UX Series

UX 300 / UX 301 / UX 410

PCI PTS POI Security Policy

Version 3.2 – 4 June 2020

UX SERIES: UX 300 / UX 301 / UX 410

PCI PTS POI SECURITY POLICY

Contents

PURPOSE

- This Security Policy provides guidance for the proper and secure usage of the PCI PTS POI v5.1 approved UX 300 / UX 301 / UX 410 Secure Card Readers including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements.
- Any deviation from the approved use of the device will invalidate the PCI PTS POI approval.

GENERAL DESCRIPTION

PRODUCT NAME AND APPEARANCE

- Figure 1, Figure 2, Figure 3 shows UX 300 / UX 301 / UX 410 terminals appearance.
- The product name is visible on the label at the back side of the device; see Figure 4, Figure 5, Figure 6

Figure 1, UX 300 and antenna, SCR

Figure 2, UX 301 and optional antennas, SCR

Figure 3, UX 410 and antenna, SCR

PRODUCT TYPE

- UX 300 / UX 301 / UX 410 are modular Point-of-Interaction (POI) terminals designed to process online and offline transactions in an unattended environment. The terminals are PCI PTS POI v5.1 approved as SCR class of device.
- They are equipped to handle a variety of payment methods including: EMV chip and PIN, chip and signature, magnetic-stripe and contactless.
- They provide Ethernet, USB, RS 232, MDB, GPRS, PSDN, RS 485, and two Secure Access Modules (SAMs) slots.

UX SERIES: UX 300 / UX 301 / UX 410

PCI PTS POI SECURITY POLICY

IDENTIFICATION

- Please find the current approved hardware and firmware versions in the PCI PTS Letter of approval or in the list of approved PTS devices on the PCI SSC web page.
- Current hardware and firmware versions:

Model	Hardware	Firmware
UX 300	M159-300-xxx-xxx-x Rev Axx M159-300-xxx-xxx-x Rev Bxx M159-300-xxx-xxx-x Rev Cxx	Vault: 18.x.x AppM: 11.x.x SRED: 11.x.x OP: 8.x.x
UX 301	M159-301-xxx-xxx Rev Axx M159-301-xxx-xxx Rev Bxx	Vault: 18.x.x AppM: 11.x.x SRED: 11.x.x OP: 8.x.x
UX 410	U629-04-02-xxx-xx-A0	Vault: 18.x.x AppM: 11.x.x SRED: 11.x.x OP: 8.x.x

- The product model name (Model) and hardware version (Prod. No., HW ID) is printed on the label at the back side of the device; see Figure 4, Figure 5, Figure 6. The label should not be torn off, covered or manipulated in any way.

- Hardware version numbers include variable fields for designating product options.

Hardware version variable positions																										
	M	1	5	9	-	x	x	x	-	x	x	x	-	x	x	x	-	x		R	e	v	:	x	x	x
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

6-8	Device type
10-12	Communication option
14-16	Country code
24-26	Security version

Table 1, UX 300 Hardware version variable positions

- Variable “x” Position:
  - 10 Environmental
    - '0': Standard
  - 11 Interface
    - '0': Standard
    - '1': MDB
    - '2': PSTN
    - '3': ISDN
    - '4': GPRS
    - '5': Petrol
    - '7': WPWR
  - 12 Memory configurations
    - ‘0’: Standard
    - ‘1’: Extended
  - 14, 15 Country code
    - 'WW': Standard
    - 'EU'
    - ‘KR’
    - 'LA'
    - ‘UK’
  - 16 Accessory
    - 'A': Standard
    - ‘E’: Extended
  - 18 Security and safety accessory
    - B: UKCC security approval
    - C: FCC modular approved
  - 24 Security relevant changes
    - ‘A’: Security relevant modification
    - ‘B’: Security relevant modification

- ‘C’: Security relevant modification
- 25, 26 Minor none security relevant changes
  - '00': Standard

Hardware version variable positions																							
	M	1	5	9	-	x	x	x	-	x	x	x	-	x	x	x	-	R	e	v	:	x	x	x
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

6-8	Device type
10-12	Communication option
14-16	Country code
22-24	Security version

Table 2, UX 301 Hardware version variable positions

- Variable “x” Position:
  - 10 Environmental
    - '0': Standard
    - '2': FMTA
  - 11 Interface
    - '0': Standard
    - '1': MDB
    - '2': PSTN
    - '3': ISDN
    - '4': GPRS
    - '5': Petrol
    - '7': WPWR
  - 12 Memory configurations
    - ‘0’: Standard
    - ‘1’: Extended
  - 14, 15 Country code
    - 'WW': Standard
    - 'EU'
    - ‘KR’
    - 'LA'
    - ‘UK’
  - 16 Accessory
    - 'A': Standard
  - 22 Security relevant changes
    - ‘A’: Security relevant modification
    - ‘B’: Security relevant modification

- 23, 24 Minor none security relevant changes
  - '00': Standard

Hardware version variable positions																			
	U	6	2	9	-	0	7	-	x	x	-	x	x	x	-	x	x	-	A	0
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
9, 10	Communication options																			
12	Privacy-shield option																			
13	Keypad artwork																			
14	Device color																			
16	Memory configuration																			
17	Extra features																			
20	Hardware revision																			

Table 3, UX 410 Hardware version variable positions

- Variable “x” Position:
  - 12 Privacy shield
    - ‘0’: none
  - 13 Keypad type
    - ‘0’: none
  - 14 Device color
    - '0': Standard
  - 16 Memory configurations
    - ‘0’: Standard
    - ‘1’: Standard / µSD
    - '2': Extended
  - 17 Extra features
    - Bit 0: Media

Figure 4, UX 300 Hardware identification

Figure 5, UX 301 Hardware identification

Figure 6, UX 410 Hardware identification

- The firmware versions can be retrieved from the boot splash screen. Shortly after powering up, a splash screen on a connected display (vending machine, PED, etc.) displays the version number for the four security kernels; see Figure 7. You must be able to find these numbers on the list of Approved PIN Transaction Security (PTS) Devices. If these numbers do not match, notify your service provider immediately.

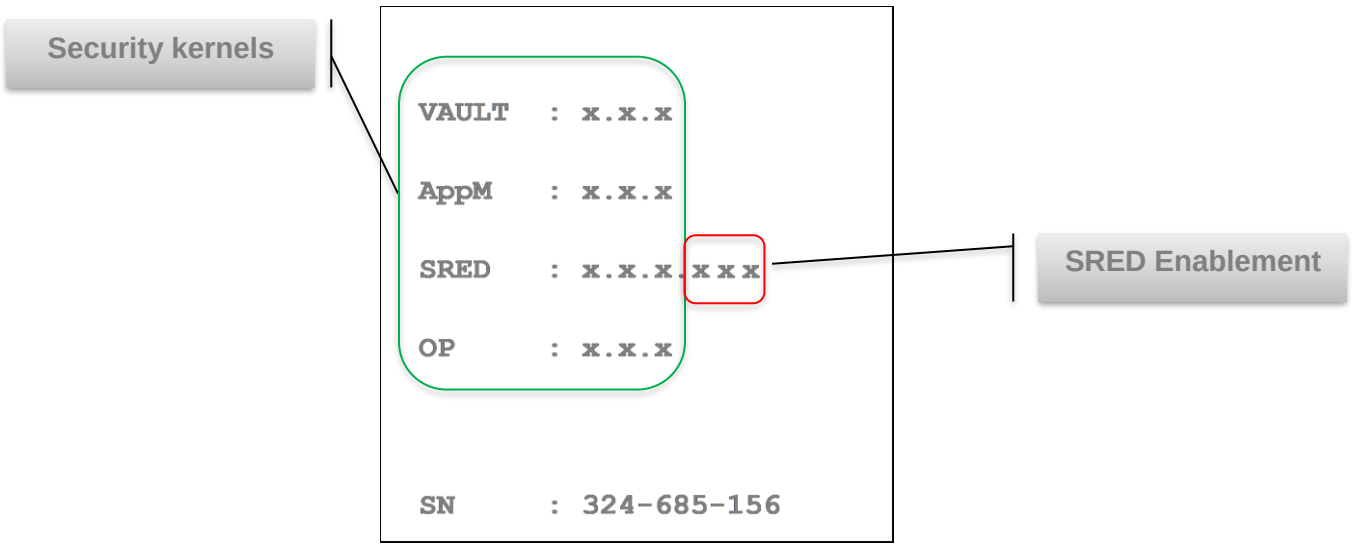

Figure 7, Boot Splash Screen

- The three last digits in SRED version number show the SRED enablement status which is encoded according Table 4.

SRED Enablement			
	x	x	x
	1	2	3
1	VCL/ADE encryption: • 0 = VCL and ADE are disabled • 1 = ADE is enabled • 2 = VCL is enabled • 3 = ADE and VCL are enabled		
2	ATOS Encryption: • 0 = ATOS is disabled • 1 = ATOS is enabled		
3	Voltage encryption: • 0 = Voltage is disabled • 1 = Voltage is enabled		

Table 4, SRED Enablement

- In addition, the detailed information about the security kernel versions can be shown on request from the “Basic information” panel in System Mode. To view the security kernel versions, login in System mode and select “Home > Information > Basic information” panel. Scroll through the screen and locate the four kernels; see Figure 8.
- Security kernels are:
  - Vault
  - SRED (equivalent to SRED in boot splash screen)
  - Open Protocol (equivalent to OP in boot splash screen)
  - Application Manager (equivalent to AppM in boot splash screen)

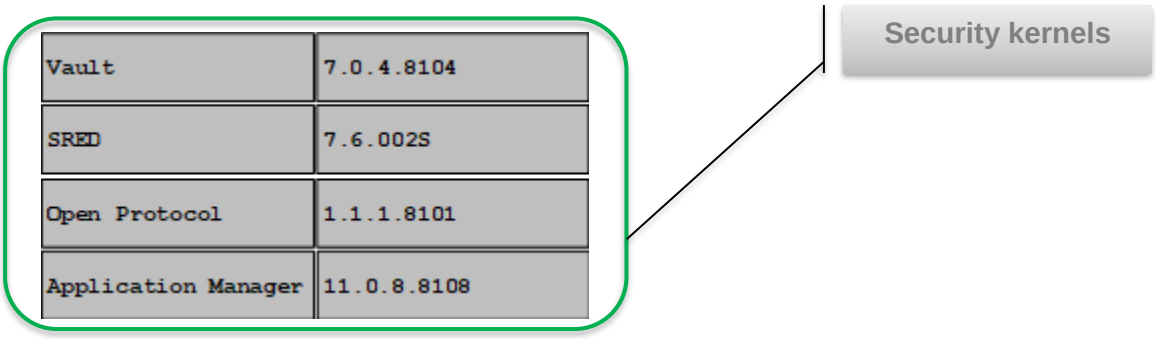

Figure 8, Basic information panel

INSTALLATION AND USER GUIDANCE

INITIAL INSPECTION

1) Carefully inspect the shipping carton and its contents for possible tampering or damage.
2) Validate the authenticity of the sender by verifying the shipping tracking number and other information located on the product order paperwork.
3) Remove the UX 300 / UX 301 / UX 410 unit and antenna from the shipping carton.
4) Remove any protective plastic wrap.
5) Inspect the terminal for possible tampering; see how to identify signs of tampering in section Periodic Inspection.
6) Save the shipping carton and packing material for future repacking or moving the device.

INSTALLATION

- Prior to usage and deployment, familiarize yourself with the [R7] Installation Guides. These guides provide information on verifying terminal equipment, usage, safety, security, environmental requirements, and troubleshooting steps if needed.
- UX 300 / UX 301 / UX 410 terminals are intended for an unattended environment.

- The terminal contains no user serviceable parts. Do not, under any circumstances, attempt to disassemble the terminal.

ENVIRONMENTAL CONDITIONS

- The following are the temperature and humidity specifications:
  - UX 300
    - -20° to 70° C (-4° to 158° F) operating temperature
    - -25° to 70° C (-13° to 158° F) storage temperature
    - 10% to 90% relative humidity, non-condensing
  - UX 301
    - -30° to 70° C (-22° to 158° F) operating temperature
    - -30° to 70° C (-22° to 158° F) storage temperature
    - 10% to 90% relative humidity, non-condensing
  - UX 410
    - -30° to 70° C (-22° to 158° F) operating temperature
    - -30° to 80° C (-22° to 176° F) storage temperature
    - 10% to 90% relative humidity, non-condensing
- Subjecting the devices to extreme environmental conditions will result in tamper events. Any temperatures above 100 ºC (± 5 degrees) or below -37 ºC (± 5 degrees) will result in a tamper condition. Additionally, should the battery voltage drift outside of the range of 2.4 VDC to 3.7 VDC, the unit will tamper as well.

COMMUNICATIONS AND SECURITY PROTOCOLS

- UX 300 / UX 301 / UX 410 terminals support the communications methods and protocols listed below. Use of any method not listed here invalidates the device PCI PTS approval.
- The following interfaces are available in the device:
  - Ethernet
  - USB Host

  - USB Device
  - RS 232
  - MDB (if available)
  - GPRS (if available)
  - PSDN (if available)
  - RS 485 (if available)
- The following protocols and services are supported by the device:
  - TLS / SSL
  - SFTP
  - DHCP, DNS, OCSP
  - ICMP, TCP, IP, UDP
  - PPP
  - MDB (if available)
- The security guidance described in this Security Policy and in [R9] V/OS IP Stack Security Guidance Users Guide specifies how protocols and services must be used/configured for each interface that is available on the device.

CONFIGURATION SETTINGS

- The device is functional when received by the merchant or acquirer. No security sensitive configuration settings are necessary to be modified by the end user to meet security requirements.

UNATTENDED INSTALLATION

- The UX Series devices are designed for unattended environments. Please refer to [R7] Installation Guides for proper mounting procedures.

HANDHELD DEVICES

- Not applicable.

OPERATION AND MAINTENANCE

PERIODIC INSPECTION

- Inspect the terminal for possible tampering after receipt, during installation and periodically. 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
  - Tamper message on a connected display (vending machine, PED, etc.); see Figure 9
  - Flashing red warning LED on the UX Series SCRs.
- 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. 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.
- Verify that there are no foreign objects inserted into the mag stripe reading slot or any noticeable additional mag stripe read head.
- Develop a breach response plan. This identifies the steps to take if a suspected breach occurs and as well as who will perform each step. 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 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.
- 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] Installation Guides.

SELF-TEST

- UX 300 / UX 301 / UX 410 terminals employ a self-test to confirm firmware integrity and reinitialize memory. 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 (system mode passwords required) may configure UX 300 / UX 301 / UX 410 to perform self-test at a specified time or manually invoke 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, UX 300 / UX 301 / UX 410 limits its functionality based on the severity of the issue discovered. Device response ranges from partial disablement of applications to non-functionality. In all cases PIN-processing is disabled.

ROLES AND RESPONSIBILITIES

- Authorized terminal administrators can perform local downloading operations using the System Mode. Also, they can perform local key injection operations under dual control.

PASSWORDS AND CERTIFICATES

- Passwords used for entering in System Mode and entering sensitive services (key loading) are pre-expired and must be changed upon first use. These passwords must be at least 7 decimal characters (0-9) in length.

TAMPER RESPONSE

- Security mechanisms employed within the terminal can detect physical tampering and triggers a tamper event. This causes the terminal to cease performing transactions and indicates that it has been tampered on the display; see Figure 9.

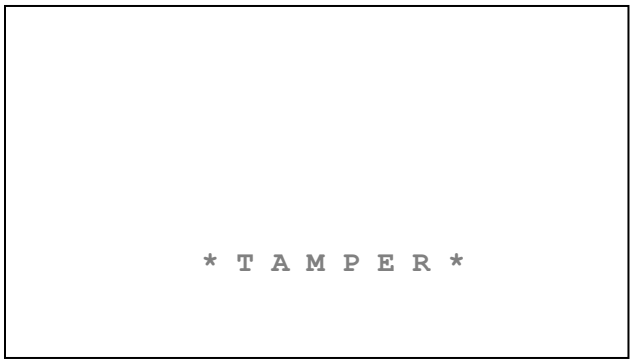

Figure 9, Tamper message on a connected terminal display

PRIVACY SHIELD

- UX 300 / UX 301 / UX 410 are unattended SCRs without PIN entry support.

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.

DECOMMISSIONING

- 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, and Data encryption keys.
- If the device is permanently decommissioned from service, it can be done by disassembling the device to force 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; see Figure 9.

REMOVAL DETECTION

- UX 300 / UX 301 / UX 410 are unattended devices supporting removal-detection.
    - Please refer to the [R7] Installation Guides for proper mounting procedures.

SECURITY

SOFTWARE DEVELOPMENT GUIDANCE

- Applications must be designed and implemented in accordance with the PA-DSS requirements document entitled, [R13] PA-DSS Program Guide v3.0.
- All payment-based applications must undergo a formal source code 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 application code. Only application code that has been authorized for release should be signed and released to the field. 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 process must show any problems noted during the code review and security testing. Such reviews must happen after each and every code change.

- When developing IP capable payment-based applications, developers must follow the guidance listed in the following documents:
    - This Security Policy
    - [R8] V/OS Programmer's Manual
    - [R9] V/OS IP Stack Security Guidance Users Guide
    - [R12] VeriShield File Signing Overview
- All referenced best practices regarding coding practices 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.
- 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

TLS / SSL / SFTP

- 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.

- Cipher suites using single DES or RC4 are not supported.
- Cipher suites using TDES are no longer allowed by PCI PTS, because NIST no longer considers TDES to be a strong cipher suite, hence they are disabled by default. They can be enabled only if required on an interim basis to facilitate interoperability as part of a migration plan. Using cipher suites not compliant to NIST will void the PCI PTS compliance.
- It is strongly advised to use TLS/SSL with mutual authentication enabled to protect the communications over a network connection.

BLUETOOTH

- Not applicable.

SIGNING

- VeriShield FST (File Signing Tool) manages the generation and signing of device certificates. See DevNet and [R12] VeriShield File Signing Overview for more information on signing tool implementation.
- UX 300 / UX 301 / UX 410 terminals employ 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 UX 300 / UX 301 / UX 410 terminal to logically secure access to the terminal by controlling who is authorized to download applications or firmware updates 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.
- Only application codes that have been authorized for release should be signed and released to the field. The signing must occur under dual control and split knowledge.

ACCOUNT DATA PROTECTION

- If the product is SRED enabled:
  - The working buffers associated with PAN encryption clears automatically as soon as the transaction completes.
  - The encryption of PAN data is automatic and transparent to your application – there are no added API calls needed.
- The device supports account data protection using format-preserving encryption (FPE) revised FF2 method. The pass-through of clear-text account data is supported using whitelisting technique (BIN table).
- In addition, the device supports account data encryption operations using TDEA DUKPT algorithm (ADE and ATOS Poseidon ZVT Security), AES DUKPT (VCL) and VISA DSP.

ALGORITHMS SUPPORTED

- The device supports the following algorithms:
  - Triple DES (112 bits, 168 bits)
  - AES (128 bits)
  - RSA (2048 bits)
  - ECDSA (256, 384, 521 bits)
  - SHA-256, SHA-384, SHA-512

KEY MANAGEMENT

- The device supports the following key management schemes:
  - Fixed key (TDES)
  - Master Key / Session Key (TDES)
  - DUKPT (TDES and AES)
- Employing key management schemes that do not comply with PCI PTS with PCI payments will invalidate the PCI PTS approval for this POI.

- Injecting plaintext secret or private keys for payment purposes via a key loader will void the PCI PTS compliance.
- The device must be rebooted before starting any key loading session.
- For devices to be deployed in countries requiring Common.SECC certification, the use of fixed key or master/session key management schemes and PIN block format 0 for PIN encryption must be avoided and unique keys per transaction or the use of PIN block format 1 (random included) shall be used instead.
- The following table lists all supported key management schemes. For more information, refer to [R11] 2.0 Encryption Services Organization Key Management Procedures“.

Key Name	Size (bytes)	Algorithm	Purpose
KLK (Key Loading Key)	16, 24	TDEA (ANSI X9.52)	To load encrypted master keys
Master Keys	16, 24	TDEA (FIPS 46-3, ANSI X3.92, X3.106); TDEA (ANSI X9.52)	Encryption of working keys (PEK, MEK, DK) for down-line transmission to the device
PIN Encryption Key (PEK)	16, 24	TDEA (FIPS 46-3, ANSI X3.92, X3.106); TDEA (ANSI X9.52)	PIN Encryption per master/session key scheme
MAC Encryption Key (MEK)	16	TDEA MAC (ANSI X9.19)	Message authentication per master/session key scheme
Data Keys (DK)	16	TDEA (ANSI X9.52)	Account balance decryption per master/session key scheme
PIN Fixed Keys	16, 24	TDEA (FIPS 46-3, ANSI X3.92, X3.106); TDEA (ANSI X9.52)	PIN Encryption per fixed key scheme
MAC Fixed Keys	16	TDEA (FIPS 46-3, ANSI X3.92, X3.106); TDEA (ANSI X9.52)	Message authentication per fixed key scheme
DUKPT TDEA Keys (PIN, MAC)	16	TDEA DUKPT (ANSI X9.24)	PIN encryption and message authentication per TDEA DUKPT scheme
DUKPT AES Keys (PIN, HMAC and	16	AES DUKPT (ANSI X9.24 - 3)	PIN encryption, message authentication and account data encryption per AES DUKPT scheme

data encryption)			
DUKPT TDEA ADE Keys	16	TDEA DUKPT (ANSI X9.24)	Account data encryption and MAC calculation per TDEA DUKPT scheme
ATOS Poseidon Keys	16	TDEA (ANSI X9.52)	PIN Encryption, message authentication, bitmap encryption and end-to-end encryption per ATOS Poseidon scheme
VCL Keys	16	AES-128	Keys for Format Preserving Encryption of card data per Verifone VCL scheme
Application Signer		RSA 2048 SHA-256	Used by customer to sign Applications to install to device.

Table 5, Key Table

KEY LOADING

- 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 follow PCI PIN Transaction Security requirements.

KEY REPLACEMENT

- Key replacement must be performed upon any known or suspected compromise of any cryptographic or sensitive information, and whenever the time deemed feasible to determine the key by exhaustive attack elapses, as defined in NIST SP 800-57-1.

ANNEX

RELATED DOCUMENTATION

[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] UX 300: DOC159-024-EN
UX 301: DOC159-026-EN
UX 410: DOC159-039-EN
Installation Guides

[R8] V/OS Programmer's Manual (VPN – DOC00501)

[R9] V/OS IP Stack Security Guidance Users Guide

[R10] PCI PTS POI - Modular Security Requirements v5

[R11] 2.0 Encryption Services Organization Key Management Procedures

[R12] VeriShield File Signing Overview

[R13] 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
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:	PIN Transaction Security
RH:	Relative Humidity
RSA:	Rivest Shamir Adleman
SCR:	Secure Card Reader
SHA:	Secure Hash Algorithm

SRED:	Secure Reading and Exchange of Data
TDEA:	Triple Data Encryption Algorithm
TMK:	Terminal Master Key
VPN:	Verifone Publication Number