MX900 SERIES PCI PTS POI SECURITY POLICY

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 4.0 devices, such as the Mx915 and Mx925.

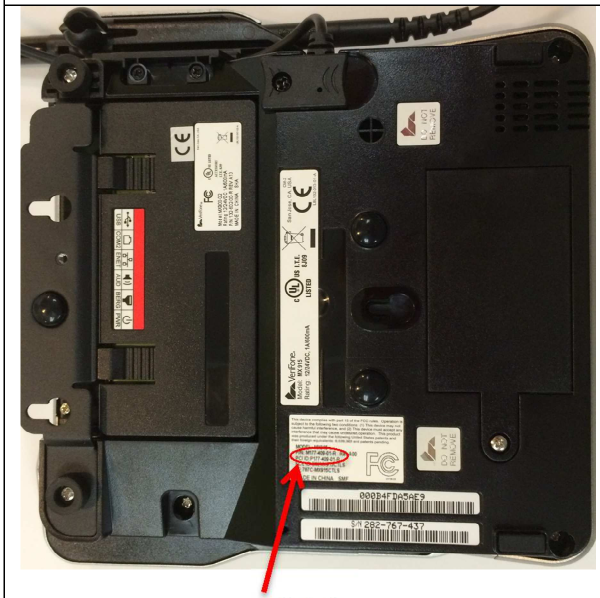
SCOPE

The security policy herein applies to the VeriFone Mx900 series PCI PTS version 4.x POI approved devices. Failure to use the terminal in accordance with this security policy will cause the terminal to not be in compliance to the PCI PTS POI Modular Security Requirements version 4.0 approval of the device.

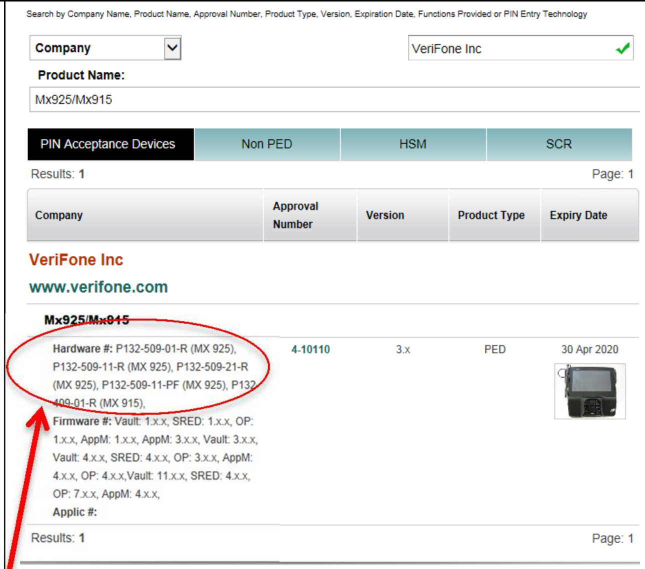
PRODUCT IDENTIFICATION & INSPECTION

- Upon receiving the Mx900 series terminal, you must validate that the intended sender is indeed who shipped the terminal by verifying the shipping tracking number and other information located on the product order paperwork.
- The terminal must be visually inspected prior to placement into service to ensure the device has not been tampered with and is in pristine condition.
- You must first verify that your MX900 series product is PCI approved as a PED (PIN Entry Device). Locate the PCI Identification number on the bottom of the device. Verify that this number is covered by the Hardware # scheme in the PCI listing on the PCI SSC PTS approval web site. See image below for assistance.

PCI IDENTIFICATION NUMBER



Match the PCI ID Number listed on the device



Search by Company Name, Product Name, Approval Number, Product Type, Version, Expiration Date, Functions Provided or PIN Entry Technology

Company: VeriFone Inc

Product Name: Mx925/Mx915

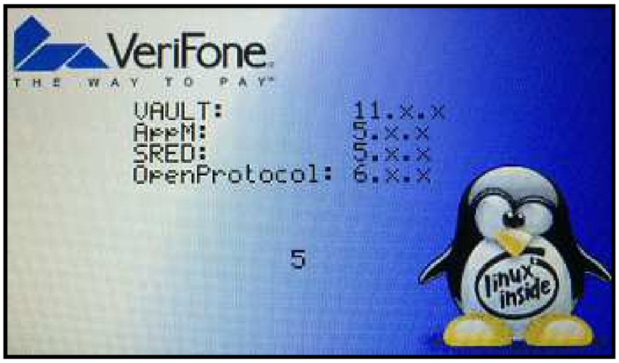
Results: 1 Page: 1

Company	Approval Number	Version	Product Type	Expiry Date
VeriFone Inc www.verifone.com				
Mx925/Mx915				
Hardware #: P132-509-01-R (MX 925), P132-509-11-R (MX 925), P132-509-21-R (MX 925), P132-509-11-PF (MX 925), P132-409-01-R (MX 915), **Firmware #:** Vault: 1.x.x, SRED: 1.x.x, OP: 1.x.x, AppM: 1.x.x, AppM: 3.x.x, Vault: 3.x.x, Vault: 4.x.x, SRED: 4.x.x, OP: 3.x.x, AppM: 4.x.x, OP: 4.x.x,Vault: 11.x.x, SRED: 4.x.x, OP: 7.x.x, AppM: 4.x.x, **Applic #:**	4-10110	3.x	PED	30 Apr 2020

Results: 1 Page: 1

The PCI Approved device Hardware # and Firmware # are available at the following URL: https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

- You must also verify that your MX900 series product is running firmware that is PCI PED approved. Shortly after powering up, a splash screen will display the version numbers for the four security kernels, such as the image to the right. To determine whether or not the firmware is approved, you must be able to find these numbers on the PCI listing just as was done for the hardware identifier. If these numbers do not match, notify your service provider immediately.

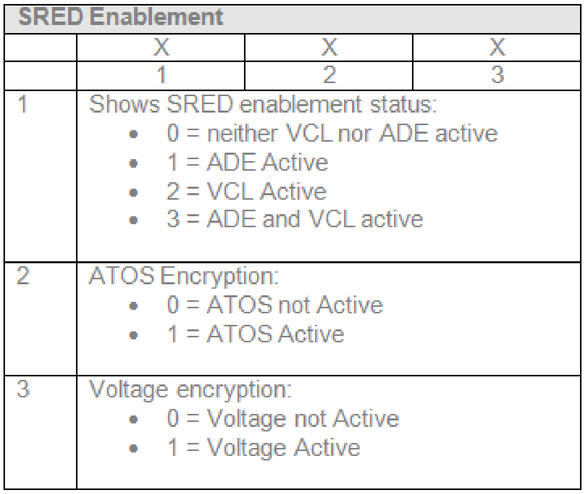


```
VAULT:         11.x.x
AppM:          5.x.x
SRED:          5.x.x
OpenProtocol:  6.x.x

          5
```

- The current hardware identifier version numbers are:
  - P177-409-01-R (MX915)
  - P177-509-01-R (MX925)
- In this example, the firmware version numbers are:
  - Vault: 11.x.x
  - AppM: 5.x.x
  - SRED: 5.x.x.xxx
  - OP: 6.x.x

  The “xxx” suffix of the SRED kernel version depicts SRED enablement.



SRED Enablement			
	X	X	X
	1	2	3
1	Shows SRED enablement status: • 0 = neither VCL nor ADE active • 1 = ADE Active • 2 = VCL Active • 3 = ADE and VCL active		
2	ATOS Encryption: • 0 = ATOS not Active • 1 = ATOS Active		
3	Voltage encryption: • 0 = Voltage not Active • 1 = Voltage Active		

ROLES

DEPLOYERS OF MX 900 SERIES TERMINAL TO END-USERS SITES

Perform specific tasks required to deploy a new MX 900 Series terminal into the field, such as terminal configuration, application software download, and testing of the terminal prior to deployment.

ADMINISTRATORS OR SITE MANAGERS

Change passwords, perform routine tests and terminal maintenance, and configure terminals for remote diagnostics and downloads.

FIRMWARE AND APPLICATION MAINTENANCE

LOCAL OPERATIONS

Local operations within the system mode allows for standalone terminals to perform data transfers between the terminal and another terminal or computer, as well as perform local System Mode operations to configure, test and display information about the terminal.

System mode procedures can be found in reference 7 section 4.

REMOTE OPERATIONS

Remote operations require communication between the terminal and a host computer over a connection. This System Mode operation performs application software downloads, upload software from one terminal to another and perform diagnostics.

Application software download procedures can be found in reference 7 section 5.

SECURITY POLICY

These policies are provided to ensure that these devices are employed in a secure manner and in compliance to the PCI PTS POI standards version 4.x.

ENVIRONMENTS

- The MX 900 Series terminal has security architecture called VeriShield Retain, which has both physical and logical components. The logical security component of the VeriShield architecture, which is part of the terminals operating system software, is called file authentication (FA). File Authentication is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process enables the sponsor of an MX 900 Series 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 Files origin, Senders identity and the integrity of the files information. If any of these three items are not verified then the download is rejected.
- Prior to usage and deployment into the terminal’s intended environment, review of the Mx900 Series Reference Guide (reference 7) must be performed to verify terminal equipment, usage, safety, security, environmental requirements and troubleshooting steps if needed.
- The MX900 series products must be used in an attended environment. They are to be mounted on a swivel stand or placed on flat surfaces such as a sale counter, cash register stand.
- These devices have a built-in privacy shield installed, the privacy shield protects the customers PIN entry from being seen by the cashier or other customers. Please refer to the Mx900 Series Installation Guide for guidance on using the MX900 series product in a secure and compliant manner.
- Periodically inspect the terminal for possible tampering. Signs of tampering include: wires protruding out of the device, and foreign objects inserted into the smart card slot or mag stripe slot.
- The terminal contains no user serviceable parts. Do not, under any circumstances, attempt to disassemble the terminal.
- Do not use a terminal that has been damaged or tampered with. The Mx9x5 devices come equipped with tamper evident labels. If a label or component appears to be

damaged, please notify your company security officer and you service provider immediately.

- The Mx900 Series products are designed to operate within a temperature range of 0 to 40 degrees Celsius, within 5% to 90% relative humidity (non-condensing). While in storage, their environment must be kept to -30 to 70 degrees Celsius and within 5% to 90% relative humidity (non-condensing)
- Subjecting the Mx900 Series product to extreme environmental conditions will result in tamper events. Any temperatures above 95 degrees Celsius (+-4 degrees) or below 40 degrees Celsius (+- 4 degrees) will result in a tamper condition. Additionally, should the battery voltage drift outside of the range of 2.7 VDC to 3.6 VDC, the unit will tamper as well.

KEY MANAGEMENT

- Key management techniques supported by the terminal are defined in references 1 & 2.
- 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 to references 1,2,4
- 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 shall be in compliance to PCI PIN Transaction Security requirements.
- Employing key management schemes that do not comply with PCI PTS with PCI payments will invalidate PCI PTS approval for this POI.
- Key replacement must be performed upon any known or suspected compromise of any cryptographic or sensitive information.

1. Please reference the document entitled, “2.0 Encryption Services Organization Key Management Procedures”.

Key Name	Size (bytes)	Algorithm	Purpose
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
ATOS Poseidon Keys	16	TDEA (ANSI X9.52)	Per ATOS Poseidon scheme: PIN Encryption, Message authentication, Bitmap encryption, and End-to-end encryption

Key Name	Algorithm	Purpose
Application Signer	RSA 2048 SHA-256	Used by customer to sign Applications to install to device.

ADMINISTRATION SECURITY

- Configuration of the terminal must be performed prior to installation and use. See section 4 System Mode of reference 7, Mx900 Series Reference Guide for instructions.
- This configuration mode must limited to administrators and maintenance/support personnel. The administrators should setup the maintenance user prior to installation and use.
- Password-protected sensitive services utilize dual control passwords and are pre-expired and must be changed prior to configuring the terminal for installation and use. These passwords must be at least 7 decimal characters (0-9) in length.
- Passwords are pre-expired and must be changed upon first use
- Updates and/or patches to the operating system can be performed by the administrators using the system mode (see reference 7 section 4 for steps to perform

this operation. Updates/patches are RSA certificate authenticated, if the signature of the updates cannot be authenticated, the update/patch is rejected and not installed.

- Develop a process to monitor devices that consistently do not work properly, such as high read failures or debit card declined transactions as they could be an indication of a tampered terminal.
- Implement a procedure to require 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 to validate the PIN pad serial number every time the device is started or powered on to insure the device has not been replaced, and if it has, cease using that terminal and notify your VeriFone customer relations manager.
- Implement a daily visual inspection of the PIN pad 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 which identifies steps to take if a suspected breach occurs and who will perform each step. The plan needs to include isolation of your payment systems, have a list of who needs to be notified including your local law enforcement, your acquiring bank, your processor, security assessor, as well as your payment system vendor.
- Institute a procedure to track each instance in which a terminal is replaced 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 more information regarding signing tool implementation.

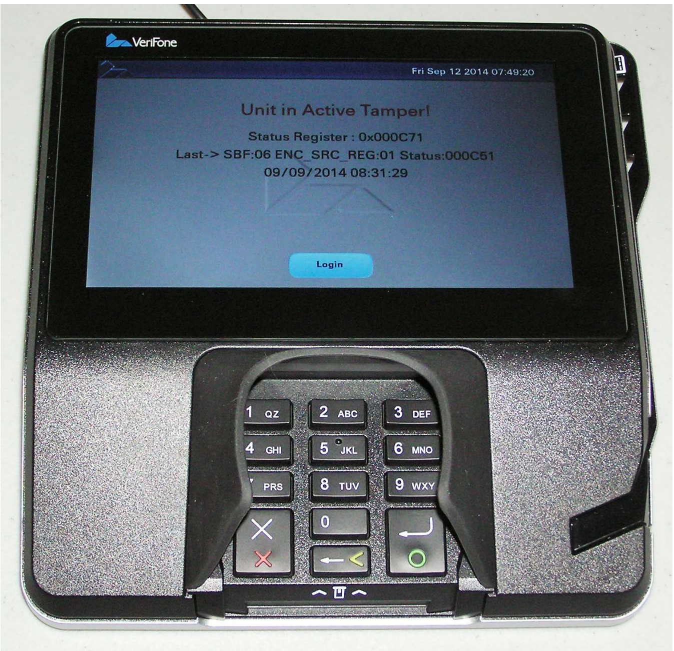
DEVICE DIAGNOSTICS

- MX9xx Series products employ a self-test to confirm firmware integrity. The self-test is performed:
    - When the unit is powered on, and
    - When the unit is rebooted, and
    - At least once every 24 hours, and
    - Upon demand.
- Authorized maintenance personnel may configure the MX9xx series PED such that the self-test occurs at a specific hour.
- 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 tests are performed during self-test:
    - The integrity of the TMK (Terminal Master Key) is checked
    - The integrity of the other key files is checked
    - The tamper detection system is checked
    - The VeriShield certificate tree is checked
    - The firmware is checked
- If a self-test fails, the MX9xx series product’s response is to limit its functionality in a manner proportional to the severity of the issue discovered. Device response ranges from partial disablement of applications to non-functionality.

DEVICE SECURITY

- Security mechanisms are employed within the terminal that will detect physical penetration and will trigger a tamper event. This event will cause the terminal to cease performing transactions and indicate it has been tampered.

- The security of the terminal must not be compromised by altering the environmental conditions. The power and temperature operating ranges must be adhered to in accordance to the Mx900 Series Reference Guide (reference 7); operating the terminal outside of these ranges will cause a tamper event, the event will cause the terminal to cease performing transactions and indicate it has been tampered on the display.
- The terminal must perform a self-test upon start up and at least once per 24 hour period. This self-test is performed by the operating system and doesn't require user intervention nor intervention from the application.



Fri Sep 12 2014 07:49:20

Unit in Active Tamper!

Status Register : 0x000C71

Last-> SBF:06 ENC_SRC_REG:01 Status:000C51

09/09/2014 08:31:29

CODERS/DEVELOPERS (Both Firmware and Application)

- All payment based applications and firmware must undergo a formal review and security audit before they may be signed and used.
    1. The reviewer must be a qualified individual who was not involved with the authorship of the POI PED code.
    2. Code review must be governed by an auditable process that shows the code review and security testing have been performed, and requiring sign-off by the person(s) performing the code review and security tests.
        1. The tester shall confirm that the process will show any problems noted during the code review and security testing
    3. Such reviews must happen after each and every code change.
    4. The firmware must be reviewed against PCI POI PED requirements as well as the guidance listed in this document, as well as the VOS Programmer's Manual (reference #13).
- Applications are authenticated by the terminal operating system prior to being executed. The authentication is performed by verifying the RSA certificate and signature of the application.
- Applications must be designed and implemented in accordance with the PA-DSS requirements document entitled PA-DSS Program Guide v3.0.
- Only application code that has been authorized for release should be signed and released to the field. The 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:
    1. Programmer's Guide SPC132-021-01-A (reference 8)
    2. This Security Policy
    3. VOS Programmer's Manual DOC00501
    4. VeriShield File Signing Overview (reference #14)
- All referenced best practices must be adhered to regarding coding practices and device configurations.

- 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:
    1. The working buffers associated with PAN encryption are automatically cleared for you, as soon as the transaction completes.
    2. The encryption of PAN data is automatic and transparent to your application – there are no added API calls needed.
- Allowable application behavior:
    1. Write to the display
    2. Fetch keypad entries
    3. Request an encrypted PIN block
- Forbidden application behavior:
    1. Change PIN entry retry limit
    2. Attempt to alter PIN entry time-out.
        1. Note: PIN entry time-outs are set and enforced by the OS. The application is not capable of altering these.
        2. PIN Entry time-outs are set to:
            1. 30 Seconds without key presses, or
            2. 300 Seconds with key presses.
    3. Modify a key
    4. Generate a subordinate certificate
    5. Execute another application
    6. Encrypt arbitrary data

1. All firmware must be written in accordance with the standards put forward in the document entitled, “VD-Software-Assurance-060514”, reference 16.

CRYPTOGRAPHY

- Only use acceptable cryptographic algorithms listed here in SP800-57 Part1: Recommendation for Key Management.
- The cryptographic strength used should be at minimum 112 bits.
- Cryptographic algorithms used should be at minimum: SHA-256, 2TDEA, RSA-2048, AES-128.
- Although other cryptographic algorithms may be supported by the PED, they may not be used for payment-based applications.

COMMUNICATION

The MX9xx Series of products possess many API functions that may be used by payment applications. It should be noted that not all of the available functions offered may be used for payment-based applications. Also, care must be used to ensure that each function is used in a manner compliant with PCI POI PED requirements as all modes are not necessarily compliant.

Where the following interfaces are used to transfer any sensitive authentication data, including but not limited to the encrypted PIN or account data:

- Bluetooth Security modes 1 & 2 and the “Just Works” secure pairing option should not be used.
- WiFi should use encryption; WEP should not be used.
- TLS 1.2 should be used.

- All encryption algorithms, key lengths, and encryption strengths must be used in accordance with the “Cryptography” section of this document.
- PTS approval is only valid for the platform containing the IP and link layer, the IP protocols, the security protocols and the IP services, as provided by the vendor and when used in accordance with the guidance supplied in this document.
- Keys may NOT be shared between security protocols.

FIRMWARE UPDATES

The MX9xx Series products support firmware updates. For guidance governing compliant firmware updates, please see reference #7, the MX900 Series Reference Guide, section 5.

DECOMMISSIONING/REMOVAL FROM SERVICE

Prior to removing the device from service for repairs or permanent removal, all sensitive data must be erased. Sensitive data includes credit card data and all encryption keys inclusive of ALL Private, PIN, Data encryption keys. See reference 17 for Decommissioning/Removal from Service Procedures.

REFERENCES

1. ANS x9.24 Part 1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
2. ANS x9.24 Part 2:2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
3. 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
4. X9 TR-31:2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
5. ISO 9564-2, Banking, Personal Identification Number Management and Security Part 2: Approved Algorithms for PIN Encipherment
6. SP800-57 Part1: Recommendation for Key Management
7. SPC132-020-01-A VeriFone Mx900 Series Reference Manual
8. SPC132-021-01-A Mx900 Series Programmer Guide
9. Point of Interaction (POI) Modular Security Requirements v4.0
10. SP800-121 Guide to Bluetooth Security
11. VeriShield FST Basics
12. 2.0 Encryption Services Organization Key Management Procedures
13. V/OS Programmer’s Manual, DOC00501 Rev F (or later)
14. VeriShield File Signing Overview
15. VD-Software-Assurance-060514
16. Mx900 Series Decommissioning/Removal From Service Procedures