MX Series

Reference Manual

VeriFone®

THE WAY TO PAY™

MX Series Reference Manual

Part Number 23754, Revision E

March 29, 2011

VeriFone®, Inc.
2099 Gateway Place
Suite 600
San Jose, CA 95110
Telephone: 408-232-7800
http://www.verifone.com

Printed in the United States of America.

CONTENTS

PREFACE 1

Intended Audience 1
Document Organization 1
Conventions Used in this Document 2
Acronyms 3

CHAPTER 2
Features

Overview 5
Modular Design 5
Display Features 6
Features and Benefits 6

CHAPTER 3
File Authentication

Overview 9
The VeriFone Certificate Authority 9
Required Files 9
How FA Works 11
Planning for FA 16
Authentication Requirements for Specific File Types 16
Which Files to Authenticate in a Specific Application 16
How Signature Files Authenticate Target Files 16
Determine Successful Authentication 16
Digital Certificates and the FA Process 17
Two Common FA Scenarios 22
The FILESIGN.EXE File Signing Tool 24
FILESIGN.EXE System Requirements 24
Operating Modes for FILESIGN.EXE 24
Command-Line Entries for FILESIGN.EXE 25
Command-Line Mode Syntax Example 26
FILESIGN.EXE Graphical Interface Mode 27
Steps to Sign Files 27
Download File Structure 28

CHAPTER 4
System Mode

When to Use System Mode 29
Local and Remote Operations 29
Verifying Terminal Status 30
Entering System Mode 30
Exiting System Mode 31
System Mode Menus 32
System Mode Procedures 32
Information Submenu 33
Configure Submenu 34
Diagnostics Submenu 38
File Transfer Submenu 40
File Manager Submenu 42

Security Submenu 43
Screen Traversal and Selection Alternatives 44

CHAPTER 5
Performing Downloads

Requirements 47
Direct Downloads 47
DDL Command Line Syntax 48
DDL Command Line File 49
DDL Example 49
Download Procedures 49
Downloading without an Onboard Application 49
Downloading with an Onboard Application 50
IBM ECR Downloads 52
Network Download Utility 52
PCLANCNV Utility 52
PCLANCNV Command Line Options 54
Command Line Example 55
File Signing and Signature Files 56

APPENDIX A
Troubleshooting

Display is Blank 57
Serial Port Does Not Work 57
Transaction Fails to Process 58
No Response From the Stylus 59
Gap in Captured Signature 59
No Response From the Touch Screen 59

APPENDIX B
ASCII Table

ASCII Table for the MX Series 61

APPENDIX C
Specifications

Terminal Specifications 63

INDEX 65

PREFACE

This manual is your primary source of information for MX 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, Features, explains the features of the MX Series terminals.

Chapter 2, File Authentication discusses usage of the file signing utility, and generating and authenticating the files on the MX Series terminals.

Chapter 3, System Mode, provides information about the usage of System Mode, local and remote operations, and terminal status verification.

Chapter 4, Performing Downloads, provides information about requirements, download procedures, and the PCLANCNV utility.

Appendix A, Troubleshooting, provides troubleshooting guidelines.

Appendix B, ASCII Table, provides ASCII information for the MX Series terminals.

Appendix C, Specifications, provides information on power supply, environment, and dimensions of the hardware.

Conventions Used in this Document

The following table describes the conventions used:

Table 1 Document Conventions

Convention	Meaning
Blue	Text in blue indicates terms that are cross referenced.
`Courier`	Courier font is used when specifying text that you would enter at a command prompt.
Italic	Italic font style indicates book titles or emphasis.
SCREENTEXT	Used when specifying on-screen text that is tapped or selected, and for keys to be pressed.
Note:	Indicates important information.
CAUTION:	Indicates possible hardware or software failure, or loss of data.
WARNING:	Warns that bodily injury might occur.

The various conventions used throughout this manual are listed in Table 2.

Table 2 Conventions

Abbreviation	Definition
cm	Centimeters
KB	Kilobytes
mA	milliampere
MB	Megabytes
sec	Seconds

Acronyms

The following table describes the acronyms used:

Table 3 Acronyms

Convention	Meaning
AC	Alternating Current
ATM	Automated Teller Machine
CDMA	Code Division Multiple Access
CR	Check Reader
CRC	Cyclic Redundancy Check
DDL	Direct Download Utility
DIN	Document Identification Number
DMM	Download Management Module
DUKPT	Derived Unique Key Per Transaction
DTK	Developer's Toolkit
ECR	Electronic Cash Register
EMV	Europay MasterCard and VISA
GID	Group Identification
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
FA	File Authentication
ICC	Integrated Circuit Card
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MRA	Merchandise Return Authorization
MSAM	Micromodule-Size Security Access Module
NAND	Not And (electronic logic gate)
PED	PIN Entry Devices
PCI	Payment Card Industry (MasterCard data security standard)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLAN	PinStripe Local Area Network
PSP	Payment Service Provider
PTID	Permanent Terminal Identification Number
RAM	Random Access Memory
RJ45	Registered Jack 45
SAM	Security Access Module
SC	Smart Card
SDK	Software Development Kit
SRAM	Static Random-Access Memory
TIFF	Tagged Image File Format
USB	Universal Serial Bus
VPN	VeriFone Part Number
Wi-Fi	Wireless Fidelity

CHAPTER 2

Features

This chapter contains information on the features of the MX Series terminals, the MX 870™, MX 860™, MX 850™, MX 830™and MX 760™.

For installation procedures, see the *MX 800 Series Installation Guide* and the *MX 760 Installation Guide*.

MX Series terminals are designed to offer customers outstanding flexibility with the help of the terminals' unique modular design that supports a full line of payment and value-added applications, such as loyalty or prepaid cards. In addition, they are easy to use, secure, and highly reliable–backed by two decades of VeriFone leadership in electronic payment.

Overview

The MX Series offers customers the opportunity to efficiently mix terminals within the same store or chain of stores–saving time and money on implementation, maintenance, and training. The MX 870, MX 860, MX 850, and MX 830 share the following:

- **Architecture** — Linux, similar printed circuit boards, many of the same applications.
- **Upgrade modules** — Terminals in different locations can be equipped with different modules, as needed. Built-in upgradability protects investment, allowing stores to adapt to changing trends.
- **Multifunction connector** — Accepts all available cables, reduces cost by simplifying implementation and allowing cable upgrades.
- **Mounting stands and wedges** — Share the same keyhole pattern for secure mounting.
- **Footprint and "look and feel"** — Offers consistency and simplifies training.

Note: The MX 760 is based on the same architecture as MX 800 devices, but it is designed for unattended applications. For this reason the Upgrade Modules, Multifunction Connector, Mounting Stands and Wedges, and Footprint are not applicable.

Modular Design

The MX Series terminals offer outstanding flexibility due to their modular design. One of the modules that can be added can read contactless smart cards that use radio frequency identification (RFID) based on ISO 14443 standards. The MX 760 has a factory-specified built-in contactless reader option.

Display Features

MX 870

The MX 870 is a color 1/4 VGA payment device with a 5.6-inch display, and is operated exclusively by touch screen.

MX 860

The MX 860 has a 4.3-inch color display, touch screen, and numeric keypad.

MX 850

The MX 850 has a 3.5-inch color 1/4 VGA display, touch screen, and ATM-style screen-addressable keys.

MX 830

The MX 830 has a 3.5-inch backlit, 16-shade grayscale display with optional touch screen and ATM-style screen-addressable keys.

MX 760

The MX 760 has a 5.7” color 1/4 VGA display, but does not have a touch screen.

Stylus

The signature capture stylus is available for any MX Series terminal with a touch screen. Signature capture capability allows capture of virtual signatures, which can be stored as tagged image file format (TIFF) files using capacitive touch technology.

Note: Signature capture is not available on the MX 760 terminal.

Features and Benefits

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

Table 4 Features and Benefits

Features	Benefit
Optional upgradable modules	Lets customers economically address today's needs, while adding capabilities as desired; protects investment. Not applicable for MX 760.
Ethernet/USB (Universal Serial Bus) connectivity	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. **Note**: Ethernet is optional on the MX 830 terminal.

Table 4 Features and Benefits (Continued)

Features	Benefit
Safety glass touch screen	The capacitive and electrostatic technology is highly effective; provides better response with fingertip and stylus; scratch-resistant. **Note**: Touch screen is optional on the MX 830 terminal. **Note**: Not available on MX 760.
Signature capture capability	Speeds customers through lanes; allows digital storage and retrieval, lowers costs. **Note**: Not available on MX 760
Triple-track magnetic card reader	Logically oriented for improved read rates; handles magnetic stripe cards, including drivers' licenses.
Smart card reader/writer	Accepts chip cards conforming to the latest global standards. **Note**: MX 760 has a combined manual insertion magnetic stripe and smart card reader.
PCI PED-compliant PINpad	Virtual PINpad complies with PCI regulations for improved security.
High Resolution Display	Supports sophisticated applications with full-motion video.
Privacy Filter (Optional)	PED-compliant privacy screen, protecting the consumer's PIN entry.
Sophisticated security	Includes 3DES encryption, Master Key/Session Key and Derived Unique Key Per Transaction (DUKPT) key management; also incorporates VeriShield file authentication and tampering safeguards.
32-bit microprocessor	Streamlines processing, even on complex transactions.
Flash and RAM	Ample memory to support multiple payment and value-added applications simultaneously.
RS-232/RS-485 ports	Provides connectivity for ECRs in tailgate mode using RS-485, and for peripherals using RS-232.
Audio	MX 870 — Internal speakers. Includes output jacks for external speakers. MX 860 and MX 850 — Audio is optional. MX 830 — No audio. MX 760 — Line-out connection for external amplifier.

CHAPTER 3

File Authentication

This chapter provides an overview of File Authentication (FA) and explains how to use the file signing utility to generate the signature files required to perform downloads and authenticate files on the MX Series terminals. In Chapter 5, the topic of file authentication is also discussed in the context of specific file download procedures.

Overview

The MX 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).

FA is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process enables the sponsor of an MX 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 Series terminal.

Required Files

The following specially formatted files support the FA process:

- A *digital certificate* is a digital, public document used to verify the signature of a file.
- A *digital signature* 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* (`*.key` files) are securely conveyed to clients on smart cards. 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.

Some files, such as private key files, are encrypted and password-protected for data security. Others, such as digital certificates and signature files need not be secured to safeguard the overall security of VeriShield.

Within the `FILESIGN.EXE` tool, 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 Series terminal clients — either internally within VeriFone or externally to sponsors.

Note: All certificates that are issued by the VeriFone CA for the MX 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 Series terminal, the designated signer uses the signer private key issued by the VeriFone CA as a required input to the file signing tool, `FILESIGN.EXE`. 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 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 FA Works

FA consists of three basic processes:

1. **Development:** The file signing software tool `FILESIGN.EXE` creates a signature file for each application file to authenticate.
2. **Pre-deployment:** An optimal certificate structure is determined, and the necessary certificates and keys created.
3. **Deployment:** The development and pre-deployment processes, once complete, are used in combination to prepare a terminal for deployment.

Development Process

In this process:

1. The application developer creates an application file.
2. The developer assigns a name to the application file.
3. The application file becomes a required input for the `FILESIGN.EXE` tool (included in the DTK).

4. The default certificate (`default.crt`) and default key (`default.key`) included in the SDK are inputs for the `FILESIGN.EXE` tool.
5. Using the application file, default certificate, and default key, `FILESIGN.EXE` creates a signature file (`*.p7s`).
6. The signature file and the original application file are loaded into a development terminal, where the following actions occur:
    a. When an attempt is made to execute an application, a matching signature file must be present.
    b. When a matching application file is found, the operating system compares the signature file's signature against the values stored in the application file's calculated signature.
7. The application file is tested and debugged.
8. After the application file is fully debugged, it becomes an input for the deployment process.

The development process is illustrated in Figure 1.

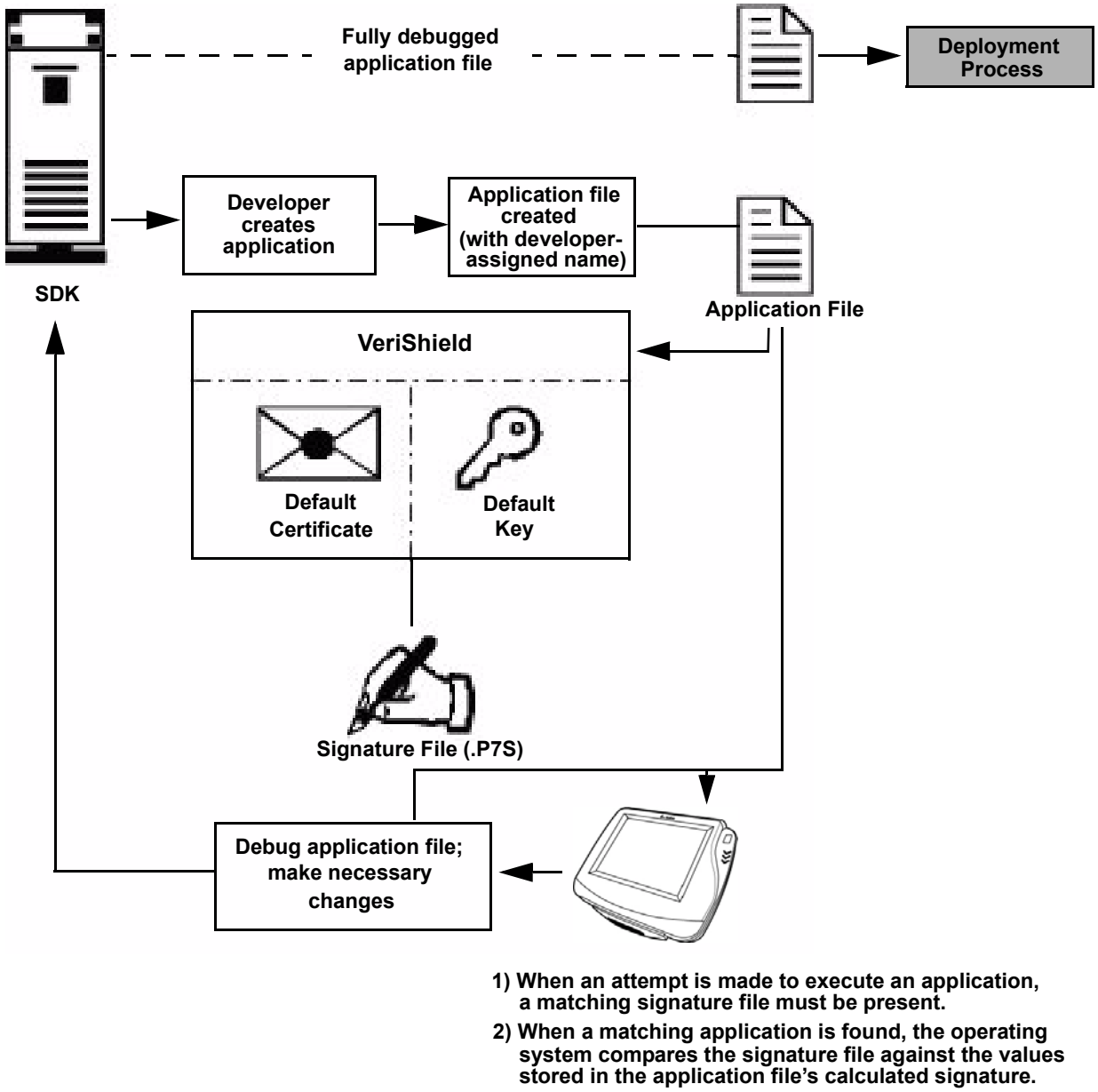


Figure 1 Development Process

Pre-Deployment Process

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 pre-deployment process is illustrated in Figure 2.

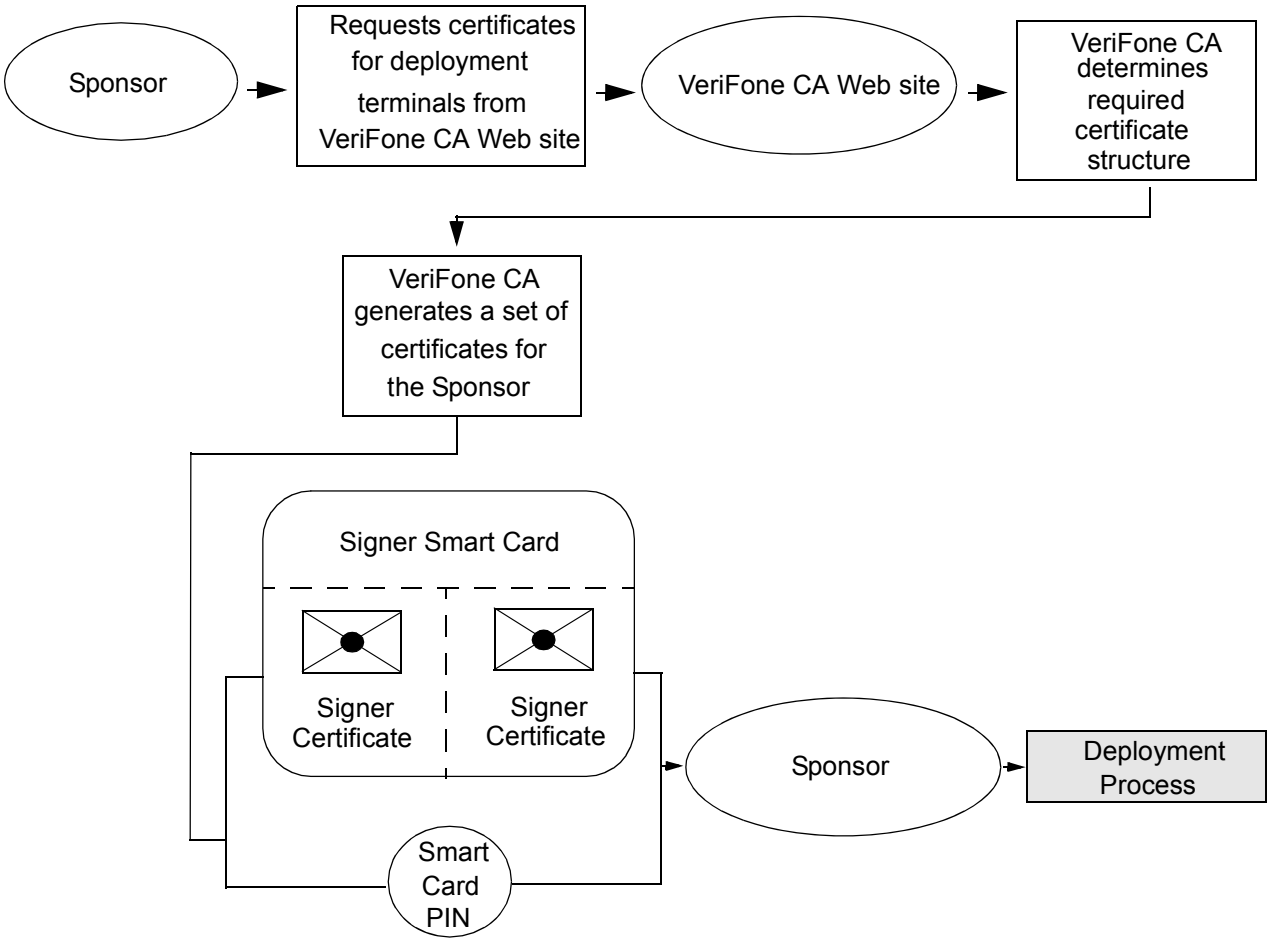


Figure 2 Pre-Deployment Process

Deployment Process

1 The sponsor provides the application file (from the development process) and the smart card and smart card PIN (from the pre-deployment process) as inputs to VeriShield.

2 VeriShield extracts the signer key, 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 extracted 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 execute an application, a matching signature file must be present.

   b When a matching application file is found, the operating system compares the signature file's signature against the values stored in the application file's calculated signature.

6 Each successfully authenticated executable application file is allowed to run on the terminal. (Otherwise, the executable remains stored in the terminal memory but is not allowed to run. An error message displays.)

The deployment process is illustrated in Figure 3.

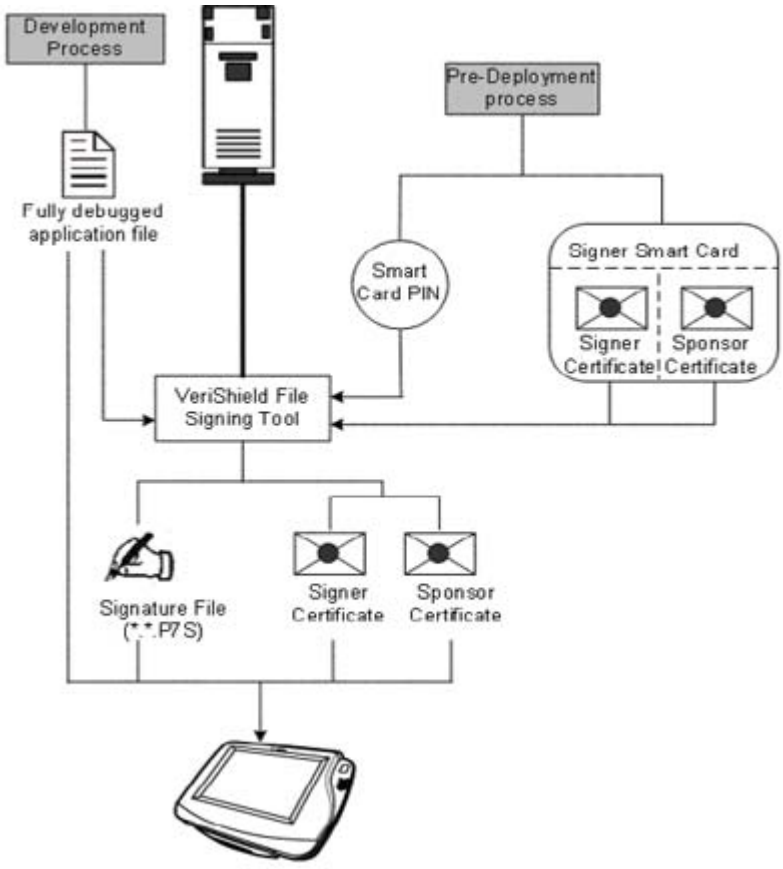


Figure 3 Deployment Process

Planning for FA

FA is an integral part of every MX Series terminals. To safeguard the terminal's logical security, FA requires that *any executable code file* must be successfully authenticated before the operating system allows it to execute on the terminal.

Authentication Requirements for Specific File Types

For FA purposes, executable code files are only `*.out` files. Depending on the logical security requirements of specific applications, other file types used by an application (that is, non-executable files) also need to be authenticated. The application must enforce data authentication.

Which Files to Authenticate in a Specific Application

The first step in the FA process is to determine which files must be authenticated for an application to meet its design specifications for logical security under the VeriShield security architecture.

In most cases, application designers make these decisions based on specifications provided by the terminal sponsor. Which files to authenticate can be completely transparent to the person or business entity responsible for signing, downloading, and authenticating an application prior to deployment.

How Signature Files Authenticate Target Files

Signature files are usually downloaded together with their target application files in the same data transfer operation. This recommended practice lets you specify and confirm the logical security status of the MX Series terminal each time you perform an application download.

When an attempt is made to execute an application, a matching signature file must be present. When a matching application file is found, the operating system compares the signature file's signature against the values stored in the application file's calculated signature.

It is not mandatory to always download a signature file at the same time as its target application file. For example, you can download the corresponding signature file in a separate operation. A non-authenticated application can reside in the terminal memory, but is not authenticated or allowed to run on the terminal until the signature files for the application executable files are processed by FA after a subsequent download procedure and terminal restart.

Determine Successful Authentication

To ensure the MX Series terminal's logical security, never assume that a target file was authenticated simply because it downloaded to the MX Series terminal together with its signature file.

Confirm that all downloaded executable files run.

If an executable code file is not successfully authenticated, the operating system does not allow it to execute and run, either following the initial download or on subsequent terminal restarts. The effect of this rule depends on whether or not all executable files are successfully authenticated:

- If the executable file that failed to authenticate is the main application (`*.out`) specified in the `CONFIG.SYS *GO` variable, the main application is not allowed to run.

- If the executable that failed to authenticate is a secondary executable (`*.out`) or shared library (*.lib) used by the main application, the `CONFIG.SYS *GO` application executes and runs until it issues a function call to that library. When the main application attempts to access a non-authenticated executable, the main application may crash.

For non-executable files, it is the application's responsibility to confirm that all files it uses are successfully authenticated on download completion, and when the application executes the first time following a restart.

Digital Certificates and the FA Process

FA 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, `FILESIGN.EXE`, 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. The data from up to 21 individual related certificates (including root, OS, and other VeriFone-owned certificates) can be stored concurrently in a 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 development set of higher-level certificates is downloaded into each MX Series terminal at manufacture. When you take a new MX Series terminal out of its shipping packaging, certificate data is already stored in the terminal's certificate tree. In this "just-out-of-the-box condition," the MX Series terminal is called a *development terminal*.

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 Series terminal when the terminal is being prepared for deployment. When this procedure is complete, the MX Series terminal is called a deployment terminal.

Add New Certificates

When you add a new certificate file to an MX Series terminal, FA detects it by filename extension (`*.crt`). On restart, 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. The corresponding certificate file (`*.crt`) is then deleted from RAM.
- 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 retained in application memory.

Development Terminals

A development terminal is an MX Series terminal that maintains the original factory set of certificates in its certificate tree. This set of certificates includes several higher-level system certificates and a special client certificate called a default signer certificate (see Figure 4).

In the development terminal, the level of logical security provided by FA is minimal, even though applications must still be signed and authenticated before they can run on the terminal. In most application development and test environments, tight security is not required, and the flexibility offered by the MX Series development terminal is more important.

Note: With the factory set of certificates stored in the terminal memory, anyone who has the MX Series PSP and included file signing tool, `FILESIGN.EXE`, can generate valid signature files for downloading and authenticating files on the MX Series platform.

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 Series terminal is prepared for deployment.

Customer–specific sponsor and signer certificates are usually downloaded to an MX 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, as shown in Figure 4.

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 FA 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.

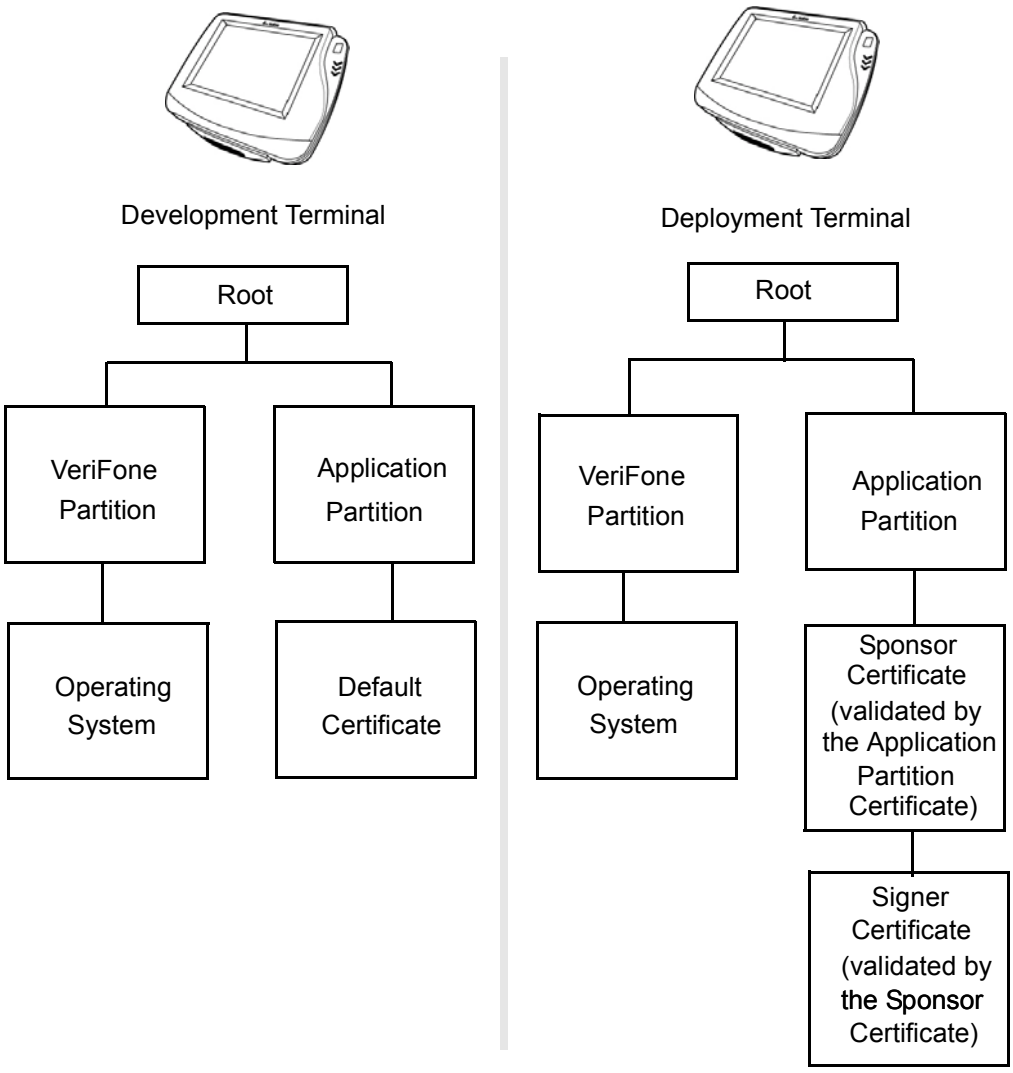


Figure 4 Certificate Trees in Development and Deployment Terminals

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 certificate file can then be deleted by the application. The certificate tree file is stored in the SRAM file system.

Required Inputs to the File Signing Process

The required inputs to the file signing process are somewhat different for development terminals than deployment terminals. The significant differences are shown in Table 5.

Table 5 Differences Between Required Inputs

Development Terminals	Deployment Terminals
Manufacturing inputs to the file signing process are included, together with the file signing tool, `FILESIGN.EXE`, in the MX Series PSP. These inputs make it possible for anyone who has the MX Series PSP to sign and authenticate files.	The required inputs to `FILESIGN.EXE` must be obtained from the VeriFone CA to logically secure the sponsor and signer privileges for the terminal.
The following two factory inputs are required for the file signing process, in addition to the application files you want to sign and authenticate: • **Default signer certificate**, with the filename `default.crt` • **Default signer private key**, with the filename `default.key`	The default certificate and key files can be used with the signing tool, `FILESIGN.EXE`. To sign files at deployment. Use the VeriShield file signing tool (PN P006-217-02-MK) with the included smart card.
Note: A default signer password is not a required entry when using `FILESIGN.EXE` to sign files for an MX Series development terminal.	**Note:** The customer sponsor certificate, which authenticates the customer signer certificate, is usually downloaded to the terminal with the customer signer certificate, but it is not a required `FILESIGN.EXE` input when signing files to be downloaded to (and authenticated on) a deployment terminal.

Replace a Sponsor Certificate

A sponsor may need to clear the current sponsor certificate from a terminal so that a new sponsor can load certificates and applications. To do this, the original sponsor must order a “clear” smart card from the VeriFone CA. The clear smart card is specific to the requesting sponsor. It restores a deployment terminal to the development state (see Figure 5) by:

- Deleting the current sponsor and signer certificates from the terminal’s application partition.
- Restoring the default certificate to the terminal’s application partition.

Note: The process for replacing a signer certificate is the same as for replacing a sponsor certificate.

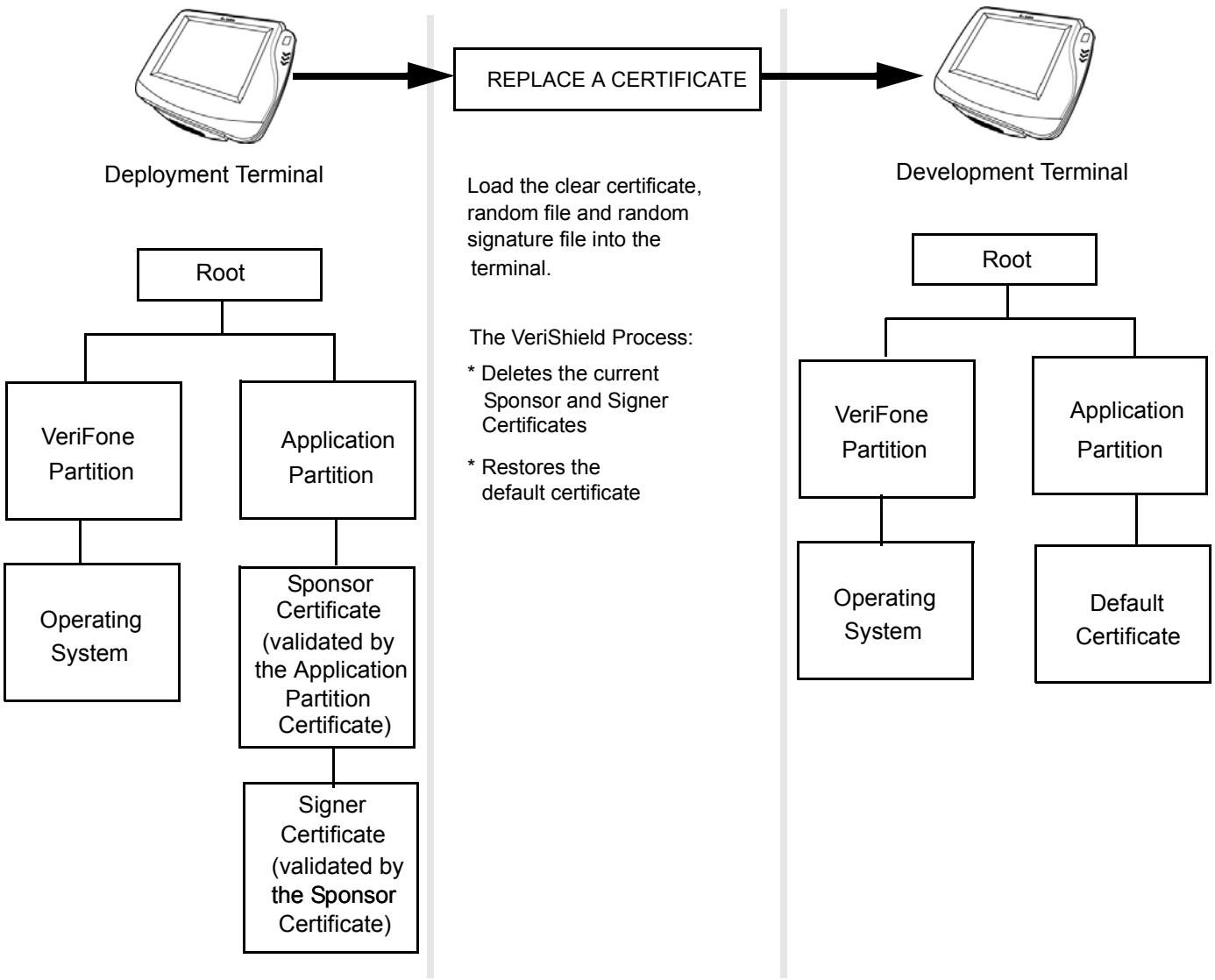


Figure 5 Certificate Replacement Process

Two Common FA Scenarios

Now that we have established which inputs are required to sign files for development terminals and for field terminals, and how certificates, signature files, and keys are interrelated, we can proceed to a more detailed view of the entire FA process.

The two most common task-oriented development terminals for FA implementation:

- **Scenario #1 — Development Terminals:** This case illustrates the file signing process flow for MX Series development terminals.

  The factory default set of certificates is stored in the certificate tree of the download terminal. In this case, the terminal is still a *development* terminal with the minimum level of logical security. This scenario is typical for MX Series application developers.

To support development terminals, you only need the `FILESIGN.EXE` tool, provided with the PSP, and the default certificate and key to generate valid signature files for application downloading and FA.

- **Scenario #2 — Field Terminals:** This case illustrates the process flow for MX Series field terminals.

  A customer has requested from the VeriFone CA a Customer Owner Certificate and a Customer Signer Certificate to establish ownership of, and access to, the terminal as a prerequisite step to deploying the terminal at an end-user site.

  To support field terminals, the additional items previously listed are required inputs to the file signing tool, `FILESIGN.EXE`. When the Customer Owner and Signer Certificates have been downloaded and authenticated, only the entity that is issued a Customer Signer Certificate at the owner's request is authorized to authenticate an application on the owner's terminal.

  To sign files at deployment, use the VeriShield file signing tool (PN P006-217-02-MK) and included smart card.

Authenticate Files Stored in RAM or Flash

All `*.p7s` files must reside in the same file system as the application it signs.

To perform back-to-back downloads, as described in Chapter 5, all signature files *must* be retained in the MX Series terminal's application memory, together with the target application files they authenticate.

Restrictions on Downloading Different File Types

A typical application download to the MX Series terminal includes different file types. The following table provides downloading restrictions and storage information for the different file types.

File Type	Restriction
Certificate (`*.crt`)	*Must* be downloaded into RAM.
Signature (`*.p7s`)	*Must* be downloaded into the same file system as the application it signs.
Operating system	*Must* be downloaded into RAM. When the OS files and related certificates and signature files are authenticated, they are automatically moved from RAM into the FLASH-partition, reserved for the operating system.

The normal size of a signature file is approximately 400 bytes. Depending on the application's size and on how memory space is allocated, the area available for storing multiple signature files must be carefully managed. The memory space required by a certificate file is also approximately 400 bytes, but certificate files are temporary. When a certificate is authenticated, the data it contains is copied to the certificate tree, and the certificate file can be erased from the target file's RAM by the application.

The FILESIGN.EXE File Signing Tool

To generate the signature files required for FA, you must sign all executable files and other files to be logically protected, using the `FILESIGN.EXE` software tool. This section provides information on how to use this tool, which is included on the VeriShield CD.

The file signing tool, `FILESIGN.EXE`, generates a formatted file called a *signature* file, recognized by the filename extension `*.p7s`.

You can run `FILESIGN.EXE` on a host computer (PC) in DOS command-line mode, or invoke the program under Windows® and then use the FileSign dialog box to make the required entries.

Note: The file signing process for operating system files is done for MX Series terminal customers by the VeriFone CA. For operating system updates, VeriFone provides customers with a complete download package that includes all certificates and signature files required for authentication.

FILESIGN.EXE System Requirements

The `FILESIGN.EXE` tool requires one of the following computing environments:

- Windows® NT® Version 4.0, SP5
- Windows® 95
- Windows® 2000
- Windows® XP
- Internet Explorer®

Internet Explorer can be downloaded from the Microsoft® Web site: www.microsoft.com.

Operating Modes for FILESIGN.EXE

`FILESIGN.EXE` can run on the host computer in two user modes:

- **Command-line mode (Windows PC DOS shell):** Command-line mode is useful for application developers who perform batch file downloads and is convenient when using file download tools provided by VeriFone such as VeriTalk and the direct download utility, `DDL.EXE`. In command-line mode, you can sign a batch of files in a single operation.
- **Graphical interface mode (Windows):** Use the FileSign dialog box (Figure 6) to select the file to sign and assign a name and destination location for the generated signature file on the host computer. When you run the `FILESIGN.EXE` tool under Windows, you can sign only one file at a time.

You can also specify to store the target file in the target file's RAM (default location) or in the flash file system. If required, you can navigate through the file system on your PC to select the signer certificate file (`*.crt`) and signer private key file (`*.key`) to use as inputs to the file signing process.

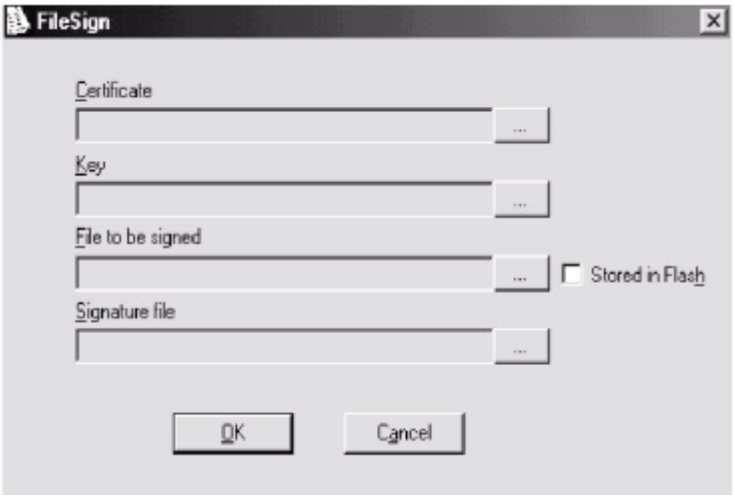


Figure 6 FileSign Dialog Box for FILESIGN.EXE Under Windows

Note: If the entry of a signer password is a required input, a secondary dialog box displays to enter and confirm the password. A signer password is required for a deployment terminal, but not for a development terminal.

Command-Line Entries for FILESIGN.EXE

Table 6 lists and describes the *switches* that make up the command-line mode syntax for `FILESIGN.EXE`.

Table 6 Command-Line Mode Switches for FILESIGN.EXE

Switch	Description	Requirements
`-C, -c`	Signer certificate file name (`*.crt`).	Required input for development terminals and deployment terminals. For development terminals, you can use the default signer certificate, default.crt. For deployment terminals, you must use the signer certificate issued by the VeriFone CA.
`-K, -k`	Signer private key filename (`*.key`).	Required input for development terminals and deployment terminals. For development terminals, you can use the default signer private key, default.key. For deployment terminals, you must use the signer private key provided by the VeriFone CA.

Table 6 Command-Line Mode Switches for FILESIGN.EXE (Continued)

Switch	Description	Requirements
`-P, -p`	Signer password for decrypting the signer private key.	Required input only for deployment terminals. The VeriFone CA issues and securely conveys this password to an authorized signer.
`-F, -f`	Name of the application file to sign (`*.out`, `*.lib`, or other file type).	Required for development terminals and for deployment terminals.
`-S, -s`	Name of the signature file (`*.p7s`) for `FILESIGN.EXE` to generate for the target application file.	Required for development terminals and for deployment terminals.

Command-Line Mode Syntax Example

In the `FILESIGN.EXE` command-line entry example below, note that the syntax used applies to an MX Series development terminal with the factory set of certificates, and not to a deployment terminal. The differences are the following:

- The default signer certificate and default signer key file names that are provided by VeriFone as part of the MX Series PSP are entered on the command line instead of customer-specific customer signer certificate and customer signer private key file names, and
- The switch for signer password (`-P password`) is not used, because a customer signer password is only required to sign and authenticate files for MX Series deployment terminals being prepared for deployment.

Note how the command-line mode switches described in Table 6 are used in this example:

```
filesign -f file.out -s file.p7s -c default.crt -k default.key
```

- The `-f` switch indicates that the application file "`file.out`" must be signed by the `FILESIGN.EXE` tool.

  Executable files, such as `*.out` and `*.lib` files, must always be signed if they are to run on the terminal following a download. Depending on the application's logical security requirements, other types of files, such as data files and font files, may also need to be signed and are authenticated on download.
- The `-s` switch is followed by the name of the signature file to generate, `file.p7s`.
- The `-c` switch is followed by the name of the default signer certificate to use for FA with the development terminal, "`default.crt`".

- The `-k` switch is followed by the name of the default signer private key file, `default.key`. A signer private key is a required input to the file signing process for development terminals and for deployment terminals.

FILESIGN.EXE Graphical Interface Mode

When you execute `FILESIGN.EXE` in the Windows environment, the FileSign dialog box displays (see Figure 6).

The FileSign dialog box has four entry fields, each of which is followed by a “Next” **[...]** selection button, as well as one check box, and the OK and Cancel buttons:

- Press ALT+C or click on the **[...]** button to the right of the “Certificate” field to locate and select the certificate file (`*.crt`) that you want to use to sign the file.
- Press ALT+K or click on the **[...]** button to the right of the “Key” field to locate and select the signer private key file (`*.key`).
- Press ALT+F or click on the **[...]** button to the right of the “File to be signed” field to locate and select the application file (`*.out`, `*.lib`, or other) to sign. If necessary, you can also modify the filename.

  If you want to store the file in flash memory on download to the terminal, check the “Stored in Flash” check box. This adds the “F:” prefix to the target file name.
- Press ALT+S or click on the **[...]** button to the right of the “Signature file” field to enter a filename for the signature file to be generated. The filename extension must always be `*.p7s`. You can also choose another directory in which to store the generated signature file.
- When all entries are complete, press ALT+O or click the OK button to execute `FILESIGN.EXE` and generate the signature file. Or, press ALT+A, or click Cancel to exit the `FILESIGN.EXE` utility.

When the necessary signature files are generated to authenticate the application or applications on the MX Series terminal, you are ready to perform the application download procedure.

For more information about FA within the context of specific download procedures, see Chapter 5.

Steps to Sign Files

Use the following procedure to successfully sign files using the default `.crt` and default `.key` files.

1. Produce the `.OUT` file. If there are multiple `.OUT` files to download, then each file must be signed.
2. Launch the `FILESIGN.EXE` application.

Note: FILESIGN has a Windows and DOS command line mode. This procedure is for the Windows mode.

3. Select the `DEFAULT.CRT` certificate file.

4 Select the DEFAULT.KEY file.

5 Select the *.OUT file to be signed, for example, APP.OUT.

6 Click OK to produce the .P7S file.

Note: The signature file name must be the same as the .OUT file, but must have the .P7S extension, for example, APP.P7S.

7 Download both the application *.OUT file the *.P7S signature file.

From DDL, use the -i option. For example, -iAPP.P7S.

The OS authenticates the application before it can execute. An error message displays if the application fails authentication. Enter System Mode (ENTER+7+password) to clear the error message.

Signature files (*.P7S) are saved in the file system. This allows back-to-back transfers to authenticate properly.

Use the following command to sign from the DOS command line:

```
filesign -c default.crt -k default.key -f app.out -s app.p7s
```

Note: Replace the app.out and app.p7s filenames in the command line with the proper application filename.

Download File Structure

The MX Series file system supports a hierarchical structure. Applications are downloaded to the directory /home/usr1. The application may define subdirectories under /home/usr1 as needed. The signature file (.p7s) for an executable must reside in the same directory as the executable. If new certificates are to be added to a system, they must be downloaded into a subdirectory called crt (lower case). The absolute path is /home/usr1/crt. The system scans the crt directory as needed. In order to create subdirectories during download, use the Linux tar command.

CHAPTER 4

System Mode

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

Note: The MX 760 does not have a touch panel (touch screen) or LEDs. Signature capture is not available on the MX 760.

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 Series application program under development, test and debug the application until validated and ready to download to other terminals.
- **Deployers of MX Series terminals to end-user sites:** Perform specific tasks required to deploy a new MX 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 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 Chapter 5, “Performing Downloads.”

Verifying Terminal Status

The MX Series terminal you are working with may or may not have an application program running on it. After you have set up the terminal as discussed in Chapter 2, 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 application 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.

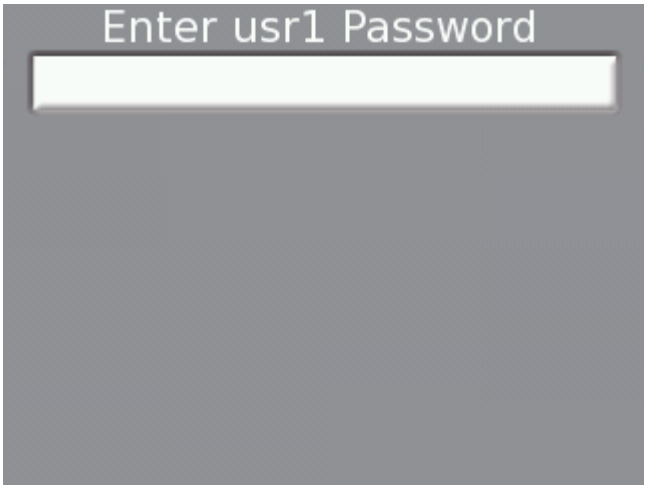
Note: Before entering System Mode and selecting the function(s) to perform, verify that the MX Series terminal has been installed as described in the *MX 800 Series Installation Guide* or the *MX 760 Installation Guide*. Make sure that the terminal is connected to a power source, connected to the network, and is turned on.

1 With the application running, push a paper clip into the small recessed button near the top of the Magnetic Stripe Reader. The three blue LEDs light. Release the button.

Note: To enter System Mode on the MX 760, press down **1**, **5**, and **9** at the same time on the keypad.

The standard logins for usr1 - usr8 display in addition to the maintenance and level1 and level2 accounts. Pressing the “GO” label will restart the application if there is an application properly installed.

2 Once the login has been selected, the System will prompt for a 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.



3 If the password is entered correctly, the System Mode idle screen displays. If the password is not entered correctly, the password 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 **FILE MANAGER** and then **RESTART**.

System Mode Menus

Access the submenus by tapping the icon or menu name. The System Mode screen and submenus are shown below.

See Screen Traversal and Selection Alternatives later in this chapter for all terminals that do not have touchscreens.

Figure 7 System Mode Screen

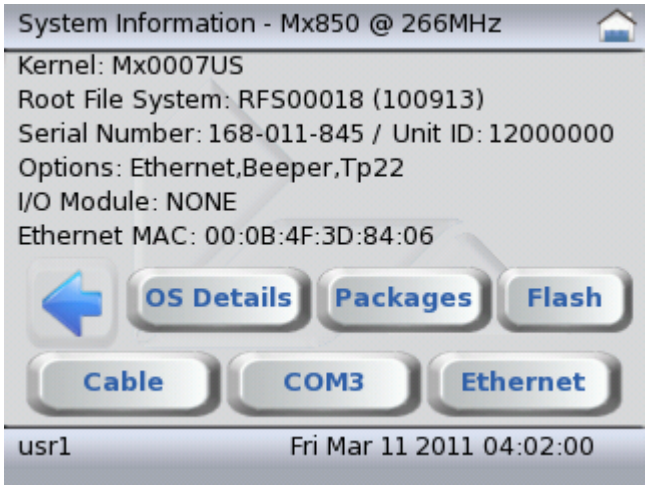
System Mode Procedures

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

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

Information Submenu

Tap the INFORMATION icon on the System Mode screen to view the following information. (Tap the icons that appear for more system information.) Take note of the serial numbers and IDs when viewing the displayed information.

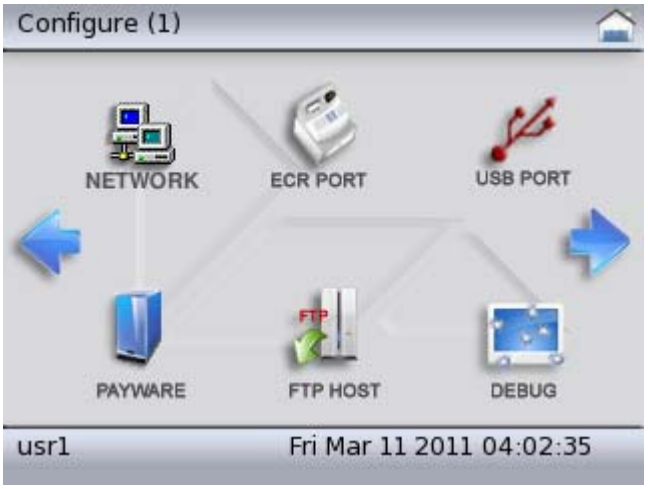


Item	Function
KERNEL	The MX Series operating system (OS) is defined by two components. The first component is the kernel. The kernel version always starts with “Mx.”
ROOT FILE SYSTEM	The second OS component is the Root File System. Its version starts with “RFS.”
SERIAL NUMBER	Serial number of the MX Series terminal.
UNIT ID	ID number of the MX Series terminal.
OPTIONS	Shows the population options installed on the unit. These include: Ethernet, Smartcard, Audio, Tpad (Touch Panel) and Beeper.
I/O MODULE	Displays the type of I/O module installed. Values include: NONE and Contactless Reader.
ETHERNET MAC	Displays the Ethernet MAC address.
OS DETAILS	The operating system version, followed by the load date.
PACKAGES	Displays the installed packages: All, OS, USR, SvcPak.
FLASH	Displays the status of the flash file system. This includes total file system space, used space, and free space. Applications and data files are stored in the flash file system.
CABLE	The device interfaces supported by the attached MX Series multiport cable.

Item	Function
COM3	The COM3 controller version must be V 1.00 or greater.
ETHERNET	Tap the **ETHERNET** icon to view RX and TX packets information. Tap the **ETHERNET** icon again to view RX and TX bytes settings.

Configure Submenu

Tap the **CONFIGURE** icon on the System Mode screen to configure the MX Series terminal. Tap the right and left arrows to see all of the configuration options.



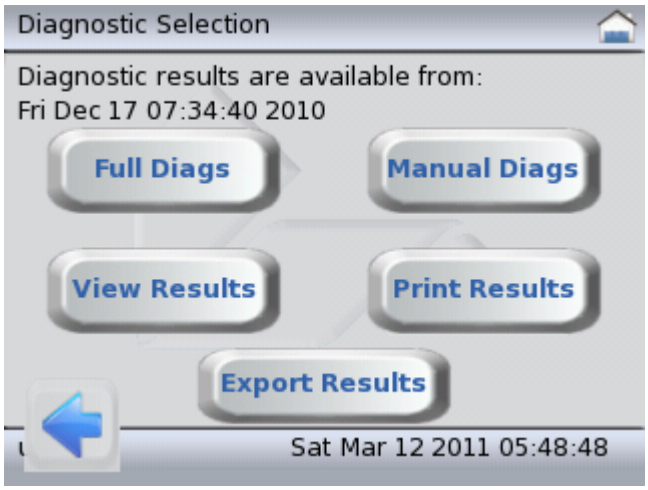
Item	Function
ETHERNET PORT	**DISABLE** — Disable the Ethernet or set your connection via Ethernet DHCP or Static Ethernet. **DHCP** — To set up DHCP to send a broadcast to the network to allow a dynamic IP address to be set, tap the DHCP check box. The unit must be restarted for the change to take effect. **STATIC** — To set up Static Ethernet connection, enter the IP address, Internet mask, Gateway, and DNS settings by tapping the appropriate buttons. **NOTE**: The MX Series terminal must be restarted to apply the Ethernet configuration.
ECR PORT	The current status of your ECR setting is displayed. **TAILGATE** — Configure the ECR Tailgate Address by tapping the button beside the numbered slot, then tap the right arrow to enter the lane number. Press the **ENTER** key. **FEATURE C** — Set up connection options for Feature C by tapping the Port, Character Size, Parity, and Stop Bits. Tap the right arrow to continue. Select the Baud Rate and Flow Control. Tap the right arrow and enter the Lane Number. Press the **ENTER** key. Press the **CLEAR** key to return to the Configure ECR screen. **UNCONFIGURE** — Tap to remove ECR Port configuration.
USB PORT	The USB PORT menu varies depending on the cable connected. Some cables support USB Host, while others support USB Device. **USB HOST** — The menu allows the selection of the USB Host Mode. Valid options are Cable Detect (default) and Disabled. Cable detect allows plug and play with supported devices. Disabled causes the terminal to ignore an attached USB device. **USB DEVICE** — The menu allows the selection of the USB Device Mode. Valid options are disabled (default) or Serial Port (COM5). Selecting Serial Port (COM5) and rebooting causes the terminal to emulate a serial port. **NOTE**: The options Ethernet Adaptor and Mass Storage are currently not available.
PAYWARE	**SET ADDRESS** — Enter the server address. **SET NAME** — Enter the name. **SET PORT** — Enter the port address. **ENABLE PAYWARE** — Tap to enable PAYware on next boot up. **START PAYWARE** — Tap to start PAYware immediately.

Item	Function
FTP HOST	Current FTP information is displayed. After each edit, press **ENTER** or the **CLEAR** key to return to the FTP Host Configure screen. **HOST ADDRESS** — Enter the Host IP address. **HOST NAME —** Enter the FTP Host name. **FTP PORT** — Enter the FTP port address. **USER ID —** Enter the FTP User ID. **PASSWORD** — Set the FTP password.
DEBUG	Enables debug options. ***Note:*** Only enabled in Developer Mode.
EDITOR	Allows you to edit the **usr1** configuration file (`config.usr1`). The display shows a table with each row representing a line from config.usr1. Entries in brackets [ ] are section titles. To change an entry, touch the row and tap the appropriate button. **EDIT VARIABLE** - The variable appears on the left of the = sign in the usr1 file entry. **EDIT VALUE** - The variable appears on the right of the = sign. **DELETE** - Removes the entry. Touching a section title [ ] allows new entries and sections to be created under that section. **Note**: When adding entries under the [PERM] section, do not precede the entry with an asterisk (*). Tap the **EXIT** button to return to the Configuration submenu.
TTY	Use to Initiate a console session with the MX Series. Connect a PC running a program such as HyperTerminal (or any other terminal emulator program) to COM1 on the MX Series. Communication parameters are: **BAUD** — 115200 **BITS** — 8 **PARITY** — No **FLOW CONTROL** — No The unit will prompt for a login and password. **USER ID** — usr1 **PASSWORD** — The same as the System Mode password for usr1.

Item	Function
DATE/TIME	Enter the current date in YYMMDD format: **MM** — Two-digit month (valid values 01–12) **DD** — Two-digit day (valid values 01–31) **YY —** Two-digit year (for example, 07 = 2007) 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) Press the **ENTER** key to accept new Time/Date settings. Press the **CLEAR** key to retain the current settings.
AUDIO	Use to configure the sound settings of the MX Series terminal. **Internal Speakers** — Tap to enable or disable. A red “X” indicates that the internal speakers are disabled. **BASS - VOLUME - TREBLE** — Tap plus **(+)** or minus **(-)** buttons to increase or decrease. **TEST** — Tap to test audio settings.
CALIBRATE	Tap the **CALIBRATE** icon. The touch screen is calibrated automatically. **NOTE**: Do not touch the screen while the calibration is in progress.
DISPLAY	Adjust the MX Series terminal display backlight by tapping the plus **(+)** or minus **(-)** buttons.

Diagnostics Submenu

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



Tap the **FULL DIAGS** button to perform the monitored diagnostics for the terminal. The existing diagnostic record is cleared and a new record is created. Tap the **MANUAL DIAGS** button to perform specific diagnostics on the following:

Item	Function
DISPLAY	Performs a diagnostic procedure on the terminal display. **IMAGE TEST** — 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. Tap the screen once to go to the next diagnostic step. **BACKLIGHT CONTROL TEST** — The screen goes blank to test the backlight control. Tap the display once to proceed to the next step. Tap the **PASS** button if the test was successful. Tap the **FAIL** button if the test was not successful.
TOUCH PANEL KEYPAD	Performs a diagnostic procedure on the touch screen. **COMPENSATION TEST** — Tests the touch screen. A Pass/Fail value is displayed. **SIGNATURE CAPTURE** — Touch the screen with your finger. There should be no lines displayed when your finger is on the screen. Then use the stylus to draw an X-mark on the entire screen (start from below the edge of the screen's title bar to the edge above the time/date bar) and draw a large circle on the center of the X. If the screen displays the circle over the X, the terminal passes the diagnostic test. **CREATE TIFF** — Creates a high resolution TIFF file from the screen image in `/home/usr1/test.tif`. **KEYPAD TEST** — Follow the instructions to test all keys. After "Keypad Test Passed!" appears, press the **ENTER** key. **Note**: Not supported on the MX 760

Item	Function
MAG STRIPE	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.
COM PORT	Validates the state of the COM ports. For manufacturing test purposes only.
AUDIO	Checks the audio settings of the internal speakers. The terminal says “Home Sweet Home” and the beeper plays a series of tones. Tap the **PASS** button if the test was successful. Tap the **FAIL** button if the test was not successful.
MEMORY	Checks the three memory sub-systems: SRAM, SDRAM, and NAND FLASH. All diagnostic procedures must show **PASSED** in order to pass this test. **NOTE**: The NAND Flash may contain errors but still show **PASSED**. If the NAND Flash shows **FAIL**, replace it immediately.
BATTERY	Determines the state of the internal battery. The terminal will fail this test if the voltage shows a value below 2.4 volts.
ETHERNET PORT	Sends a ping to the Ethernet host. For manufacturing test purposes only.
USB PORT	Determines the state of the USB hardware. For manufacturing test purposes only.
CONTACTLESS	Determines the state of the contactless module.
SMART CARD	Determines the state of the smart card reader. For manufacturing test purposes only.
KEY INTEGRITY	Tests the key retention circuit. For manufacturing test purposes only.

Viewing Diagnostic Test Results

Tap the **VIEW RESULTS** button.

- **UP** or **DN** button— Scroll up and down the list.
- **ALL** button — View all of the diagnostic test results.
- **PASS** button — View tests that passed.
- **FAIL** button — View tests that failed.
- **NOT RUN** button — View tests that were not run.
- **PRINT RESULTS** button — Connect a Printer 250 or Printer 900 to the terminal before tapping this button to print the results of the diagnostics procedures.

File Transfer Submenu

Tap the **FILE TRANSFER** icon to download files to the MX Series terminal via the following methods. For detailed information about downloads, see Chapter 5, “Performing Downloads.”

Item	Function
DOWNLOAD	Perform a direct download to the terminal. **PORT — COM1, COM2, COM3** **BAUD RATE — 115200, 19200, 9600, AUTO** **DOWNLOAD TYPE — FULL, PARTIAL** **NOTE**: A **FULL** download removes all files and directories under /home/usr1 and also removes non-permanent entries from config.usr1 file. A **PARTIAL** download does not automatically delete files or configuration entries. Tap the **GO** button to perform the download. USB will be an available port if the terminal is configured for a USB device and connected to a host. Baud rate does not effect USB direct downloads.
ECR DOWNLOAD	Perform a download through an ECR connection. **CONFIGURE ECR** — See “Configure Submenu > ECR Port” for information. **DOWNLOAD TYPE — FULL, PARTIAL** **NOTE**: A **FULL** download removes all files and directories under /home/usr1 and also removes non-permanent entries from config.usr1 file. A **PARTIAL** download does not automatically delete files or configuration entries. Tap the **GO** button to perform the download.
FTP DOWNLOAD	Perform an FTP download. **FTP FILE NAME** — Enter file name and press the **ENTER** key. **PING HOST** — Test status of FTP host before performing the FTP download. **ENABLE AUTO FTP, DISABLE AUTO FTP** — Toggles to enable or disable FTP. Enabling this feature causes the terminal to automatically attempt an FTP download on the next boot-up if no application is loaded. **PERFORM FTP** — Tap to start FTP download.
USB STORAGE	Perform a download via the USB port. Tap USB Storage, tap the file to install, tap Full or Partial. **NOTE**: A **FULL** download removes all files and directories under /home/usr1 and also removes non-permanent entries from config.usr1 file. A **PARTIAL** download does not automatically delete files or configuration entries. Tap the Install button and wait until “Application Install Complete” appears.
NET DOWNLOAD	Perform a download from the PC client software by tapping Net Download.

File Manager Submenu

Tap the **FILE MANAGER** icon to perform the following functions.

Item	Function
RUN APPLICATION	Run the application defined by the configuration variable `*GO` stored in the usr1 configuration file
RESTART	Shut down and restart the MX Series terminal.
EXPLORE FILES	Explore files saved in the `/home/usr1` memory. In the list, tap the file name to view the details of the file if a USB memory device is connected to the terminal. The files stored on the device may also be viewed.

Security Submenu

Tap the **SECURITY** icon to perform the following functions.

Item	Function
VERISHIELD	View the serial numbers and IDs in the VeriShield Certificate list. Tap any part of the screen to return to the Security submenu.
KEY STATUS	View the IPP key status for master key (MK) and DUKPT. Tap Key Status one time to see MK. Tap Key Status two times to see DUKPT. Tap Key Status three times to see the VRK Key Status. Tap Key Status four times to see the Injected User Key Status. Tap the screen to return to the Security submenu.
KEY LOADING	Use to load keys from a secure loading device. (Default values for the two passwords are: 6547649 and 9467456.) Enter the passwords. Two download modes are available. For IPP downloads, select IPP Injection Mode. The system waits for up to one minute to begin the secure key loading procedure. In a secure area, connect a key loading device to COM2 on the MX Series terminal. The key loading device must be configured for 1200 baud, 7 bits, Even parity. For Remote Key downloads, the device must be pre-loaded with a unique RSA key pair. Select RKL Mode. The system waits for up to one minute to begin the key loading procedure. Connect a Key Loading Device (KLD) to COM2. **NOTE**: In conformance with PCI PED, the terminal will disable key loading mode if any of a number of timeout situations occur.

Item	Function
SET PASSWORD	Enter or change the passwords for the following: **USR1** — Set password for opening the usr1 file. **KEY LOAD 1** — Set password #1 for entry into key loading mode. **KEY LOAD 2** — Set password #2 for entry into key loading mode. **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. **EXPIRE PASSWORDS** — Expires passwords Press the **ENTER** key to set keys. Press the **CLEAR** key to cancel.
SECURITY POLICY	View the secure and expired users in the Security Policy list.

Screen Traversal and Selection Alternatives

System Mode is designed to be fully operational on the MX Series terminals. Due to the display size of the MX 850 and MX 830, and that there are variations of this product family that do not have a touch screen, the ATM keys and numeric keypad of the MX 850 and MX 830 have been incorporated into the interface of System Mode.

To enable the ability to select and/or traverse lists on the MX 850 and MX 830 (especially those units without a touch screen), a “hand” selector (an image of a pointing human hand) is used. Since the same software version of System Mode is used for all MX platforms, the hand selector is invisible by default. To make the hand selector visible, the **ENTER**, **F1**, or **F4** key can be pressed. After the hand selector is visible, these keys perform other tasks, as outlined below.

The MX 860 has virtual ATM keys that display on the screen and are used in the same manner as the MX 850 and MX 830 hard ATM keys.

Note: The following table applies to the MX 760 keypad also.

Here is the general rule and use for each key:

F1	Traverse the icon selections on a screen in a clockwise direction.
F4	Traverse the icon selections on a screen in a counter-clockwise direction.
CANCEL (red "X" key)	Cancel a selection and/or operation or, when entering data, clear any previously entered data.
BACKSPACE (yellow key)	Used to exit a screen (go back to previous screen), or, when entering data, to clear previous entry.

ENTER (green key)	Used for selection.
F2	Used to traverse down a list of entries (file browsing, etc.).
F3	Used to traverse up a list of entries.
Numeric keys	Used for entering numeric data such as an IP address.
Alpha-numeric keys	Used for entering text with numbers, letters, and punctuation. The keys, when pressed repeatedly, have the following values: 1 key: ". , ? ! ' " - _ ( ) @ / : 1" 2 key: "a b c 2" 3 key: "d e f 3" 4 key: "g h i 4" 5 key: "j k l 5" 6 key: "m n o 6" 7 key: "p q r s 7" 8 key: "t u v 8" 9 key: "w x y z 9" 0 key: " 0" (space character, then zero character)

Note: F2 and F3 are only active when displaying a list of entries/items.

The main selection screens use the numeric keypad as alternate shortcuts for selection. For example, Main System Mode screen:

- 1 key selects Information
- 2 key selects Configure
- 3 key selects Diagnostics
- 4 key selects File Transfer
- 5 key selects File Manager
- 6 key selects Security.
- If the Back-Arrow is visible, the 7 key selects it.
- If the Forward-Arrow is visible, the 9 key selects it.

CHAPTER 5

Performing Downloads

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

- Develop applications for the MX Series terminal.
- Prepare MX Series terminals for deployment.
- Maintain MX 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 Chapter 3 for further FA discussion.

The MX 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

Requirements

Downloads require moving the application and/or application data files from a remote computer to the terminal. In the MX 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 Linux operating system supports a hierarchical file system with complex file attributes and permissions. For this reason all files downloaded should first be contained in a `.tar` file. Tar files can have the following formats:

- `.tar` - Uncompressed file that may contain multiple files.
- `.tgz` - Compressed file that may contain multiple files.

Direct Downloads

The usual download utility program is Direct Download (DDL) utility. It is normally available with the VeriFone *MX 800 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) download from a PC to a terminal (versus the VeriTalk modem-based functionality).

As the DDL utility sends files from the PC, the MX 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]
```

Flag	Description
`-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`.
`-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 Series terminal.

For additional information about downloading files to the MX Series terminals, see File Transfer in Chapter 4.

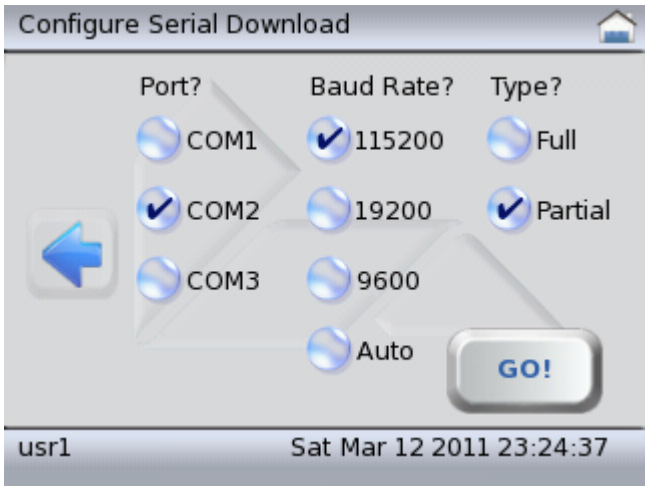
Downloading without an Onboard Application

Use the following procedure to perform a download from a host PC to an MX 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 **FILE TRANSFER** on the System Mode menu.

5 Tap the **DOWNLOAD** icon to perform direct download to the terminal.



6 Set the port, baud rate, and download type (**FULL** or **PARTIAL** download).

Note: A full download removes all files and directories and also removes non-permanent entries. A partial download does not automatically delete files or configuration entries.

7 Tap the **GO** button to perform the download.

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

Downloading with an Onboard Application

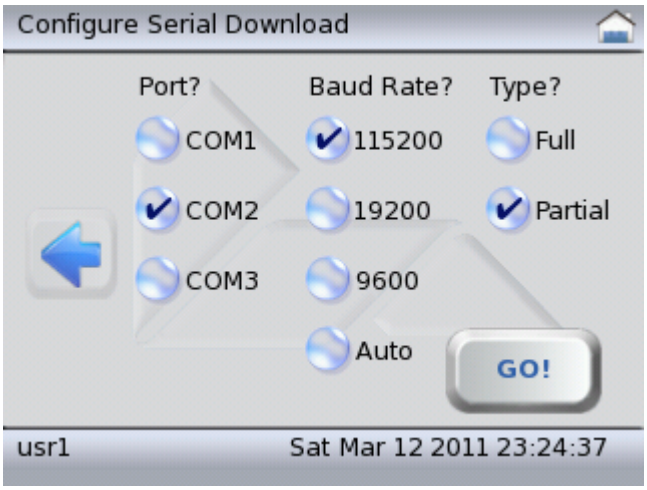
Use the following procedure to perform a download from a host PC to an MX Series terminal with an application(s) installed. The terminal must be in System Mode to begin the procedure.

1 The terminal displays the main System Mode screen.

2 Launch the DDL application on the host PC.

3 Tap **FILE TRANSFER** on the System Mode menu.

4 Tap the **DOWNLOAD** icon to perform direct download to the terminal.



5 Set the port, baud rate, and download type (**FULL** or **PARTIAL** download).

Note: A full download removes all files and directories and also removes non-permanent entries. A partial download does not automatically delete files or configuration entries.

6 Tap the **GO** button to perform the download.

Asterisks (*) display onscreen 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 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 tranfers files from a PC to the MX Series terminal. A network download client, included with the DTK, 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 “Net Download” under File Transfer.

PCLANCNV Utility

On the MX 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 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 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 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.

Table 7 PCLANCNV Command Line Input Options

Input File 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.

Table 8 PCLANCNV Command Line Input Options

Input File 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"

Table 8 PCLANCNV Command Line Input Options

Input File Options	
`location*`	Clears an environment variable (delete the environment variable).
`-x<password>`	Set terminal password.

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 as listed in Table 9 and Table 10. Command Line Example 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.

Table 9 PCLANCNV Command Line Input Options

Input File Options	
`filename`	Input application code file (no control parameter before filename).
`-i<filename>`	Input application data file or signature file.

Table 9 PCLANCNV Command Line Input Options

Input File Options	
`-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.

Table 10 PCLANCNV Command Line Output Options

Output Format Definition	
`-n`	Uncompressed format with no blocking.
`-p`	MX Series compressed PinStripe format with no blocking.
`-p<blocksize>`	MX Series compressed PinStripe format in blocks of `<blocksize>` bytes.
`-r`	MX Series compressed IBM ECR format in blocks of 128 bytes.
`-r<blocksize>`	MX 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 Series. Signature files are also supported as input files. These are specified just like application data files, with a *-i* option.

APPENDIX A

Troubleshooting

During normal, day-to-day operation of your MX Series terminal, it is possible for minor malfunctions to occur. Following are some examples of possible problems, and steps to resolve them.

VeriFone follows stringent quality control standards in the manufacture of MX Series terminals. Each unit that leaves the factory has been rigorously tested to ensure quality and reliable operation. However, should you encounter a problem in operation, read this section for possible causes and solutions.

WARNING: Perform only the procedures specified in this guide. For all other services, contact your local VeriFone distributor or service provider. Service conducted by parties other than authorized VeriFone representatives may void the product warranty.

Each MX Series terminal is equipped with tamper-evident labels. Do not, under any circumstances, attempt to disassemble the terminal.

The troubleshooting guidelines provided in this section identify various problems and suggest the appropriate corrective action(s). If you have problems operating your MX Series terminal, please read through these troubleshooting examples. If the problem persists or if it is not described below, contact your local VeriFone representative for assistance.

Display is Blank

If the terminal display does not show correct or readable information, check all cable connections. If the problem persists, contact your local VeriFone representative for assistance.

Serial Port Does Not Work

The following are the corrective steps to be taken if the serial port does not work.

1. Check whether the device connected to the serial port or serial port of the multiport connector of the MX Series terminal has power and is functioning correctly. If possible, perform a self-test on the device.
2. The cable connecting the optional device to the MX Series terminal's serial port may be defective. Try a different serial cable.
3. If the problem persists, contact your local VeriFone representative for assistance.

Transaction Fails to Process

The following are the corrective steps to be taken if the terminal does not process the transaction.

There are several possible reasons why the terminal may not be operating correctly or processing transactions. To check the most likely causes, follow the steps below.

Step 1: *Check the magnetic card reader*

Note: For MX 760 terminals with a hybrid reader, the magnetic stripe should be on the bottom of the card on the right-hand side.

1. Make sure that you are swiping cards correctly with the MX Series terminal. For the MX Series terminal reader, the black, magnetic stripe on the card should face down and towards the screen.
2. Perform a test transaction using several different magnetic stripe cards to ensure that the problem is not a defective card.
3. Process a transaction manually using the screen instead of the card reader. If the manual transaction works, the problem may be a defect in the card reader. Contact your VeriFone distributor or service provider.
4. If the manual transaction does not work, proceed to Step 3: Check the cable connections.

Step 2: *Check the smart card reader*

1. Make sure you are inserting the cards correctly with the MX Series terminal smart card reader. The chip on the card should face up and inward.
2. Perform a test transaction using several different smart cards to ensure that the problem is not with the card.
3. Ensure any MSAM cards are correctly inserted and that the cardholders are properly secured.
4. If the problem persists, contact your VeriFone distributor or service provider.

Step 3: *Check the cable connections*

1. Ensure that all cables are correctly connected.
2. If cables are connected properly, check that the cable is in working order by connecting a known good cable. If transactions process with this cable, replace the defective cable.
3. If the problem persists, contact your local VeriFone representative for assistance.

No Response From the Stylus

The following are the corrective steps to be taken if the terminal does not respond to the stylus inputs. (This procedure does not apply to the MX 830 terminal without touch screen or to the MX 760 terminal.)

1. Check the documentation to ensure that the terminal supports this stylus.
2. Unplug the stylus that does not respond and connect a known working stylus.
3. If the problem persists, contact your local VeriFone representative for assistance.

Gap in Captured Signature

The following are the corrective steps to be taken if there is a gap in captured signature. (This procedure does not apply to the MX 830 terminal without touch screen or to the MX 760 terminal.)

1. Ensure that the stylus is pressed hard during signature capture.
2. If the problem persists, contact your local VeriFone representative for assistance.

No Response From the Touch Screen

The following are the corrective steps to be taken if the touch screen does not respond or displays the incorrect response. (This procedure does not apply to the MX 830 terminal without touch screen or to the MX 760 terminal.)

Note: The MX Series terminal requires a touch screen calibration at the time of installation. The terminal should be powered on and allowed to stabilize at normal operating temperature; usually this takes no longer than 30 minutes, even if the terminal was previously in a cooler or warmer location. The touch screen calibration procedure (below) should then be performed.

To perform a touch screen (panel) calibration, follow this procedure:

1. Press the recessed button near the top of the Magnetic Stripe Reader with a straightened paper clip and hold while three LEDs in the MSR track turn on. Release the button when the middle LED turns off. Keep hands away from the display until the prompt appears for password entry.
2. Enter the password.
3. In System Mode, perform a manual touch screen compensation. Tap **CONFIGURE** > right blue arrow > **CALIBRATE** > **CALIBRATE**. Follow the directions on the display.
4. If the problem persists, contact your VeriFone representative for assistance.

APPENDIX B

ASCII Table

ASCII Table for the MX Series

An ASCII table for the MX Series display is in Figure 8. The table is formatted for quick reference, as follows:

- The letters and numbers in the column to the left of the table and in the row above the table are, when combined, the hexadecimal value of an ASCII character located in the corresponding row and column coordinate.
- The numbers shown in white on a black background within the table itself are the decimal value of the ASCII character in that table cell.
- The large character located in the middle of each cell is the ASCII character.

For example, to determine the hexadecimal value of the plus (+) sign:

1. Locate the plus sign ASCII character in the table (decimal 43).
2. From this position, follow the row to the left and view the hexadecimal value in the column outside the table. This value (2) is the first character of the ASCII character's hexadecimal value.
3. Now, from the plus sign, follow the column to the top of the table and view the hexadecimal value in the row above the table. This value (B) is the second part of the hexadecimal value.
4. The hexadecimal value for the ASCII plus sign (+) is therefore 2Bh.

See the ASCII Table for a visual reference.

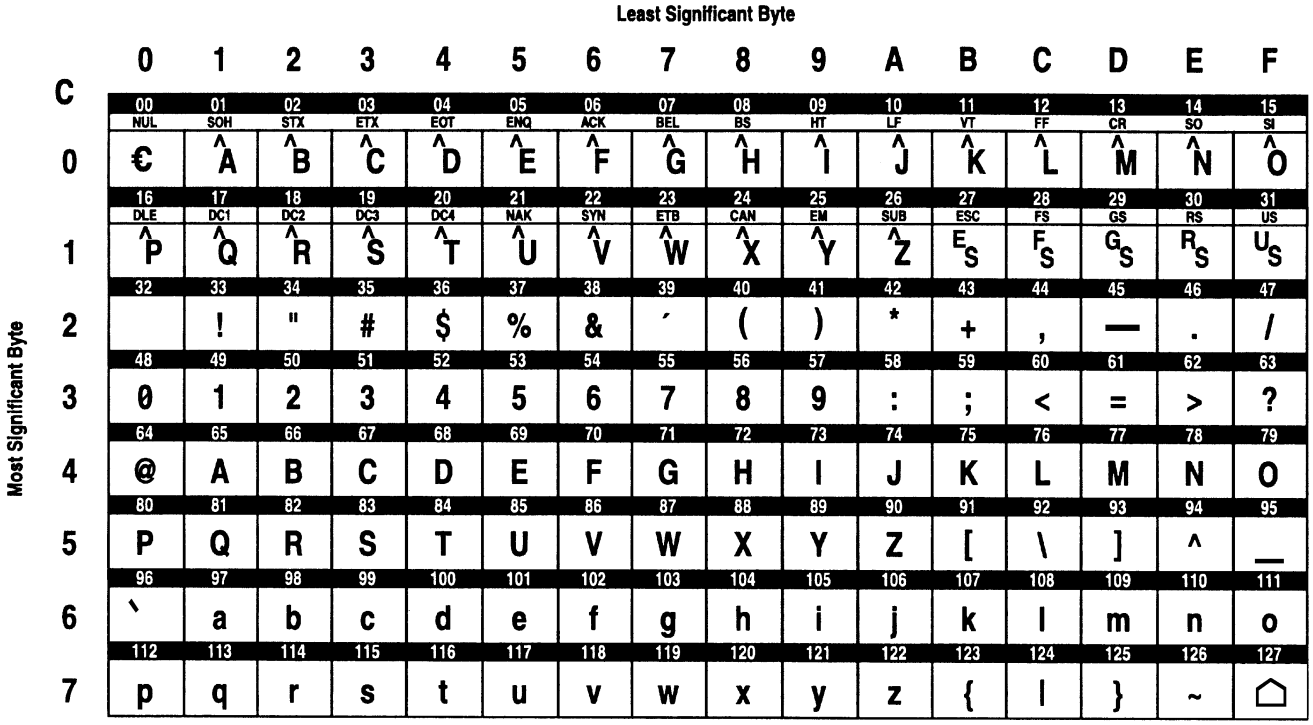


Figure 8 ASCII Table

APPENDIX C

Specifications

Terminal Specifications

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

Table 11 MX Series Terminal Specifications

Power	**MX 870, MX 860, MX 850, MX 830** • Peripheral power requirements: DC power pack: 12 V DC at 1.0 A • Power pack requirements:120 V AC at 60 Hz (U.S.) **MX 760** • MX 760 Standalone: 12V @ 2A or 24 V @ 1A • MX 760 with Printer (powered by MX 760): 24V @4A
Environmental	**MX 870, MX 860, MX 850, MX 830** • 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 **MX 760** • Operating temperature: -20° to 65° C (-4° to 149° F) • Storage temperature: -30° to 75° C (-22° to 167° F) • Humidity: 15% to 95% relative humidity, no condensation

Table 11 MX Series Terminal Specifications

Dimensions	**MX 870** • Height: 153 mm (6.0 inches) • Width: 192 mm (7.5 inches) • Depth: 57 mm (2.24 inches) **MX 860** • Height: 153 mm (6.0 inches) • Width: 192 mm (7.5 inches) • Depth: 71 mm (2.8 inches) **MX 850** • Height: 153 mm (6.0 inches) • Width: 192 mm (7.5 inches) • Depth: 71 mm (2.8 inches) **MX 830** • Height: 153 mm (6.0 inches) • Width: 192 mm (7.5 inches) • Depth: 71 mm (2.8 inches) **MX 760** • Height: 246 mm (9.7 inches) • Width: 240 mm (9.5 inches) • Depth: 147 (5.8 inches - depth behind panel)
Weight	**MX 870:** 1.68 lbs. (.77kg) **MX 860:** 1.62 lbs. (.74 kg) **MX 850:** 1.62 lbs. (.74 kg) **MX 830:** 1.62 lbs. (.74 kg) **MX 760:** 16.7 lbs. (7.6 kg)

Shipping weight MX 870, MX 860, MX 850, MX 830: 1.08 kg (2.38 lb); includes terminal, cable tie-down strap and screw, and the appropriate *Quick Installation Guide.*

Shipping weight MX 760: 3.55 kg (7.83 lb).

INDEX

A

acronyms, Reference Manual **3**
application partition certificate **10**
ASCII table **61**
audience, Reference Manual **1**

C

captured signature, troubleshooting **59**
certificates **9**
  and downloads **19**
  application partition **10**
  certificate tree **17**
  default signer **18**
  development **17**
  file size **24**
  signer **11, 19**
  sponsor **10, 19**
Configure, System Mode **34**
conventions, documentation **2**

D

default signer certificate **18**
development certificate **17**
Diagnostics
  System Mode **38**
  view results **40**
Direct Download (DDL) utility **47**
  command line syntax **48**
Display
  features **6**
  troubleshooting **57**
downloads
  certificate and **19**
  overview **47**
  procedures **49**
  requirements **47**
  with onboard application **50**
  without onboard application **49**

E

entering System Mode **30**
environment variables **48**
  changing through download **53, 54, 55**
exiting System Mode **31**

F

features **6**
  Display **6**
  modular design **5**
file authentication
  and non-executable application files **16**
  certificates
    application partition **10**
    certificate tree **17**
    default signer **18**
    definition **9**
    development certificate **17**
    download sponsor and signer certificate **19**
    file size **24**
    hierarchical relationships **10**
    platform root **10**
    signer **11**
    sponsor **10**
  definition **9**
  deployment process **14**
  development process **11**
  digital signature file **9**
  file signing **11, 16, 20**
  FILESIGN.EXE utility **21, 24**
  guidelines **23**
  key, private cryptographic **9**
  overview **9**
  pre-deployment process **13**
  signature file, file size **24**
  special files **10**
  VeriFone Certificate Authority **9**
  VeriFone PKI **9**
  VeriShield security architecture **16**
File Manager, System Mode **42**
file signing **20, 24**

File Transfer, System Mode **40**
FILESIGN.EXE utility **21, 24**
switches for command-line entries **25**
syntax **26**

I

Information, System Mode **33**

K

key, private cryptographic **9**

M

measurements, Reference Manual **2**
MX Series
ASCII table **61**
features **6**
overview **5**
specifications **63**
System Mode **29**
troubleshooting **57**
verifying terminal status **30**

O

overview
downloads **47**
file authentication **9**
troubleshooting **57**

P

P7S file **24**
password **30**
procedures
downloads **49**
System Mode **32**

R

Reference Manual
acronyms **3**
audience **1**
measurements **2**
requirements for downloads **47**

S

screen traversal **44**
Security, System Mode **43**
serial port, troubleshooting **57**
signature file **9, 24**
file size **24**
signer certificate **11, 19**
smart cards, clear **21**
specifications, MX Series **63**
sponsor certificate **10, 19**
stylus, troubleshooting **59**
System Mode
Configure **34**
Diagnostics **38**
Diagnostics, view results **40**
entering **30**
exiting **31**
File Manager **42**
File Transfer **40**
Information **33**
local and remote operations **29**
overview **29**
procedures **32**
screen traversal **44**
Security **43**
verifying terminal status **30**
when to use **29**

T

terminal
modular design **5**
password **30**
verify status **30**
touch screen, troubleshooting **59**
transaction failure, troubleshooting **58**
troubleshooting
captured signature **59**
Display **57**
overview **57**
serial port connection **57**
stylus **59**
touch screen **59**
transaction failure **58**

V

variables **48**
VeriShield **16**

VeriFone, Inc.
2099 Gateway Place, Suite 600
San Jose, CA, 95110 USA
Tel: (800) VeriFone (837-4366)
www.verifone.com

MX Series

Reference Manual

Part Number 23754, Revision E