), locate the PCI Identification number at the bottom of the device (Figure 1). Go to the PCI Security Standards Council web site (www.pcisecuritystandards.org) and verify that the PCI Hardware Version matches the **Hardware #** on the list of Approved PIN Transaction Security (PTS) Devices (Figure 2).

VX 690 PCI PTS POI V4.X SECURITY POLICY



Figure 1a, VeriFone VX 690 POS terminal

VX 690 PCI PTS POI V4.X SECURITY POLICY

Figure 1b

Example of the location of the PCI Hardware Version number on the label on the back of the VX 690



Figure 1c, Location of the Label inside the back of the Device

VX 690 PCI PTS POI V4.X SECURITY POLICY


Company	Approval Number	Version	Product Type	Expire Date
Verifone Inc www.verifone.com				
VX 690				
Hardware #: M260-xxx-xx-xx-xx Firmware #: QT690500.xxxxxxxx Applic #:	TBD	4.x	PED	

Figure 2:

Example listing of hardware version number and firmware number of PCI approved devices on the PCI Security Standards Council website

VX 690 PCI PTS POI V4.X SECURITY POLICY

The reader must also verify that the VX 690 product is running a PCI PED approved firmware as listed on the PCI website.

Shortly after powering up, a splash screen displays the version number of the Operating System (Figure 3). The installer must be able to find these numbers on the list of Approved PIN Transaction Security (PTS) Devices, just as it was done for the Hardware identifier.

In case these numbers do not match, notify your service provider immediately!!!

In this example, the firmware version number is on the second line:

Figure 3. Boot splash screen of the VX 690 for FW # verification





VX 690 PCI PTS POI V4.X SECURITY POLICY

In the above Firmware version number, QT690500.**0**, the “.**0**” refers to the SRED Run Time Digit. The value assigned here is according to the table below:

SRED Enablement
Status: <ul style="list-style-type: none">• 0 = Neither VCL nor ADE active• 1 = ADE Active• 2 = VCL Active• 3 = ADE and VCL active

The specific firmware version numbers can be retrieved via the device menu and be displayed during the start-up.

The IP Stack software version can be obtained going to System Mode menu and look at System information, or from the Verix Terminal Manager “Software Versions menu”. The obtained version number must match any of the listed IP stack version numbers for this product. If these numbers do not match, notify your service provider immediately.



VX 690 PCI PTS POI V4.X SECURITY POLICY

CHAPTER 2

FIRMWARE AND APPLICATION MAINTENANCE

LOCAL OPERATIONS

Local operations within the Verix Terminal Manager (VTM) allow for standalone terminals to perform data transfers between the terminal and another terminal or computer. Please perform local VTM operations to configure, test, and display.

For more information about Verix Terminal Manager, refer to Appendix A for the [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301).

REMOTE OPERATIONS

Remote operations require communication between the terminal and a host computer over a network connection. Please perform remote VTM operations to download application software to the terminal, upload software from one terminal to another, or perform diagnostics over a network.

For more information about Verix Terminal Manager, refer to Appendix A for the [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301).



VX 690 PCI PTS POI V4.X SECURITY POLICY

CHAPTER 3

SECURITY POLICY

This policy ensures secure deployment of VX 690 terminals and complies with the PCI PTS POI standards version 4.x.

The device is built to comply with the security policy and does not require subsequent configuration to do so.

ENVIRONMENT

- The VX 690 has a security architecture called VeriShield Retain, which has both physical and logical components. The logical security component, called File Authentication (FA) is part of the terminal's operating system software.

File Authentication is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process enables the sponsor of a VX 690 terminal to logically secure access to the terminal by controlling who is authorized to download applications or firmware update files to the terminal. It proves and verifies the file's origin, sender's identity and the integrity of the file's information. If any of these three items are not verified, then the download is rejected.

- Prior to usage and deployment, familiarize yourself with the [R7] VX 690 Installation Guide . This guide provides information on verifying terminal equipment, usage, safety, security, environmental requirements, and troubleshooting steps if needed.
- The VX 690 must be used in an attended environment.
- The supported card readers include, the Smart Card Reader (ICCR), Magnetic Stripe Reader (MSR), and Contact Less Reader (CTLS).
- PIN entry mechanism is the Physical keypad through which the PIN value is entered.
- The VX 690 terminals are portable, handheld devices. As such a privacy shield is not required because the cardholder can shield the entry of their PIN using their body Always assist the cardholder to exercise extreme caution during PIN entry:
 - Remember to pass the VX 690 to the cardholder for PIN entry.
 - Encourage the cardholder to get close to the VX 690 to avoid others observing the information entered. The cardholder can use his body or a method of his choice to hide the keypad while entering his PIN.
- Periodically inspect the terminal for possible tampering. Signs of tampering include:
 - Wires protruding out of the device
 - Foreign objects inserted into the smart card slot or mag stripe slot
 - Signs of damage to the tamper evident labels

VX 690 PCI PTS POI V4.X SECURITY POLICY

- Signs of damage to the plastic such as a local mismatch of colors or deep cuts
- 'Tamper' warning message on the device display.
- Look into the ICCR, MSR slots for evidence of foreign objects indicating tampering.
- Tamper Detection Mechanisms:
 - The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data.
 - These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information.
- There are also environmental sensors which provide additional protection:
 - Temperature sensor to detect out of range CPU temperatures
 - Battery voltage sensor to detect out of range backup battery voltages
 - RTC frequency sensor to detect out of range RTC clock frequency
- When the TOE is in tampered state:
 - The display shows a tamper message (Figure 35)
 - PIN entry and encryption are un-accessible from application calls
 - Applications are not allowed to run until the tamper (condition and cause) is cleared and system mode passwords are entered.



VX 690 Tamper warning screen



VX 690 PCI PTS POI V4.X SECURITY POLICY

- If any device is found in tamper state, please remove it from service immediately. Do not attempt to put the device back in operation, this is not possible.

Important: Please keep the device available for potential forensics investigation. Then immediately notify your company security officer and your local Verifone representative or service provider.

For contacting Verifone, please see section “Verifone Service and Support” in [R7] VX 690 Installation Guide

- The following are the temperature and humidity specifications of the VX 690:
 - Operating temperature: 0° to 50° C (32° to 104° F)
 - Storage temperature: -20° to 70° C (-4° to 122° F)
 - Relative humidity: 5% to 95% RH (non-condensing)
- Subjecting the VX 690 to extreme environmental conditions will result in tamper events. Any temperatures above 60 degrees Celsius (± 5 degrees) or below -30 degrees Celsius (± 5 degrees) will result in a tamper condition. Additionally, should the battery voltage drift outside of the range of 2.3 VDC to 3.8 VDC, the unit will tamper and will not operate.
- The terminal contains no user serviceable parts. Do not, under any circumstances, attempt to disassemble the terminal. Trying to disassemble the terminal will tamper the device and require specific maintenance.

KEY MANAGEMENT

- See items [R1] and [R2] in References for key management techniques supported by the terminal.
- The terminal does not support manual cryptographic key entry.

Key injection and management equipment must be managed in a secure manner to minimize the opportunity for compromise in accordance with items [R1], [R2], and [R4] in References.

- Physical keys, authorization codes, passwords, and other credentials must be managed under dual control and split knowledge so that no one person can use two credentials simultaneously.
- Key management security objectives must be in compliance with PCI PIN Transaction Security requirements.
- Employing key management schemes that do not comply with PCI PTS for PCI payments will invalidate the PCI PTS approval for this POI.



VX 690 PCI PTS POI V4.X SECURITY POLICY

- In order to comply to CAS POI security requirements, exhaustive PIN determination must be prevented. This is achieved by excluding the use of PIN block format 0 in combination with Fixed key for PIN encryption. Since PIN block format 0 is the only format available on the VX 690 for ONLINE PIN verification, Fixed key must not be used for online PIN verification.
- TLS 1.2 should be used. SSL is supported but this protocol is inherently weak and should be removed unless required on an interim basis to facilitate interoperability as part of a migration plan. For SSL 3, or older versions of TLS, if supported, all cipher suites using single DES or RC4 must be removed.
- Key replacement must be performed upon any known or suspected compromise of any cryptographic or sensitive information.
- Keys must be replaced whenever the time deemed feasible to determine the key by exhaustive attack elapses, as defined in NIST SP 800-57-1.

The following table lists all supported key management schemes. For more information, refer to [R13] 2.0 Encryption Services Organization Key Management Procedures“.

VX 690 PCI PTS POI V4.X SECURITY POLICY

Key Name	Size (bytes)	Algorithm	Purpose
KLK	16, 24	TDEA	To load encrypted master keys. KLK is loaded in the clear in a secure environment.
DUKPT (PIN)	16	DUKPT (ANSI X9.24)	PIN encryption
DUKPT (MAC)	16	(ANSI X9.24) MAC (ANSI X9.19)	Message MAC'ing
Master Key	16, or 24	DES (FIPS 46-3, ANSI X3.92, X3.106); TDEA ANSI X9.52)	Encrypt/Decrypt Session Keys from host per Master Session Key Management
Session (PIN) Key	16, or 24	DES (FIPS 46-3, ANSI X3.92, X3.106); TDEA ANSI X9.52)	PIN block encryption
Session (MAC) Key	16	MAC (ANSI X9.19)	Message MAC'ing
Fixed (PIN) Key	16, or 24	DES (FIPS 46-3, ANSI X3.92, X3.106); TDEA ANSI X9.52)	PIN encryption block
Fixed (MAC) Key	16, or 24	DES (FIPS 46-3, ANSI X3.92, X3.106); TDEA ANSI X9.52)	Message MAC'ing
Application Signer		RSA 2048 SHA-256	Used by customer to sign Applications to install to device.

Figure 4:

All supported key management schemes

KEY LOADING

- Two methods used to load cryptographic keys into the device:



VX 690 PCI PTS POI V4.X SECURITY POLICY

- **Local Key loading using a Key Loading Device (KLD)** - used within an authorized key injection facility. After the firmware and implicitly the embedded public key certificates are loaded, the (16-byte TDES) Key Loading Key (KLK) must be injected. The KLK, which is the property of the sponsor of the terminal, can be loaded both in clear text or encrypted under the previous value of the KLK. The initial (clear text) loading of the KLK is performed in a secure environment using an HSM that enforces dual control and split knowledge. The terminal requires the entry of a password to enter the sensitive key loading state. Loading a key in clear text, will result in the erasure of all previously loaded keys.
- **Remote Key Loading (RKL)** - The device supports remote key loading using the VeriShield Remote Key (VRK) solution which is based on "ANSI X9 TR34 Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 –Using Factoring-Based Public Key Cryptography Unilateral Key Transport".
- For VCL:
 - The keyloading function is enabled by entry of a cryptographic key (KIF_KEK) via magstripe input (two command cards) under split knowledge and dual control.
 - The loading of the KIF_KEK to enable keyloading must take place in a secure facility under split knowledge and dual control.
 - Key loading can only be performed once.
 - Keyloading is disabled once keys have been loaded.
 - Keyloading is restricted by multiple cryptographic authentications and a process that requires dual control.
 - The wrapped keys to be loaded are placed in a configuration file that is signed by a sponsor certificate and cannot be loaded if the signature on the file is not valid.
 - The device does not respond to actions that would try to access other functionality during key loading.

For ADE: ADE keys are loaded and managed as the IPP keys.

ADMINISTRATION SECURITY

- The configuration modes like Key injection mode, and any downloading operations using System mode, are and must remain limited to administrators and maintenance/support personnel.

The administrators should setup the maintenance user prior to installation and use.

- Passwords are pre-expired and must be changed upon first use. These passwords must be at least 7 decimal characters (0-9) in length. Passwords can be changed by entering the System mode. System mode menus will guide the user to enter unique and proper passwords.



VX 690 PCI PTS POI V4.X SECURITY POLICY

- Updates and/or patches to the operating system can be performed by the administrators using the Verix Terminal Manager. Updates/patches are authenticated using RSA certificates. If the signature of the updates cannot be authenticated, the update/patch is rejected and is not installed.
- Develop a process that monitors consistently problematic devices, such as high read failures or debit card declined transactions. These are indications of a tampered terminal. Check whether the 'Tamper' warning is shown on the display.
- Implement a policy that requires all repair technicians who visit your store to sign in, verify their identity with photo identification, and remain accompanied by store personnel during any work performed on PIN pads and/or terminals.
- Implement a procedure that checks the terminal serial number every time the device is started or powered on to insure the device has not been replaced. A good security practice is to routinely check the terminal serial number while proceeding to a routine inspection of the terminal. If the device has been replaced, cease using the terminal and notify your Verifone customer relations manager.
- Visually inspect the terminal daily to ensure there are no foreign objects present in the smartcard slot; ensure there are no wires emanating from the smartcard slot.
- Develop a breach response plan. This helps to identify the steps to take if a suspected breach occurs and as well as who will perform each step. Each personnel must be aware of the actions to take. The plan needs to include isolation of your payment systems and a list of all personnel who need to be notified. These personnel include your local law enforcement, your acquiring bank, your processor, security assessor, as well as your payment system vendor.
- Track and log each instance of replaced terminals within the store. Whether from the in store inventory, by a repair technician or with terminals shipped into the store.
- VeriShield FST (File Signing Tool) manages the generation and signing of device certificates. See DevNet and [R12] VeriShield FST Basics for more information on signing tool implementation.

DEVICE DIAGNOSTICS

- VX 690 terminals implement a self-test to confirm firmware integrity. The self-test is performed:
 - When the unit powers
 - When the unit is rebooted
 - At least once every 24 hours
 - Upon demand
- Authorized maintenance personnel may configure the VX 690 to perform self-test at a specified time.



VX 690 PCI PTS POI V4.X SECURITY POLICY

- Authorized maintenance personnel may manually invoke the self-test by entering System Mode, (system mode passwords required), and selecting the self-test option.
- The following components are checked during self-test:
 - Integrity of the TMK (Terminal Master Key)
 - Integrity of the other key files
 - Tamper detection system
 - VeriShield certificate tree
 - Firmware
- If a self-test fails, the VX 690 limits its functionality based on the severity of the issue discovered. Device response ranges from partial disablement of applications to non-functionality.

DEVICE SECURITY

- Security mechanisms employed within the terminal can detect physical tampering and trigger a tamper event. This causes the terminal to cease performing transactions and indicates that it has been tampered by showing 'Tamper' on the device display.
- Terminal security must not be compromised by altering the environmental conditions. The power and temperature operating ranges should be within the specifications specified in [R7] VX 690 Installation Guide . Operating the terminal outside of these ranges triggers a tamper event and causes the terminal to cease performing transactions and the message 'tamper' will be seen on the device display.
- The terminal performs a self-test upon start up and at least once per 24 hour period. The operating system performs the self-test automatically and does not require intervention from the user or the application.
- If any device is found in tamper state, please remove it from service immediately, keep it available for potential forensics investigation, and notify your company security officer and your local Verifone representative or service provider. For contacting Verifone, please see section "Verifone Service and Support" in [R7] VX 690 Installation Guide



VX 690 PCI PTS POI V4.X SECURITY POLICY

CODERS/DEVELOPERS (Firmware and Application)

- All payment based applications and firmware must undergo a formal review and security audit before they may be signed and used.
 - The reviewer must be a qualified individual who was not involved with the authorship of the POI PED code.
 - Code review must be governed by an auditable process that shows the code review and security testing have been performed, and requires a sign-off by the person(s) performing the code review and security tests.
 - The tester shall confirm that the process will show any problems noted during the code review and security testing
 - Such reviews must happen after each and every code change.
 - The firmware must be reviewed against PCI POI PED requirements, the guidance listed in this document, as well [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301).
- The terminal operating system authenticates the applications prior to execution. The authentication process includes verifying the RSA certificate and signature of the application.
- This unit does not support default certificates. The developer must acquire signed sponsored certificates for development of applications.
- Applications must be designed and implemented in accordance with the PA-DSS requirements document entitled, [R15] PA-DSS Program Guide v3.0.
- Only application codes that have been authorized for release should be signed and released to the field. The digital signing must occur under dual control and split knowledge.
- When developing IP capable payment based applications, developers must follow the guidance listed in the following documents:
 - [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301)
 - [R9] Verix eVo Volume II: Operating System and Communication Programmers Guide (VPN – DOC00302)
 - [R10] Verix eVo IP Stack Security Guidance Users Guide (VPN – DOC00326)
 - This Security Policy
 - [R14] VeriShield File Signing Overview
- All referenced best practices regarding coding practices, security and device configurations must be followed.
- Transaction data must be cleared as soon as the transaction is completed, including but not limited to working registers and buffers.
- If the product is SRED enabled:
 - The working buffers associated with PAN encryption clears automatically as soon as the transaction completes.



VX 690 PCI PTS POI V4.X SECURITY POLICY

- The encryption of PAN data is automatic and transparent to your application – there are no added API calls needed.
- Allowable application behavior:
 - Write to the display
 - Fetch keypad entries
 - Request an encrypted PIN block
- Forbidden application behavior:
 - Change PIN entry retry limit
 - Attempt to alter PIN entry time-out.
 - PIN entry time-outs are set and enforced by the OS. The application is not capable of altering these.
 - PIN Entry time-outs are set to: 30 seconds without key presses, or 300 seconds with key presses.
 - Modify a key
 - Generate a subordinate certificate
 - Execute another application
 - Encrypt arbitrary data

COMMUNICATION METHODS AND PROTOCOLS

The VX 690 device supports the communications methods and protocols listed below. Use of any method not listed here invalidates the device PCI PTS approval.

Interfaces:

- USB
- Bluetooth
- Wi-Fi
- GSM / GPRS / HSPA+

Protocols/services:

- IP
- TLS/SSL
- PPP
- DHCP
- ICMP
- FTP/FTPS
- OCSP
- DNS
- WiFi
- Bluetooth
- 3G

The security guidance described in [R10] Verix eVo IP Stack Security Guidance Users Guide (VPN – DOC00326) specifies how protocols and services must be used/configured for each



VX 690 PCI PTS POI V4.X SECURITY POLICY

interface that is available on the device.

Please note that FTP/FTPS can only be used as a client and FTPS must be used instead of FTP to maintain PCI compliance. FTP is an application context utility which only executes when it is invoked by an authenticated (signed) application.

CRYPTOGRAPHY

- Only use acceptable cryptographic algorithms listed in [R6] SP800-57 Part 1: Recommendation for Key Management.
- The cryptographic strength should be at least 112 bits.
- Cryptographic algorithms used should be at least: SHA-256, 2TDEA, RSA-2048, AES-128.
- Although other cryptographic algorithms may be supported, they may not be used for payment-based applications.
- The following Cryptographic Algorithms are used. For:
 - PIN management: ANSI X9.8
 - DUKPT Algorithm: VISA Spec - ANSI X9.24
 - MAC Algorithm: ANSI X9.19
 - Advanced Encryption Standard (AES): FIPS PUB 197
 - Bank Of Philippine Islands (BPI) MAC Algorithm
 - RSA signature: ANSI X9.31-1 - PKCS#1 - PKCS#7
 - ISO9797-1 MACing algorithm
 - SHA-256 and RSA-2048, to generate and verify the digital signatures for file authentication. Same algorithm and key size are used for software application/configuration authentication.
 - The verification of the OS, device drivers and authenticated files in general (user programs and libraries); is performed by a HMAC SHA-256.
 - HMAC SHA-256 is performed against each authenticated component using a key generated from the SoC RNG.
- TLS 1.2 should be used. SSL is supported but this protocol is inherently weak and should be removed unless required on an interim basis to facilitate interoperability as part of a migration plan. For SSL 3, or older versions of TLS, if supported, all cipher suites using single DES or RC4 must be removed.
- The following cipher suites are used with TLS 1.2:
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384



VX 690 PCI PTS POI V4.X SECURITY POLICY

(The above cipher suites are equivalent with the below suite mentioned in FAQ Q69:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256)

PATCHING AND UPDATING

- Updates and/or patches to the operating system can be installed in the device. Updates/patches are RSA certificate authenticated. If the signature of the updates cannot be authenticated, the update/patch is rejected and not installed.
- For the secure operation of the device, it is recommended to use the latest versions of the released software.

FIRMWARE UPDATES

The VX 690 supports firmware updates. For more information on performing compliant firmware updates, please refer to [R7] VX 690 Installation Guide .

DECOMMISSIONING/REMOVAL FROM SERVICE

Before removing the device from service permanently or for repairs, all sensitive data must be erased. Sensitive data includes credit card data and all encryption keys inclusive of all Private, PIN, Data encryption keys.

To decommission the device from service (permanent non reversible operation), this can be done by disassembling the device. Disassembling the device forces a tamper condition, so all sensitive data will be erased automatically. After performing this operation, turn on the terminal and verify that the unit is in tamper state as shown on the device display.



VX 690 PCI PTS POI V4.X SECURITY POLICY

CHAPTER 4

REFERENCES

- [R1] ANS x9.24 Part 1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
- [R2] ANS x9.24 Part 2:2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
- [R3] ISO 9564-1, Financial Services Personal Identification Number (PIN) Management and Security Part 1: Basic Principles and Requirements for PIN's in Card-Based Systems
- [R4] X9 TR-31:2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
- [R5] ISO 9564-2, Banking, Personal Identification Number Management and Security Part 2: Approved Algorithms for PIN Encipherment
- [R6] SP800-57 Part 1: Recommendation for Key Management
- [R7] VX 690 Installation Guide DOC260-003-EN-C, Revision C
- [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301)
- [R9] Verix eVo Volume II: Operating System and Communication Programmers Guide (VPN – DOC00302)
- [R10] Verix eVo IP Stack Security Guidance Users Guide (VPN – DOC00326)
- [R11] Point of Interaction (POI) Modular Security Requirements v4.0
- [R12] VeriShield FST Basics
- [R13] 2.0 Encryption Services Organization Key Management Procedures
- [R14] VeriShield File Signing Overview
- [R15] PA-DSS Program Guide v3.0

ACRONYMS

: Number

AES : Advanced Encryption Standard

ANSI : American National Standards Institute

API : Application Programming Interface

DES : Data Encryption Standard

DUKPT : Derived Unique Key Per Transaction

FIPS : Federal Information Processing Standards

FA : File Authentication

FST : File Signing Tool

LCD : Liquid Crystal Display

MAC : Message Authentication Code



VX 690 PCI PTS POI V4.X SECURITY POLICY

PA-DSS : Payment Application Data Security Standard

PAN : Personal Account Number

PCI : Payment Card Industry

PED : PIN Entry Device

PIN : Personal Identification Number

POI : Point of Interaction

PTS : Point of sale Terminal Security

RH : Relative Humidity

RSA : Rivest Shamir Adleman

SHA : Secure Hash Algorithm

SRED : Secure Reading and Exchange of Data

TBD : To Be Disclosed

TDEA : Tripe Data Encryption Algorithm

TMK : Terminal Master Key

VPN : Verifone Publication Number

VTM : Verix Terminal Manager