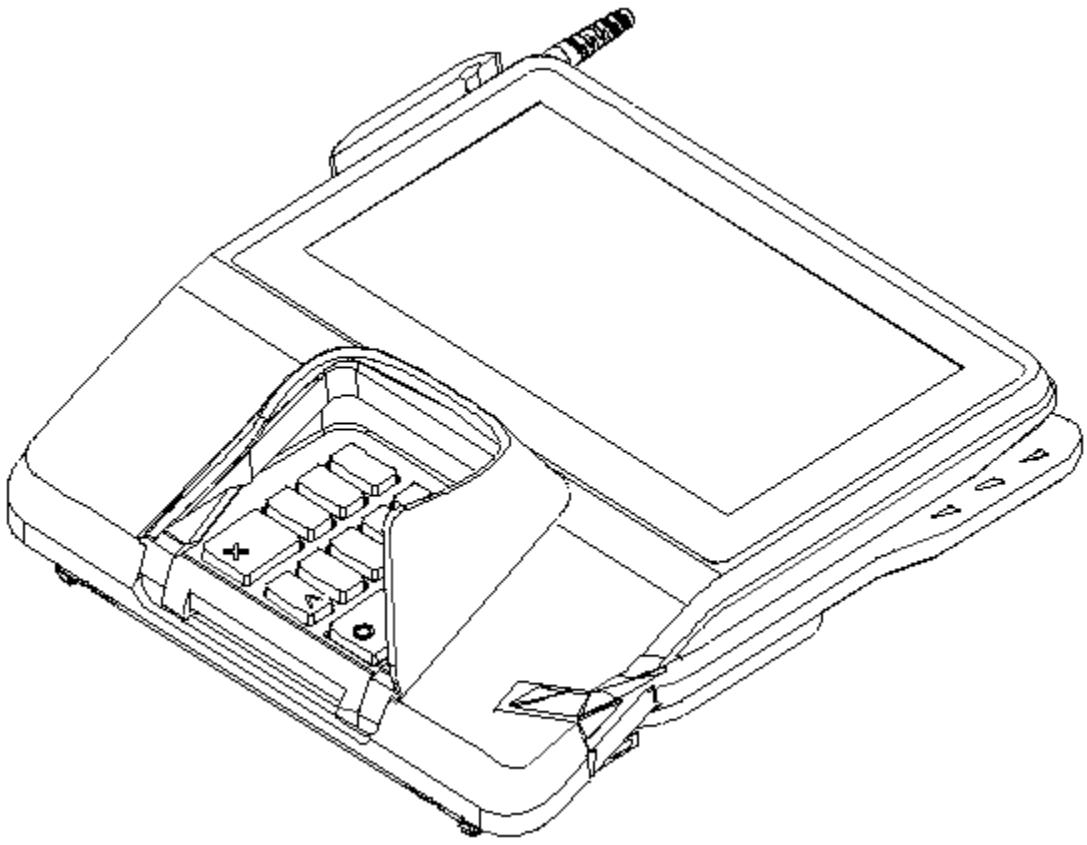
MX 900 Series

Reference Manual

Part Number SPC132-020-01-D, Revision D



Verifone®

MX 900 Series Reference Manual

Part Number SPC132-020-01-D, Revision D

March 16, 2017

Verifone®, Inc.
88 West Plumeria Drive
San Jose, CA 95134
Telephone: 408-232-7800
http://www.verifone.com

Product Warranty

For product warranty information, go to: *www.verifone.com/terms*.

MX 900 Series Reference Manual
Revision History

Date	Revision	Description
September 14, 2012	A	Initial Documentation Release
February 27, 2015	B	Changed PCI requirement to 4.x
June 19, 2015	C	Rebranded the document
March 16, 2017	D	Added warranty blurb

Contents

1 INTRODUCTION

This manual is your primary source of information for MX 900 Series technical information.

Intended Audience

This manual is intended for system administrators, application developers, and support personnel.

Document Organization

The following chapters are included:

Chapter 1, Introduction, explains the reference guide.

Chapter 2, Features, explains the features of the MX 900 Series terminals.

Chapter 3, File Authentication, discusses usage of the file signing utility, and generating and authenticating the files on the MX 900 Series terminals.

Chapter 4, System Mode, provides information about the usage of System Mode, local and remote operations, and terminal status verification.

Chapter 5, VRK Ready Device, explains how to check your MX 900 Series terminal for a valid RSA Key Pair.

Chapter 6, Performing Downloads, provides information about requirements, download procedures, and the PCLANCNV utility.

Chapter 7, PINpad Security Best Practices, details methods for minimizing fraud through education, routine inspection, vendor management, and prompt action.

Chapter 8, Terminal Specifications, provides information on power, environment, and dimensions of the hardware.

Acronyms

The following table describes the common acronyms used:

Convention	Meaning
AC	Alternating Current
ADA	Americans with Disabilities Act
ATM	Automated Teller Machine
BT	Bluetooth
CDMA	Code Division Multiple Access
CR	Check Reader
CRC	Cyclic Redundancy Check
CTLS	Contactless
DDL	Direct Download Utility
DIN	Document Identification Number
DMM	Download Management Module
DUKPT	Derived Unique Key Per Transaction
DTK	Developer's Toolkit
DVD	Digital Versatile Disc
ECR	Electronic Cash Register
EDR	Enhanced Data Rate
EE	Electrical Engineering
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMV	Europay MasterCard and VISA
FA	File Authentication
GID	Group Identification
GPIO	General Purpose Input/Output
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HW	Hardware
ICC	Integrated Circuit Card
IO	Input Output
ISM	Industrial, Scientific, and Medical
LCD	Liquid Crystal Display

Convention	Meaning
LED	Light Emitting Diode
MRA	Merchandise Return Authorization
MSAM	Micromodule-Size Security Access Module
MSR	Magnetic Stripe Reader
NAND	Not And (electronic logic gate)
PCB	Printed Circuit Board
PCI	Payment Card Industry
PED	PIN Entry Devices
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLAN	PinStripe Local Area Network
PLL	Phase Lock Loop
PSP	Payment Service Provider
PTID	Permanent Terminal Identification Number
RAM	Random Access Memory
RGB	Red, Green, and Blue
RJ45	Registered Jack 45
RSSI	Receive Signal Strength Indicator
RTC	Real Time Clock
SAM	Security Access Module
SC	Smart Card
SDK	Software Development Kit
SoG	System-on-Chip
SRAM	Static Random-Access Memory
TIFF	Tagged Image File Format
USB	Universal Serial Bus
UPF	BT SIG Unplug Fest (UPF) Interoperability Testing
VPN	Verifone Part Number
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity

2 FEATURES

This chapter contains information on the features of the MX 900 Series terminals, the MX 915, and the MX 925.

For installation procedures, see the MX 900 Series Installation Guide.

Overview

The two new MX 900 Series models are the MX 915 and MX 925. The common features between both models are: core hardware design based on the proven MX 900 Series architecture (includes system processor, power management unit, and backup power supervisor), compatibility with existing Berg cable, single MSR head, smart card connector, micro SD card slot, contactless antenna and circuitry, audio codec with stereo speaker and headphone output, three SAM card slots, support for 802.11n and Bluetooth wireless, IBM® Tailgate protocol support, and a low power or hibernation mode.

The MX 915 features a color 4.3" display with a capacitive touch panel and keypad for user input.

The defining feature of the MX 925 is a color 7" screen with hardware accelerated DVD quality video. It uses a capacitive touch panel with signature capture capabilities and keypad for user input.

Modular Design

The MX 900 Series terminals offer outstanding flexibility due to their modular design. Both units feature a card edge connector on the bottom of the unit facing the rear. I/O modules will connect to this edge connector. All external connections to the units connect through this I/O module. This includes power, USB, Ethernet, serial, and audio. Two of the I/O modules also have support for the existing Berg connector and cabling.

Display Features

MX 915

The MX 915 has a 4.3-inch display with a resolution of 480 horizontal by 272 vertical pixels.

MX 925

The MX 925 is a 7-inch display with a resolution of 800 horizontal by 480 vertical pixels.

Both displays are capable of 24 bit RGB color.

Features and Benefits

The following are features and benefits of the MX 900 Series terminals:

Features	Benefit
Sophisticated Security	All systems are PCI 4.x compliant. Includes 3DES encryption, Master Key/Session Key and Derived Unique Key Per Transaction (DUKPT) key management; also incorporates VeriShield file authentication and tampering safeguards.
Optional upgradable modules	Lets customers economically address today's needs, while adding capabilities as desired; protects investment.
USB (Universal Serial Bus) Device Connector	Allows LAN connections for high-speed data transfer, back-end clearing, and settlement. Supports connections to electronic cash registers (ECRs) and PCs using USB or Ethernet. USB Host functionality supports other USB devices such as USB memory drives.
Serial Ports	Provides connectivity for the Berg connector.
Security Board	Both units have a microSD slot capable of supporting microSD cards up to 32GB. Both units are capable of supporting up to three SAM cards.
32-bit microprocessor	Streamlines processing, even on complex transactions.

Features	Benefit
Flash and RAM	Ample memory to support multiple payment and value-added applications simultaneously.
High Resolution Display	Supports sophisticated applications with full-motion video. Both units are capable of displaying video with a minimum frame rate of 20 fps.
Smart card reader	Accepts chip cards conforming to the latest global standards.
Triple-track magnetic card reader	Logically oriented for improved read rates; handles magnetic stripe cards, including drivers' licenses.
Contactless Reader	The contactless antenna is designed to accept a card when presented in either a vertical or horizontal orientation.
Touch Screen	Both terminals have a capacitive touch panel.
Audio	MX 915 — One internal single speaker. Includes output jacks for external speakers. MX 925 — Two internal speakers. Includes output jacks for external speakers.
ADA Compatibility	When a user plugs headphones in to the headphone jack on the left side near the Stylus Holster, the terminal has the ability to assist both visually and hearing impaired individuals per the ADA standards.

Factory Options

Factory options are available for the MX 900 Series terminals, depending on your needs.

Speakers

Both terminals have built-in speakers for tones and prompts. A line-out port is available to drive externally powered speakers.

Optional Modules

The MX 900 Series offers upgradable modules that can be installed in the factory or upgraded after distribution to the field. All modules can be installed easily and efficiently. Complete installation instructions are found in the Installing Optional Components section.

Contactless Reader Module

The MX 915 has a built-in contactless antenna. The MX 925 requires an external/removable contactless module. The contactless feature is enabled in System Mode. A smart card is read when it is placed above the MX 915 display or the MX 925 contactless module reducing wear and tear on card readers and cards. Contactless readers can be used to support any number of payment and value-added applications. See Installing Optional Components in the *MX 900 Series Installation Guide* for more information.

Applications

Standard payment applications are available from Verifone to interface with most ECRs. Applications for the terminals are written using a C-based programming language. These programs can be downloaded directly from an ECR or a development PC using the MX 900 Series terminal System Mode.

Terminal System Mode can also be used for diagnostics, changing the password, and debit Key injection. See the System Mode chapter for more information.

Total Cost of Ownership

The MX 900 Series terminals have been designed to be flexible and *future proof*, delivering a low total cost of ownership.

The modular terminals can be configured at the factory or in the field by a trained technician. The flexibility and versatility of the terminals allow use of the terminals with different capabilities in different stores or locations. The terminals can be purchased with the modules that meet today's requirements, and other capabilities can be added as and when needed.

3 FILE AUTHENTICATION

This chapter discusses the following topics:

- Introduces File Authentication (FA).
- Explains how the file authentication process may affect the tasks normally performed by application programmers, terminal deployers, site administrators, or by entities authorized to download files to an MX 900 Series terminal.
- Describes how to use the file signing utility to generate the signature files required to perform downloads and authenticate files on the MX 900 Series of terminals.
- Presents Steps to Sign Files.

In the Performing Downloads chapter, the topic of file authentication is also discussed in the context of specific file download procedures.

Overview

The MX 900 Series terminal has a security architecture, called VeriShield, which has both physical and logical components. The logical security component of the VeriShield architecture, which is part of the terminal's 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 application files to that terminal. It proves and verifies the following information:

- File's origin
- Sender's identity
- Integrity of the file's information.

The Verifone Certificate Authority

To manage the tools and processes related to FA, Verifone has established a centralized Verifone Certificate Authority, or Verifone CA. This agency is responsible for managing keys and certificates. The Verifone CA uses an integrated set of software tools to generate and distribute digital certificates and private cryptographic keys to customers who purchase the MX 900 Series terminal.

Required Files

The following specially formatted files support the FA process:

- A digital certificate (*.crt file) is a digital, public document used to verify the signature of a file.
- A digital signature (*.p7s file) is a piece of information based on both the file and the signer's private cryptographic key. The file sender digitally signs the file using a private key. The file receiver uses a digital certificate to verify the sender's digital signature.
- Signer private keys are securely conveyed to clients on smart cards. On MX 900, private keys are not kept in files. (The .key file in the File Signing Tool is for legacy platforms supporting a default signer certificate.) The secret passwords required by clients to generate signature files, using signer private keys, are sent as PINs over a separate channel such as registered mail or encrypted e-mail.

Digital certificates and signature files need not be secured to safeguard the overall security of VeriShield.

The special file types that support the file authentication process are recognized by their filename extensions:

File Type	Extension
Signature	*.p7s
Signer private key	*.key
Digital Certificate	*.crt

All digital certificates are generated and managed by the Verifone CA, and are distributed on request to MX 900 Series terminal clients — either internally within Verifone or externally to sponsors.

Note: All certificates that are issued by the Verifone CA for the MX 900 Series terminal platform, and for any Verifone platform with the VeriShield security architecture, are hierarchically related. That is, a lower-level certificate can only be authenticated under the authority of a higher-level certificate.

The security of the highest-level certificate called the platform root certificate is strictly controlled by Verifone.

The required cryptographically related private keys that support the file authentication process are also generated and distributed by the Verifone CA.

Certificates Contain Keys that Authenticate Signature Files

- **Sponsor certificate:** Certifies a client's sponsorship of the terminal. It does not, however, convey the right to sign and authenticate files. To add flexibility to the business relationships that are logically secured under the file authentication process, a second type of certificate is usually required to sign files.

  A sponsor certificate is authenticated under a higher-level system certificate called the application partition certificate.

  Note: Only one sponsor certificate is permitted per terminal.

- **Signer certificate:** Certifies the right to sign and authenticate files for terminals belonging to the sponsor.

  A signer certificate is authenticated under the authority of a higher-level client certificate (the sponsor certificate).

The required sponsor and signer certificates must either have been previously downloaded and authenticated on the terminal, or they must be downloaded together with the new signature files and target files for them to authenticate correctly.

Signer Private Keys are Issued to Secure the File Signing Process

Signer private keys are loaded onto a smart card. This smart card is securely delivered to the business entity that the terminal sponsor has authorized to sign, download, and authenticate applications to run on the sponsor's terminal.

The Verifone CA can also issue additional sets of sponsor and signer certificates, and signer private keys to support multiple sponsors and multiple signers for a specific platform.

To establish the logical security of applications to download to an MX 900 Series terminal, the designated signer uses the signer private key issued by the Verifone CA as a required input to the file signing tool. Every signature file contains information about the signer private key used to sign it.

When a signature file generated using a signer private key downloads to the MX 900 Series terminal, a successful authentication depends on whether the signer private key used to sign the target file matches the signer certificate stored in the terminal's certificate tree.

How File Authentication Works

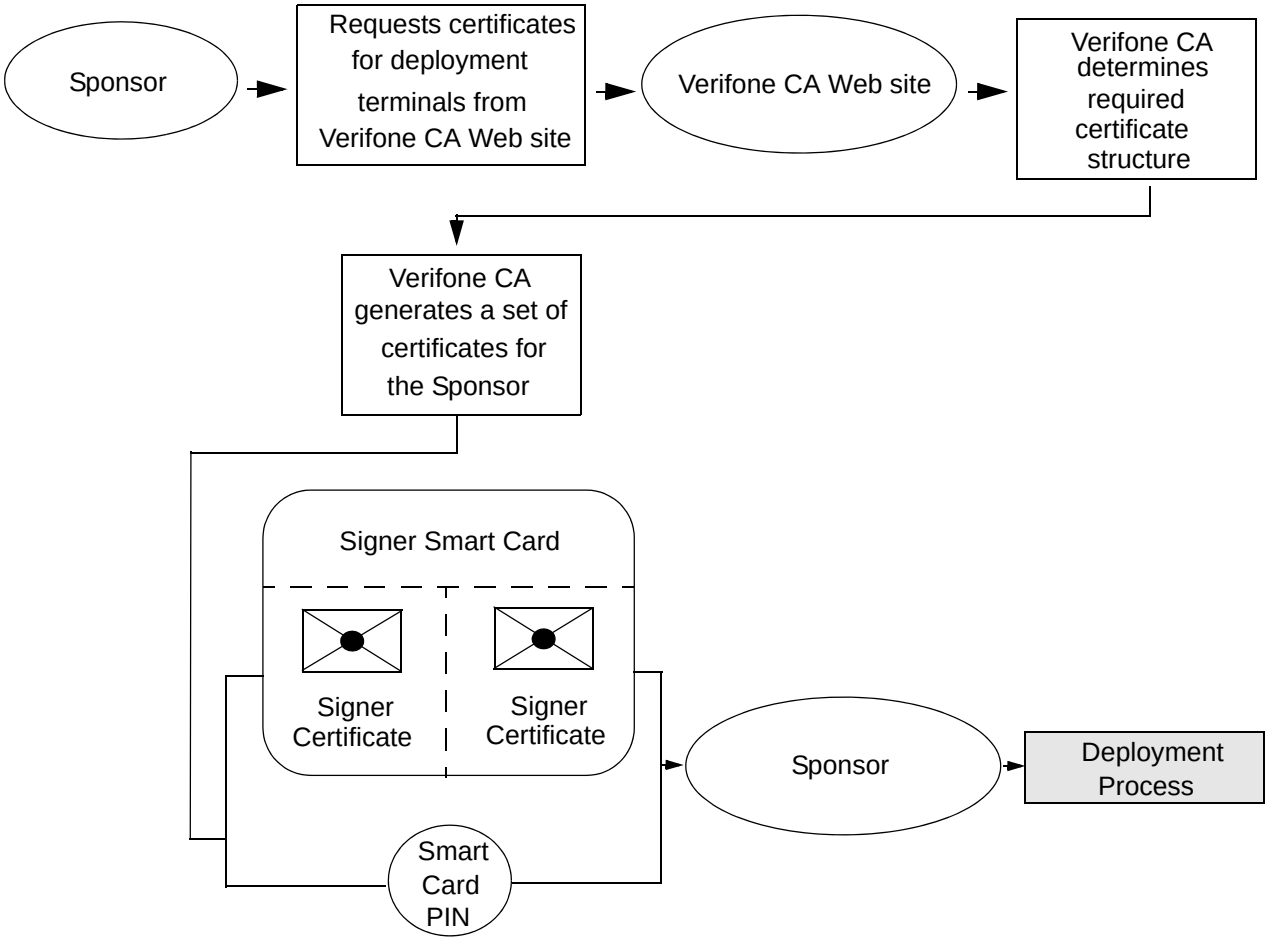
File Authentication consists of three basic processes:

1. **Certificate Request:** An optimal certificate structure is determined, and the necessary certificates and keys created.
2. **Development:** The file signing software tool creates a signature file for each application file to authenticate.
3. **Deployment:** After the certificate and development processes are completed, they are used in combination to prepare a terminal for deployment.

Certificate Request

1. A sponsor connects to the Verifone CA Web site and requests certificates for deployment terminals.
2. Based on information provided by the sponsor through the Verifone CA Web site, the Verifone CA determines the required certificate structure.
3. Verifone CA generates the following items for the sponsor:
   a. Smart card containing a set of certificates and keys.
   b. Smart card PIN.
4. Verifone CA sends the smart card and smart card PIN to the sponsor.
5. The sponsor uses the smart card and smart card PIN as inputs for the deployment process.

The certificate request is illustrated in the figure below.



Development Process

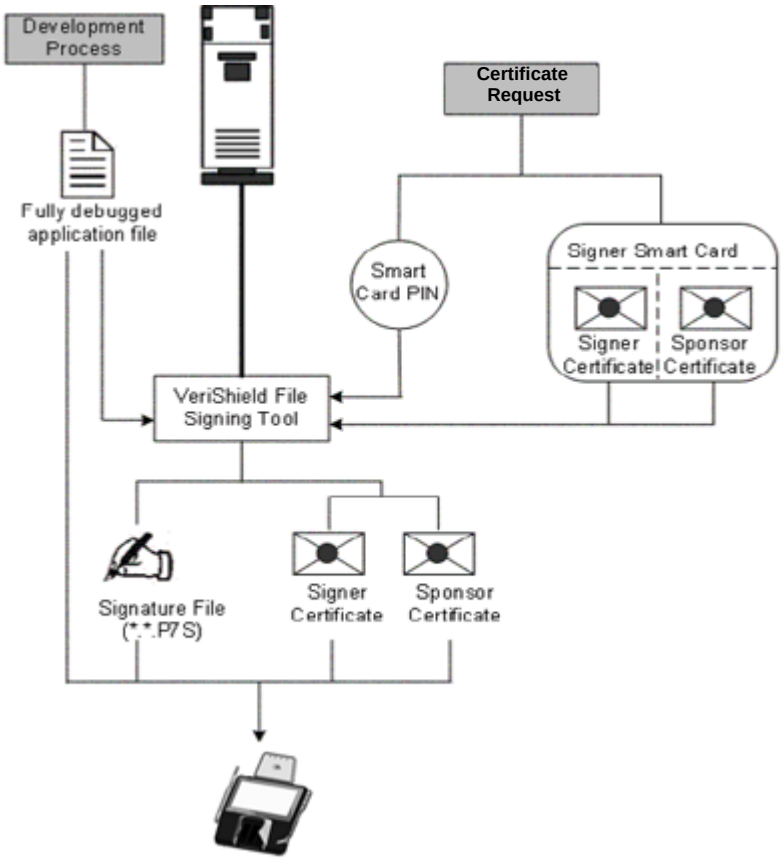
The Development Process is the same as the Deployment Process except different cards are ordered and used. Proceed to the Deployment section.

Deployment Process

1. The sponsor provides the application file (from the development process) and the smart card and smart card PIN (from the certificate request process) as inputs to VeriShield.
2. VeriShield unlocks the smart card with the provided PIN, sends the file to be signed to the smart cart that will compute the signature with the resident private key. VeriShield extracts the signature, signer certificate, and sponsor certificate from the smart card.
3. VeriShield uses the extracted data, along with the application file, to create a signature file (*.p7s).

4. VeriShield creates files suitable for downloading from the smart card data.
5. The signature file, the application file, and the extracted signer and sponsor certificates are downloaded into a deployment terminal, where the following actions occur:
   a. When an attempt is made to install an application executable or data file, a matching signature and certificate must be present.
   b. The operating system compares the application file's signature against the values stored in the application file's calculated signature.
6. Each successfully authenticated application file is installed on the terminal (otherwise, the application file is deleted on failed authentication and an error message is displayed.)

The development and/or deployment process is illustrated in the flowchart below.



Planning for File Authentication

File Authentication is an integral part of every MX 900 Series terminals. To safeguard the terminal's logical security, FA requires that any downloaded application file must be successfully authenticated before the operating system installs on the terminal.

Download and Installation

The MX 900 Series Secure Installer plays a critical role on system and application startup as well as authenticating and installing all components; application, system and OS.

The MX 900 Series terminal supports the following download mechanisms:

Download Mechanism	Description
Serial Direct	Supported over all serial ports (COM1/ COM2/COM3 and USB Serial Gadget
IBM ECR	Supported over all serial ports and Tailgate (COM3 RS-485)
USB/SD	Supported over USB memory devices and microSD memory
Netloader	Verifone proprietary TCP-IP file transfer
FTP/SFTP	File Transfer Protocol / Secure File Transfer Protocol (Client only)

All content, regardless of download mechanism, is downloaded to /mnt/flash/ install/dl. Content is not usable until it is actually installed by the Secure Installer. The Secure Installer authenticates all downloaded content and then installs it. At this point the content becomes usable. For example, the Secure Installer installs authenticated downloaded application content to the application user's home directory.

How Signature Files Authenticate Target Files

Signature files are downloaded together with their target application files in the same data transfer operation. When an attempt is made to install an application executable or data file, a matching signature and certificate must be present. The operating system compares the application file's signature against the values stored in the application file's calculated signature.

Determine Successful Authentication

All downloaded files must have an associated signature as part of the download otherwise the installation will fail. To ensure a target file successfully authenticated after a download. Confirm all downloaded files installed. If an application file is not successfully authenticated, the operating system does not allow it to install and run, either following the initial download or on subsequent terminal restarts.

Digital Certificates and the File Authentication Process

File Authentication always processes certificates before it processes signature files. Digital certificates (`*.crt` files) generated by the Verifone CA have two important functions in the FA process:

- To define the rules for file location and use (for example, replaceable *.crt files, parent `*.crt` files, whether child `*.crt` files can exist, and so on).
- To convey the public cryptographic keys generated for terminal sponsors and signers that are the required inputs to the file signing tool to verify file signatures.

Hierarchical Relationships Between Certificates

All digital certificates are hierarchically related to one another. Under the rules of the certificate hierarchy managed by the Verifone CA, a lower-level certificate must always be authenticated under the authority of a higher-level certificate. This rule ensures the overall security of VeriShield.

To manage hierarchical relationships between certificates, certificate data is stored in terminal memory in a special structure called a certificate tree. New certificates are authenticated based on data stored in the current certificate tree.

This means that a new certificate can only be authenticated under a higher-level certificate already resident in the terminal's certificate tree. This requirement can be met in two ways:

- The higher-level certificate may have already been downloaded to the terminal in a previous or separate operation.
- The higher-level certificate can be downloaded together with the new certificate as part of the same data transfer operation.

A higher-level production certificates is downloaded into each MX 900 Series terminal at manufacture. When you take a new MX 900 Series terminal out of its shipping packaging, certificate data is already stored in the terminal's certificate tree.

Typically, a sponsor requests an additional set of digital certificates from the Verifone CA to establish sponsor and signer privileges. This additional set of certificates is then downloaded to the MX 900 Series terminal when the terminal is being prepared for deployment. When this procedure is complete, the MX 900 Series terminal is called a deployment terminal.

Add New Certificates

When you add a new certificate file to an MX 900 Series terminal, the system detects it by filename extension (`*.crt`). The terminal then attempts to authenticate the certificate under the authority of the resident higher-level certificate stored in the terminal's certificate tree or one being downloaded with the new certificate.

In a batch download containing multiple certificates, each lower-level certificate must be authenticated under an already-authenticated, higher-level certificate. Whether or not the data that the new certificate contains is added to the terminal's certificate tree depends on its successful authentication. The following points explain how certificates are processed:

- If a new certificate is successfully authenticated, the information it contains is automatically stored in the terminal's certificate tree in Flash. The corresponding certificate file (`*.crt`) is not retained.
- If the relationship between the new certificate and an existing higher-level certificate cannot be verified, the authentication procedure for the new certificate fails. In this case, the certificate information is not added to the certificate tree and the failed certificate file (usually ~400 bytes) is not retained.

Development Terminals

A development terminal is an MX 900 Series terminal that maintains a set of certificates in its certificate tree. This set of certificates includes a special client certificate called a development signer certificate.

In the development terminal, applications must still be signed and authenticated before they can run on the terminal. A development terminal provides additional application debug capabilities.

Deployment Terminals

While the application development process is being completed and while the new application is being tested on a development terminal, a sponsor can order specific sponsor and signer certificates from the Verifone CA that can be used to logically secure sponsor and signer privileges when the MX 900 Series terminal is prepared for deployment.

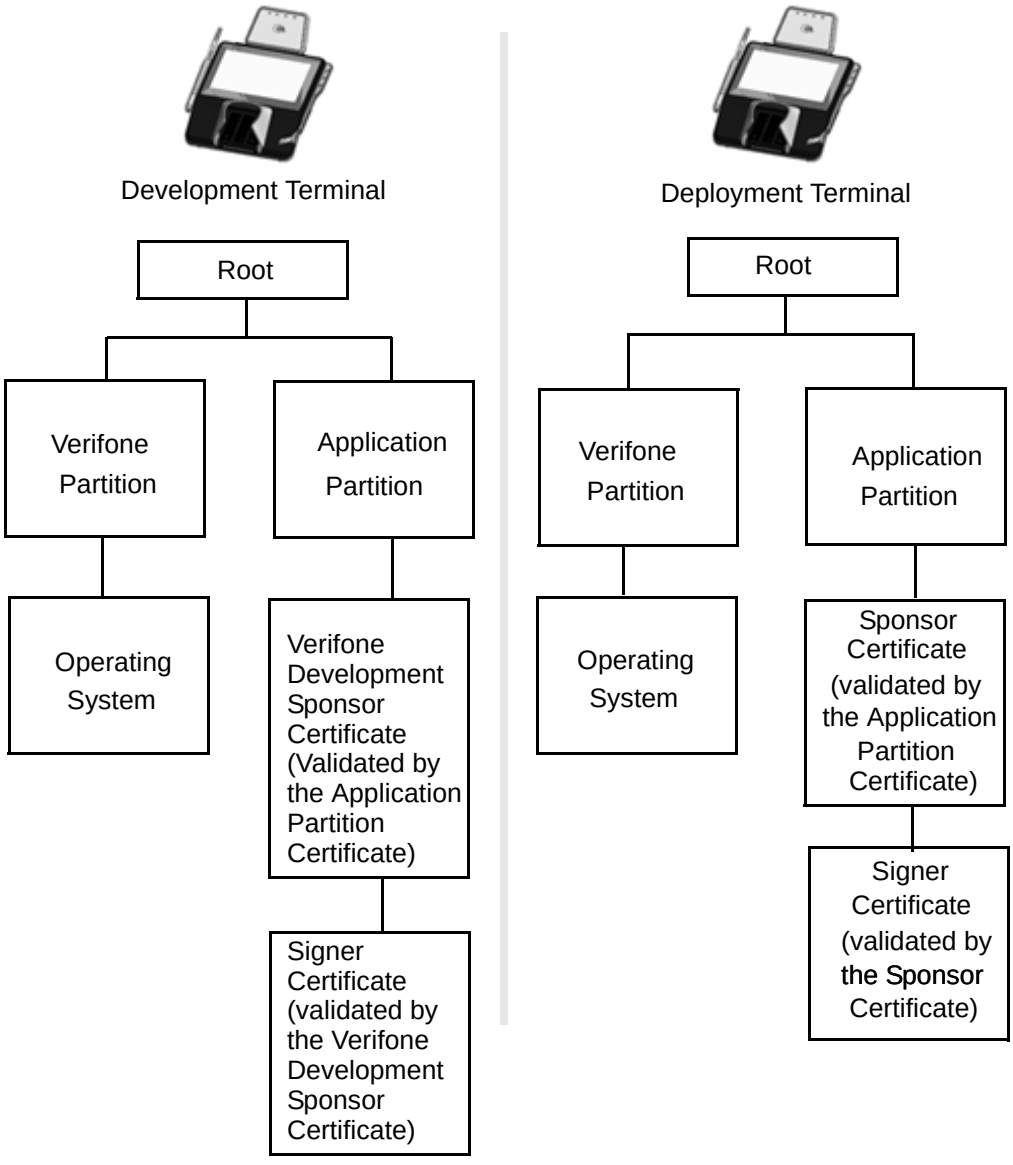
Customer–specific sponsor and signer certificates are usually downloaded to an MX 900 Series terminal as part of the standard application download procedure performed by a deployment service. In this operation, the new sponsor and signer

certificates replace the development sponsor certificate that is part of the factory set of certificates in the figure below.

When the sponsor and signer certificates are downloaded and successfully authenticated, the terminal is ready for deployment.

Ultimately, the sponsor will decide how to implement the logical security provided by File Authentication on a field-deployed terminal. Additional certificates can be obtained from the Verifone CA at any time to implement new sponsor and signer relationships in deployment terminals.

The Certificate Trees in Development and Deployment Terminals is illustrated in the flowchart below.



Permanency of the Certificate Tree

The data contained in a digital certificate is stored in the terminal's certificate tree when the certificate is authenticated. The system automatically removes the .crt file once processed.

Required Inputs to the File Signing Process

- Files to be signed.
- VeriShield signer card. It contains the sponsor and signer certificates, and the signer private key.
- Smart Card PIN to access the private key on the card.

File Signing and Packaging Tools

VeriShield File Signing Tool (FST)

Unlike the MX 800 Series terminals, MX 900 Series terminals are shipped from manufacturer without a development certificate — a development certificate is not available for download.

For development, like for deployment, customers must obtain VeriShield signer cards and use the VeriShield File Signing Tool to sign all executable and other file to be logically protected. MX 800 Series development signing tool (like FILESIGN.EXE) are not supported on MX 900 terminals.

Development and production signer cards must be generated under distinct sponsor certificates, so that development cards could be distributed, without any security concern to personnel non-authorized to sign production software.

Steps to Sign Files

1. Launch The VeriShield File Signing tool. In the Windows Start menu, it is typically located under All Programs > Verifone > VeriShield > File Signing Tool.
2. Log in. "Dual logon" is required to sign files.
3. Click "Sign File" and follow the wizard.
4. Click "Next" at the Welcome screen.
5. Select "Sign Files with new settings' and click Next at the settings selection screen.
6. Click "Add" and browse to the file(s) to be signed (DO NOT CHECK the "flash" box. It is only for Verix terminals ONLY and may cause authentication failure on MX 900 Series terminal).
7. Click "Next" once all files to be signed have been added.

8. Select “Secured” and click “Next” at the security level screen (default is not supported on the MX 900 Series terminal).
9. Select the name and location to export the signer certificate file (the sponsor certificate is always exported as SponsorCert.crt in the same location).
10. Click “Sign File” at the “Summary of Settings” screen.
11. Enter first officer PIN.
12. Enter next officer PIN.
13. Click “Close” at the “results” screen.

If the signing was successful, there should be a new signature file (.p7s) for each of the files that have been signed. Two certificate files (.crt) should have been created in the specified location.

Packaging Tool

Application files are downloaded as packages. To download a package or packages to the device, the following must be done.

1. Generate one or more install packages.
2. Sign the individual install packages with FST.
3. Combine one or more install packages and package signatures into a bundle.
4. The bundle may also contain signer certificates and a remove file (to remove previous version of the application).
5. Sign the bundle.
6. Combine one or more bundles and bundle signatures into a single download file.

A file named “control” in the package CONTROL directory contains information relating to the package. A packaging tool with built-in help information is available to create packages.

4 System Mode

This chapter describes *System Mode Operations*. System Mode is used exclusively by those responsible for configuring, deploying, and managing MX 900 Series terminal installations in the field.

When to Use System Mode

Use System Mode functions to perform different subsets of related tasks:

- **Application programmers:** Configure a development terminal, download versions of the MX 900 Series application program under development, test and debug the application until validated and ready to download to other terminals.
- **Deployers of MX 900 Series terminals to end-user sites:** Perform specific tasks required to deploy a new MX 900 Series terminal in the field, such as terminal configuration, application software download, and testing of the terminal prior to deployment.
- **Terminal administrators or site managers:** Change passwords, perform routine tests and terminal maintenance, and configure terminals for remote diagnostics and downloads.

Local and Remote Operations

The System Mode operations available on an MX 900 Series terminal can be divided into the following two categories or types:

- **Local operations:** Addresses a standalone terminal and does not require communication or data transfers between the terminal and another terminal or computer. Perform local System Mode operations to configure, test, and display information about the terminal.
- **Remote operations:** Requires communication between the terminal and a host computer (or another terminal) over a connection. Performs remote System Mode operations to download application software to the terminal, upload software from one terminal to another, and perform diagnostics.

For information on performing remote operations, such as downloads, see the “Performing Downloads” chapter.

Verifying Terminal Status

The MX 900 Series terminal you are working with may or may not have an application program running on it. After you have set up the terminal and the terminal is turned on, use the following guidelines to verify terminal status regarding software and current operating mode.

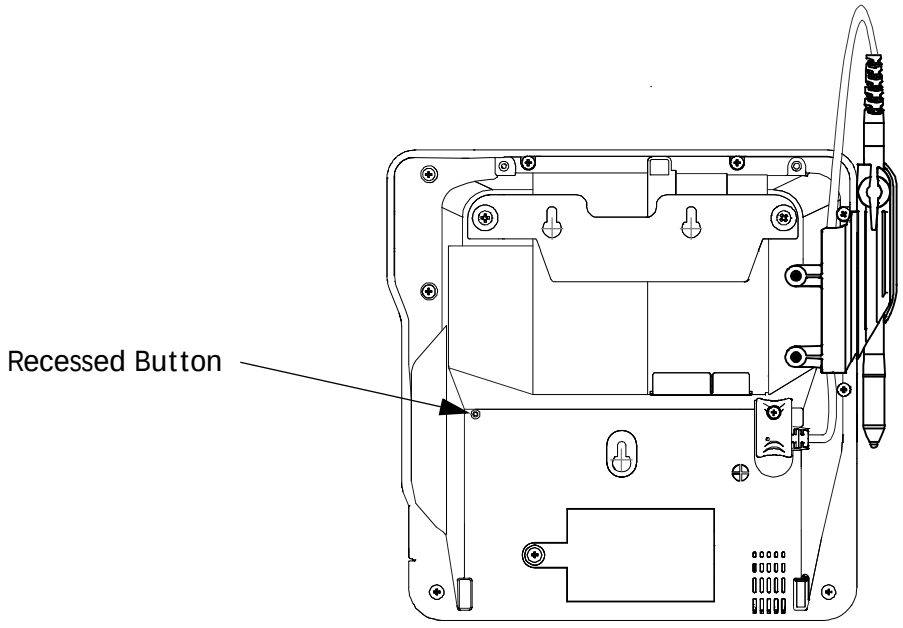
- If there is no application program loaded into terminal flash, the terminal enters the System Mode screen.
- If an application program is loaded into terminal flash, an application-specific prompt appears. The application runs and the terminal is in normal mode.

Entering System Mode

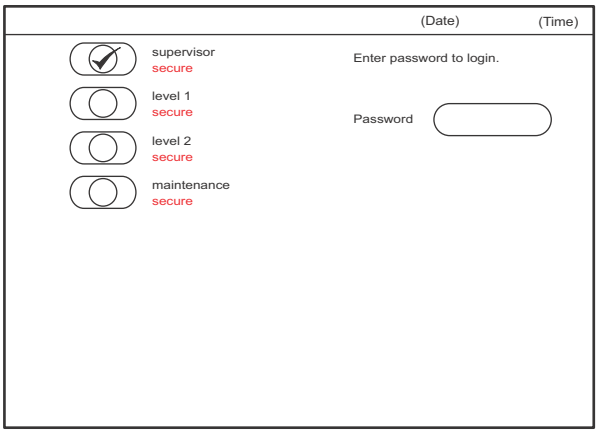
With an application loaded, use the following procedure to enter System Mode.

Note: Before entering System Mode and selecting the function(s) to perform, verify that the MX 900 Series terminal has been installed as described in the *MX 900 Series Installation Guide.* Make sure that the terminal is connected to a power source and is turned on.

1. With the application running, push a paper clip into the small recessed button on the bottom near the serial number. The three blue LEDs light. Release the button. Alternatively, pressing the '1', '5', '9' keys at the same time will cause the terminal to go into System Mode.



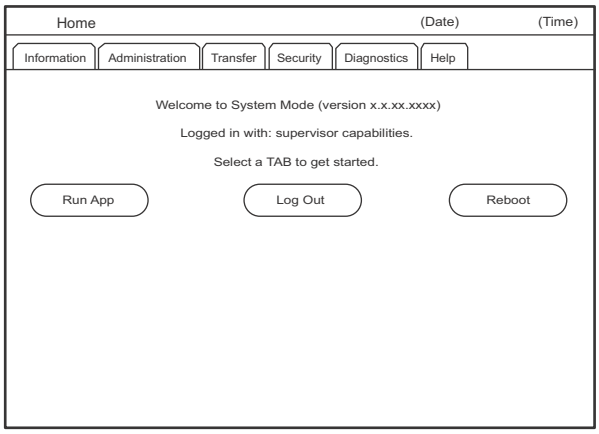
2. Select one of the four possible System Mode logins:



   - **Supervisor**: Full capability
   - **Level1**: User defined capability
   - **Level2**: User defined capability
   - **Maintenance**: Intended for Verifone repair, allows minimal access

3. Once the login has been selected, enter the password. If the password is pre-expired or is pending change the user must enter the current password and then a new password (pre-defined in the case of a pending password change). The new password must be entered twice for validation. The default System Mode password is:166831 or 166832.

4. If the password is entered correctly, the System Mode idle screen displays. If the password is not entered correctly, the error “A password was entered incorrectly” displays and the login screen displays again.

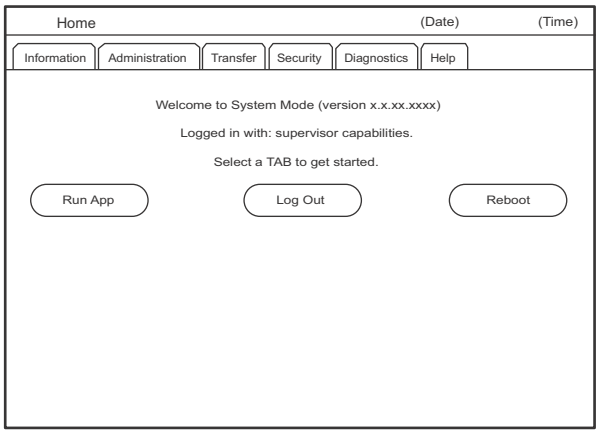


Exiting System Mode

After successful completion, some operations automatically exit System Mode and restart the terminal. Other operations require that you manually exit System Mode and restart the terminal by tapping **Home**.

System Mode Menus

Access the submenus by tapping the tab name. The System Mode screen and submenus are shown below. In recent years, UI navigation breadcrumbs have become popular because they allow the user to see their location within a program and they allow a quick return back to any point within the breadcrumb trail. The “>” greater than symbol is used to separate points (crumbs) along the path. Touching any of the words/abbreviations along the path will instantly move the user to that point.



System Mode Procedures

1. At the idle System Mode screen, select an operation by tapping the corresponding on-screen tab.
2. Complete the operation.
3. Return to the main MX 900 Series System Mode screen.

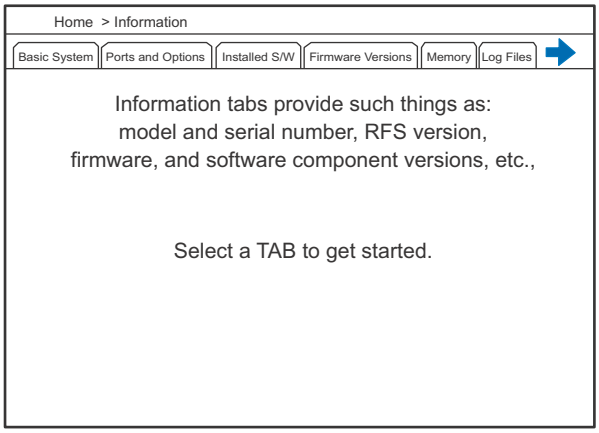
Note: When on a System Mode menu screen, tap **Home** to return to the System Mode idle screen.

Navigation

- Blue arrows are used to scroll the tabs (left and right).
- Home screen has buttons to support:
  - Run App: Start application
  - Log Out: Log out of System Mode
  - Reboot: Restart the application

Information Submenu

Tap the **INFORMATION** tab on the System Mode screen to view the following information. Tap the right and left arrows to see all of the configuration options. (Tap the tabs that appear for more system information.)

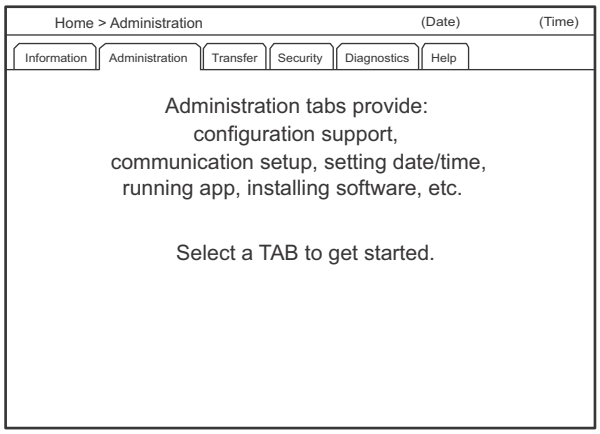


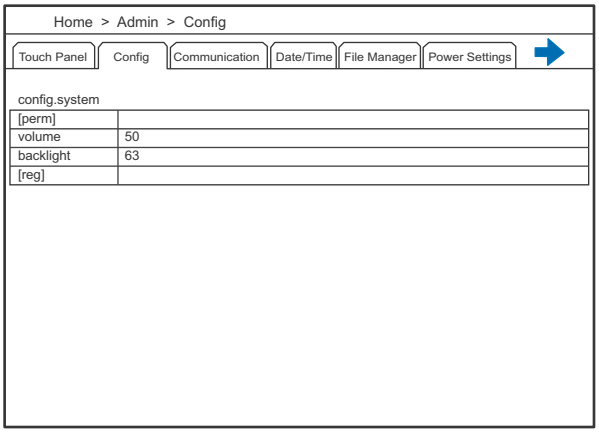
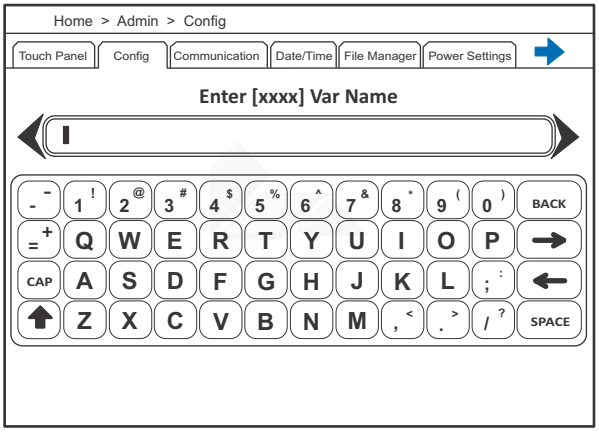
Item	Function
BASIC SYSTEM	Displays basic information such as model, serial number, unit id, RFS version, etc. Critical Values: - **Build**: Base build release date - **Vault Version**: Security vault version
PORTS & OPTIONS	Displays I/O module configuration, Multiport cable configuration (if connected), and COM port status.
INSTALLED SOFTWARE	Displays a list of installed and activated bundles/packages. Bundles appear in brackets "[]". Touching the two right hand columns will expand a bundle to show the packages it contains.
FIRMWARE VERSIONS	Displays a list of all co-processors and their F/W version.
MEMORY	Displays total SDRAM and NAND flash memory. Available NAND flash memory will also be displayed.

Item	Function
LOG FILES	The Log File is maintained by the secure installer. **TAMPER** — Displays tamper information. **INSTALL** — Displays a list of installed and activated components/ packages.
COUNTERS	Display operating system and application diagnostic counters.

Administration Submenu

Tap the **ADMINISTRATION** tab on the System Mode screen to configure the MX 900 Series terminal. Tap the right arrow to see all of the configuration options.

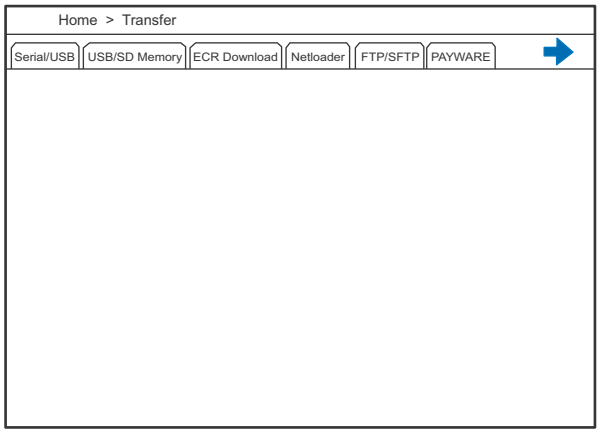


Item	Function
TOUCH PANEL	Support touch panel compensation.
CONFIGURATION	The unit will display a list of available configuration files. Select the desired file and its contents will be displayed. Sections are displayed enclosed in brackets "[]". Touch a section to add a new variable under it. Touch a variable to delete it. Touch a value to edit the value.  In the editor below, press the 'X' key on the hard keypad to abort changes and press the 'O' (Enter) key to accept changes. 
COMMUNICATION	Allows configuration of all ports including: ECR, USB, Ethernet, Bluetooth, and WiFi.

Item	Function
DATE/TIME	Enter the current date: Tap to date field to display a window where you can specify the day, month, and year. Use the up and down arrows to make the selection and then tap the **OK** button. Enter the current time in HHMMSS format: **HH** — Two-digit hour (valid values 01–23) **MM** — Two-digit minute (valid values 00–59) **SS** — Two-digit second (valid values 00–59) Set 24 hour reboot time: To reboot the device on a preset time, select **ENABLE** and then specify the reboot time in HHMMSS format. Tap the **APPLY** button to accept new Time/Date settings.
FILE MANAGER	Basic file management allows files to be copied to/from USB and SD. It also supports playing media files and viewing images.
POWER SETTINGS	Configure basic power settings, display sleep time…
DISPLAY	To adjust the MX 900 Series terminal display backlight by tapping the ^ UP ^ or v DOWN v buttons.
AUDIO	Use to configure the sound settings of the MX 900 Series terminal. To adjust the audio volume: - Press ^ UP ^ to increase the volume. - Press v DOWN v to decrease the volume.
UNINSTALL BUNDLES	Select a bundle file to uninstall. A bundle file consists of install packages and package signatures.

Transfer Submenu

Tap the **TRANSFER** tab on the System Mode screen to download files to the MX 900 Series terminal via the following methods. For detailed information about downloads, see the “Performing Downloads” chapter.



Item	Function
SERIAL/USB	Perform a download via the USB/Serial port. Tap the **GO** button to perform the download. For Serial/USB download the port and baud rate (serial only) can be selected. AUTO baud allows the serial port to cycle through the available baud rates until communication is established.
USB/SD MEMORY	Perform a file transfer via the USB/SD memory device. Tap the **APPLY** button to perform the download.
ECR DOWNLOAD	Allows download via an IBM ECR over tailgate or feature C protocol.
NETLOADER	Perform a download from the PC client software by tapping Netloader. Netloader is Verifone's proprietary network based download protocol.
FTP/SFTP	Transfer files via FTP/SFTP.
PAYWARE	Allows configuration of the PAYWARE server.

Security Submenu

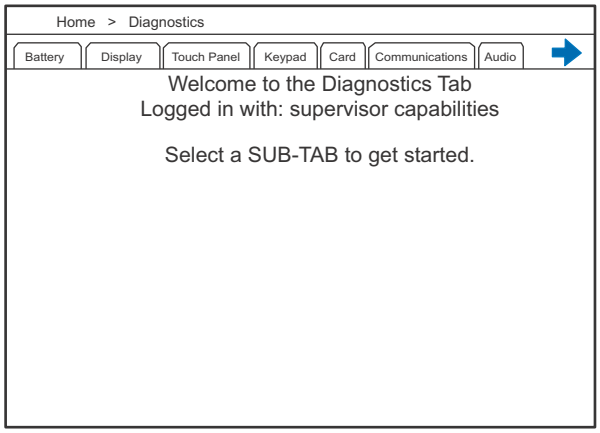
Tap the **SECURITY** tab on the System Mode screen to perform the following functions.

Item	Function
KEY LOADING	After presenting both keyload1 and keyload2 passwords, enable the key loading state that will allow data to pass from a serial port to the security module for bank/ADE and VRK keys.
KEY STATUS	View the key status for Master Session, DUKPT, User, VRK, VSS, Feature Licenses, and ADE.
PASSWORD MANAGER	Enter or change the passwords for the following: EXPIRE: • **EXPIRE USER PASSWORDS** • **EXPIRE KEYLOAD PASSWORDS** Keyload: • **KEY LOAD 1 — Set password #1 for entry into key loading mode.** • **KEY LOAD 2 — Set password #2 for entry into key loading mode.** Users: • **SUPERVISOR — Set password for opening the usr1 file.** • **LEVEL 1 — Set password #1 to act as a subset of User 1.** • **LEVEL 2 — Set password #1 to act as a subset of User 1.** • **MAINTENANCE — Set password for repair facility.** Press **ENTER** to set keys. Press **CLEAR** to cancel. **Note:** *With PCI 4 sensitive state, passwords must be a minimum of 7 digits. This rule is enforced for Key Load 1 and Key Load 2 password.* *All passwords in the system must be unique. This is enforced across all the user and key load passwords.*

Item	Function
SECURITY POLICY	View the secure and expired users in the Security Policy list.
TAMPER STATUS	View the security tamper status. This display will show the current and logged status. Touch a log entry for more detail.
VERISHIELD TREE	View the serial numbers and IDs in the VeriShield Certificate list. Tap any part of the screen to return to the Security submenu.
VSP STATUS	View the details of VSP/VCL functionality.

Diagnostics Submenu

Tap the **DIAGNOSTICS** tab on the System Mode screen. Diagnostic test results can be viewed and printed.



Item	Function
BATTERY	Determines the state of the internal battery. The terminal will fail this test if the voltage shows a value below 2.4 volts.
DISPLAY	Performs a diagnostic procedure on the terminal display. When the diagnostic image is shown on the terminal screen, note the image colors and consistency. The image should appear solid and show no motion. Press **ENTER** to go to the next diagnostic step.
TOUCH PANEL	Performs a diagnostic procedure on the touch screen. **TOUCH** — Tests the touch screen. X,Y coordinates are displayed. Press **ENTER** to stop the test. **SIGNATURE** — Touch the screen with your finger. The diagnostic will allow signing with either a stylus or a finger. If both a finger and a stylus are on the touch panel, the system will prioritize the stylus input.
KEYPAD	**KEYPAD TEST** — Press each key and the keypress will be displayed on the screen.

Item	Function
CARD	**MAGREADER** — Swipe a magnetic-stripe card in the mag card reader to determine if data can be read on all three tracks. Swipe a sample card once to determine if all three tracks can read the card. All tracks should display **GOOD** to pass the test. Swipe the card at least ten times. To pass the diagnostic test, the unit must show **GOOD** results in nine out of ten swipes. All three LEDs must light up in sequence. **SMARTCARD READER** — Determines the state of the smart card reader. If a card is present when the test is run, the first few bytes of the ATR is displayed. For manufacturing test purposes only. **CONTACTLESS READER** — Determines the state of the contactless module. Tapping a card will beep the beeper, light the LEDs (if present) and display the first few bytes of data.
COMMUNICATIONS	**SERIAL** — Performs a loopback test to determine the state of the Serial hardware. **USB** — Determines the state of the USB hardware. For manufacturing test purposes only. **ETHERNET** — Sends a ping to the network gateway over Ethernet. Also allows a unique IP address to be pinged. **WI-FI** — For future use. **BLUETOOTH** — For future use.
AUDIO	Checks the audio settings of the internal speakers. The terminal says “Home Sweet Home.”

Help Submenu

Tap the **HELP** tab to perform the following functions.

Item	Function
HELP	For future use.

5 PERFORMING DOWNLOADS

This chapter contains information and procedures for performing the various types of data transfers required to:

- Develop applications for the MX 900 Series terminal.
- Prepare MX 900 Series terminals for deployment.
- Maintain MX 900 Series terminal installations in the field.
- Transfer data to/from terminals.

Information pertaining to file authentication is only discussed in the context of procedures while performing file downloads. See the File Authentication for further discussion.

The MX 900 Series terminal can perform a download via the following connectivity options:

- Using FTP via an Ethernet network
- Using the IBM Download Protocol via an IBM ECR
- Using the ZonTalk Protocol via a PC
- Using the Network Download utility via an Ethernet Network
- Using the Transfer function from a local USB memory device / SD device.

Requirements

Downloads require moving the application and/or application data files from a remote computer to the terminal. In the MX 900 Series application development, application files are downloaded from a development PC directly to the terminal. In the field, application files must be transferred from the terminal's controlling device (ECR, LAN controller, and so on) to the terminal.

The MX 900 supports a module called the Secure Installer (SI). The secure installer is responsible for authentication and installation of applications and operating system components. The secure installer follows a well defined specification requiring bundles and packages. The detailed information on creation of download files for MX 900 is contained in the Programmer's Manual.

Also note that the MX 900 SDK includes a tool called the Package Manager to aid developers and deployment personal create and maintain bundles and packages.

Direct Downloads

The usual download utility program is Direct Download (DDL) utility. It is normally available with the Verifone *MX 900 Series Developer's Toolkit* (DTK), and can be obtained through Verifone. DDL is a subset program of the Verifone VeriTalk download application. It is designed specifically for a direct (RS-232/USB) download from a PC to a terminal (versus the VeriTalk modem-based functionality).

As the DDL utility sends files from the PC, the MX 900 Series display shows the progression of the download.

The file name is shown on Line 1 of the display with `nnn` showing the number of blocks downloaded. Line 2 indicates the percent complete of the download where each asterisk represents 10%.

DDL Command Line Syntax

The format of the DDL program is:

```
DDL [options] file1 [file2 …] [config-data]
```

Features	Benefit
`-b<baud>`	Specifies the baud rate, for example, • -b300 • -b1200 • -b2400 • -b4800 • -b9600 • -b19200 (default) • -b38400 • -b115200
`-p<port>`	Specifies the PC serial port: • 1 (COM1). The default is `-p1` (COM1). • 2 (COM2)
`-i<filename>`	Specifies the name of a binary file to include in the download, for example: `-IBINARY.DAT`.

Features	Benefit
`-c<delta time>`	Sets the date and time on the terminal to the host PC's date and time. Also, specifies a delta value to add or subtract from the hour, for example, `-c+1` specifies the PC's time plus one hour. Note: The maximum hour value that can be set is ±23 hours.
`-x<password>`	Sets the terminal's password.
`-F<filename>`	Processes the contents of the specified file as command line data.
`file1 [file2 …]`	Specifies one or more files to download. Files with the `.OUT` extension are treated as binary data; all others are assumed text files.
`[config-data]`	Specifies terminal or application environment variables. If the specified variable exists, it is replaced by the new value; otherwise, a new entry is created. For example, the string `*ZT=TERMID` sets the value of the terminal identifier variable to `"TERMID"`. Note: To remove an existing entry, use an empty string. For example, `*ZT=""` removes the `*ZT` variable.

DDL Command Line File

If you need to specify more variables than the DOS command line allows, you can use a simple configuration file (`-F` option) to extend the length of the command line. A command line file is an ASCII text file that allows you to supply as many variables as required.

DDL Example

Download the file `app.tgz` using the PC's COM port 2 (`app.tgz` is a binary file).

```
DDL -p2 -iapp.tgz
```

Each line in the command line file should consist of one variable:

```
-p2 app.tgz
```

The command line would be:

```
DDL -F<filename>.
```

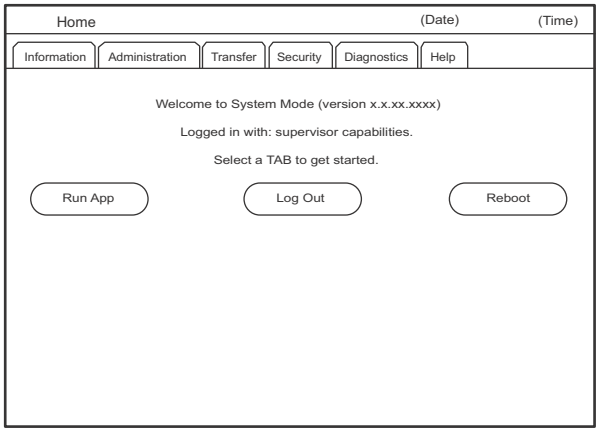
Download Procedures

Use the following procedures to perform downloads to an MX 900 Series terminal. For additional information about downloading files to the MX 900 Series terminals, see Transfer in the System Mode chapter.

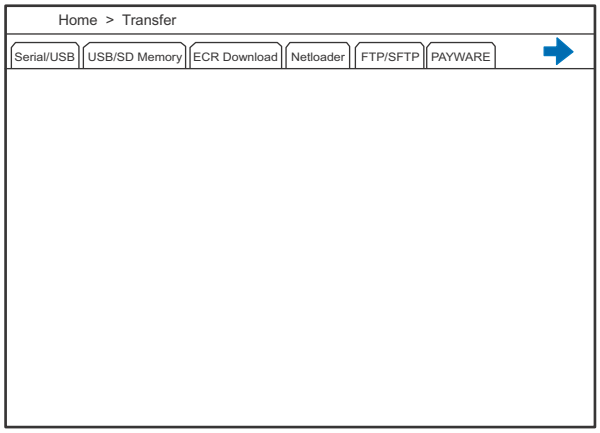
Downloading without an Onboard Application

Use the following procedure to perform a download from a host PC to an MX 900 Series terminal with no application installed. The terminal must be powered on to begin the procedure.

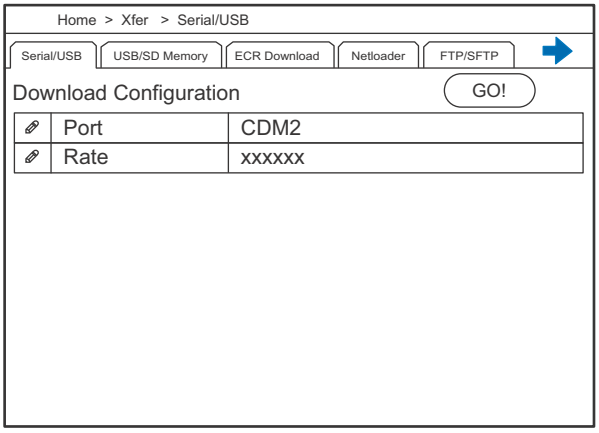
1. Make all cable connections.
2. Launch the DDL application on the host PC.
3. Enter System Mode using a secure user password.



4. Tap **TRANSFER** on the System Mode menu.



5. Tap the **SERIAL/USB** tab to perform direct download to the terminal.



6. Set the port and baud rate.
7. Tap the **GO** button to perform the download.

Asterisks (*) display on screen to indicate the state of the download. Each asterisk denotes approximately 10% completion. On download completion, the terminal returns to the main screen.

IBM ECR Downloads

The IBM ECR supports the download of a single file that is composed of one or more compressed or uncompressed files. The download file may contain operating system file(s), application code and data files, as well as configuration parameters.

The IBM ECR download file is generated off-line on a PC using the Verifone utility PCLANCNV, discussed in the PCLANCNV Utility section. After creating an IBM ECR download file, it must be copied to the ECR and downloaded via the ECR protocol driver.

The MX 900 Series terminal receives the IBM ECR download file and processes its contents appropriately. If the download file includes operating system components, the terminal will automatically reboot.

Network Download Utility

Network Download transfers files from a PC to the MX 900 Series terminal. A network download client, included with the SDK, must be installed onto a PC. Before the file transfer can begin, the network settings must be configured and then the transfer starts by tapping the “Netloader” under Transfer.

PCLANCNV Utility

On the MX 900 Series terminal, the PCLANCNV utility is used to create a download file that is compatible with the IBM ECR. On legacy retail platforms, the PCLANCNV utility was used to create compressed files. On the MX 900 Series, the standard Linux tar utility is used to create compressed files. The compression used by the PCLANCNV utility is no longer supported. A file that has been created using the Linux tar utility can become the input file to PCLANCNV for conversion to IBM ECR format.

PCLANCNV is a command line utility that runs under DOS. PCLANCNV has been run successfully under the Command Prompt on Windows® XP.

The MX 900 Series does not support the –p Pinstripe LAN or the –t compressed ZonTalk formats (these formats are used by legacy terminals). The –r IBM ECR format is supported and is in fact the only reason to use PCLANCNV.

It is strongly recommended that the Linux tar utility be used to combine/compress files prior to running PCLANCNV. The IBM ECR does not understand or support the complex directory structure and file permissions of the MX 900 Series. Using a tar file as input to PCLANCNV will preserve the file structure information.

For testing, PCLANCNV supports the –d command line option. The –d option causes PCLANCNV to expand the specified file into the original input files in a TEMP subdirectory on the PC. The TEMP subdirectory must exist prior to running the –d option.

Once a download file has been completely received, the MX will expand and install the contents of the file. If operating system components were included in the download file, the terminal will reboot.

- If the environment variable ends with an asterisk (“*”), add an additional asterisk to clear that variable.
- If the <value> for an environment variable includes a space, <value> must be enclosed in quotation marks.

PCLANCNV Command Line Options

The format of the PCLANCNV command is:

```
pclancnv-i<filename> -k<C|D> location= <value> -x<password>
{-n -p<blocksize> -r<blocksize> -t} -v -o<filename>
-d<filename> -f<filename>
```

The command line options for PCLANCNV are listed in the tables below. The Command Line Example at the end of this chapter shows a sample compressed IBM ECR download file preparation.

Command Line Rules

PCLANCNV command line options must conform to several rules:

- Each application code file is specified without a control parameter.
- Each application data file and signature filename must be preceded with an -i.
- Files must be specified in the order:
  a. Application code file
  b. Application code signature file
  c. Application data file
  d. Application data signature file
- No spaces are allowed between the control parameter and its item.
- Control parameters may be upper- or lowercase.
- Other than the required order of files (a – d above), the order of items in the command line is not significant.
- If the environment variable ends with an asterisk (“*”), add an additional asterisk to clear that variable.

If the <value> for an environment variable includes a space, <value> must be enclosed in quotation marks.

PCLANCNV Command Line Input Options	
filename	Input application code file (no control parameter before filename).
-i<filename>	Input application data file or signature file.
-k<C|D>	FileToBeSigned.nam, CertFile.crt, KeyFile.key, KeyPassword | where, C=AppCode and D=AppCode.
Input Options (not files)	
location= <value>	Sets an environment variable to <value>, for example, *ZA="TEST" and *ZT="TERMID"
location*	Clears an environment variable (delete the environment variable).
-x<password>	Set terminal password.

Output Format Definition	
-n	Uncompressed format with no blocking.
-p	MX 900 Series compressed PinStripe format with no blocking.
-p<blocksize>	MX 900 Series compressed PinStripe format in blocks of <blocksize> bytes.
-r	MX 900 Series compressed IBM ECR format in blocks of 128 bytes.
-r<blocksize>	MX 900 Series compressed IBM ECR format in blocks of <blocksize> bytes.
-t	Compressed VeriTalk format with no blocking.
-v	Override error checking of output file content, count, and order.
Output File Name	
-o<filename>	Output filename is <filename>.
Other Controls	
-d<filename>	Decode a previously-created output file to existing TEMP subdirectory.
-f<filename>	Use <filename> as ASCII source file for above options.

Command Line Example

The following is an example of command line code:

Example

```
pclancnv -r -iapp.tgz -oappIBMecr.out
```

This example creates an IBM ECR download file named appIBM.ecr.out that includes the files contained in app.tgz (a Linux tar file that was created using gnu zip).

File Signing and Signature Files

File signing is required. File signing is performed with the VeriShield File Signing tool. The result of signing a file is a new signature file also called a .P7S file. The .P7S file must be included as part of the download. The -k option is not used by the MX 900 Series. Signature files are also supported as input files. These are specified just like application data files, with a *-i* option.

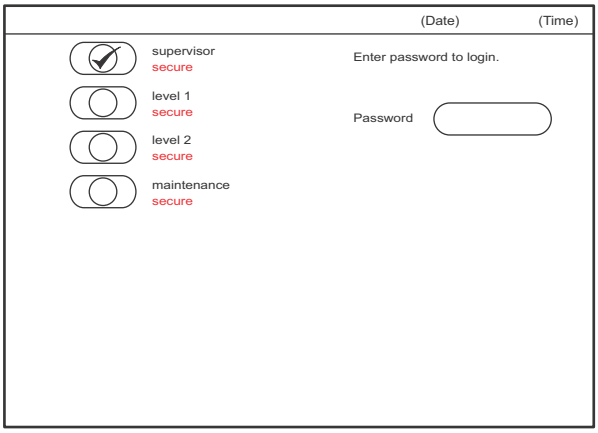
6 VeriShield Remote Key (VRK) Ready Device

The purpose of this chapter is to provide instructions to check your MX 900 Series terminal for a valid VRK RSA Keys. It is required to be VRK Ready.

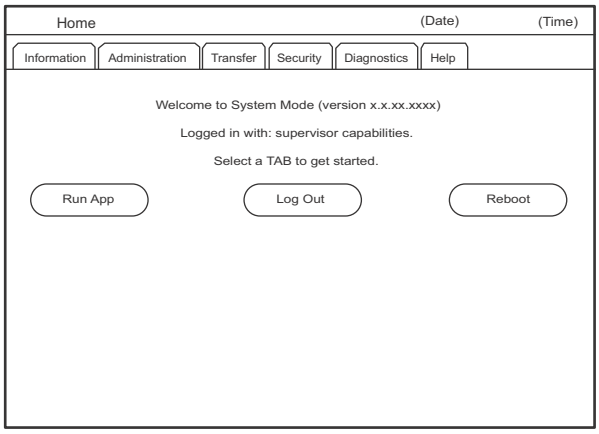
Note: VRK was formerly known as RKL.

Check for Valid VRK RSA Keys

1. Put the terminal into System Mode by using a straightened paperclip to press the reset button on the bottom side of the terminal near the serial number.

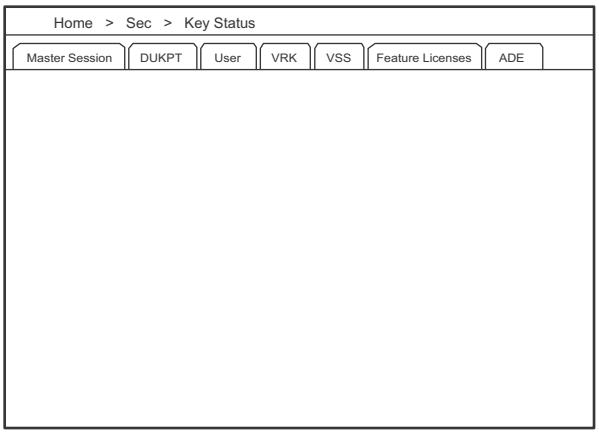


2. Select Supervisor. Key in the password and press enter.

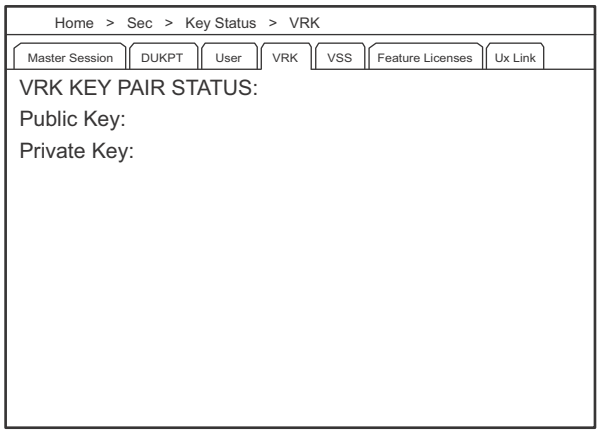


3. Tap **Security**.

4. Tap **Key Status.**



5. Tap the VRK (RKL) tab and the following screen displays a valid VRK RSA Key Pair is installed and the terminal OS is VRK Ready. If the screen displays “Not Installed,” the terminal OS is not VRK Ready.



7 PINpad Security Best Practices

This chapter contains information on PINpad security Best Practices for the MX 900 Series terminals, the MX 915, and the MX 925.

Introduction

Retailers are facing a new and growing threat. Locked out of the payments chain by EMV and encryption, today's criminals are now turning to the Payment Entry Device (PED) itself.

Fraudsters can steal and re-engineer PEDs before re-installing them into retail outlets, such as supermarkets and petrol stations, often conspiring with a staff member. They can then capture and transmit card details and PINs to create fake cards for use at home or abroad.

The negative publicity, damage and cost that can result from PED theft and subsequent customer data fraud, is considerable. Indeed, the threat is so great that some retailers have already received a recommendation to improve physical PED security by tethering and locking their PED assets.

Administrative Security Activities

1. Develop a process to monitor devices that consistently do not work properly, such as high read failures or debit card declines. These can be indicators of tampered terminals.
2. 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 units shipped into the store.
3. Implement a procedure to require all repair technicians who visit your stores to sign in, verify their identity with photo identification, and remain accompanied by store personnel during any work on PINpads.
4. If the PIN pad supports electronic serial numbers, implement a scheme to validate the PIN pad serial number every time the POS starts up to insure the device has not been replaced, and if it has, automatically send an alert.

5. Make sure the password for device access is not the original default password. If it is, have it changed, as default passwords become widely known.
6. Develop a response plan before you suspect you have had a breach. Identify the steps you need to take if you suspect a breach. Understand what to do to isolate your payment systems, and prevent future sensitive information loss. Have a list of who needs to be called including your local law enforcement, your acquiring bank, your processor, your security assessor and your payment system vendors. Make sure you have clear assignments for who needs to do what after a suspected attack and how you will respond.

Physical Security Activities

1. Have a visual inspection performed on every device to look for potential signs of tampering. These include anything that does not look normal such as lack of tamper seals, damaged or altered tamper seals, mismatched keys, missing screws, incorrect keyboard overlays, external wires, holes in the terminal or anything else unusual. If anything out of the ordinary is noticed, stop using the device, disconnect it from the POS or network, but do not power it down. Contact the security officer at the manufacturer to determine the next steps. Continue to perform visual inspections weekly.
2. If your terminal contains an electronic serial number, have the electronic serial number compared to the serial number printed on the bottom of the terminal. If these do not match stop using the device, disconnect it from the POS or network, but do not power it down. Contact the security officer at the manufacturer to determine the next steps.
3. Store spare devices under lock and key to prevent unauthorized removal.
4. Only obtain PIN pads from a manufacturer or manufacturer’s authorised partner. Unauthorized sellers, such as those found on websites such as eBay and Craig’s List, may potentially sell devices that are already compromised, whether intentionally or unwittingly.
5. For similar reasons, have your PIN pads repaired at the manufacturer or an authorised manufacturer’s repair centre.
6. Review the physical installation of your PIN pads. By far, one of the most effective solutions to deter theft is to physically tether your PIN pad to the POS with a purpose designed high security lock.

Wireless Applications - Required Actions, Best Practices

For applications that employ a wireless interface, application writers must familiarize themselves with general risks associated with attacks particular to the wireless interface. Moreover, application writers must employ the direction specified by MasterCard Worldwide to ensure the wireless interface is operating in a secure manner.

Use the following link to secure the required reading http://www.mastercard.com/us/sdp/assets/pdf/wl_entire_manual.pdf.

The following table lists the applicable wireless interfaces and includes pointers within the MasterCard Worldwide manual to detail the security concerns and the accepted operational modes necessary to mitigate them.

Wireless Interface	Basic Information	Security Risks	Security Guidelines
Wi-Fi	2-2	2-2 through 2-3	2-4 through 2-7
GPRS and GSM	2-12	2-12	2-13
Bluetooth	2-14	2-14 through 2-15	2-16

Note: Visa, Payment Card Industry (PCI), and/or other important entities may offer documents detailing requirements as well. Application writers should inquire with any such pertinent entities for documentation before initiating application development.

8 TERMINAL SPECIFICATIONS

Terminal Specifications

This chapter discusses power requirements, dimensions, and other specifications of the MX 900 Series terminals.

Power	• Power pack output requirements: 12W, 12-24VDC. • Power pack input requirements: 100-240VAC, 50/60Hz.
Environmental	• Operating temperature: 0° to 40° C (32° to 104° F) • Storage temperature: – 18° to + 66° C (0° to 150° F) • Humidity: 15% to 95% relative humidity; no condensation
Dimensions	**MX 915** • Height: 56 mm (2.2 inches) • Width: 182 mm (7.2 inches) • Depth: 225 mm (8.9 inches) **MX 925** • Height: 56 mm (2.2 inches) • Width: 218 mm (8.6 inches) • Depth: 230 mm (9.1 inches)
Weight	**MX 915:** 1.3 lbs. (0.6 kg) **MX 925:** 2.0 lbs. (0.9 kg)

INDEX

O

P

R

S

T

V