VX 520

Reference Guide

VeriFone Part Number DOC252-004-EN-B, Revision B

VX 520 Reference Guide

The information contained in this document is subject to change without notice. Although VeriFone has attempted to ensure the accuracy of the contents of this document, this document may include errors or omissions. The examples and sample programs are for illustration only and may not be suited for your purpose. You should verify the applicability of any example or sample program before placing the software into productive use. This document, including without limitation the examples and software programs, is supplied “As-Is.”

Comments? Please e-mail all comments in this document to your local VeriFone Support Team.

VeriFone, Inc.
2099 Gateway Place, Suite 600
San Jose, CA, 95110 USA

www.verifone.com

VeriFone Part Number DOC252-004-EN-B, Revision B

CONTENTS

CHAPTER 9 VeriFone Service and Support

CHAPTER 10 Troubleshooting Guidelines

APPENDIX A System Messages

APPENDIX B Port Pinouts

APPENDIX C ASCII Table

APPENDIX D Keypress Scan Codes

PREFACE

This guide is your primary source of information for setting up and installing the VX 520 series of terminals.

Audience

This document has two primary audiences, but is useful for anyone installing and configuring the VX 520 terminal:

- **Deployment Administrators** who prepare multiple units for deployment to their customers, configuring the units with applications, network configurations, phone numbers, and security. Deployment Administrators may work for a bank, credit card service company, or any company with a vertical application for the VX 520 terminal.
- **Local Administrators** who integrate and maintain VX 520 terminals into a single business site. Business owners or store managers generally perform this function.

Organization

This guide is organized as follows:

Chapter 1, Terminal Overview. Provides an overview of the VX 520 series of terminals.

Chapter 2, Terminal Setup. Explains how to set up and install the VX 520 terminal. It tells you how to select a location, establish power and telephone line connections, and how to configure optional peripheral devices.

Chapter 3, Using the Terminal Keys. Explains the operational features of the VX 520 unit and describes how to use the VX 520 keys to perform all the data entry or Terminal Manager tasks described in this manual.

Chapter 4, Verix Terminal Manager. Describes password-controlled, system-mode operations, as well as how to use it to perform a variety of test and configuration procedures.

Chapter 5, File Authentication. Describes the file authentication module of the VeriShield security architecture and provides reference to the VeriShield File Signing Tool to generate signature files.

Chapter 6, Performing Downloads. Documents procedures for downloading applications and files to VX 520 units.

Chapter 7, Specifications. Discusses the power requirements and dimensions of the VX 520 terminal.

Chapter 8, Maintenance. Explains how to maintain your VX 520 terminal.

Chapter 9, VeriFone Service and Support. Provides information on contacting your local VeriFone representative or service provider, and information on how to order accessories or documentation from VeriFone.

Chapter 10, Troubleshooting Guidelines. Provides troubleshooting guidelines, should you encounter a problem in terminal installation and configuration.

This guide also contains appendices for System Messages, Port Pinouts, ASCII Table, Keypress Scan Codes, and Glossary.

Related Documentation

To learn more about the VX 520 terminal, refer to the following set of documents:

VX 520 Certifications and Regulations	VPN DOC252-001-EN
VX 520 Quick Installation Guide	VPN DOC252-002-EN
VX 520 Installation Guide	VPN DOC252-003-EN
VX 520 GPRS Certifications and Regulations	VPN DOC252-021-EN-A
VX 520 GPRS Quick Installation Guide	VPN DOC252-022-EN-A
Verix V Operating System Programmers Manual	VPN 23230
Verix eVo Volume I: Operating System Programmers Manual	VPN DOC00301
Verix eVo Volume II: Operating System and Communication Programmers Manual	VPN DOC00302
Verix eVo Volume III: Operating System Programming Tools Reference Manual	VPN DOC00303

Conventions and Acronyms

This section describes the conventions and acronyms used in this guide.

Document Conventions

Various conventions are used to help you quickly identify special formatting. Table 1 describes these conventions and provides examples of their use.

Table 1 Document Conventions

Convention		
Blue	Text in blue indicates terms that are cross referenced.	See Conventions and Acronyms.
Italics	Italic typeface indicates book titles or emphasis.	You *must* install a roll of thermal-sensitive paper in the printer.
`Courier`	The courier type face is used while specifying onscreen text, such as text that you would enter at a command prompt, or to provide an URL.	`http://www.verifone.com`
NOTE ✎	The pencil icon is used to highlight important information.	RS-232-type devices do not work with the PIN Pad port.

Table 1 Document Conventions

Convention		
CAUTION	The caution symbol indicates possible hardware or software failure, or loss of data.	The terminal is not waterproof or dust proof, and is intended for indoor use only.
WARNING	The lighting symbol is used as a warning when bodily injury might occur.	Due to risk of shock do not use the terminal near water.

Acronym Definitions

Various acronyms are used in place of the full definition. Table 2 presents acronyms and their definitions.

Table 2 Acronym Definitions

Acronym	Definitions
AC	Alternating Current
ATM	Asynchronous Transfer Mode
CA	Certificate Authority
CPU	Central Processing Unit
CR	Check Reader
CTLS	Contactless
DC	Direct Current
EMV	Europay MasterCard and VISA
GPRS	General Packet Radio Service
IPP	Integrated PIN pad
ITP	Internal Thermal Printer
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MRA	Merchandise Return Authorization
MSAM	Micromodule-Size Security Access Module
PCI	Payment Card Industry
PED	PIN-Entry Device
PIN	Personal Identification Number
RAM	Random Access Memory
RJ-11	Registered Jack 11
RJ-45	Registered Jack 45
RS-232	Recommended Standard 232
SAM	Security Access Module
TMA	Terminal Management Agent
VPN	VeriFone Part Number

CHAPTER 1

Terminal Overview

This chapter provides a brief description of the VX 520 terminal:

- The VX 520 is a high performance countertop terminal with enhanced communication options.
- The VX 520 offers several communication options, enhanced display, increased processing power, expanded memory, and two USB peripheral ports.

The VX 520 terminal uses a robust, sleek, and highly functional design.

NOTE VeriFone ships variants of the VX 520 terminals for different markets. Your terminal may have a different configuration from the features described in this section.

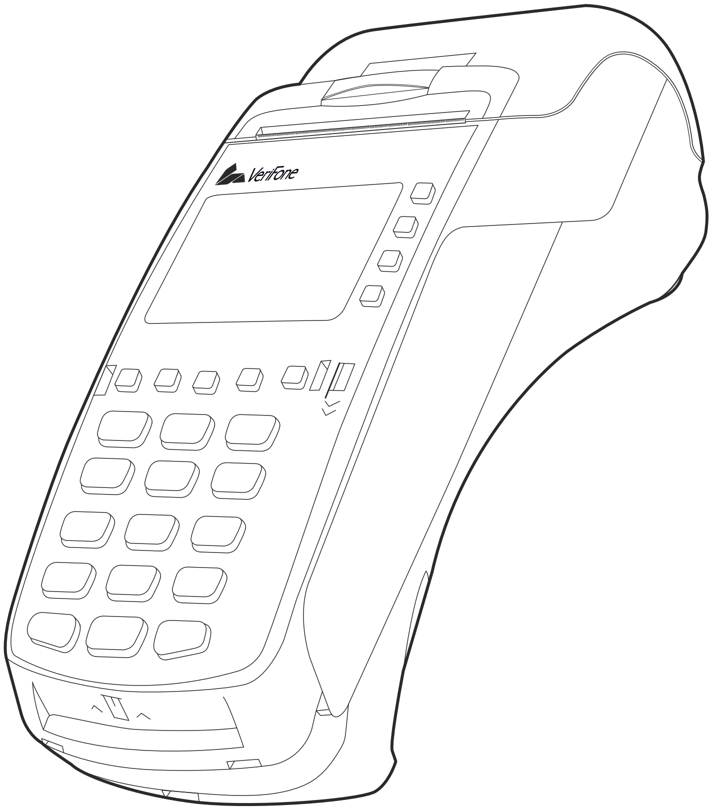


Figure 1 VX 520 Terminal

Features and Benefits

VX 520 terminals provide the right combination of features and functions. This includes a triple-track magnetic-stripe card reader, landed smart card reader, integrated PIN pad, a quiet internal thermal printer (ITP). The VX 520 GPRS is a portable, line- or battery-powered device with added GPRS wireless technology.

Connectivity

- Host USB port
- Client USB port
- RJ-11 port
- RS-232 port
- Ethernet Port

NOTE

The connectivity ports are easily accessible from the underside of the terminal.

NOTE

VeriFone ships variants of the VX 520 terminals for different markets. Your terminal may have a different configuration from the features described in this section.

Performance

- 400 MHz processor (CPU)
- Increased memory (128 MB Flash, 32 MB RAM)
- 128/64 white backlit LCD
- Fastest encryption/decryption appliance on the market
- Backlit keypad

Security

- Increased security (PCI 2.0)
- SDA DDA encryption ready
- Leading ECC performance benchmark

Form Factor

- The VX 520 is ergonomically designed to fit both the traditional countertop and handover models.

Exceptional Ease of Use

- The bold design is sleek, stylish, and lightweight for conveniently handing the terminal to the consumer for PIN entry or other input.
- An intuitive ATM-style interface, a large 8-line by 21-character backlit display with backlit keypad, and extra-size menu prompts, simplify training and reduce help desk calls.
- The integrated thermal printer simplifies paper loading and reduces paper jams.
- The triple-track, high-coercivity card reader handles most magnetic stripe cards.

Countertop Performance in a Handover Design

- The 32-bit processing and multi-tasking capabilities ensures fast processing of payment, payment-related, and value-added applications.
- Exceptional display and printer graphics-handling capabilities that quickly render logos, graphical fonts, and character-based languages.
- The VX 520 series of terminals ensures uncompromising reliability from VeriFone, the worldwide leader in e-payment.
- The VX 520 GPRS series meets the needs of TablePAY, DeliveryPAY, and CarsidePAY markets.

True Multi-Application Capability

- The VX 520 terminal offers 32 MB of RAM, and 128 MB Flash memory, which supports multiple applications on a single terminal.
- The primary smart card reader and the MSAMs safeguard sensitive financial data and support multiple smart card schemes.
- VX 520 terminals and SoftPay EMV software are certified for EMV Level 1 and Level 2 Type approval for smart card solutions. The Verix V or V^{X} EMV Library provides development of other EMV-compliant applications.
- The VeriShield security architecture meets published specifications for PCI PED and provides sophisticated file authentication to prevent execution of unauthorized software on VX 520 terminals.

Wireless Connectivity (VX 520 GPRS Only)

- Customers are not tied to a fixed location with the VX 520 GPRS terminals – the point of payment can be almost anywhere.
- “Always-on” wireless connection uses the latest wireless technology (GPRS) for faster transmission and enhanced compatibility with access points and routers.

CHAPTER 2

Terminal Setup

This chapter describes the terminal setup procedure. You will learn about:

- Selecting Terminal Location
- Unpacking the Shipping Carton
- Examining Terminal Features
- Installing the Smart Battery (VX 520 GPRS Only)
- Establishing Telephone Line Connections
- Installing the Paper Roll in the Printer
- Installing/Replacing MSAM Cards
- Installing/Replacing SIM Card (VX 520 GPRS Only)
- Connecting Optional Devices
- Connecting the Terminal Power Pack
- Charging the Smart Battery (VX 520 GPRS Only)
- Privacy Shield (Optional)
- Using the Smart Card Reader
- Using the Magnetic Card Reader

Selecting Terminal Location

Use the following guidelines when selecting a location for your VX 520 terminal.

Ease of Use

- Select a location convenient for both merchant and cardholder.
- Select a flat support surface, such as a countertop or table.
- Select a location near a power outlet and a telephone/modem line connection. For safety, do not string the power cord in a walkway or place it across a walkway on the floor.

Environmental Factors

- Do not use the terminal where there is high heat, dust, humidity, moisture, or caustic chemicals or oils.
- Keep the terminal away from direct sunlight and anything that radiates heat, such as a stove or motor.

- Do not use the terminal outdoors.

CAUTION

The terminal is not waterproof or dustproof, and is intended for indoor use only. Any damage to the unit from exposure to rain or dust may void any warranty.

Electrical Considerations

- Avoid using this product during electrical storms.
- Avoid locations near electrical appliances or other devices that cause excessive voltage fluctuations or emit electrical noise (for example, air conditioners, electric motors, neon signs, high-frequency or magnetic security devices, or computer equipment).
- Do not use the terminal near water or in moist conditions.

Unpacking the Shipping Carton

Open the shipping carton and carefully inspect its contents for possible tampering or shipping damage. The VX 520 terminal is a secure product and any tampering may cause the device to cease to function properly.

To unpack the shipping carton

1. Remove and inspect the following items:
   - Terminal
   - Power pack
   - Power cord
2. Remove all plastic wrapping from the terminal and other components.
3. Remove the clear protective film from the LCD screen.

CAUTION

Do not use a terminal that has been damaged or tampered with. The VX 520 terminal comes equipped with tamper-evident labels. If a label or component appears damaged, please notify the shipping company and your VeriFone representative or service provider immediately.

4. Save the shipping carton and packing material for future repacking or moving the terminal.

Examining Terminal Features

Before you continue the installation process, notice the features of the VX 520 terminal (see Figure 2).

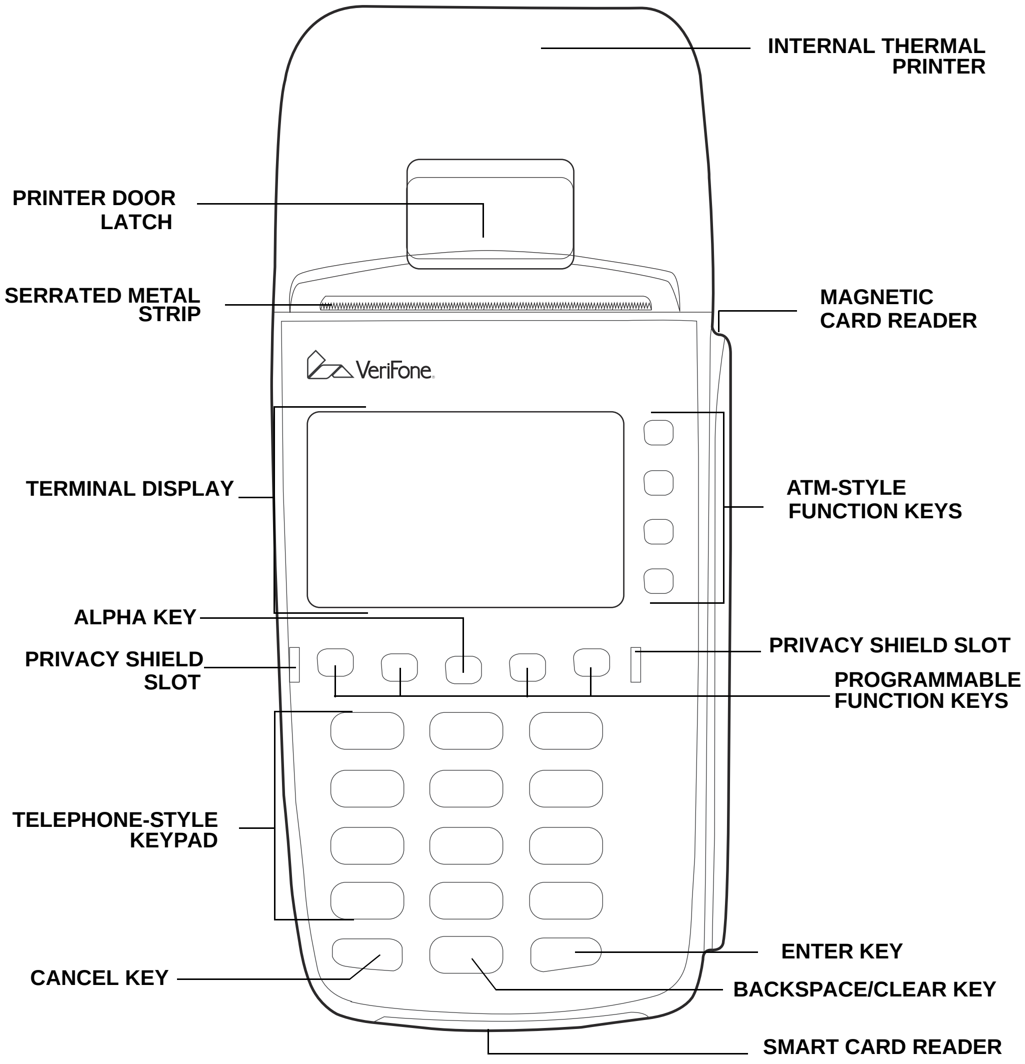


Figure 2 VX 520Terminal Features (Front Panel)

Front Panel

The front panel includes the following features:

- A **terminal display**, backlit LCD screen.
- Five types of keys:

  a A backlit 12-key, **telephone-style keypad**.

  b Four **ATM-style function keys**, labeled F1 to F4, to the right of the LCD screen.

  c Four unlabeled, **programmable function keys** above the keypad.

  d Three **color-coded function keys** below the keypad (icons at right; from left to right: CANCEL, BACKSPACE/CLEAR, ENTER).

  e An **ALPHA key** centered at the top of the keypad.

- A **magnetic card reader**, built into the right side. The icon at the right shows the proper swipe direction, with the stripe down and facing inward, toward the keypad.
- The VeriFone logo **blue indicator LED** indicates power is ON.
- An **internal thermal printer**.
- A **smart card reader**, built into the front of the terminal. The icon indicates the proper card position and insertion direction.
- Three **SAM (security access module) compartments**, built into the side of the terminal. The VX 520 terminal contains MSAM cardholders to support multiple stored-value card programs or other merchant card requirements.

NOTE VeriFone ships variants of the VX 520 terminal for different markets. Your terminal may have a different configuration. The basic processes described in this guide remain the same, regardless of terminal configuration.

Connection Ports

Turn the terminal upside down and remove the rear cover to view the connection ports. Notice that the ports are recessed. Different ports provide connections to a communications line, optional peripheral devices, and the power supply.

Figure 3 shows how to open the rear cover of the VX 520 terminal.

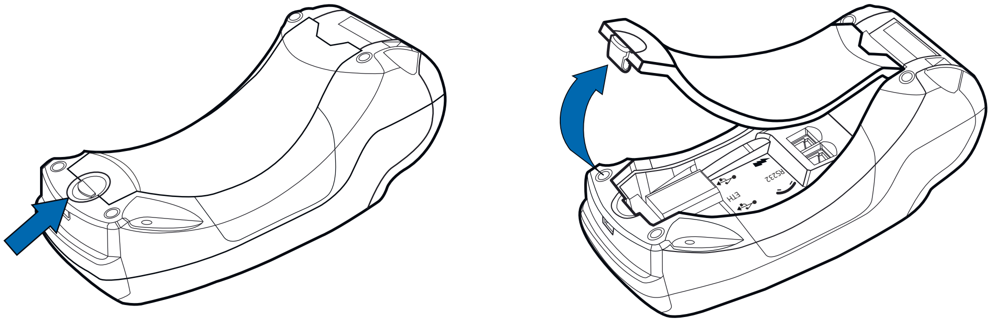


Figure 3 Opening the Rear Cover

Figure 4 and Figure 5 show the connection ports for the VX 520 terminal.

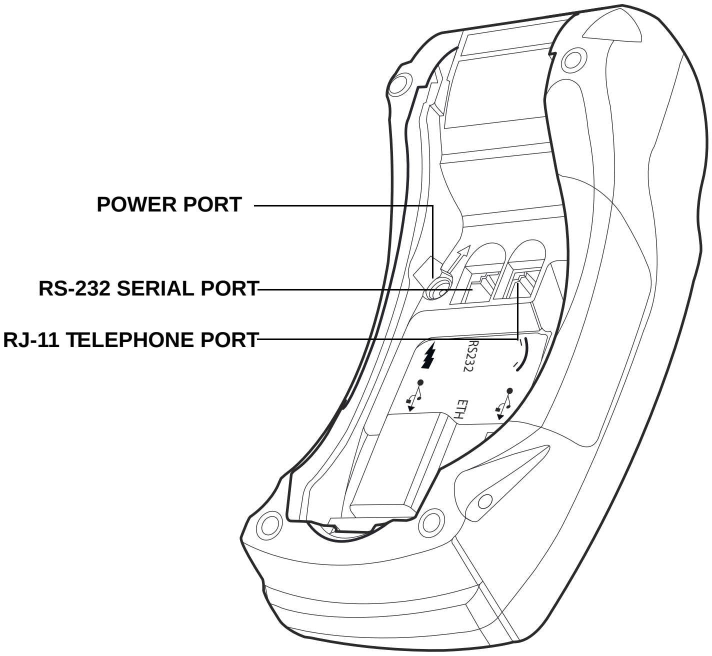


Figure 4 VX 520 Power and Connection Ports

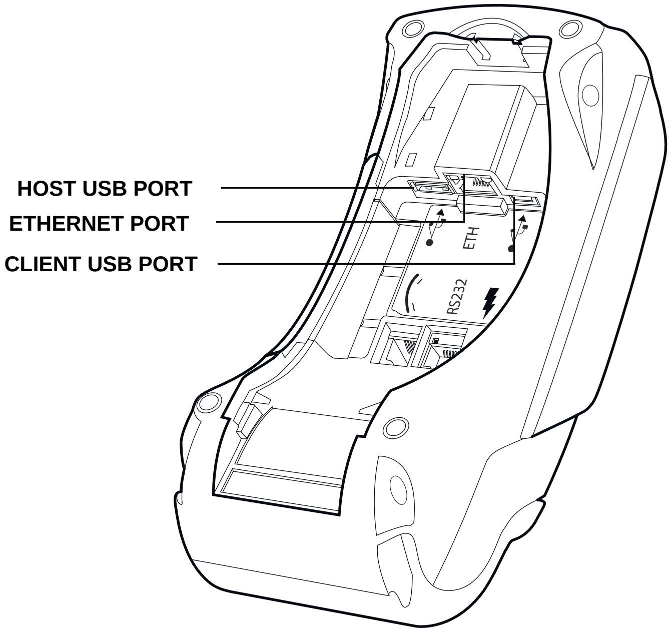


Figure 5 Additional VX 520 Connection Ports

WARNING Do not connect the terminal to the power supply until all the peripherals are attached. Do not disconnect peripherals from the terminal while the power supply is connected.

To use the connection ports

The connection ports offer multiple connectivity for the VX 520 terminal. Please refer to the following list of peripheral devices for the connectivity options.

Host USB Port

- PINpad 1000 USB
- V^{x}810 USB
- Barcode reader
- Biometric reader
- USB flash disk
- USB keyboards

Ethernet Port

- Ethernet cable to router, hub or switch

Client USB Port

- PC
- ECR/Cash register

RJ-11 Port

- Telephone line

RS-232 Port

- PINpad 1000
- V^{x}810
- PC download cable
- Computer
- ECR
- Check reader
- CTLS reader
- Biometric reader
- Barcode reader
- Keyboard

For information on how to attach peripheral devices, see Connecting Optional Devices.

Installing the Smart Battery (VX 520 GPRS Only)

The smart battery fits in a slot on the back of the VX 520 GPRS terminal. The locking tab clicks when the battery is in place. The slot is keyed, so that there is only one way to insert the battery.

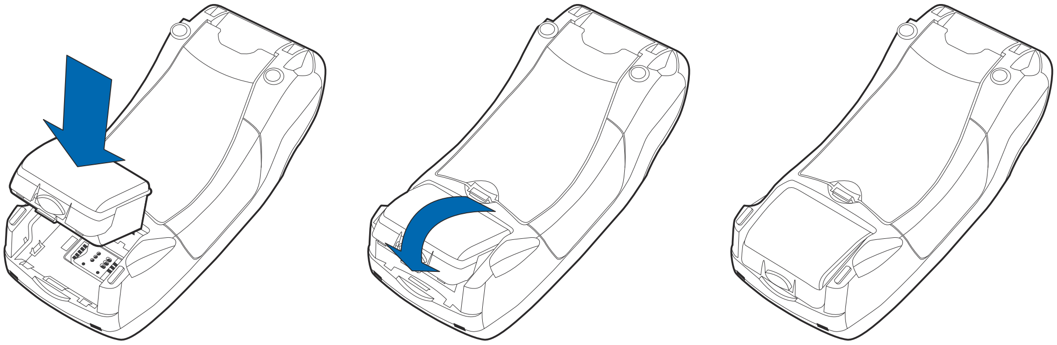


Figure 6 Installing the Smart Battery

Removal

To remove the VX 520 GPRS smart battery, press the locking tab and pull the smart battery from its slot.

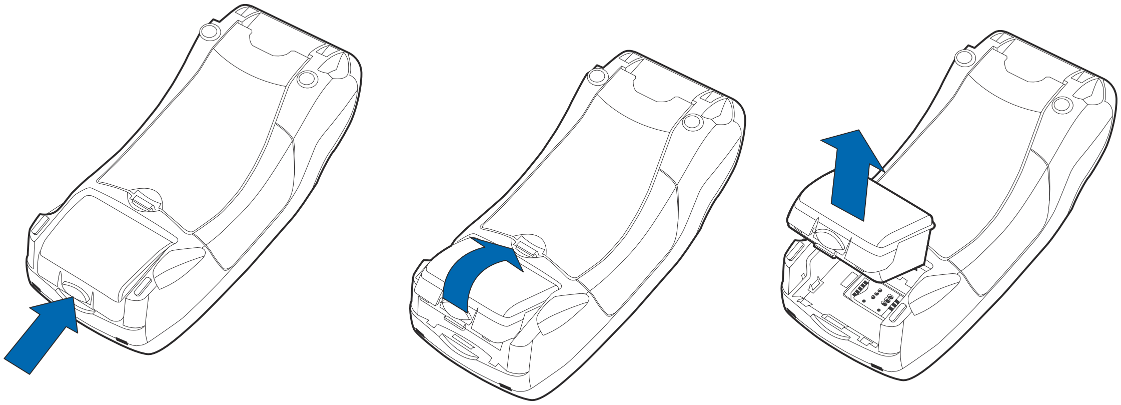


Figure 7 Removing the Smart Battery

Establishing Telephone Line Connections

Connect the telephone cord to the communication port on the terminal, then route it directly to a telephone wall jack (see Figure 8). This is a direct connection and the line is dedicated to the terminal.

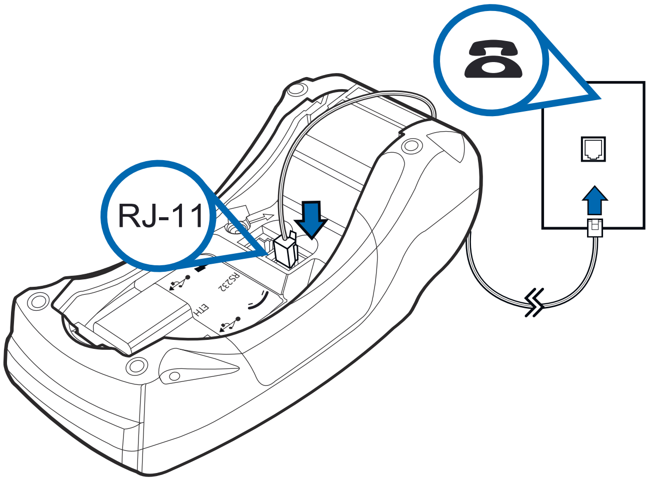


Figure 8 VX 520 Direct Telephone Connection

WARNING

To reduce the risk of fire, use only No. 26AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Installing the Paper Roll in the Printer

A fast, quiet thermal printer is built into the VX 520 terminal. Before you can process transactions that require a receipt or record, you *must* install a roll of thermal-sensitive paper in the printer.

The VX 520 uses a roll of single-ply, thermal-sensitive paper for either the 38 mm- or the 49 mm-diameter version.

NOTE VeriFone ships variants of the VX 520 terminal for different markets. Your terminal may have a different configuration. The basic processes described in this guide remain the same, regardless of terminal configuration.

A pink *out-of-paper* indicator line appears on the edge of the paper approximately 18 in before the end of the roll. After this line appears, there is enough paper remaining on the roll to conclude at least one transaction.

CAUTION Poor-quality paper can jam the printer and create excessive paper dust. To order high-quality VeriFone paper, refer to Accessories and Documentation.

Store thermal paper in a dry, dark area. Handle thermal paper carefully: impact, friction, temperature, humidity, and oils affect the color and storage characteristics of the paper.

Never load a roll of paper with folds, wrinkles, tears, or holes at the edges.

To install a paper roll

1 Hook your finger under the latch and lift up to swing the paper roll cover open (see Figure 9).

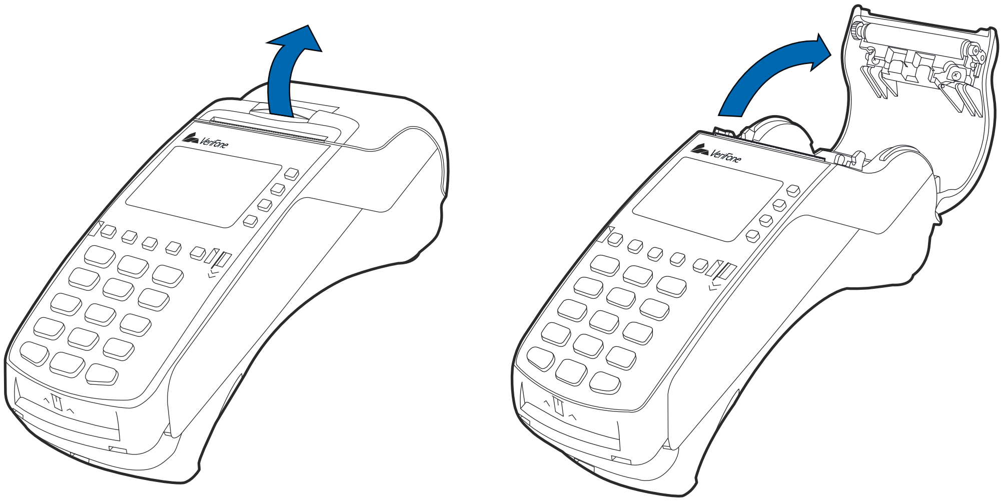


Figure 9 Opening the Printer Cover

2 Remove any partial roll of paper in the printer tray by lifting it up.

3 Loosen the glued leading edge of the new paper roll or remove the protective strip. Unwind the paper roll past any glue residue.

4 Hold the roll so the paper feeds from the *bottom* of the roll.

5 Drop the paper roll into the printer tray.

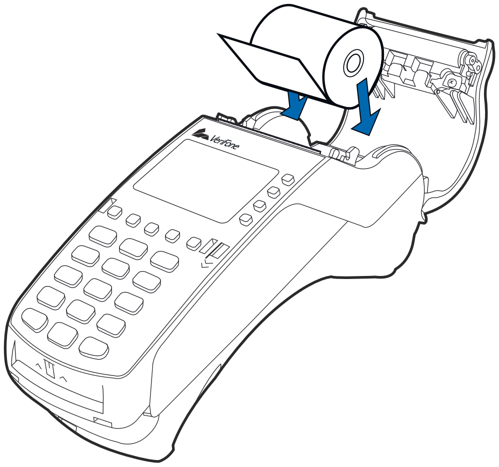


Figure 10 Loading Paper Roll

6 Pull paper up past the glue residue.

7 Close the paper roll cover by gently pressing directly on the cover until it clicks shut, allowing a small amount of paper past the glue residue to extend outside the printer door. (see Figure 11).

CAUTION

To prevent the paper roll cover from damaging the print roller, always gently press down on the printer dust cover to close it.

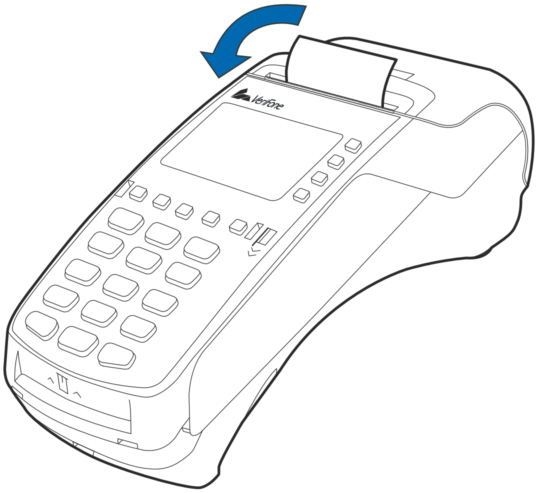


Figure 11 Closing Paper Roll Cover

8 Tear the paper off against the serrated metal strip in the printer.

NOTE

For paper ordering information, refer to Accessories and Documentation.

Installing/ Replacing MSAM Cards

When you first receive your VX 520 terminal, you may need to install one or more MSAM cards or you may need to replace old cards.

CAUTION

Observe standard precautions when handling electrostatically sensitive devices. Electrostatic discharges can damage this equipment. VeriFone recommends using a grounded anti-static wrist strap.

To install or replace MSAMs

1 Remove the power cord from the power outlet.

2 Place the terminal upside down on a soft, clean surface to protect the display from scratches.

3 Press the unlocking button and then lift the rear cover to access the MSAM cardholder panel.

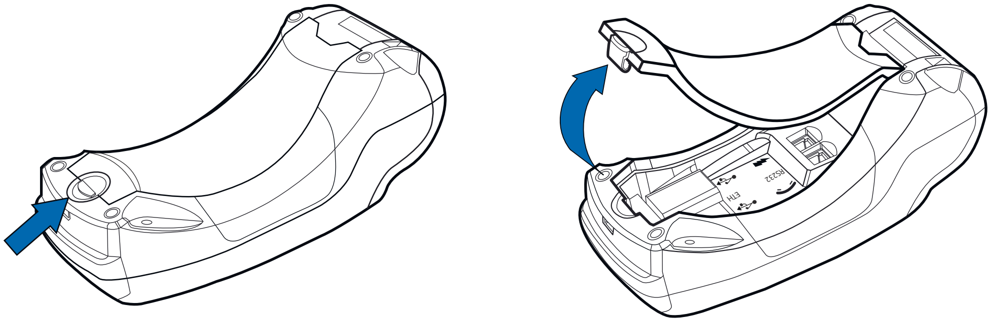


Figure 12 Opening VX 520 Rear Cover

4 Hold the MSAM cardholder panel, grasp firmly and pull upward to expose the MSAM slots.

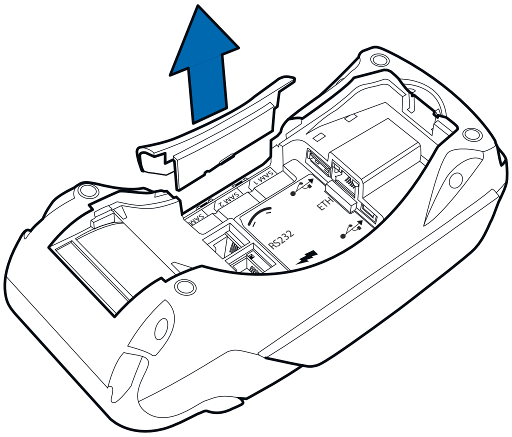


Figure 13 Removing MSAM Cover

4 Remove any previously installed MSAM card by sliding the card from the MSAM cardholder.

5 Install an MSAM card by carefully sliding it into the slot until it is fully inserted.

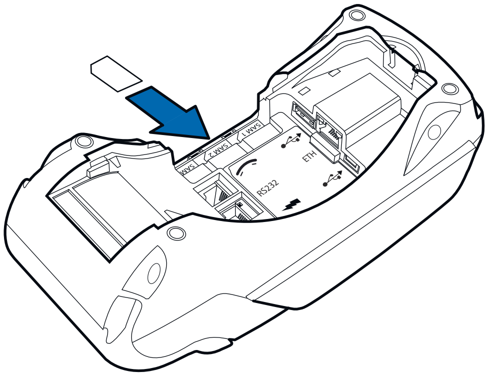


Figure 14 Installing an MSAM Card

NOTE Before inserting the MSAM card, position it as shown in Figure 14, with the card's gold contacts facing down. The cardholder connector base has an image resembling the notched corner of an MSAM card to ensure the card is positioned correctly.

6 Close the MSAM cardholder panel, and then replace the terminal rear cover.

Installing/ Replacing SIM Card (VX 520 GPRS Only)

The VX 520 GPRS terminal supports the installation of a SIM (Subscriber Identity Module) card. Use the following procedure to replace or install a SIM card.

1 Place the terminal upside down on a soft, clean surface to protect the display from scratches.

2 Remove the battery.

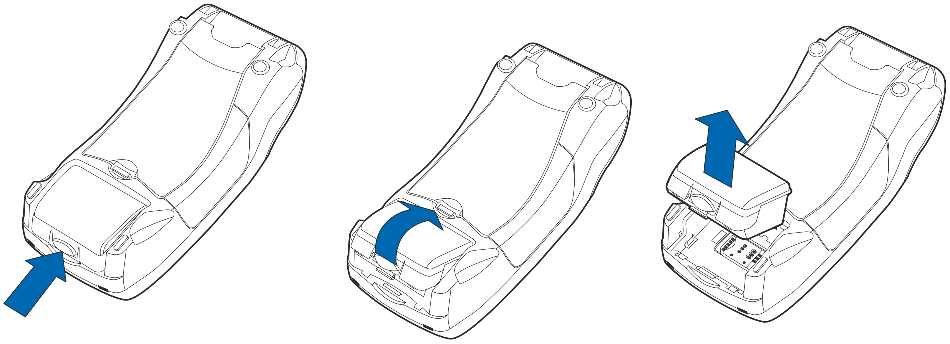


Figure 15 Removing the Smart Battery

3 After removing the battery, you will see the SIM compartment.

4 Insert the SIM into the cardholder.

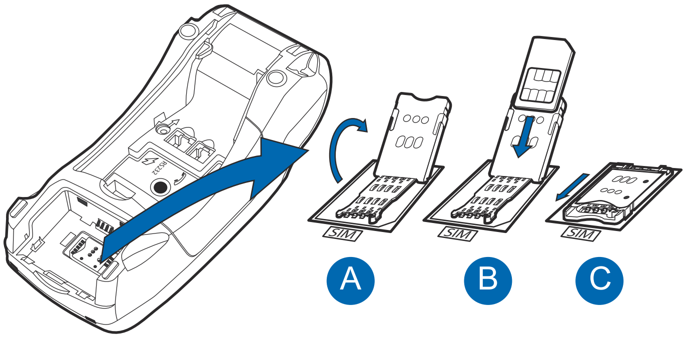


Figure 16 Inserting SIM Card

5 Install the battery.

Connecting Optional Devices

The VX 520 terminal supports some peripheral devices designed for use with electronic point-of-sale terminals.

CAUTION Before connecting any peripheral device, remove the power cord from the terminal and ensure that the green indicator LED is not lit. Reconnect the power cord only *after* you are finished connecting the peripheral device(s). For complete information about peripheral installation and use, refer to the user documentation supplied with those devices.

Different terminals support different devices. For more information about optional devices, please contact your VeriFone distributor.

Optional Device Connections

The VX 520 terminal has a port that can operate either as a PIN Pad port or an RS-232 port, depending on the power source available.

Connecting the PIN Pad or Smart Card Reader to the VX 520

Use the following procedures to connect a PIN Pad or smart card reader.

NOTE When the VX 520 terminal is powered via the corded power supply, the terminal provides 4.0 A at 9.3V DC. This power will drive most VeriFone accessories. Contact your local VeriFone representative for more information.

1. Remove the VX 520 terminal rear cover.
2. Insert the RJ-45-type connector of the PIN Pad or smart card reader into the port of the peripheral device.

   To install a PINpad 101, PINpad 201, or PINpad 1000, position and insert the grommet to secure the cable connection.

   If a cable is not already connected to the smart card reader or PIN Pad, insert the small modular plug on one end of the interface cable into the optional device's modular jack.
3. Insert the larger RJ-45-type connector on the other end of the PIN Pad cable into the PIN Pad serial port on the terminal. Figure 17 provides an example of a smart card reader and PIN Pad connection to the PIN Pad serial port.

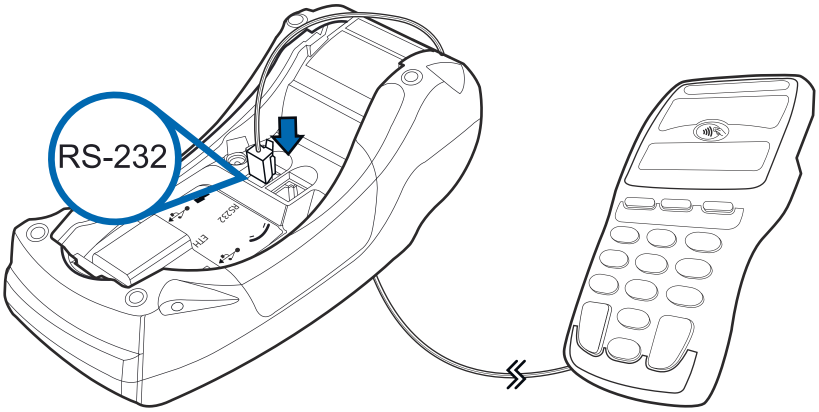


Figure 17 VX 520 Sample PIN Pad Connection

Connecting ECRs to the VX 520

The VX 520 terminal also supports Electronic Cash Registers (ECR). Contact your VeriFone representative or visit the online store at *www.store.verifone.com* for information on these devices.

Figure 18 provides an example of a peripheral connection to the USB port.

CAUTION ECRs require a separate power source. Before connecting a check reader or similar device, remove the power cord from and ensure that the indicator LED is not lit.

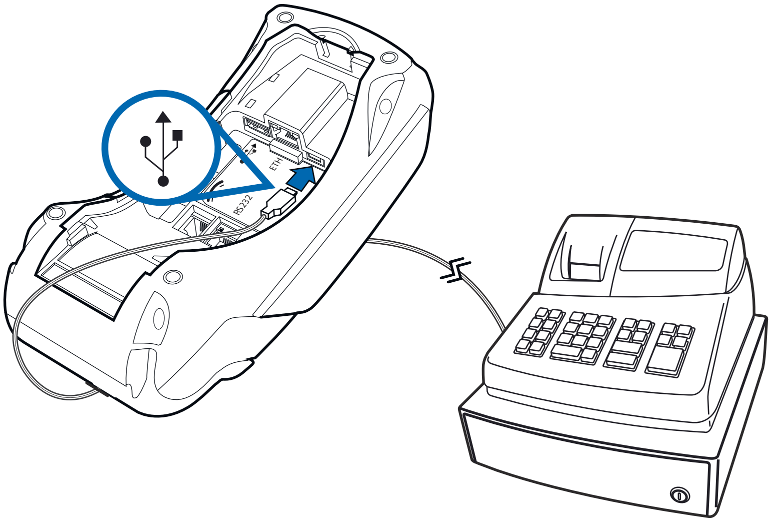


Figure 18 VX 520 Sample ECR Connection

Connecting the Terminal Power Pack

When you have finished connecting optional peripheral(s), you are ready to connect the VX 520 terminal to the provided power source.

CAUTION Using an incorrectly rated power supply may damage the terminal or cause it not to work as specified. Before troubleshooting, ensure that the power supply being used to power the terminal matches the requirements specified on the bottom of the terminal. (See Chapter 7, Specifications, for detailed power supply specifications.) Obtain the appropriately rated power supply before continuing with troubleshooting.

NOTE Plugging in the power pack to a power source automatically turns on the terminal.

To connect the terminal power pack

1. Remove the terminal rear cover to access the power port.
2. Insert the round barrel connector (see Figure 19) into the power port.

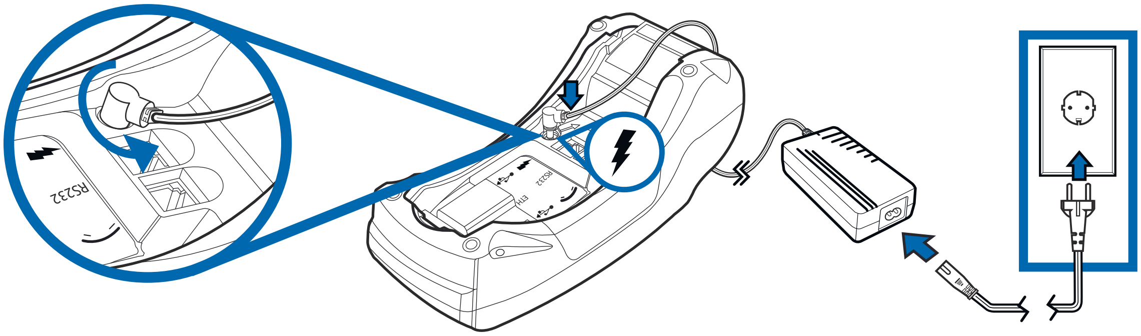


Figure 19 VX 520Power Pack Connection

3. Rotate the power plug counter-clockwise and flush against the side panel to lock the plug in place.
4. Route the cable in the direction of the arrow above the power port and sling the cable over the underside of the thermal paper container.
5. Close the terminal rear cover.
6. Insert the AC power cord into the power pack.

7 Plug the AC power cord into a wall outlet or powered surge protector.

WARNING Do not plug the power pack into an outdoor outlet or operate the terminal outdoors.

Disconnecting the power during a transaction may cause transaction data files not yet stored in terminal memory to be lost.

To protect against possible damage caused by lightning strikes and electrical surges, consider installing a power surge protector.

NOTE VeriFone recommends connecting wall power in the following order:

1 Connect the terminal to the power supply.

2 Connect the power supply to the power cord.

3 Connect the power cord to the wall outlet.

When the terminal has power, the terminal lights are activated and the LED indicator remains lit.

If an application is loaded in the terminal, it starts after the initial VeriFone copyright screen and usually displays a unique copyright screen. If no application is loaded in the terminal, **DOWNLOAD NEEDED** appears on screen after the initial VeriFone copyright screen.

Charging the Smart Battery (VX 520 GPRS Only)

After unpacking your VX 520 GPRS terminal, install the battery and connect the power pack to the unit for 6 hours or until fully charged.

The smart battery has a safety circuit to protect the Li-ion cells from overcharging and over-discharging. If the battery is over-discharged, the safety circuit shuts down the battery. The battery must then be recharged to restore operation.

NOTE The VX 520 GPRS terminal automatically shuts off when the smart battery reaches the critically low charge state. If this occurs, the smart battery must be recharged for a minimum of 1/2 hour before it can power the terminal. It may take several recharge attempts to reset the safety circuit when charging a smart battery that has been discharged below this critical state.

Battery Life

The VX 520 GPRS smart battery can be charged and discharged hundreds of times, but will eventually wear out. When operating times are noticeably shorter than usual, it is time to buy a new battery (see Accessories and Documentation for ordering information).

WARNING Do not dispose of batteries in a fire. Li-ion batteries must be recycled or disposed of properly. Do not dispose of Li-ion batteries in municipal waste sites.

Privacy Shield (Optional)

The privacy shield protects the customers' PIN entry from being seen by the cashier or other customers. The illustration shows an example of a VX 520 with the optional privacy shield.

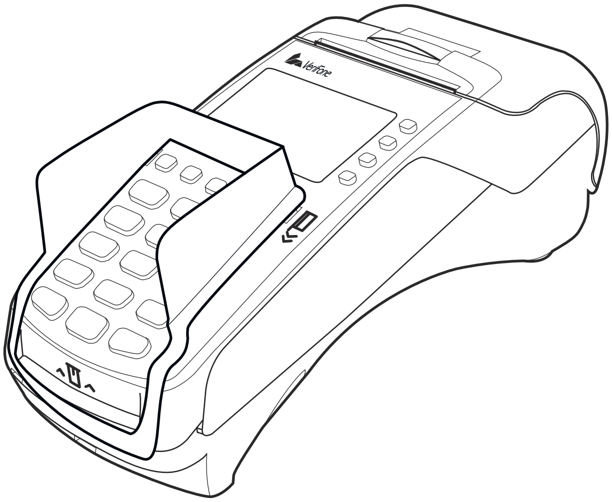


Figure 20 VX 520 Optional Privacy Shield

NOTE Merchants who install the terminal without the privacy shield must ensure the cardholder's privacy when entering his PIN by positioning the terminal away from open view.

Using the Smart Card Reader

The smart card transaction procedure may vary from one application to another. Verify the procedure with your application provider before performing a smart card transaction.

To conduct a smart card transaction

1 Position a smart card with the contacts facing upward (see Figure 21).

2 Insert the smart card into the smart card reader slot in a smooth, continuous motion until it seats firmly.

3 Remove the card only when the application indicates the transaction is complete.

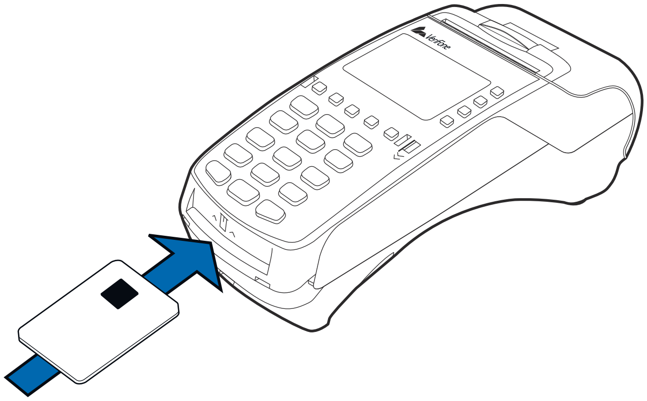


Figure 21 Inserting a Smart Card

CAUTION

Leave the smart card in the card reader until the transaction is complete. Premature card removal will invalidate the transaction.

Using the Magnetic Card Reader

The VX 520 terminal supports credit or debit card transactions.

To conduct a credit or debit card transaction

1 Position a magnetic card with the stripe in the card reader and facing inward, toward the keypad.

2 To ensure a proper read of the magnetic swipe card, the user should insert the magnetic card from the top of the unit, as shown in Figure 22.

3 Swipe the card through the magnetic card reader.

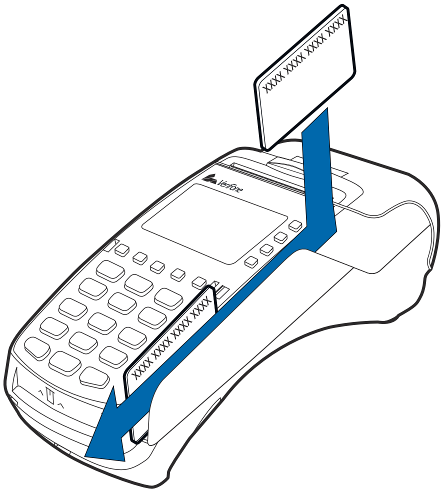


Figure 22 Using the Magnetic Card Reader

CHAPTER 3

Using the Terminal Keys

Before proceeding to other tasks, familiarize yourself with the operational features of the VX 520 terminal keypad to enter data.

This section describes how to use the keypad, which consists of a 12-key Telco-style keypad, three color-coded keys below the keypad, the ALPHA key above the keypad, four ATM-style function keys (F1, F2, F3, and F4) to the right of the display (Figure 23), and four *programmable* function (PF) keys directly above the keypad. Using these keys you can perform all data-entry tasks described in this manual.

The function keys allow you to navigate though the terminal manager menus and select specific operations.

NOTE The PF and ATM-style keys can also be assigned application-specific functions in addition to those assigned to terminal manager operations. These functions are not discussed in this manual.

For added convenience, the keypad is automatically back-lit when you power on the terminal. The backlight may be turned off at any time.

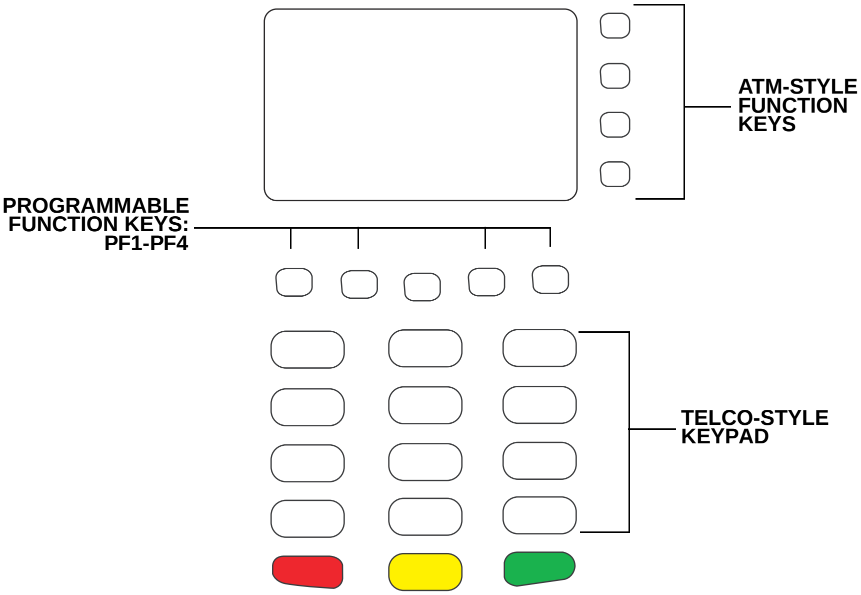


Figure 23 Front Panel Key Arrangement

Data Entry Modes

Before you can use the keys on the front panel to enter ASCII characters, the VX 520 terminal must be in a mode that accepts keyed data entry. There are two terminal operating modes, each enables you to press keys to enter data under specific circumstances:

- **Normal mode:** This is the terminal operating mode where an application program is present in SRAM and currently running.
- **Verix Terminal Manager:** This is a special, password-controlled terminal operating mode for performing a variety of test and configuration procedures that cannot be performed when an application is running.

CAUTION If you enter Verix Terminal Manager while a terminal application is running in normal mode, terminal manager preempts the application and takes control of the display and keyboard. The only way to exit terminal manager is to restart the terminal. For this reason, once you enter terminal manager, you cannot return to the application in the same session.

If you turn on a VX 520 terminal that does not have an application stored in terminal memory, the system prompt **DOWNLOAD NEEDED** appears. You can enter Verix Terminal Manager by simultaneously pressing F2 and F4, and then entering the password (Entering Verix Terminal Manager). Once in terminal manager, you can configure the terminal as required and perform the necessary download.

NOTE Enter Verix Terminal Manager by simultaneously pressing F2 and F4 or the 7 and enter keys. For simplification in this manual, only F2 and F4 are mentioned from this point on.

If you turn on a VX 520 terminal with an application stored in SRAM, the application executes and the terminal automatically enters normal mode. The application then controls how terminal keys—including the PF keys and the ATM-style keys—process transactions and when you can use specific keys to type characters or respond to prompts.

NOTE If an application is in terminal memory, the default system password into Verix Terminal Manager may have changed. If so, you must press the F2 and F4 keys and then enter the required system password to enter terminal manager. The behavior of key entries depends on the specific active terminal manager menu.

Keypad Functions

The keypad is a 13-key arrangement, consisting of a 12-key Telco-style keypad and the ALPHA key (Figure 23).

NOTE The terminal manager functions described in the Entering Verix Terminal Manager section requires you to enter numbers, letters, or symbols using the keypad.

Using the keypad, you can enter up to 50 ASCII characters, including the letters A–Z, the numerals 0–9, and the following 20 special characters: (*), (,), (‘), (“), (-), (.), (#), (%), (:), (!), (+), (@), (=), (&), (space), (;), ($), (_), (\), and (/).

Function Key Descriptions

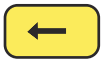
The following are the function keys of the terminal’s keypad.

NOTE The terminal’s operating mode and context determine the specific action performed when you press one of the function keys. The following descriptions are provided solely to acquaint you with some general characteristics of these function keys before presenting more detailed terminal manager procedure descriptions.

Cancel Key

Pressing the cancel key in normal mode—when the terminal’s application is loaded and running—usually has the same effect as pressing the Esc (escape) key on a PC. That is, it terminates the current function or operation.

In terminal manager, use cancel to perform a variety of functions. The most common use of cancel in terminal manager is to exit a terminal manager submenu and return to the main Verix Terminal Manager menu. The specific effect of pressing the cancel key depends on the currently active terminal manager menu.



Backspace Key

In normal mode, the backspace key is commonly used to delete a number, letter, or symbol on the terminal’s display screen. Press backspace one time to delete the last character typed on a line. To delete additional characters, moving from right-to-left, press backspace once for each character or hold down backspace to delete all characters in a line.

In Verix Terminal Manager, the specific effect of pressing the backspace key depends on the currently active terminal manager menu.

ALPHA Key

In normal mode, the ALPHA key enables you to enter one of the two or more characters or symbols assigned to individual keys on the 12-key Telco-style keypad (note that this is in normal mode and is application-specific).

Use the ALPHA key to enter up to 50 different ASCII characters through the following procedure:

1. Press the key on the 12-key keypad that shows the desired letter or symbol (for example, press 2 to type 2, A, B, or C). The number (1–9 or 0) or the symbol (* or #) pressed now displays.
2. Press ALPHA once to display the first letter. Continuing our example, press the 2 key, then ALPHA to display the letter A.
3. Press ALPHA as many times as required to display the desired character. For example, press 2 to display the number 2; press ALPHA once to display the letter A, twice to display B, or three times to display C. If you press ALPHA one more time, the number 2 displays.

NOTE If you firmly press and hold down one of the keys on the 12-key keypad without using ALPHA, the same character repeats until you stop pressing the key. For example, if you press 2 and hold it down, “2222222...” appears on the display.

If two or more characters display on the VX 520 screen, pressing ALPHA changes the last character on the line to the next letter, number, or symbol in the key sequence.

Table 3 provides additional examples of how to use the ALPHA key to select ASCII characters from the 12-key Telco-style keypad.

Table 3 Example ALPHA Key Entries

Desired Character	Press Keys
2	2
A	2 ALPHA
S	7 ALPHA ALPHA ALPHA
!	# ALPHA
Space	0 ALPHA ALPHA
Comma (,)	* ALPHA
Plus sign (+)	0 ALPHA ALPHA ALPHA

Table 4 lists all the ASCII characters you can type using the ALPHA key and the Telco keypad.

Table 4 Using ALPHA and the 12-Key Keypad

Key to Press	Without Pressing ALPHA	Press ALPHA One Time	Press ALPHA Two Times	Press ALPHA Three Times
1 QZ.	1	Q	Z	.
2 ABC	2	A	B	C
3 DEF	3	D	E	F
4 GHI	4	G	H	I
5 JKL	5	J	K	L
6 MNO	6	M	N	O
7 PRS	7	P	R	S
8 TUV	8	T	U	V
9 WXY	9	W	X	Y
0 -SP	0	–	[space]	+
* ,′ "	*	,	′	"
#[a]	#	!	:	;

[a] The # key also supports eight additional characters: (@), (=), (&), (/), (\), (%), ($), and (_). To enter @, press # once, then ALPHA four times. To enter =, press # once, then ALPHA five times. To enter &, press # once, then ALPHA six times. To enter /, press # once, then ALPHA seven times. To enter \, press # once, then ALPHA eight times. To enter %, press # once, then ALPHA nine times. To enter =, press $ once, then ALPHA ten times. To enter _, press # once, then ALPHA eleven times.

Enter Key

In normal mode, the enter key is generally used the same as the enter key on a PC, that is, to end a procedure, confirm a value or entry, answer “Yes” to a query, or select a displayed option.

In Verix Terminal Manager, press the enter key to begin a selected procedure, step forward or backward in a procedure, and confirm data entries. The specific effect of the enter key depends on the currently active terminal manager menu.

Programmable Function (PF) Key Descriptions

The row of four PF keys directly above the keypad (Figure 23) from left-to-right are referred to as PF1, PF2, PF3, and PF4. These keys can be assigned application-specific functions. Because such functions are often unique and can vary greatly between applications, they are not discussed in this manual.

NOTE

For questions regarding application-specific PF-key functions, please contact your application service provider.

The PF keys are also used to navigate through the Verix Terminal Manager menus. These keys are functioning when arrows appear in the display screen above the associated key, indicating that the keys can be used as follows:

- PF1 ↑ Move to the previous menu or screen
- PF2 ↓ Move to the next menu or screen
- PF3 ↑ Scroll up menu options
- PF4 ↓ Scroll down menu options

CHAPTER 4

Verix Terminal Manager

This chapter describes a category of terminal functions called *terminal manager operations*.

- Press F2 and F4 at the same time and enter the password to invoke Verix Terminal Manager. See Entering Verix Terminal Manager.
- Assign files and applications to groups for access control. See File Groups.
- Use the system and file group passwords to secure applications and information on the terminal. See Passwords.
- Use the terminal manager menus and submenus to configure terminals; download, test, and debug applications; and perform routine tests and terminal maintenance. See Verix Terminal Manager Menus.

Verix Terminal Manager is used exclusively by those responsible for configuring, deploying, and managing on-site VX 520 terminal installations.

When to Use Verix Terminal Manager

Use the Verix Terminal Manager functions to perform different subsets of related tasks:

- **Application programmers** configure a development terminal, download development versions of the VX 520 application program, then test and debug the application until it is validated and ready to be downloaded to other terminals.
- **Deployers of terminals to end-user sites** perform the specific tasks required to deploy a new VX 520 terminal on-site, including configuring the terminal, downloading application software, and testing 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.

To perform the subset of tasks that corresponds to a job, select the appropriate terminal manager menu(s) and execute the corresponding procedure(s).

Local and Remote Operations

The terminal manager operations available on a VX 520 terminal can be divided into the following two categories or types:

- **Local operations** address a stand-alone terminal and do not require communication or data transfers between the terminal and another terminal or computer. Perform local terminal manager operations to configure, test, and display information about the terminal.
- **Remote operations** require communication between the terminal and a host computer (or another terminal) over a telephone line or a cable connection. Perform remote terminal manager operations to download application software to the terminal, upload software from one terminal to another, perform diagnostics over a telephone line, or update the operating system.

This chapter contains descriptions on how to perform local terminal manager operations. For information on performing remote operations, such as downloads, refer to Chapter 6, Performing Downloads.

Verifying Terminal Status

The VX 520 terminal you are using may or may not have an application program running on it. After you have set up the terminal (Chapter 2, Terminal Setup) and the terminal is turned on, use the following guidelines to verify terminal status regarding software and current operating mode:

- If no application program is loaded into terminal RAM or flash, the message **DOWNLOAD NEEDED** appears on the display screen. From this point, press F2 and F4 to access terminal manager and perform the required download.

NOTE

You can enter Verix Terminal Manager either by simultaneously pressing F2 and F4 or by pressing the 7 and Enter ↵ keys. For simplification in this manual, only F2 and F4 are mentioned from this point on.

- If an application program is loaded into terminal RAM or flash, an application-specific prompt appears. The application is running and the terminal is in normal mode. If all installation steps are complete, the terminal can process transactions.

TIP

If necessary, you can press F2 and F4 simultaneously to interrupt the application and enter Verix Terminal Manager.

Entering Verix Terminal Manager

To prevent unauthorized use of the Verix Terminal Manager menus, the VX 520 terminal OS requires a system password each time you enter terminal manager. To access the Verix Terminal Manager password entry screen, simultaneously press the F2 and the F4 keys.The default, factory-set system password is “1, Alpha, Alpha, 66831.” After entering the correct password, the terminal enters the terminal manager and displays the first terminal manager main menu, **VERIX TERMINAL MGR MENU 1.** You can now toggle through all three terminal manager main menus by pressing ↵ or the PF1 and PF2 keys.

File Groups

The VX 520 Verix operating system implements a file system in RAM and in flash memory. Files are assigned to one of the groups for access control. Groups are similar to computer directories---in that different applications can be stored in separate file groups, just like different computer applications can be stored in separate directories. Groups are referred to as *Group n* or *GIDn* throughout this manual.

Each group is protected by a separate password, and each has a separate `CONFIG.SYS` file. The following rules apply to the VX 520 file group system:

- The primary application must be downloaded into Group 1.
- On terminal power up and after a restart, the terminal defaults to Group 1 as the controlling group.
- Group 1 applications have access to files stored in *all* groups. Other applications can reside in Groups 2–14.
- Applications in a group other than Group 1 have access only to themselves and files stored in Group 15.
- Group 15 is globally accessible, making it an ideal location for files shared by multiple applications, such as shared libraries.
- File Groups 1–15 are empty until they are filled through a download to the VX 520 terminal.

For more information on managing file groups, refer to the *Verix V Operating System Programmers Manual* (VPN 23230).

Passwords

Handle passwords as you would PC passwords.

System Password

When you key in the system password to enter terminal manager, an asterisk (*) appears for each character you type. These asterisks prevent your password from being seen by an unauthorized person. You can use the ALPHA key to change the characters or symbols you enter. This does not cause additional asterisks to appear.

NOTE

Some application program downloads automatically reset the system password. If your system password no longer works, check if a download has changed your password.

File Group Passwords

The default password for each file group is “1, Alpha, Alpha, 66831” (without the quotation marks).

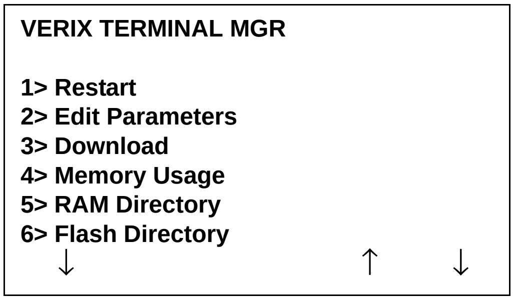
NOTE

This default password is the same as the password for Verix Terminal Manager entry.

Verix Terminal Manager Menus

The three main terminal manager menus are listed in the following table.

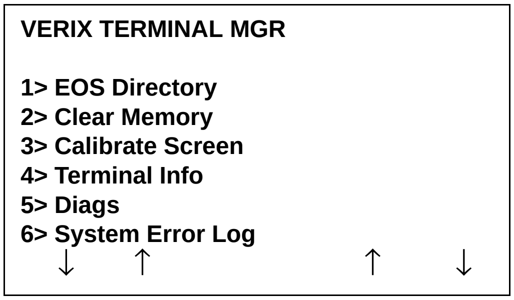
Table 5 Verix Terminal Manager Menus



```
VERIX TERMINAL MGR

1> Restart
2> Edit Parameters
3> Download
4> Memory Usage
5> RAM Directory
6> Flash Directory
  ↓                    ↑     ↓
```

Figure 24 Menu 1

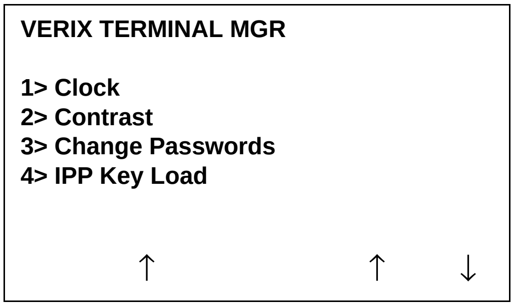


```
VERIX TERMINAL MGR

1> EOS Directory
2> Clear Memory
3> Calibrate Screen
4> Terminal Info
5> Diags
6> System Error Log
  ↓    ↑               ↑     ↓
```

Figure 25 Menu 2

Table 5 Verix Terminal Manager Menus



VERIX TERMINAL MGR

1> Clock
2> Contrast
3> Change Passwords
4> IPP Key Load

↑ ↑ ↓

Figure 26 Menu 3

To return to a previous menu, press the PF1 key (the leftmost key above the keypad). To go to the next menu, press the PF2 key. To return to the main terminal manager menu and cancel any changes, press the cancel key.

To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press the enter key. Use the PF4 key to scroll up the menu options.

When performing downloads or operations that change or clear files, the password for each file group is required. The password is only required once per session per file group.

Verix Terminal Manager Procedures

The procedures in this section explain how to use each of the terminal manager menus listed in Table 5. Each procedure description starts at a main Verix Terminal Manager menu. Each procedure takes you step-by-step through a complete terminal manager operation in the following sequence:

1. When the main terminal manager menu appears, select an operation by pressing the corresponding number on the keypad or scroll down to the option using the PF3 button then press the enter key. Use the PF4 key to scroll up the menu options.
2. Complete the operation.
3. Return to the main Verix Terminal Manager menu.

Procedure descriptions are arranged in the following table:

Table 6 Procedural Description Example

Display	Action
Screen displayed	Action required

Table 6 Procedural Description Example

Display	Action
Submenu Row	
Screens displayed on submenu selection	Action required

The Display column in Table 6 indicates what appears on the terminal display screen at each step of the procedure. Please note the following conventions used in this column:

- If a prompt or message appears on the screen exactly as it is described, it is shown in Arial bold font and ALL CAPS. For example, **DOWNLOAD NEEDED**.
- If text is enclosed in parentheses, the actual text or message may vary depending on the terminal version you have. For example, in (Application Prompt), the normal font is used and text is typed in initial caps.

The *Action* column provides a procedural description that:

- Describes the current step and context of the procedure.
- Indicates the entries to perform using the keypad in response to a prompt or message.
- Provides additional explanations or information about the steps of that particular terminal manager menu.

A submenu row indicates a specific menu evoked from a main menu screen. A description of that screen and procedure immediately follows the submenu row.

The following keys have the same function on all submenus:

↵
- Press the enter key to save changes from a submenu and return to the menu screen.

X
- Press the cancel key to exit any submenu without saving changes.

Enter and Exit Verix Terminal Manager

To enter terminal manager after you have turned on the VX 520 terminal, follow the procedure described in Table 7.

NOTE

On successful completion, some operations automatically exit terminal manager and restart the terminal. Other operations require that you exit terminal manager and restart the terminal. To manually exit terminal manager, select **1> RESTART** in **VERIX TERMINAL MGR.**

Table 7 Enter Verix Terminal Manager

Display	Action
VERIFONE VX 520 **QT52E20K** **02/26/2010 Verix** **COPYRIGHT 1997-2010** **VERIFONE** **ALL RIGHTS RESERVED**	At startup, the terminal displays a copyright notice screen that shows the terminal model number, the OS version of the VX 520 stored in the terminal's flash memory, the date the firmware was loaded into the terminal, and the copyright notice. This screen appears for three seconds, during which time you can enter Verix Terminal Manager by simultaneously pressing F2 and F4. You can extend the display period of this screen by pressing any key during the initial three seconds. Each keypress extends the display period an additional three seconds.
VERIFONE VX 520 **QT52E20K** **02/26/2010 Verix** **COPYRIGHT 1997-2010** **VERIFONE** **ALL RIGHTS RESERVED**	If some other certificate is loaded by a reseller (e.g., bank), the fourth line is left blank.
VERIFONE VX 520 **QT52E20K** **02/26/2010 Verix** ****TAMPER**** **COPYRIGHT 1997-2010** **VERIFONE** **ALL RIGHTS RESERVED**	If an attempt to break into the terminal's system has been made, the message ****TAMPER**** is displayed in place of the certificate. The terminal will remain in this state until the condition has been remedied.
<application prompt>	If an application already resides on the terminal, an application-specific prompt is displayed. Otherwise, an error message is displayed. For more information on startup errors, see STARTUP ERRORS.

Table 7 Enter Verix Terminal Manager

Display	Action
TERMINAL MGR ENTRY **Please Enter Password** ______________	If an application prompt appears and you choose to enter terminal manager, you are prompted to type the system password. Use the default password “1, Alpha, Alpha, 66831”. Use ← to delete the entry and correct any mistakes. If you enter an incorrect password, the terminal exits the **TERMINAL MGR ENTRY** screen. Verify your password and reenter it. To quit this operation and return to the application prompt or **DOWNLOAD NEEDED** screen, press ✕.
VERIX TERMINAL MGR **1> Restart** **2> Edit Parameters** **3> Download** **4> Memory Usage** **5> RAM Directory** **6> Flash Directory** ↓ ↑ ↓	The first of three **VERIX TERMINAL MGR** menus is displayed. To toggle through to the other two menus, press the PF1 and PF2 keys. To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press the enter key. Use the PF4 key to scroll up the menu options.

Menu 1

In this menu you can restart the terminal, edit parameters, download terminal software updates, check memory usage and availability, as well as view the contents of RAM and Flash directories.

NOTE

Before performing a download to flash memory in an initialized terminal (one that contains an application), reclaim all available flash space. Unused RAM/flash and duplicate RAM/flash information are automatically reclaimed after a doing FULL download. To reclaim this space, perform a merge operation from terminal manager (refer to the procedure 1> EOS DIRECTORY). This operation makes all files in flash memory contiguous. You must also clear some or all flash memory if your terminal does not have enough space for the impending download.

CAUTION

Some application program downloads automatically reset the system password.

Edit Keyed Files

A *keyed* file is a collection of individual records that contain data and are identified by unique search keys. You can edit the data directly from the terminal keypad using the terminal's built-in keyed file editor. Each record has two parts: *parameter* and *value*. A parameter identifies the record while value is the information assigned to a specific parameter.

NOTE A parameter has a maximum length of 32 characters and its value has a maximum length of 128 characters. In some documents, 'parameter' is also sometimes referred to as 'key'

For example, `*ZT` is the terminal ID used by VeriCentre to identify which downloads should be sent to the terminal. The value for the key is the actual application ID number. By entering `*ZT` using the editor, the terminal can quickly locate the application serial ID number. You can also use the PF keys to scroll through the list of parameters instead of entering the characters `*ZT` through the keypad. Press ↵ to toggle between a parameter and its value.

NOTE For a complete list of the ASCII characters supported by the VX 520 series, as well as their decimal and hexadecimal equivalents, please refer to Appendix C.

CONFIG.SYS: Protected and Non-protected Records

The concept of protected and non-protected records applies only to the `CONFIG.SYS` files in your terminal. Protected records are those with search keys beginning with an asterisk (`*`) or a pound/hash symbol (`#`).

Prior to a download, the recommended procedure is to clear RAM files. Protected records in the file Group 1 `CONFIG.SYS` file are retained in a full application download and when RAM is cleared. Non-protected records, all other `CONFIG.SYS` parameters/files not beginning with the symbols '`*`' and '`#`', and records of other files are deleted when RAM is cleared.

Editing CONFIG.SYS with an External Editor

You can create and edit the `CONFIG.SYS` files of VX 520 applications through an IBM PC-compatible computer when you download files to the terminal. For more information on editing an application's `CONFIG.SYS` file, refer to the *VeriCentre Reference Manual* and the *Verix V Operating System Programmers Manual* (VPN 23230), or contact your local VeriFone representative.

For more information about using VeriCentre Download Management Module in client/server installations, please contact your local VeriFone representative.

Table 8 Verix Terminal Manager Menu 1

Display	Action
VERIX TERMINAL MGR **1> Restart** **2> Edit Parameters** **3> Download** **4> Memory Usage** **5> RAM Directory** **6> Flash Directory** ↓ ↑ ↓	To restart the terminal, select **1> RESTART**. To edit the `CONFIG.SYS` or another keyed file, select **2> EDIT PARAMETERS**. (For more information, refer to the Edit Keyed Files section that follows this main menu description.) To download an application to your terminal, select **3> DOWNLOAD**. To check the memory used and available memory allocation, select **4> MEMORY USAGE**. To view the contents of the RAM directory, select **5> RAM DIRECTORY**. To view contents of Flash memory, select **6> FLASH DIRECTORY**. To toggle to Verix Terminal Manager menu 2, press PF1.
2> EDIT PARAMETERS	
Select group **GROUP ID: nn** **APP: <*APNAME or application or EMPTY>** ↑ ↓	To search for keyed records in a particular file group, type the appropriate group number and press ↵. You can also press PF1 or PF2 to scroll through the group ID numbers to find the application you are looking for. If you cannot locate a particular keyed record, it may be stored in another file group. Press ← to delete the number and type a new entry.
VERIX TERMINAL MGR EDIT GROUP nn PASSWORD __________	**Note:** If you have not previously entered a group's password in this session, the terminal prompts for the group's password prior to editing variables. To continue, enter the required password. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↵. Verify your password and reenter it.
TERMINAL MGR EDIT Gnn **FILE CONFIG.SYS_** __________	To edit the `CONFIG.SYS` file, press ↵. You can also create a new keyed file or edit an existing one. First, press ← to clear any previous filename from the display screen. Then, type a filename and press ↵. Skip to 2> EDIT PARAMETERS 1> ADD VARIABLE / 1> NEW or 2> EDIT PARAMETERS 3> EDIT for the next procedures.

Table 8 Verix Terminal Manager Menu 1

Display	Action
GID nn: *APNAME **FILE CONFIG.SYS** **<curr value>** **1> Add Variable**	To create a new variable, select **1> ADD VARIABLE**.
GID nn: *APNAME **Parameter:** **nn** **Value:** **nn** **1> New 3> Edit** **2> Find 4>Clear**	If the GID contains a keyed file, you have the option to create a new file (**1> NEW**), find files (**2> FIND**), edit (**3> EDIT**) or clear files (**4> CLEAR**). **Note:** Use **2> FIND** to search for a keyed file. You can then edit or delete the file. If the specified parameter name does not exist, it can be added as a new file. After completing your edit operations, press x to return to the first **VERIX TERMINAL MGR** menu.
2> EDIT PARAMETERS 1> ADD VARIABLE / 1> NEW	
GID nn: *APNAME **PARAMETER:** ____________________ ____________________	After selecting **1> ADD VARIABLE** or **1> NEW**, enter a parameter name and press ↵ .
GID nn: *APNAME **PARAMETER:** **<parm name>** **VALUE:** ________________________ ________________________	Enter a value for the new parameter and press ↵ . Press x to cancel creating a new variable.

Table 8 Verix Terminal Manager Menu 1

Display	Action
2> EDIT PARAMETERS 2> FIND	
GID nn: *APNAME **PARAMETER:** ____________________ ____________________	After selecting **FIND**, enter the parameter name to locate and press ↩ . The current value of the parameter is displayed on the next screen. Press ↩ to select the parameter and go back to the parameter editor.
GID nn: *APNAME **PARAMETER:** **<parm name>** **VALUE:** **<curr value>** ______________ __________________________ **1> New 3> Edit** **2> Find 4>Clear** ↑ ↓	If the entered parameter name cannot be found, **<parm name> NOT FOUND** appears. Select **1> CANCEL** to go back to the parameter editor or **2> ADD VARIABLE** to add the entered parameter name as a new variable. Press ✕ to cancel locating a variable.
2> EDIT PARAMETERS 3> EDIT	
GID nn: *APNAME **PARAMETER:** **<parm name>** **VALUE:** **<curr value>** ______________ __________________________	After selecting **3> EDIT**, enter the new value for the variable. To correct a mistake, press ← and type the new entry. After completing your edits, press ↩ . Press ✕ to cancel editing a variable.
2> EDIT PARAMETERS 4> CLEAR	
GID nn: *APNAME **DELETE PARAMETER:** **<parm name>** **<curr value>** **1> Yes** **2> No** ↑ ↓	After selecting **4> CLEAR**, select **1> YES** to continue or **2 >NO** to cancel the deletion.
3> DOWNLOAD	
VERIX TERMINAL MGR **GROUP ID: nn**	Type the number of the file group (1 for the primary application; between 1–15 for other applications) into which to perform the download. (Refer to Chapter 6 for detailed download instructions and information.) After you type a file group number, press ↩ .

Table 8 Verix Terminal Manager Menu 1

Display	Action
VTM DOWNLOAD MGR Gnn 1> Single-app 2> Multi-app	Select to download single or multiple applications.
VTM DOWNLOAD MGR Gnn 1> Full dnld 2> Partial dnld	Select full or partial download. A full download will delete all data on the group's RAM and flash memory. The flash memory is then merged before downloading new data. A partial download only adds new files to the group's memory. If a downloaded file is identical to an existing file in the memory, the existing file is replaced. For detailed download instructions and information, see Chapter 6.
VERIX TERMINAL MGR DOWNLOAD Gnn **** WARNING **** ALL FILES WILL BE CLEARED FROM GROUP nn	If you selected **FULL** on a single application download, a screen will appear warning you that all existing files in the selected group will be deleted. Press F3 to cancel or F4 to continue downloading an application.
VERIX TERMINAL MGR DOWNLOAD Gnn CLEAR Application FROM GROUP nn?	If you selected **FULL** on a multiple application download, you will be prompted to clear the existing application on the currently selected group. Select **YES** to continue or **NO** to cancel downloading applications.
VERIX TERMINAL MGR DOWNLOAD Gnn **** WARNING **** CONFIRM DELETION FOR Application	If you selected **YES** from the previous screen, a confirmation screen appears. Select **YES** to confirm or **NO** to cancel the deletion.

Table 8 Verix Terminal Manager Menu 1

Display	Action
VERIX TERMINAL MGR **DOWNLOAD Gnn** **GIDS TO REASE:** **1,2,4**	If a FULL multiple download has been previously done, this screen appears instead of the previous two screens. This screen lists all the erased GIDs on the previous download. Select **CONTINUE** to erase all RAM and flash memory. The flash memory is then merged.
VTM DOWNLOAD MGR Gnn **1> Modem** **2> COM1** **3> COM2** **4> SD Card** **5> Memory Stick** **6> TCPIP** ↓ ↑ ↓	Select a download mode. Press the PF1 key to view more system download modes. An application that supports the TCP stack *must* be loaded to use the **6> TCPIP** option. If no application can be found, an error message appears. **Note:** `*ZTCP` is the name of the application that implements the TCP/IP functionality (e.g., `*ZTCP=TCPAPP.OUT` in the `CONFIG.SYS` file). Verix Terminal Manager runs the `TCPAPP.OUT` when you select **6> TCPIP**. To return to the main menu without saving your selection, press ✕.
VTM DOWNLOAD MGR Gnn **1> USB Dev** **2> COM6** ↑ ↑ ↓	
VTM DOWNLOAD MGR Gnn ***ZP Host Phone num** _______________ _______________	If you selected **1> MODEM** and `*ZP` (host phone number) is not defined, you must enter valid phone number (up to 32 characters long) and press ↵.
VTM DOWNLOAD MGR Gnn **Unit Receive Mode** **WAITING FOR DOWNLOAD**	Choose **2> COM1** to download via the COM 1 port. To return to the main menu without saving your selection, press ✕.

Table 8 Verix Terminal Manager Menu 1

Display	Action
VTM DOWNLOAD MGR Gnn **Unit Receive Mode** **WAITING FOR DOWNLOAD**	Choose **3> COM2** to download via the COM 2 port. To return to the main menu without saving your selection, press x.
Unavailable	Select **4> SD CARD**to download from a stored digital (SD) card. To return to the main menu without saving your selection, press x.
Unavailable	Press **5> MEMORY STICK** to download from a memory stick. To return to the main menu without saving your selection, press x.
No *ZTCP Variable and no VxEOS	Selected **6> TCPIP** to download from your TCPIP connection. An application that supports the TCP stack *must* be loaded to use the **6> TCPIP** option. If no application can be found, the error message appears. **Note:** `*ZTCP` is the name of the application that implements the TCP/IP functionality (e.g., `*ZTCP=TCPAPP.OUT` in the `CONFIG.SYS` file). Verix Terminal Manager runs the `TCPAPP.OUT` when you select **6> TCPIP**.
VTM DOWNLOAD MGR Gnn **Unit Receive Mode** **WAITING FOR DOWNLOAD**	Choose **1> USB DEV** in Menu 2 of the Download screen to download using the USB connection. To return to the main menu without saving your selection, press x.

Table 8 Verix Terminal Manager Menu 1

Display	Action
Unavailable	Choose **2> COM6** to download via the COM 6 port. To return to the main menu without saving your selection, press ✕.
VTM DOWNLOAD MGR Gnn ***ZP HOST** **ADDR (IP:PORT)** ____________________ ____________________	If you selected **6> TCPIP** and `*ZP` (TCP address) is not defined, you must enter a valid TCP address (up to 40 characters long including the colon and port number) and press ↵. **Note:** Alternatively, you can enter the address and port on separate screens. Press the PF2 key, enter the address and press ↵. Then, press the PF3 key, enter the port number and press ↵. terminal manager then inserts the colon between the address and port number. Press ↵ once the TCP address is set.
VTM DOWNLOAD MGR Gnn ***ZP HOST ADDR** ____________________ ____________________	
VTM DOWNLOAD MGR Gnn ***ZP HOST ADDR PORT** ________	
VTM DOWNLOAD MGR Gnn ***ZT TERMINAL ID** _______________	If `*ZT` (terminal ID used by VeriCentre) is not defined, you must enter a valid terminal ID (up to 15 characters long) and press ↵.

Table 8 Verix Terminal Manager Menu 1

Display	Action
VTM DOWNLOAD MGR Gnn ***ZA APPLICATION ID** ______________	If `*ZA` (application ID) is not defined, you must enter a valid application ID (up to 10 characters long) and press ↩.
VTM DOWNLOAD MGR Gnn ***ZA= nnnn** ***ZP= nnnn** ***ZR= nnnn** ***ZT= nnnn** **1> Edit** **2> Start**	You can view the specified values on the confirmation screen. Select **1> EDIT** to go back and modify the specifications or **2> START** to begin the download.
VTM DOWNLOAD MGR Gnn **GID: nn** **APP ID: nnnn** **STATUS: DOWNLOADING** *******_______	If you selected **1> MODEM** or **6> TCPIP** , this screen appears. If the download is successful, the message **DOWNLOAD DONE** is displayed. If an error occurs during connection or download, an error message is displayed. For more information on downloading errors, see DOWNLOADING ERRORS.
VTM DOWNLOAD MGR Gnn **UNIT RECEIVE MODE** *******_______	If you selected **2> COM1** or **3> COM2** , a line of asterisks appears that shows the percentage of completion. Each asterisk equals approximately 10% of the download. You can cancel a download in progress by pressing x. Doing so restarts the terminal.
VTM DOWNLOAD MGR **GROUP n PASSWORD** __________	**Note:** If you have not previously entered a group's password in this session, the terminal prompts for the group's password prior to downloading applications. To continue, enter the required password. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↩. Verify your password and reenter it.

Table 8 Verix Terminal Manager Menu 1

Display	Action
4> MEMORY USAGE	
MEMORY USAGE **RAM FILES nnnn** **INUSE nnnn** **AVAIL nnnn** ↓	This screen displays how much RAM is used and how much is available. • **INUSE** - Closest estimate of used memory (in KB). • **AVAIL** - Lowest number of free memory (in KB). Select the PF1 key to view Flash memory usage.
FLASH FILES nnnn **INUSE nnnn** **AVAIL nnnn** ↑	This screen displays how much flash memory is used and how much is available. • **INUSE** - Closest estimate of used memory (in KB). • **AVAIL** - Lowest number of free memory (in KB). Select the PF2 key to return to the RAM usage screen.
5> RAM DIRECTORY	
VERIX TERMINAL MGR **Group ID: nn**	Type the number of the file group (1 for the primary application; between 1–15 for other applications). After you type a file group number, press ↵ .
RAM DIRECTORY Gnn **I: CONFIG.SYS** **nn MM/DD/YYYY -** **PRINT**	This screen displays the RAM information. Press ↵ . to print the information.
6> FLASH DIRECTORY	
VERIX TERMINAL MGR **Group ID: nn**	Type the number of the file group (1 for the primary application; between 1–15 for other applications). After you type a file group number, press ↵ .

Table 8 Verix Terminal Manager Menu 1

Display	Action
FLASH DIRECTORY Gnn I: CONFIG.SYS nn MM/DD/YYYY - PRINT	This screen displays the Flash memory information. Press ↵. to print the information.

Menu 2

In this menu, you can view the Enterprise Open Source (EOS) directory files, clear memory, calibrate the screen, view terminal information and logs, and run diagnostic functions.

Table 9 Verix Terminal Manager Menu 2

Display	Action
VERIX TERMINAL MGR 1> EOS Directory 2> Clear Memory 3> Calibrate Screen 4>Terminal Info 5> Diags 6> System Error Log ↑ ↓ ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press ↵. Use the PF4 key to scroll up the menu options. To view EOS files, select **1> EOS DIRECTORY**. To clear internal memory, select **2> CLEAR MEMORY**. To calibrate the screen, select **3> CALIBRATE SCREEN**. To view the terminal's system information, select **4> TERMINAL INFO**. To run diagnostic applications, select **5> DIAGS**. To view error view logs, select **6> SYSTEM ERROR LOG**. To return to the previous terminal manager menu, press the PF1 key; to return immediately to the first menu of **VERIX TERMINAL MGR** or to quit any operation within this menu, press ✕; to toggle to the third menu **VERIX TERMINAL MGR**, press the PF2 key.
1> EOS DIRECTORY	
** VERIX EOS Files ** <CONTENTS>	This screen displays the Verix enterprise open source (EOS) files. To return to **SYS MODE MENU 2**, press ✕.

Table 9 Verix Terminal Manager Menu 2

Display	Action
2> CLEAR MEMORY	
VERIX TERMINAL MGR **Group ID: nn**	To clear a file group's memory, enter the group ID and press ↵.
2> CLEAR MEMORY	
VTM MGR MEMORY CLEAR **1> Clear CONFIG.SYS** **2> Clear GID Files** **3> Clear all Groups** ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press ↵. Use the PF4 key to scroll up the menu options. Select which files to delete: Select **1> CLEAR CONFIG.SYS** to delete only the `CONFIG.SYS` file. On the next screen, press 1 to completely delete the `CONFIG.SYS` file or 2 to retain protected records that begin with `*` or `#`. Select **2> CLEAR GID FILES** to delete all files in the currently selected file group from the RAM and Flash memory. Select **3> CLEAR ALL GROUPS** to delete all files in all file groups. On the next screen, press 1 to cancel or 2 to confirm the deletion. **Note:** This option is only available when file Group 1 is entered as the group ID. To go back to the second menu of the **VERIX TERMINAL MGR** without deleting files, press ✕.
3> CALIBRATE SCREEN	
Unavailable	To go back to the second menu of **VERIX TERMINAL MGR**, press ✕.

Table 9 Verix Terminal Manager Menu 2

Display	Action
4> TERMINAL INFO F3	
VTM MGR TERMINAL INFO **Serl No nnn-nnn-nnn** **PTID 12000000** **Part XXXXXXXXXXXX** **Rev nn** **OS VER QT00E20B** ↓	The following screens show configuration information specific to your terminal. For a detailed description of each screen, see TERMINAL INFORMATION. Use the PF1 and PF2 keys to scroll through the terminal information screens. To return to the main menu, press x.
VTM MGR TERMINAL INFO **Modl nnnnn** **Ctry XXX** **Keypad nn** **Display 128064** **Mag RDR nn** ↑ ↓	
VTM MGR TERMINAL INFO **PinPad nn** **Modem Type nn** **Ver: F2000B03B5000104** **Modem Model: CX93001** **Modem Ctry: B5** ↑ ↓	
VTM MGR TERMINAL INFO **Life -743271072** **Rset** **Rcnt 181639804** **Tamper Detected N** **CERT nnnnnnn** ↑ ↓	
VTM MGR TERMINAL INFO **HeaP nn** **Stack 2552** ↑	

Table 9 Verix Terminal Manager Menu 2

Display	Action
5> DIAGS	
VERIX DIAGS MGR **1> Printer Diag** **2> IPP Diag** **3> ICC Diags** **4> Keyboard Diag** **5> Mag Card Diag** **6> Debugger** ↓ ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press ↩. Use the PF4 key to scroll up the menu options. To run printer diagnostics and test the printer, select **1> PRINTER DIAG**. To test the internal PIN pad, select **2> IPP DIAG**. To test the Smart Card and list synch drivers, choose **3> ICC DIAGS**. To test the keyboard, select **4> KEYBOARD DIAG**. To check the magnetic card swipe, choose **5> MAG CARD DIAG**. To debug the terminal, select **6> DEBUGGER**. To return to the second menu of the **VERIX TERMINAL MGR** or quit any operation within this menu, press x.
5> DIAGS 1 > PRINTER DIAG	
Printer ID P **Version 0PRED1A1** **Status 22** **1> Test** **2> Paper Feed** ↑ ↓	When you select **1> PRINTER DIAG**, the printer ID, firmware version, and the printer status appear. Press 1 to run the printer test. A print sample begins that uses approximately 30.5cm (12 in) of paper. This allows you to test the print quality and adjust your code for print optimization. See the *Verix V Operating System Programmers Manual* (VPN 23230) for specifics on application development and the internal thermal printer. Press 2 to run approximately 5cm (2 in) of paper through the printer without printing. To go back to the **VERIX DIAGS MGR** screen, press x.
5> DIAGS 2 > IPP DIAG	
INTERNAL PIN PAD **MEMORY TEST PASSED** **IPP8 EMUL02A 05/08 01** **SN: nnnnnnnnnnnnnnnn** **1> RESET00** **MODE: VISA** **2> EXIT**	When you select 2, the **INTERNAL PIN PAD** screen appears and the diagnostic test begins. The firmware version and download date, IPP serial number, baud rate, and mode are displayed. To reset the IPP, press 1; to exit the test and return to the **VERIX DIAGS MGR** screen, press 2 or x.

Table 9 Verix Terminal Manager Menu 2

Display	Action
5> DIAGS 3 > ICC DIAGS	
VoyLib 03.06 0000 **VxOS11 PSCR Build 04** **SCRLIB 2.B 2/10** **1> SMART CARD DIAG** **2> LIST SYNC DRIVERS** **3> EXIT**	When you select 3, the software library version appears. Choose **1> SMART CARD DIAG** to run diagnostics on the Smart Card reader. Select **2> LIST SYNC DRIVERS** to view the drivers. Select **3> EXIT** to return to the **VERIX DIAGS MGR** screen, or press x.
5> DIAGS 4 > KEYBOARD DIAG	
TERMINAL MGR KBD TEST **KEYCODE nn**	This screen displays the hexadecimal ASCII keycode for each key you press. The value displayed corresponds to the actual key pressed. Other values assigned to keys are software dependent. To test the keyboard, press some keys and check that they match their keycodes (for example, the 1 key displays keycode 31). For more hexadecimal ASCII keycodes, refer to the ASCII table in Appendix C. For information about the keypress scan codes, see Keypress Scan Codes. To stop the test and return to the **VERIX DIAGS MGR** screen, press either x or ↵.
5> DIAGS 5 > MAG CARD DIAG	
VERIX TERMINAL MGR **TRK 1:VALID DATA** **TRK 2:VALID DATA** **TRK 3:VALID DATA**	To test the magnetic-stripe card reader, swipe a magnetic-stripe card through it. A successful test displays **VALID DATA** for each track that reads valid data. An error generates one of the following error messages for each track with an error: • **NO DATA** • **NO START** • **NO END** • **LRC ERR** • **PARITY ERR** • **REVERSE END** For more information about magnetic card error messages, refer to the *Verix V Operating System Programmers Manual* (VPN 23230). To stop the test and return to the **VERIX DIAGS MGR** screen, press x.

Table 9 Verix Terminal Manager Menu 2

Display	Action
5> DIAGS 6 > DEBUGGER	
VERIX TERMINAL MGR **Group ID: nn**	Select **6> DEBUGGER** to run the debugging application for the terminal.
VERIX TERMINAL MGR **Please enter** **Password for GID nn** **-----------------**	Enter the current password for the selected file group and press ↩. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↩. Verify your password and reenter it. To return to the **VERIX DIAGS MGR** screen press x.
5> DIAGS > PF1 KEY (second DIAGS menu)	
VERIX DIAGS MGR **1> Tamper Log** **2> RKL log** **3> RKL log export** **4> Battery Status** **5> USB Info** **6> Display Testscreen** ↓ ↑ ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press ↩. Use the PF4 key to scroll up the menu options. To view all tampering attempts, select **1> TAMPER LOG**. To view the RKL logs, select **2> RKL LOG**. To export the RKL logs, choose **3> RKL LOG EXPORT**. To check the batteries, select **4> BATTERY STATUS**. To view the USB device settings and availability, choose **5> USB INFO**. To calibrate the screen, select **6> DISPLAY TESTSCREEN**. To return to the second menu of the **VERIX TERMINAL MGR** or quit any operation within this menu, press x.

Table 9 Verix Terminal Manager Menu 2

Display	Action
5> DIAGS > PF1 KEY > TAMPER LOG	
TAMPER LOG **05/29/09 06:29 00001** **05/29/09 06:16 00009** **11/01/08 08:21 00001** **10/30/08 19:36 00001**	The Tamper Log screen displays a list of possible tamper events. The list is sorted from the most current tamper event to the oldest event. The date is displayed in MM/DD/YY format, while the time is displayed as a 24-hour clock. To go back to the **VERIX DIAGS MGR** screen, press x.
TAMPER LOG **<EMPTY>**	If the Tamper Log is empty, **<EMPTY>** is displayed on the screen. To go back to the **VERIX DIAGS MGR** screen, press x.
5> DIAGS > PF1 KEY > RKL LOG	
RKL LOG INFO pg nn **<EMPTY>**	To go back to the **VERIX DIAGS MGR** screen, press x.
5> DIAGS > PF1 KEY > RKL LOG EXPORT	
Outputting log . . . **Log output done**	To go back to the **VERIX DIAGS MGR** screen, press x.
5> DIAGS > PF1 KEY > BATTERY STATUS	
<EMPTY>	To go back to the **VERIX DIAGS MGR** screen, press x.

Table 9 Verix Terminal Manager Menu 2

Display	Action
5> DIAGS > PF1 KEY > USB INFO	
USB DEVICE INFO **USB Device 1 Info** **Serial No** ** **Vendor ID 0X0000** **NOT AVAILABLE** **Release NO 00.00** ↓	To go back to the **VERIX DIAGS MGR** screen, press x.
USB DEVICE INFO **Product ID 0X0000** ** **HUB 0** **Port 1** **Class 9** **Sub Class 0** ↓ ↑	To go back to the **VERIX DIAGS MGR** screen, press x.
USB DEVICE INFO **Power 0 mA** **Speed FULL** ↑	To go back to the **VERIX DIAGS MGR** screen, press x.
5> DIAGS > PF1 KEY > DISPLAY TESTSCREEN	
	To go back to the **VERIX DIAGS MGR** screen, press x.

Table 9 Verix Terminal Manager Menu 2

Display	Action
6 > SYSTEM ERROR LOG	
VERIX ERROR LOG **TYPE 1** **TASK 2 GID 2** **TIME 070806150146** **CPSR 20000030** **PC 7042A126** **LR 70420C5D** **ADDR 00000008**	The error log screen displays internal diagnostic information about the most recent unrecoverable software error. If you report a terminal problem, you may be asked to provide this information. This first screen displays the following: • **TYPE** - Error type • **TASK** - Task number • **TIME** - Time of crash • **CPSR** - Current Program Status Register • **PC** - Program Counter • **LR** - Link Register • **ADDR** - Fault address For detailed error log descriptions, see ERROR LOG. After making any notations, press the key under the down arrow (PF1) to view additional error log information, if shown. To go back to the **VERIX DIAGS MGR** screen, press x.

Menu 3

In this menu, you can adjust the clock, display contrast, change passwords, and check the IPP key loading mode.

NOTE When entering any password, an asterisk (*) appears on the display screen for each character you type. These asterisks prevent your password from being seen by an unauthorized person. Pressing the ALPHA key changes the characters or symbols you enter, but does not cause additional asterisks to appear. Secure a copy of every password to ensure it is not forgotten or lost.

Table 10 Verix Terminal Manager Menu 3

Display	Action
VERIX TERMINAL MGR **1> Clock** **2> Console Settings** **3> Change Passwords** **4> Key Management** ↑ ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press ↵. Use the PF4 key to scroll up the menu options. Select **1> CLOCK** to adjust date and time settings. Select **2> CONSOLE SETTINGS** to modify the terminal sound and display settings. Select **3> CHANGE PASSWORDS** to change terminal manager and file group passwords. The file groups and terminal manager all use a default password preset at the factory: “1, Alpha, Alpha, 66831”. Select **4> KEY MANANGEMENT** to test the internal PIN pad key loading mode. To return to the previous terminal manager menu, press the PF2 key; to return immediately to the first **VERIX TERMINAL MGR** menu or to quit any operation within this menu, press ✕.
1> CLOCK	
Note: The terminal clock is battery-backed to retain date and time settings when the terminal is shut off.	
VTM CLOCK MANAGER **1> INCREMENT HOUR** **2> EDIT TIME** **3> EDIT DATE** **4> DECREMENT HOUR** ↑ ↓	To adjust the current time one hour forward, select **1> INCREMENT HOUR**. To see the time, select **2> EDIT TIME**. To set the date, select **3> EDIT DATE**. To adjust the current time one hour back, select **4> DECREMENT HOUR**.

Table 10 Verix Terminal Manager Menu 3

Display	Action
1> CLOCK 1> INCREMENT HOUR	
TIME AND DATE **HH:MM:SS** **MM:DD:YY**	Select **1> INCREMENT HOUR** to add an hour to the current time setting.
1> CLOCK 2> EDIT TIME	
VTM TIME **Current Time:** **HH:MM:SS** **New Time:** __/__/__	Enter the new time in *HOURS:MINUTES:SECONDS* (HH:MM:SS) format. To correct a mistake, press ← to delete and enter the correct number; press ↵ to set the new time. The current time and date is then displayed on the next screen. Press ✕ to return to the third menu of the **VERIX TERMINAL MGR**.
1> CLOCK 3> EDIT DATE	
VTM DATE **Current Date:** **HH:MM:SS** **New Date:** __/__/__	Enter the new date in *MONTH/DAY/YEAR* (MM/DD/YY) format. To correct a mistake, press ← to delete and enter the correct number; press ↵ to set the new date. The current time and date is then displayed on the next screen. Press ✕ to return to the third menu of the **VERIX TERMINAL MGR**.
1> CLOCK 4> DECREMENT HOUR	
TIME AND DATE **HH:MM:SS** **MM:DD:YY**	Select **4> DECREMENT HOUR** to reduce an hour from the current time setting.

Table 10 Verix Terminal Manager Menu 3

Display	Action
2> CONSOLE SETTINGS	
VTM CONSOLE MGR **1> Console Beeper OFF** **2> Console Beeper ON** **3> Console Backlight OFF** **4> Console Backlight ON** **5> Contrast DOWN** **6> Contrast UP** ↓ ↑ ↓	Turn the terminal beeper sounds on or off by pressing the **1** or **2** key. Switch the backlight on or off by pressing the **3** or **4** key. Select **5> CONTRAST UP** or **6> CONTRAST DOWN** to increase or decrease display contrast respectively. To return to the main menu and save your changes, press ↩. Otherwise, press ✕ to go back to the third menu of the **VERIX TERMINAL MGR** without saving the changes.
3> CHANGE PASSWORDS	
VTM PASSWORD MGR **1> File Group** **2> VERIX TERMINAL MGR Entry** ↑ ↓	To change the password of a file group, type the number of the file group and select **1> FILE GROUP**. Then, go to the **VERIX TERMINAL MGR FILE GROUP nn PASSWORD** screen below. See Passwords for more information. To change the system password, select **2> VERIX TERMINAL MGR ENTRY**. Then, skip to **VTM PASSWORD NEW** screen below. **Note:** Some application downloads automatically reset the terminal manager password.
VERIX TERMINAL MGR **GROUP nn**	Enter the current password for the selected file group and press ↩. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↩. Verify your password and reenter it.

Table 10 Verix Terminal Manager Menu 3

Display	Action
VTM PASSWORD MGR **NEW** ________	Type the new password and press ↵. **Note:** The new password MUST be five to ten characters long. If you enter a new password that is less than or exceeds the required number of characters, the terminal will sound an alarm and display an error screen. The only way to get out of the **CHANGE PASSWORD** screen is to enter a password that is five to ten characters long, or to press ✕. If ✕ is pressed, the password will not be changed. To correct a mistake, press ← to delete the number, and then reenter the new password.
VTM PASSWORD MGR **AGAIN** ________	The terminal requests that you verify the new password. Reenter the new password and press ↵.
VTM PASSWORD MGR **PASSWORD CHANGED**	The new password is now in effect. To exit this screen, press ↵. to return to the third menu of the **VERIX TERMINAL MGR**.
4> KEY MANAGEMENT	
Key Management **1> IPP Key Load** **2> RKL Key Load** **3> RKL Key Status** ↑ ↓	

Table 10 Verix Terminal Manager Menu 3

Display	Action
4> KEY MANAGEMENT 1> IPP KEY LOAD	
VERIX TERMINAL MGR **Please enter** **Password for GID nn** __________	Enter the current password for the selected file group and press ↩. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↩. Verify your password and reenter it.
INTERNAL PIN PAD **KEY LOADING MODE** **BYTES SENT 0** **BYTES RCVD 0** **1> END**	Select this mode when you use the SecureKit or programming from your PC to inject keys into your terminal. In this mode, a pass-through connection is established between COM1 and COM5 (IPP port) to allow key loading. Press ✕ to stop the key load session; select **1> END** when finished with the key load.
4> KEY MANAGEMENT 2> RKL KEY LOAD	
VERIX TERMINAL MGR **Please enter** **Password for GID nn** __________	Enter the current password for the selected file group and press ↩. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↩. Verify your password and reenter it.
RKL RSA KEY LOADING **BYTES SENT 0** **BYTES RCVD 0** **1> END**	Press ✕ to stop the key load session; select **1> END** when finished with the key load.
4> KEY MANAGEMENT 3> RKL KEY STATUS	
RKL Key Status **Public key name** **<EMPTY>**	Press ↩ to view the Private Key Hash. Press ✕ to return to the **KEY MANAGEMENT**screen.

Table 10 Verix Terminal Manager Menu 3

Display	Action
RKL Key Status **Private key hash**	Press x to return to the **KEY MANAGEMENT**screen.

CHAPTER 5

File Authentication

This chapter discusses VeriShield's *file authentication* security architecture and provides the following:

- Overview of the VeriShield file authentication module, and the organizational infrastructure that supports it (see Introduction to File Authentication).
- Explanation of the file authentication process may affect the tasks normally performed by application programmers, terminal deployers, site administrators, or entities authorized to download files to a VX 520 terminal (see File Authentication and the File System).
- Reference to the VeriShield File Signing Tool to generate signature files (see VeriShield File Signing Tool).

In Chapter 6, Performing Downloads, the topic of file authentication is also discussed in the context of specific file download procedures.

Introduction to File Authentication

The VX 520 terminal uses the VeriShield security architecture, 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 the file authentication module.

File authentication is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process makes it possible for the sponsor of a VX 520 terminal to logically secure access to the terminal by controlling who is authorized to download application files to that terminal. It verifies the file's origin, sender's identity, and integrity of the file's information.

VeriFone Certificate Authority

To manage the tools and processes related to the file authentication module of the VeriShield security architecture, 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 VX 520 terminals.

Special Files Used in the File Authentication Process

The following specially formatted files support the file authentication 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, do not need to be kept secure to safeguard the overall security of VeriShield.

Within the VeriShield File Signing Tool, you can recognize the special file types that support the file authentication process by the filename extensions listed in Table 11.

Table 11 VeriShield File Signing Tool Filename Extensions

File Type	Extension
Signature	`*.p7s`
Private key	`*.key`
Digital certificate	`*.crt`

All digital certificates are generated and managed by the VeriFone CA, and are distributed on request to VX 520 clients—either internally within VeriFone or externally to sponsors.

All certificates issued by the VeriFone CA for the VX 520 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 tightly controlled by VeriFone.

Certificates Contain Keys That Authenticate Signature Files

- **Sponsor certificate:** Certifies a client’s sponsorship of the terminal. It does not 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 and target files to authenticate.

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.

NOTE

The signer private keys loaded onto the smart card is the only copy of the private key.

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

To establish the logical security of applications to download to a VX 520 terminal, the designated signer uses the signer private key issued by the VeriFone CA as this is a required input to the VeriShield File Signing Tool.

A signature file is generated using a signer private key. Successful authentication depends on whether the signer private key used to sign the target file matches the signer certificate stored in the terminal’s certificate tree.

How File Authentication Works

File authentication consists of three basic processes:

1 **Development:** The VeriShield File Signing Tool 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 are 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 Application developer applies for Sponsor and Signer certificates. The absence of a “default” signer certificate compels developers to apply for a dedicated Signer certificate.

3 The developer assigns a name to the application file.

4 The application file becomes a required input for the VeriShield File Signing Tool.

5 Using the application file, Signer certificate, and Signer password, the VeriShield File Signing Tool 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 The terminal’s operating system searches for signature files.

  b When a signature file is found, the operating system then searches for a matching application file.

  c 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.

  d If these values match, the operating system marks the application file “authenticated” and allows it to run.

7 The application file is tested and debugged.

8 After the application file is fully debugged, it becomes an input for the deployment process.

Figure 27 illustrates the development process.

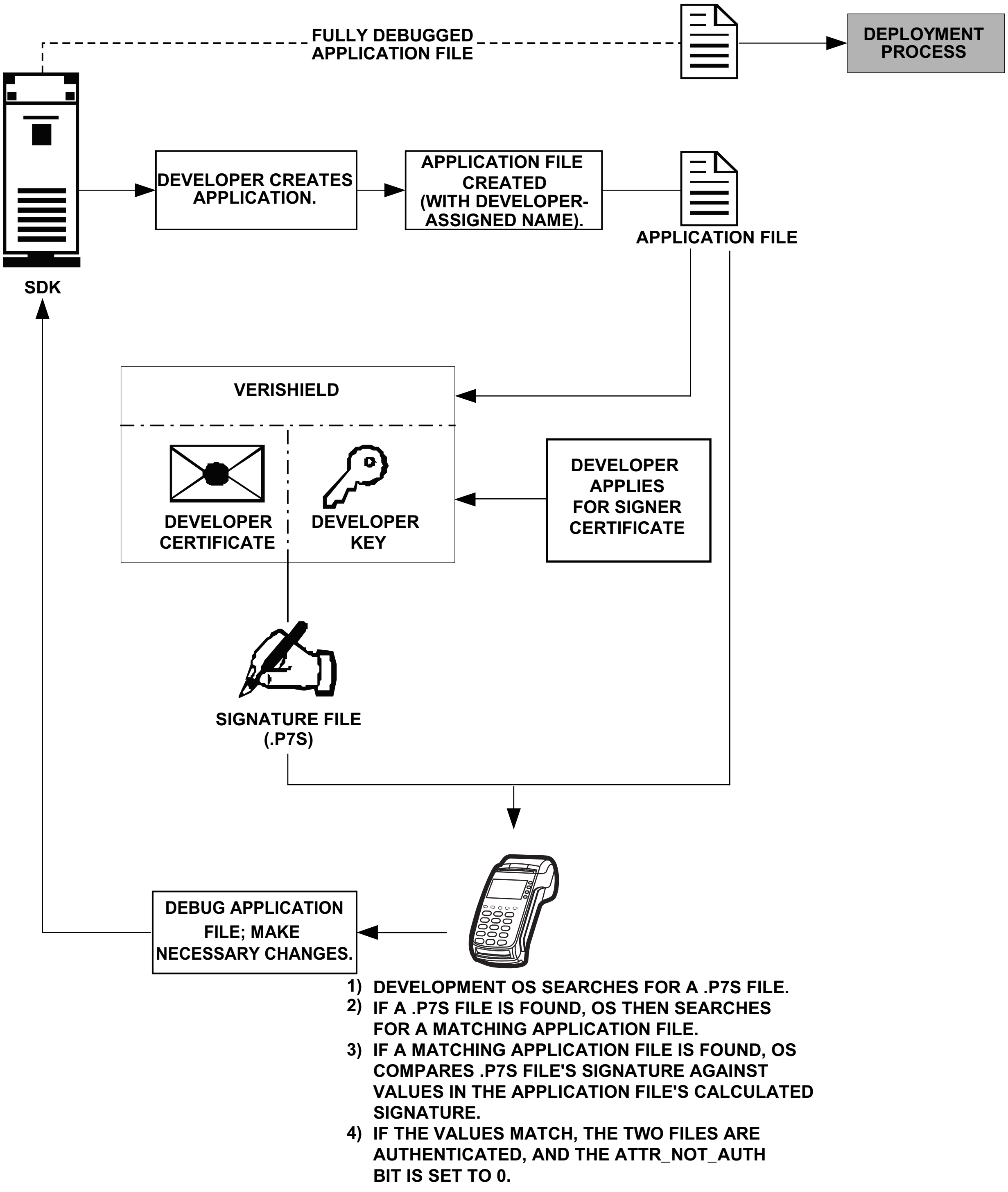

FULLY DEBUGGED APPLICATION FILE
DEPLOYMENT PROCESS
DEVELOPER CREATES APPLICATION.
APPLICATION FILE CREATED (WITH DEVELOPER-ASSIGNED NAME).
APPLICATION FILE
SDK
VERISHIELD
DEVELOPER CERTIFICATE
DEVELOPER KEY
DEVELOPER APPLIES FOR SIGNER CERTIFICATE
SIGNATURE FILE (.P7S)
DEBUG APPLICATION FILE; MAKE NECESSARY CHANGES.
1) DEVELOPMENT OS SEARCHES FOR A .P7S FILE.
2) IF A .P7S FILE IS FOUND, OS THEN SEARCHES FOR A MATCHING APPLICATION FILE.
3) IF A MATCHING APPLICATION FILE IS FOUND, OS COMPARES .P7S FILE'S SIGNATURE AGAINST VALUES IN THE APPLICATION FILE'S CALCULATED SIGNATURE.
4) IF THE VALUES MATCH, THE TWO FILES ARE AUTHENTICATED, AND THE ATTR_NOT_AUTH BIT IS SET TO 0.

Figure 27 The Development Process

Pre-Deployment Process

In this process:

1 A sponsor goes 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 The VeriFone CA generates the following items for the sponsor:

a Smart card containing a set of certificates and private key.

b Smart card PIN.

4 The 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.

Figure 28 illustrates the pre-deployment process.

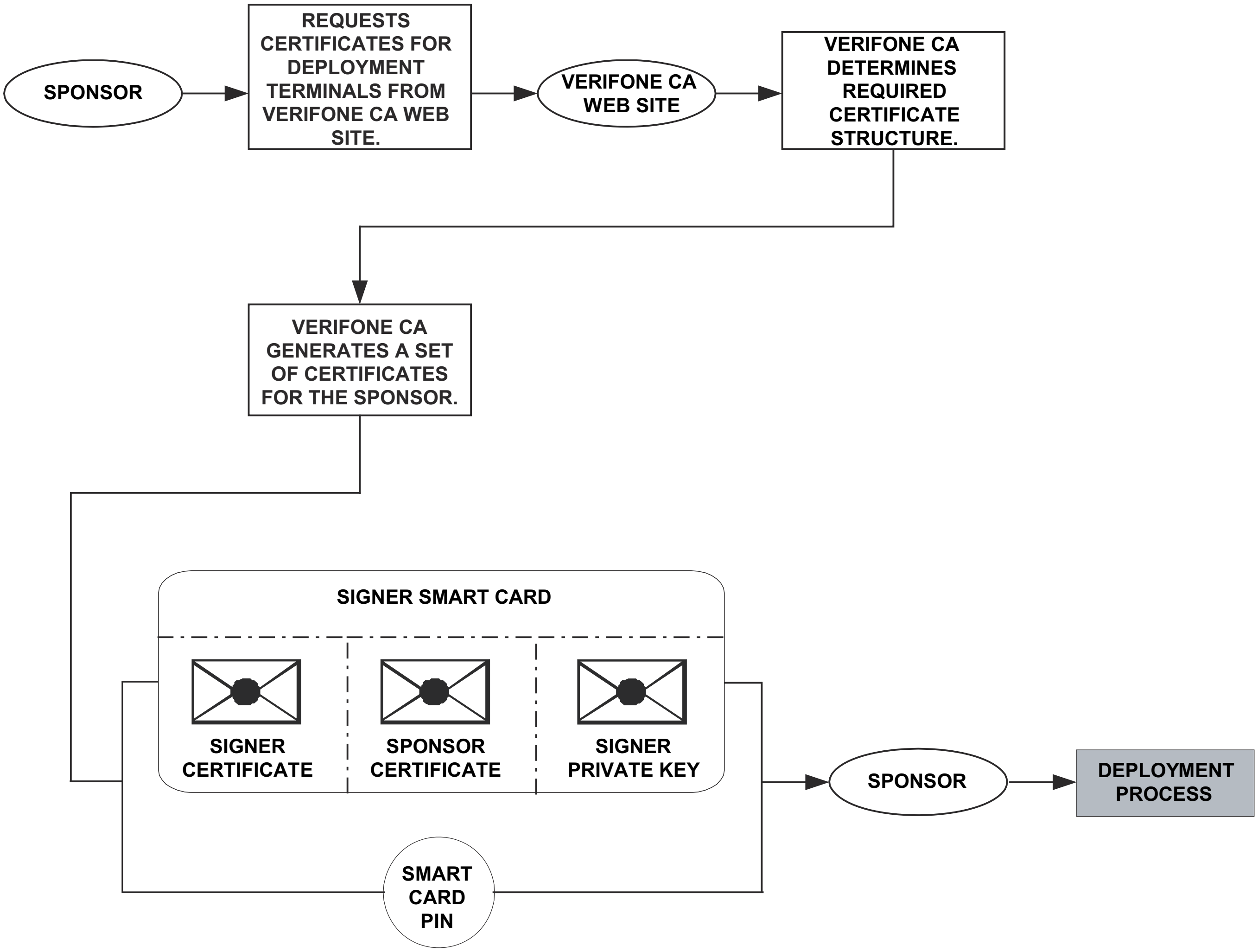

SPONSOR
REQUESTS CERTIFICATES FOR DEPLOYMENT TERMINALS FROM VERIFONE CA WEB SITE.
VERIFONE CA WEB SITE
VERIFONE CA DETERMINES REQUIRED CERTIFICATE STRUCTURE.
VERIFONE CA GENERATES A SET OF CERTIFICATES FOR THE SPONSOR.
SIGNER SMART CARD
SIGNER CERTIFICATE
SPONSOR CERTIFICATE
SIGNER PRIVATE KEY
SMART CARD PIN
SPONSOR
DEPLOYMENT PROCESS

Figure 28 The Pre-Deployment Process

Deployment Process

In this process:

1. The sponsor provides the application file (from the development process), 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, application file, and extracted signer and sponsor certificates are downloaded into a deployment terminal, where the following actions occur:

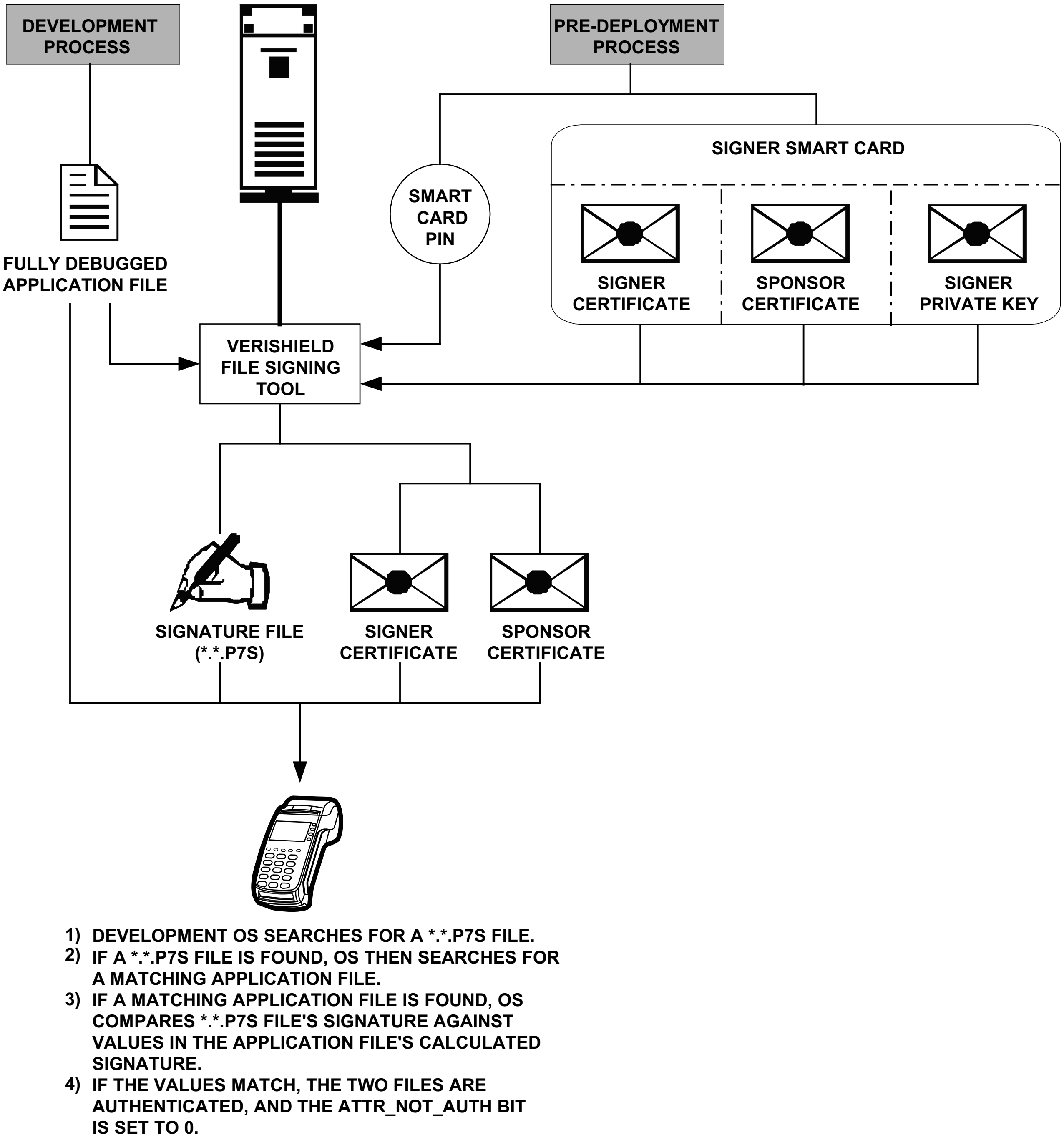
   a. The terminal's operating system searches for signature files.

   b. If a signature file is found, the operating system then searches for a matching application file.

   c. If 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.

   d. If these values match, the operating system marks the application file "authenticated" and allows it to run.
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).

Figure 29 illustrates the deployment process.



1) DEVELOPMENT OS SEARCHES FOR A *.*.P7S FILE.
2) IF A *.*.P7S FILE IS FOUND, OS THEN SEARCHES FOR A MATCHING APPLICATION FILE.
3) IF A MATCHING APPLICATION FILE IS FOUND, OS COMPARES *.*.P7S FILE'S SIGNATURE AGAINST VALUES IN THE APPLICATION FILE'S CALCULATED SIGNATURE.
4) IF THE VALUES MATCH, THE TWO FILES ARE AUTHENTICATED, AND THE ATTR_NOT_AUTH BIT IS SET TO 0.

Figure 29 The Deployment Process

Planning for File Authentication

File authentication is an integral part of every VX 520 terminal. To safeguard the terminal's logical security, the file authentication module 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 the purposes of file authentication, executable code files include two file types that can be recognized by the filename extensions listed in Table 12.

Table 12 Executable File Extensions

File Type	Extension
Compiled and linked application files	`*.out`
Global function libraries	`*.lib`

Depending on the logical security requirements of specific applications, other types of files used by an application (that is, non-executable files) must also be authenticated.

- Data files (`*.dat`) that contain sensitive customer information or other data that must be secure.
- Font files (`*.vft` or `*.fon`) may need to be secure to prevent unauthorized text or messages from being displayed on the terminal screen.
- Any other type of file used by an application in which the application designer would like to logically secure using file authentication requirements.

Decide Which Files to Authenticate in a Specific Application

The first step in the file authentication 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. Determining 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 (and When) Signature Files Authenticate Their 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 VX 520 terminal each time you perform an application download.

When the file authentication module detects a new signature file after a terminal restart, it locates and attempts to authenticate the target file that corresponds to the new signature file.

It is not mandatory to always download a signature file and its target application file at the same time. 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 the file authentication module after a subsequent download procedure and terminal restart.

Determine Successful Authentication

To ensure the VX 520 terminal's logical security, never assume that a target file was authenticated simply because it downloaded to the VX 520 terminal together with its signature file.

There are several ways to ensure a target file is successfully authenticated after a download:

- **Confirm if 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.
- **Visually (and audibly) confirm file authentication during the process.** When the file authentication module is invoked at terminal restart and detects a new signature file, it displays status information on the screen indicating success or failure of the authentication of each target file based on its corresponding signature file. (A similar status display also appears on the screen when you download digital certificates.)

  You can watch the screen display following the download to see if a specific target file fails authentication. If this happens, **FAILED** is displayed for five seconds on the screen below the filenames of the target and signature files, and the terminal beeps as an alert.

  An application program can issue a function call to read the `ATTR_NOT_AUTH` bit's current value for all relevant files to verify they were successfully authenticated. If the `ATTR_NOT_AUTH` bit's binary value is `1`, the file did *not* authenticate; if `0`, the file did authenticate.

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

NOTE Because the application is responsible for verifying data files and prompt files, it is recommended that each application checks the `ATTR_NOT_AUTH` bit of all relevant files on restart.

NOTE Each successfully authenticated file is also write-protected. That is, the file’s read-only attribute is set. If the read-only file is removed or if the file is modified in any way while stored in the terminal, the `ATTR_NOT_AUTH` bit is automatically set to 1. If the modified file is an executable, it is no longer allowed to run.

Digital Certificates and the File Authentication Process

The file authentication module always processes certificates before it processes signature files. Digital certificates (`*.crt` files) generated by the VeriFone CA have two important functions in the file authentication process:

- They define the rules for file location and usage (for example, the valid file group, replaceable `*.crt` files, parent `*.crt` files, whether child `*.crt` files can exist, and so on).
- They convey the public cryptographic keys generated for terminal sponsors and signers that are the required inputs to the VeriShield File Signing Tool to verify file signatures.

Hierarchical Relationships Between Certificates

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

To manage hierarchical relationships between certificates, certificate data is stored in terminal memory in a special structure called a *certificate tree*. New certificates are authenticated based on data stored in the current certificate tree. 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 VX 520 terminal upon manufacture. When you take a new VX 520 terminal out of its shipping carton, certificate data is already stored in the terminal's certificate tree. In this just-out-of-the-box condition, the VX 520 terminal is called a *development terminal*.

A sponsor requests a set of digital certificates from the VeriFone CA to establish sponsor and signer privileges. This set of certificates are then downloaded to the VX 520 terminal when the terminal is being prepared for deployment. When this procedure is complete, the VX 520 terminal is called a deployment terminal.

Add New Certificates

When you add a new certificate file to a VX 520 terminal, the file authentication module 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 a new certificate contains is added to the terminal's certificate tree depends on if it is successfully authenticated. 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 that file group's 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 the application memory.

Development Terminals

A development terminal is a VX 520 terminal with a Sponsor and Signer certificate issued to someone who intends to use the terminal for application development. An application developer must apply for a Sponsor/Signer certificate to allow loading an application. (see Figure 30).

In the development terminal, , the level of logical security provided by the file authentication module is the same as a deployment application. In most application development and test environments, tight security is not required, and the flexibility offered by the VX 520 development terminal is more important.

NOTE With the factory set of certificates stored in the terminal memory, *anyone* who has the VX 520 SDK and VeriShield File Signing Tool can generate valid signature files for downloading and authenticating files on the VX 520 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 to use to logically secure sponsor and signer privileges when the VX 520 terminal is prepared for deployment.

Customer-specific sponsor and signer certificates are usually downloaded to a VX 520 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 30.

When the sponsor and signer certificates are downloaded and successfully authenticated, the terminal is ready to deploy.

Ultimately, it is the sponsor’s decision how to implement the logical security provided by file authentication on a field-deployed terminal. Additional certificates can be obtained from the VeriFone CA anytime to implement new sponsor and signer relationships in deployment terminals. VeriShield allows for multiple sponsors and signing certificates in a terminal. This allows the flexibility of unique signatures for each executable or data files.

Figure 30 illustrates the certificate trees in development and deployment terminals.

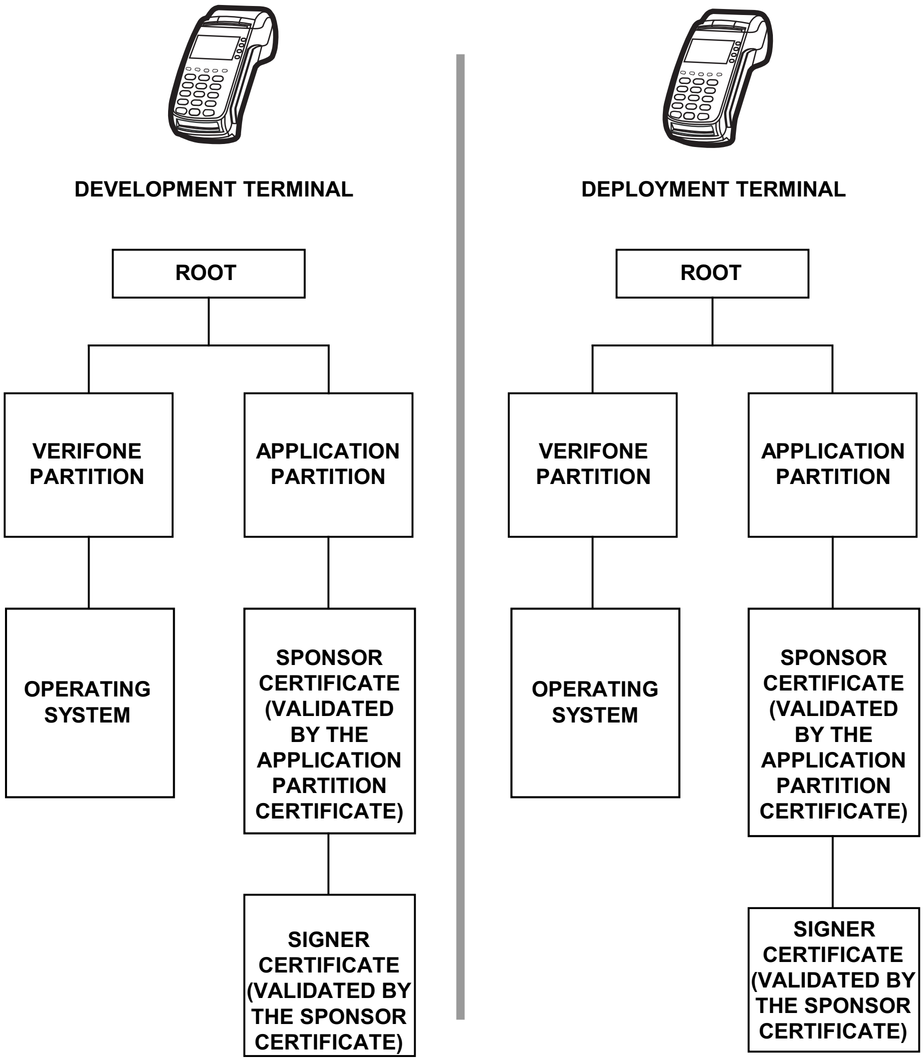

DEVELOPMENT TERMINAL
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
SIGNER CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)
DEPLOYMENT TERMINAL
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
SIGNER CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)

Figure 30 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, and the certificate file itself is erased from RAM.

The certificate tree file is stored in a reserved area of non-volatile memory and is therefore relatively permanent. New certificate data can be added to the existing certificate tree (up to a maximum of 21 certificates).

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 13.

Table 13 Differences Between Required Inputs

Development Terminals	Deployment Terminals
The following three unique inputs, which are issued at customer request by the VeriFone CA, are required for the file signing process, as well as the application files you want to sign and authenticate: • **Signer certificate**, with the filename `VxSIGN.CRT` • **Signer private key**, with the filename `VXSIGN.KEY` • **Developer signer certificate:** This unique certificate is a required input for the VeriShield File Signing Tool and must be downloaded to the terminal along with the signature files and target application files to authenticate, unless already downloaded to the terminal in a previous operation. • **Developer signer private key:** The VeriFone CA issues this unique, encrypted private key file (`*.key`) to an authorized signer at the sponsor's request. The signer private key is a required input to the VeriShield File Signing Tool, but does not have to be downloaded to the terminal. • **Developer signer PIN:** The VeriFone CA issues this unique password to an authorized signer at the sponsor's request. The customer signer password is a required input to the VeriShield File Signing Tool, but it does not have to be downloaded to the 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 VeriShield File Signing Tool input when signing files.

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 (refer to Figure 31) by:

- Deleting the current sponsor and signer certificates from the terminal’s application partition.

NOTE

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

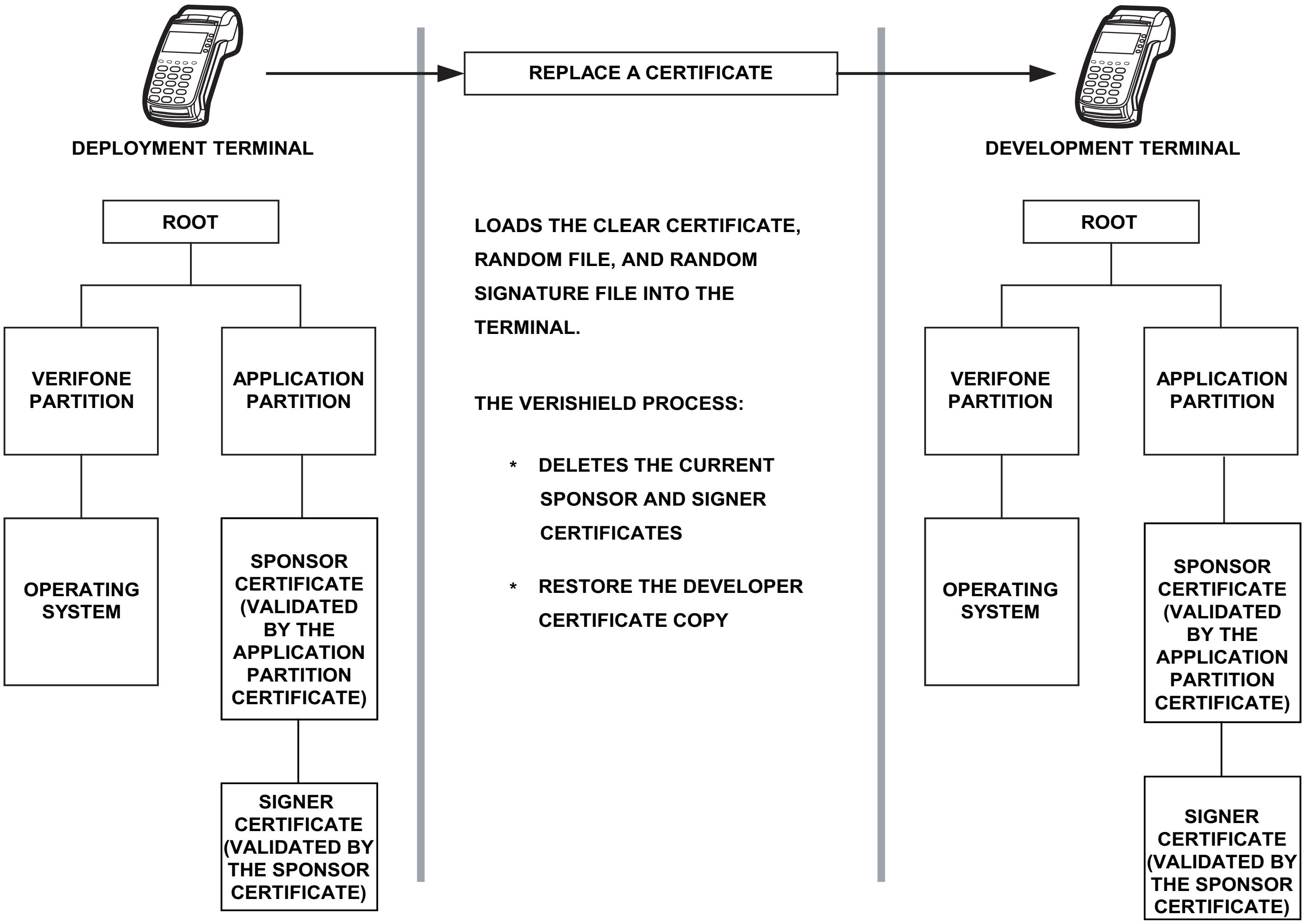

DEPLOYMENT TERMINAL
REPLACE A CERTIFICATE
DEVELOPMENT TERMINAL
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
SIGNER CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)
LOADS THE CLEAR CERTIFICATE, RANDOM FILE, AND RANDOM SIGNATURE FILE INTO THE TERMINAL.
THE VERISHIELD PROCESS:
* DELETES THE CURRENT SPONSOR AND SIGNER CERTIFICATES
* RESTORE THE DEVELOPER CERTIFICATE COPY
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
SIGNER CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)

Figure 31 Certificate Replacement Process

File Authentication and the File System

Application Memory Logically Divided Into File Groups

The memory of a VX 520 terminal is logically divided into two main areas, or partitions:

- Operating System
- Applications

The application partition is further divided into sub-partitions. These sub-partitions are called file groups or GIDs.

This system of partitions and sub-partitions makes it possible to store multiple applications in terminal memory and prevent these applications from overlapping or otherwise interfering with each other's operation.

There are a total of 16 file groups (Figure 32). Group 0 is the name of the operating system partition. Group 1 is reserved for the main application. Groups 2–14 are available for related executable files or secondary applications. Group 15 is *open*, and used for shared files such as shared libraries.

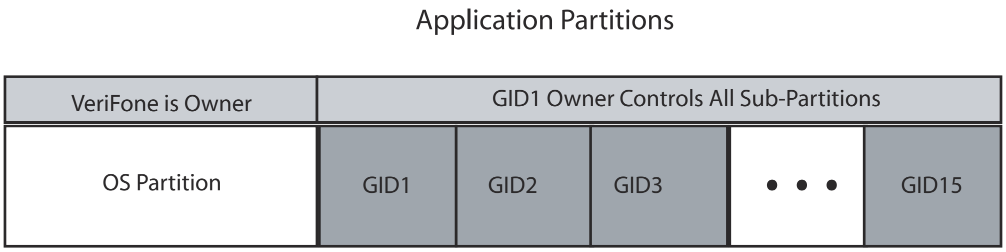


Figure 32 VX 520 Application Memory Partitions

NOTE

The VX 520 operating system only enforces the rule that the main application be always stored in GID1. You can, for example, store a shared library in any file group. Rules for Storing Applications in Specific File Groups states reasons to follow the guidelines previously described for storing applications and libraries in specific file groups.

Rules for Storing Applications in Specific File Groups

Here are some important VX 520 file system features, as they relate to storing application files in specific file groups, and how these features affect the file authentication process:

- Most applications consist of more than one executable. For *each* executable to run on the terminal, it must be signed and authenticated.
- Although not enforced by the operating system, it is recommended that only one application be stored per file group in the application partition. Any number of executable files can be stored in a single file group.
- Using the `CONFIG.SYS *GO` variable, you can specify only one application to automatically execute following a download and terminal restart. The defined

application is usually the main application stored in Group 1 and called from the *GO variable in the CONFIG.SYS file in GID1.

- The main application stored in GID1 can access files, secondary applications, or function libraries stored in *any* other file group.
- The application downloaded into GID1 is *always* the primary application for the terminal. This application is owned by the primary terminal sponsor (sponsor A) in cases where there are multiple sponsors.
- The Group 1 application controls any and all secondary applications stored in terminal memory. That is, a secondary application can only be invoked by a RUN command issued by the Group 1 application.
- An application stored in Groups 2–15 can *only* access files stored in its own file group and in Group 15. For example, an application authorized by the sponsor to be authenticated in Group 4 can only access files and libraries stored in Group 4 and Group 15.
- If multiple applications (main and secondary) are to run on the same terminal, each .OUT and/or shared library file must have its own matching signature file.

  Because each application is responsible for verifying its own data and prompt files, the other application files should have their own matching signature files. The master .OUT file should validate that these additional signature files are authenticated before they are used.
- If two or more applications will run on the same terminal, the signature files for the respective applications must be downloaded, together with the corresponding target files, into the specific file group(s) for which the applications are authorized. If an application is downloaded into a group for which is it not authorized, file authentication for that application fails.

  If, for example, Application B is downloaded into GID4, where it is authorized to run, but the signature files for all Application B executable files are downloaded into GID7, file authentication for Application B fails and it is not allowed to run.
- Each certificate contains an attribute to verify if an application is valid for a particular group.

Authenticate Files Stored in the RAM or Flash of a File Group

All *.p7s files are loaded into RAM and contain flags that indicate if the file to verify is stored in flash or RAM. A signature file must know if its matching application file is stored in flash or RAM. If a signature file cannot locate its matching application file, the application file is not authenticated.

If the signature file authenticates its target file, and if the *FA variable is present in the CONFIG.SYS file of the target file group and is set to 1, the signature file is retained in memory and is automatically moved, if necessary, into the same file system as the target file it authenticates. That is, if the target file is stored in the flash, the signature file is also stored in the flash; if the target file is stored in RAM, the signature file is also stored in RAM.

NOTE Normally signature files are retained in the terminal even after being used to authenticate executable (code) or data files. This is to facilitate back-to-back downloads, as described in Chapter 6. Users who do not intend to perform back-to-back downloads can remove signature files after use, gaining space for other files. Automatic removal is performed if the user sets *FA=0 in the CONFIG.SYS file of Group 1. The main reason for using *FA is to force automatic removal. If the user desires the default behavior (retain signature files, to allow for back-to-back downloads), the user does not need to set *FA.

If the signature file authenticates its target file and the *FA variable is present in the CONFIG.SYS file of the target file group and is set to 0, the signature file is erased when its target file is authenticated.

If you intend to perform back-to-back downloads, as described in Chapter 6, all signature files *must* be retained in the VX 520 terminal's application memory, together with the target application files they authenticate.

NOTE To control if signature files are retained or deleted when they are processed by the file authentication module, you must use the protected CONFIG.SYS variable *FA as documented in the *Verix V Operating System Programmers Manual* (VPN 23230).

Restrictions on Downloading Different File Types

A typical application download includes a variety of different file types. The following restrictions in Table 14 describe how you can download different kinds of files to the VX 520 terminal and how files are stored in the file system:

Table 14 Download File Extensions

File Type	Restriction
Certificate (*.crt)	*Must* be downloaded into the RAM of the target file group (GID1–GID15) selected in Verix Terminal Manager.
Signature (*.p7s)	*Must* be downloaded into the RAM of the target file group (GID1–GID15) selected in Verix Terminal Manager.
Operating system	*Must* be downloaded into Group 1 RAM. When the OS files, related certificates and signature files are authenticated, they are automatically moved from Group 1 RAM into the Group 0 sub-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 is erased from the target file group's RAM.

VeriShield File Signing Tool

To generate the signature files required for file authentication, you must sign all executable files and other files to be logically protected using the VeriShield File Signing Tool. This section discusses the use of this tool, which is included in the Verix V DTK.

The VeriShield File Signing Tool generates a formatted file called a *signature* file, recognized by the filename extension `*.p7s`.

You can run the VeriShield File Signing Tool on a host computer (PC) in DOS command-line mode, or invoke the program under Windows NT or Windows 95 and then use the VeriShield File Signing Tool dialog box to make the required entries.

NOTE The file signing process for operating system files is done for VX 520 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.

For more information about the VeriShield File Signing Tool, see the *VeriShield Online Help* (VPN 22311).

VeriShield File Signing Tool System Requirements

The VeriShield File Signing Tool requires one of the following computing environments:

- Windows NT, Version 4.0, SP5
- Windows 95, with Internet Explorer Version 5.0

The SP5 and Internet Explorer Version 5.0 software can be downloaded from the Microsoft Web site located at www.microsoft.com.

Operating Modes for the VeriShield File Signing Tool

The VeriShield File Signing Tool 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 the VeriCentre Download Management Module (DMM) and the `DDL.EXE` direct download utility. In command-line mode, you can sign a batch of files in a single operation.

- **Graphical interface mode** (Windows NT or Windows 95): Use the VeriShield File Signing Tool dialog box 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 VeriShield File Signing 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 group'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.

NOTE

If the entry of a signer password is a required input, a secondary dialog box is displayed to enter and confirm the password. Please also note that a signer password is required for a deployment terminal, but not for a development terminal.

Command-Line Entries for the VeriShield File Signing Tool

Table 15 lists the *switches* that make up the command-line mode syntax for the VeriShield File Signing Tool.

Table 15 Command-Line Mode Switches for the VeriShield File Signing Tool

Switch	Description	Requirements
`-C`, `-c`	Signer certificate file name (`*.crt`).	Required input for development terminals and deployment terminals. Use the `VxSIGN.CRT` developer signer certificate for development terminals. Use the signer certificate issued by the VeriFone CA for deployment terminals.
`-K`, `-k`	Signer private key filename (`*.key`).	Required input for development terminals and deployment terminals. Use the `VxSIGN.KEY` developer signer private key for development terminals. Use the signer private key provided by the VeriFone CA for deployment terminals.
`-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.

Table 15 Command-Line Mode Switches for the VeriShield File Signing Tool

Switch	Description	Requirements
`-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 the VeriShield File Signing Tool to generate for the target application file.	Required for development terminals and for deployment terminals.
`-L`, `-l`	Specifies to store the target application file to sign and authenticate in the flash (drive F:) file system. If you do not use this switch to specify flash as the target file destination, it is stored by default in the RAM file system (drive I:).	Optional entry. This switch assigns an `F:` prefix to the name of the `*.out` or `*.lib` file to download, and also stores this information in the signature file as part of the special filetype attribute. **Note:** Signature files must be downloaded into the target file group's RAM. If the target file is authenticated, the corresponding `*.p7s` file is moved to the same memory area as the target file it authenticates. For example, if the target file is stored in flash (`F:`), its `*.p7s` file is moved into the flash file system. If, however, you set the `*FA` variable in the file group's `CONFIG.SYS` file to `0`, all signature files are deleted from RAM when file authentication is complete. Removing `*.p7s` files will prevent application files from executing after a back-to-back download.

Please note also how the command-line mode switches described in Table 15 are used in this example:

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

- The `-L` switch indicates to store the application file in the flash file system instead of the target group's (default) RAM file system. (The target group for the download must be selected from terminal manager when the download is performed.)
- The `-f` switch indicates that the application file "`file.out`" must be signed by the VeriShield File Signing 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 authenticated on download.
- The `-s` switch is followed by the name of the signature file to be generated, `file.p7s`.
- The `-c` switch is followed by the name of the signer certificate to be used for file authentication with the development terminal, "`vxsign.crt`."
- The `-k` switch is followed by the name of the signer private key file, `vxsign.key`. A signer private key is a required input to the file signing process for development terminals and for deployment terminals.

VeriShield File Signing Tool Graphical Interface Mode

When you execute the VeriShield File Signing Tool, the VeriShield File Signing Tool dialog box opens.

The VeriShield File Signing Tool dialog box has four entry fields, each of which is followed by a "next" [**...**] selection button. There is one check box, and the OK and Cancel buttons.

- Press ALT+C or click the [**...**] button to the right of the Certificate field to locate and select the certificate file (`*.crt`) to be used to sign the file.
- Press ALT+K or click the [**...**] button to the right of the Key field to locate and select the signer private key file (`*.key`).
- Press ALT+F or click 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, the filename can also be modified.

  To store the file in flash memory upon 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 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 on the host PC to store the generated signature file.

- When all entries are complete, press ALT+O or click the OK button to execute the VeriShield File Signing Tool and generate the signature file, otherwise, press ALT+A or click Cancel to exit the VeriShield File Signing Tool.

When the necessary signature files are generated to authenticate the application or applications on the VX 520 terminal, perform the application download procedure.

For more information about file authentication within the context of specific download procedures, refer to Chapter 6.

CHAPTER 6

Performing Downloads

This chapter contains information and procedures to allow you to perform the various types of data transfers required to:

- Develop applications for the VX 520 terminal.
- Prepare VX 520 terminals for deployment.
- Maintain VX 520 terminals installations in the field.
- Transfer data to and from terminals.

In this chapter, information pertaining to file authentication is only discussed in the context of procedures while performing file downloads. See Chapter 5 for further file authentication discussion.

The VX 520 terminal contains ports that allow connection to a network, telephone line, or other terminals (for back-to-back downloads). See Download Methods.

Downloads and Uploads

Data can be transferred from a sending system to a receiving system while performing downloads. The term *download* also refers to a terminal receiving data. The term *upload* describes the process of a terminal sending data.

Use any of the following two operations to program, deploy, transfer data files from, and support VX 520 terminals:

- Host computer downloads: Applications, operating systems or OS updates, and associated files transfer from a host PC to a VX 520 terminal
- *Back-to-back* downloads: Applications and associated files transfer from one VX 520 terminal to another VX 520 terminal

Download Methods

The following methods are available for file and data downloads through the VX 520 download and upload procedures:

- **Direct downloads**: File and/or data transfer directly from the sending system (a host computer) to the receiving system (a VX 520 terminal). A special cable (VPN 05651-xx) connects the RS-232 serial ports of the two systems.
- **Downloads by telephone:** File and data transfer over a telephone line from the sending system (a host computer) to the receiving system (a VX 520 terminal). The modem of the sending host computer and the internal modem of the receiving terminal are connected by a telephone line. Data transfers into the VX 520 terminal through the communication port.
- **TCP/IP downloads:** File and data transfer over the TCP/IP connection from the sending system (a host computer) to the receiving system (a VX 520

terminal). A special cable (VPN 05651-xx) connects the RS-232 serial ports of the two systems.

- **Back-to-back downloads:** File and data transfer from a sending terminal to a receiving VX 520 terminal. A special cable (VPN 05651-xx) connects the RS-232 serial ports of the two terminals.
- **USB downloads:** File and data transfer from a USB-connected drive. The terminal searches for the `VeriFone.zip` file on the drive and downloads data from it.

NOTE

The terminal will automatically download the file `VeriFone.zip` from a USB flash drive without the user having to go through Entering Verix Terminal Manager under the following conditions:

- The USB flash drive is inserted before the terminal is powered up.
- The USB flash drive is inserted when the initial `DOWNLOAD NEEDED` message is displayed.

In both cases, the **USB DOWNLOAD COMPLETE** message appears on the terminal screen after the `VeriFone.zip` file has been downloaded.

Download Tools

Three software tools are available from VeriFone for performing downloads: **VeriCentre Download Management Module (DMM), VeriCentre, and DDL.EXE (Direct Download Utility)**.

NOTE

Because of the large size of some download files, VeriFone recommends only using download tools provided by VeriFone. CRC and other error checking is not supported on the GSM system. VeriFone download tools provide these error checking mechanisms.

The following tools perform direct downloads and downloads by telephone from a host computer to a VX 520 terminal:

- **VeriCentre DMM:** Multi-user environment for software downloads. DMM supports Windows NT clients and has a sophisticated database to manage up to 100,000 terminals. The VX 520 operating system supports file decompression for archives created using DMM.
- **VeriCentre:** PC-based software tool to manage applications and data for VeriFone. In addition to being a database and communications management tool, VeriCentre automates application downloads and updates to terminal records.
- **DDL.EXE:** Downloads files and data from a development system or another host computer, directly to a VX 520 terminal over a serial cable connection.

DDL.EXE is a Windows program included in the Verix V DTK (Verix V Developer's Toolkit).

NOTE

No special software tool or utility is required to perform back-to-back application downloads. Only a serial cable connected between two terminals is required. This data transfer procedure, invoked from within terminal manager, is handled by the OS software and firmware of the sending and receiving VX 520 terminals.

Download Content

In general, you can download files *and* data to a VX 520 terminal. The types of files and data can be grouped into the following functional categories:

- **Operating system files:** A set of related programs and data files provided by VeriFone to control the terminal's basic processes and functions. Files that belong to the OS are stored in a reserved area of the terminal memory.

  A complete OS is downloaded to each VX 520 terminal during the manufacture. If necessary, download newer versions during application development, or when preparing for deployment to on-site terminals.

- **Applications and related files:** An application is a computer program consisting of one or more executables, including compiled and linked object files (*.out), and one or more function libraries (*.lib). Most applications also include font files (*.vft, *.fon), data files (*.dat), and other related file types.

  VX 520 applications can be developed by VeriFone, customers, or third parties on customer request. One or more applications must be downloaded to the VX 520 terminal before it can be deployed at a customer site and used to process transactions.

- **Files related to file authentication:** The logical component of the VeriShield security architecture in the VX 520 terminal is *file authentication*. For an executable to run on a VX 520 terminal, it must be authenticated by the VeriShield file authentication module.

NOTE

For details on file authentication, see Chapter 5.

Two special types of files are required for the file authentication process: digital certificates (*.crt) and signature files (*.p7s). These file types must be downloaded to the terminal together with the application files to authenticate.

- **Terminal configuration settings:** Files or records that contain various types of data can also be downloaded to a VX 520 terminal, including CONFIG.SYS variables, passwords for accessing protected terminal manager functions, the current date and time, and the modem country code setting (refer to Chapter 4).

Full and Partial Downloads

When preparing to initiate a download procedure, choose either a *full* or *partial* download and the COM1 port, through the Verix Terminal Manager menu options (refer to Chapter 4). Depending on the type of files you are downloading and the download method you are using, there are some restrictions on whether a full or partial download is permitted.

The various types of full and partial download procedures are listed and described in Table 16.

Table 16 Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full application download	An entire application, including all executables and data files, transfers from one system to another in a single operation. Files related to the file authentication process and terminal configuration settings can be included in a full application download. During this process, RAM is cleared. Following a full application download, the terminal restarts and the file authentication module is invoked. If application files are authenticated and `CONFIG.SYS *GO` variable is set, then the application executes.	• Direct downloads • Telephone downloads • Back-to-back downloads
Partial application download	A subset of application executables, font files, and/or data files transfer from one system to another to modify or update an existing application. Files related to file authentication and terminal configuration settings can be included in a partial application download. During this process, RAM is *not* cleared. Following a partial application download, the terminal does not restart and returns control to terminal manager or the issuing application. The file authentication module is not invoked, nor are any applications allowed to execute, until the terminal is manually restarted from within terminal manager.	• Direct downloads • Telephone downloads **Note:** Partial back-to-back downloads are *not* supported.

Table 16 Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full operating system download	An *entire* OS version transfers from a host PC to the VX 520 terminal. Files related to file authentication and terminal configuration settings can be included in a full OS download. During this process, RAM is cleared. Following a full OS download, the terminal restarts and the file authentication module is invoked. If the OS files are authenticated, the new OS updates (replaces) the existing OS. Application files stored in the memory area where the OS downloads (Group 1) are erased.	• Direct downloads • Telephone downloads **Note:** Full back-to-back OS downloads are *not* supported.
Partial operating system download	Either an *entire* or a *partial* OS version transfers from a host PC to the VX 520 terminal. Files related to file authentication and terminal configuration settings can be included in a partial OS download. Following a partial OS download, the terminal does not restart and returns control to terminal manager or the issuing application. The file authentication module is not invoked, and the new OS is not processed until you manually restart the terminal from within terminal manager. If the new OS is authenticated, it then updates (replaces) the existing OS. Application files stored in the memory area where the OS downloads into (Group 1) are retained.	• Direct downloads • Telephone downloads **Note:** Partial back-to-back operating system downloads are *not* supported.

Implementation of full and partial downloads generally follow the following rules:

- The most common download procedure is a full (complete) application download.
- Partial application downloads are useful when developing and testing new applications, but are seldom performed by those who deploy terminals on-site.
- Full OS downloads are usually performed by VeriFone at the factory and, on occasion, by those who deploy terminals on-site to upgrade older terminals to a newer OS version.
- Partial OS downloads are performed mainly by VeriFone for development purposes and are rarely performed in the field.

- Partial downloads are routinely performed by many applications. This procedure, which can be automated by an application running on a remote host computer, permits the host application to update data files and terminal configuration settings in a VX 520 terminal and then return control to the main application.
- Full downloads restart the terminal; partial downloads return control to terminal manager or the issuing application. OS and application downloads can be combined. The file authentication module is not invoked until the terminal is restarted following the download procedure.

Support for Multiple Applications

The VX 520 terminal architecture supports multiple applications. This means that more than one application can reside in terminal memory, and that more than one application can run (execute) on the terminal.

The application memory of the VX 520 terminal uses a system of file groups to store and manage multiple applications, as well as operating system files. This system of file groups are used in such a way that the data integrity of each application is ensured and applications do not interfere with each other (see File Groups).

How the File System Supports Multiple Applications

The application memory partition of the VX 520 terminal is divided into 15 logically-defined sub-partitions called file groups or *GIDs* (for example, Group 1, Group 2, and so on through GID15).

Another partition of the terminal memory area, called Group 0, is reserved for the operating system and is logically separated from the application memory area. So, including Group 0, there is a total of 16 file groups.

An application must be downloaded into a specific file group, along with any related files. Select the target file group for the download using terminal manager menu options and by entering a file group password.

Usually, one application is stored in one file group. An application can consist of more than one executable program file, and any number of executables (*.out or *.lib) can be stored in a given group. In most implementations, there is a main application, one or more related programs or secondary applications, and one or more libraries.

The main application, or the application to execute set in the `*GO CONFIG.SYS` variable, must always be stored in the Group 1 sub-partition. Related programs or secondary applications can be stored in GIDs 2–14. GID15 is available to all other groups.

Main Application is Always Stored in GID1

The main application stored in GID1 is the controlling application for the terminal. Any function call that invokes a related program or a secondary application stored in GIDs 2–14 must be initiated by the GID1 application.

An application stored in a file group other than GID1 is limited in that it can only access executables and files stored in its own file group and in GID15.

Physical and Logical Access to File Groups

The VX 520 operating system controls *physical* access to GIDs 1–15 using password-protected terminal manager functions.

To download data into a specific file group, first enter terminal manager and choose the target group by making the appropriate menu selections, then, enter the correct password for that file group.

Each file group has its own `CONFIG.SYS` file. The `CONFIG.SYS` settings of the selected target group are used as the system parameters for the download operation.

The system of file groups also imposes some *logical* restrictions on which files can download into specific file groups:

- If GID1 is selected as the target group in terminal manager, you can download files into GID1 and redirect files into any of the other file groups, as required, in the same download operation.
- If another file group is selected as the target file group, you can download files only into that group and redirect files only to GID15. For example, if you select GID5 as the target group for the download, files can only download into GID5 and be redirected to GID15.

Use of RAM and Flash Memory

The VX 520 application memory partition has two separate file systems:

- RAM (battery-backed volatile memory, also called SRAM), partition designator `I:`
- Flash (non-volatile memory), partition designator `F:`

Having two different file systems has the following important implications for data transfer procedures:

- Depending on the requirements of a specific application, some files must download into RAM and others into flash.
- There are also rules that restrict which types of files you can download and store in a file system (RAM or flash).

With application files, the application designer or programmer usually decides which file types to download into which file system. Other file types, such as operating system files, digital certificates, and signature files, *must* download into RAM.

In a typical download procedure, all files are loaded into the RAM file system of the target group selected in terminal manager. Specific files included in the download package must be redirected, as necessary, to the flash file system of the target group or to the RAM or flash file system of another file group.

Defragment Flash For Application Downloads

Before performing an application download, defragment terminal flash memory. For information on performing this terminal manager operation, see Verix Terminal Manager Menu 2.

To ensure the best results when performing back-to-back downloads, defragment the flash memory of both the sending *and* receiving terminals. A terminal manager procedure is also available for clearing the RAM or flash memory, either entirely or for a specific file group, to prepare a VX 520 terminal for a *clean* download.

NOTE The flash defragment operation is not necessary for a VX 520 terminal just out of the box. In this case, the terminal flash file system is still in factory-new condition.

Redirection of Files During Application Downloads

You can download application files into RAM or flash memory. By default, files downloaded to a specific file group are stored in the RAM of that group. To store a file in the flash memory of that file group, provide instructions to redirect the file to flash as part of the procedure (see Manually Redirecting Files).

There are two methods used to redirect files during an application download, depending on the download tool:

- If you are using DMM, you must manually create and include special zero-length files called `SETDRIVE.x` and `SETGROUP.n` on the download computer, and add these files to the batch download list to direct files to a specific file system (drive) or file group.
- If you are using `DDL.EXE` to perform direct downloads, you can use a special command-line option that automatically redirects files to the drive and file group you specify.

Both of these methods are described in the following sections.

Manually Redirecting Files

To manually redirect files for DMM application downloads, create one or more files on the download computer with the special filename, `SETDRIVE.x`, where, *x* is the name of the partition (memory area) to download files to.

- Partition designator `I:` is RAM: This is the terminal manager default for downloads.
- Partition designator `F:` is flash.

To create a zero-length `SETDRIVE` file on the download computer, use the DOS command, REM, as in the following example:

```
REM >SETDRIVE.F
```

To redirect a file from the RAM of the target group to the flash memory of the same file group, insert the zero-length `SETDRIVE.F` file into the batch of application files to download. All files that follow the `SETDRIVE.F` file in the download list automatically load into the flash memory (`F:`) of the target group.

If you do not insert a `SETDRIVE.F` special file in the download list, all files download by default into the RAM (Drive `I:`) of the target file group. You can also insert a zero-length file with the name `SETDRIVE.I` into the download list at any point to indicate that all following files will download into RAM.

For example, the following batch download list loads the executable code file `FOO.OUT` into the RAM of the selected file group (default Group 1). Because the signature file, `FOO.P7S` is included, `FOO.OUT` is also authenticated when the terminal restarts after the download.

The `*GO` variable in this example indicates that the `FOO.OUT` application executes on restart, after successful authentication. The two data files that follow the zero-length `SETDRIVE.F` file, `FOO.DAT` and `FOO.VFT`, are redirected into GID1 flash. Because it follows the inserted zero-length `SETDRIVE.I` file, `GOO.DAT` downloads into Group 1 RAM.

```
FOO.OUT
FOO.P7S
*GO=FOO.OUT
SETDRIVE.F
FOO.DAT
FOO.VFT
SETDRIVE.I
GOO.DAT
```

You can also insert zero-length `SETGROUP.n` files into a batch download list to redirect files from the target file group to other file groups (see Redirecting Files to Other File Groups). Together, the zero-length `SETDRIVE.x` and `SETGROUP.n` files allow you flexibility to store files as required in the RAM or flash file systems, and in specific file groups in a single batch download operation.

NOTE

You can only use zero-length `SETDRIVE.x` files for *batch application downloads*, either direct or by telephone, and only using the DMM download tool (and not `DDL.EXE`).

You cannot use this special file convention for operating system downloads or for back-to-back application downloads.

Redirecting Files to Other File Groups

GID1 is the default terminal manager setting for performing downloads. Using the terminal manager menu options, you can select another file group (GID 2–15) as the target group for the application download. If you select another group, files download directly into the RAM of that file group.

To redirect files from the selected target file group to another file group as part of the download operation, insert a zero-length `SETGROUP.n` file in the batch download list (the same as `SETDRIVE.x`). The syntax of this convention is `SETGROUP.n`, where *n* = 1–15 for GIDs 1–15.

To create a zero-length `SETGROUP` file on the download computer, use the DOS command REM as in the following example:

```
REM >SETGROUP.2
```

If you do not insert SETGROUP.n special files into the download list, all files download into the target group selected in terminal manager. If no number is added to the SETGROUP filename, SETGROUP.1 (GID1) is assumed.

Restrictions on File Redirection

The VX 520 file system restricts how you can redirect files to other file groups. Here are the important points to remember:

- The main application must always be downloaded into GID1.
- Because of the way file groups are managed in the VX 520 file system, only two schemes are available for redirecting files during a batch application download:
  - If using terminal manager menu options, select Group 1 (default) as the target group for the download; files can be redirected to any other file group, including GID15.
  - If using terminal manager menu options, select a file group other than Group 1 (GIDs 2–14) as the target group for the download; files can be redirected only into the selected file group or into GID15.

In the following example, GID1 is selected as the target group for the download. The download list loads FOO.OUT into Group 1 RAM, GOO.OUT into GID2, and COMN.LIB shared library into GID15. When the terminal restarts after the download, the file authentication module is invoked for all three files, based on the certificate data that authorizes them to be stored in their respective file groups.

If FOO.OUT is authenticated, the GID1 application, FOO.OUT, executes as specified by the *GO variable when the terminal restarts following successful file authentication. The function library stored in GID15 can be shared by both applications, as both Group 1 and Group 2 applications can access Group 15.

```
FOO.OUT
FOO.P7S
*GO=FOO.OUT
SETGROUP.2
GOO.OUT
GOO.P7S
SETGROUP.15
COMN.LIB
COMN.P7S
```

NOTE

You can only use zero-length SETGROUP.x files for *batch application downloads*, either direct or telephone, and only using the Download Manager or ZonTalk 2000 download tools (not DDL.EXE). You cannot use this special file convention for operating system downloads or back-to-back application downloads.

Using DDL.EXE to Automatically Redirect Files

The version of `DDL.EXE` included in the VX 520 SDK allows you to change the default drive and file group for a direct download by preceding the filename(s) on the DDL command line with a special filename. The syntax is as follows:

```
SETDRIVE.<drive letter>
```

where, `drive letter` is `I:` for RAM, (default) or `F:` for flash, and/or

```
SETGROUP.<group number>
```

where, `group number` is 1–15.

For example, the command-line entry

```
DDL SETDRIVE.F cardco.lib SETDRIVE.I SETGROUP.15 card.dat
```

downloads the executable file `cardco.lib` into the flash of the selected target group and the data file `card.dat` into Group 15 RAM. (Because drive or group settings apply to all files that follow in the list, it is necessary to use `SETDRIVE.x` to reset the drive from `F:` back to `I:`.)

If you are using this `DDL.EXE` method, zero-length `SETDRIVE.x` and `SETGROUP.n` files do not need to exist as files on the download computer.

File Redirection in Operating System Downloads

When performing an operating system download, you *must* download the OS files into Group 1 RAM and not into flash memory or into another file group.

OS files are downloaded into Group 1 RAM because it is not possible to download these files directly into Group 0. OS files are redirected to Group 0 depending on if you perform a full or partial download (see Table 16).

- For full OS downloads, the redirection of OS files into Group 0 is performed automatically, after the terminal restart, and as part of the download procedure.
- For partial OS downloads, OS files are redirected from the RAM of Group 1 into Group 0 on manual terminal restart by selecting the appropriate terminal manager menu option.

A downloaded OS is processed and authenticated while stored in Group 1 RAM. As the files are authenticated under the authority of the certificates and signature files included in the OS download package, they move automatically into Group 0. This process, which usually takes a few moments, is completely transparent during the download procedure.

File Redirection in Back-to-Back Application Downloads

In a back-to-back application download, *all* application files stored on the sending terminal—in both file systems and in all file groups—transfer to the receiving terminal in a single operation.

For this type of download, you *must* select Group 1 as the target group on the sending *and* receiving terminals. When you initiate the download on the receiving terminal, all application files, as well as all special files required for file authentication and terminal configuration settings on the sending terminal, download to the receiving terminal.

In this type of data transfer operation, some file redirection does occur automatically as a result of the file authentication procedure that occurs on the receiving terminal. This redirection process is transparent during the download.

Briefly, all files initially download into RAM, and are then redirected based on the directory and subdirectory names of the sending terminal's file system. Signature files must always be authenticated in RAM. If the target file that the signature file authenticates is stored in flash, the signature file is moved to flash only after the target file successfully authenticates.

To successfully perform a back-to-back download, all signature files that are required to authenticate application executables must reside in the memory of the sending terminal. If the `*FA` variable is present in the Group 1 `CONFIG.SYS` file of the sending terminal, it must be set to 1 to retain all previously downloaded signature files.

If a signature file is missing on the sending terminal, the target application file that it authenticates is not authenticated on the receiving terminal and, if the target file is an executable, it is not allowed to run on the receiving terminal.

File Authentication Requirements

Chapter 5 provides a general introduction to the file authentication process. The following procedures show how the file authentication process affects the various download procedures.

Required Certificates and Signature Files

The following important points highlight how certificates and signature files relate to application download procedures:

- Before an executable file can be downloaded to and allowed to run on a VX 520 terminal, the file must be digitally signed on the download computer using the VeriShield File Signing Tool. The result of this procedure is a signature file recognized by its `*.p7s` filename extension.
- A signature file must be downloaded with each executable that makes up an application. An executable can be a compiled and linked object file (`*.out`) or a shared function library (`*.lib`).

  In most cases, an application consists of multiple executables and requires a number of corresponding signature files.
- In a typical batch application download, all files, including executables, signature files, and any required certificates, download in the same operation.
- After the download is complete and the terminal restarts, the file authentication module is invoked if a new signature file (or certificate) is detected. If the application (executable) is authenticated, it is allowed to run on the terminal. Otherwise, it does not execute.
- If one executable file required by an application with multiple executables fails to authenticate, the main application may crash when it attempts to access the non-authenticated executable.

- Application files other than executables (for example, font and data files) may also require logical security under file authentication. In these cases, each protected non-executable file also requires a corresponding signature file.
- Digital certificates (`*.crt`) and signature files (`*.p7s`) are required to authenticate both application files and operating system files, which must be downloaded into the RAM of the target file group.
- Certificate files are deleted from application memory after they are authenticated. If a certificate is not authenticated, it is retained in terminal memory.
- If the `*FA` variable in the `CONFIG.SYS` file of the target group is set to 1, signature files are redirected to the same location where the application file it authenticates is stored. If `*FA` is `0`, signature files are deleted from RAM when the file authentication process is complete.

File Authentication Process During an Application Download

In the following example of a typical file authentication process, assume the following:

- An application is being downloaded to prepare a VX 520 deployment terminal for deployment. That is, a sponsor certificate and a signer certificate download in batch mode to GID1 RAM of the receiving terminal, together with the application to authenticate.
- A signature file is generated for each executable that comprises the application on the download computer using the VeriShield File Signing Tool, with the signer certificate, signer private key, and signer password as required inputs. These signature files are also downloaded to the receiving terminal.

In a typical batch application download, file authentication proceeds as follows:

1. All certificate files (`*.crt`), signature files (`*.p7s`), and application files (`*.out`, `*.lib`, `*.fon`, `*.vft`, `*.dat`, and so on) download to the VX 520 deployment terminal in batch mode.

2. When the terminal restarts after the download, the file authentication module searches the RAM-based file system for the following two file types:

   - Authenticated certificate files (`*.crt`) to add to the permanent certificate tree.
   - Signature files (`*.p7s`) that authenticate corresponding target application files.

   Certificate files and signature files can download into the RAM of any file group. For this reason, the file authentication module searches through the entire file system (all file groups) for new files with these filename extensions each time the terminal restarts.

3 The file authentication module builds a list of all newly detected certificates and signature files. If no new certificates or signature files are located, the module just returns. If one or more new files of this kind are detected, the file authentication module starts processing them based on the list.

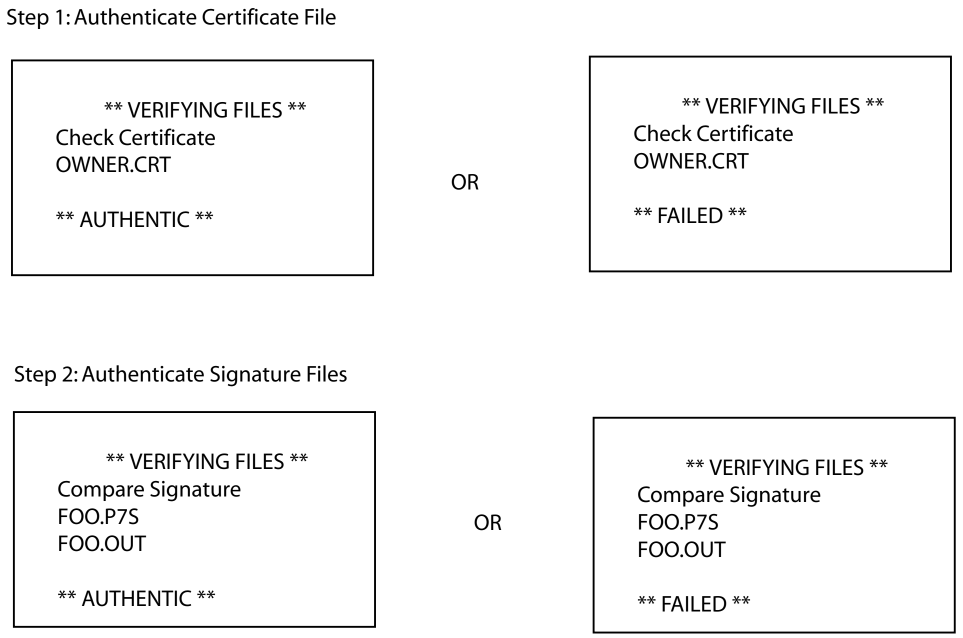
4 Certificates are always processed first (before signature files). The processing routine is called one time for each certificate in the list. If a certificate is authentic, it is noted, and the next certificate is processed. This process continues in random order until all certificates are authenticated.

When a certificate file in the processing list is authenticated, the “Authentic” message is displayed below the corresponding filename. If it fails to be authenticated, the ****FAILED**** message is displayed for five seconds and the terminal beeps three times (see Figure 33). The routine then resumes processing and continues until all certificates are successfully processed.

The processing routine gives both visible and audible indications if a specific certificate authenticates successfully. The file authentication module does not halt the process if a certificate fails to authenticate, but continues to the next step, which is authenticating signature files.

If one or more certificates fail to authenticate, the ensuing file authentication process based on signature files probably also fails, resulting to an application not authenticated and not allowed to execute on the terminal.

When a certificate file is authenticated, the data it contains is added to the certificate tree and the certificate file is deleted from the RAM. When all required certificates are authenticated and stored in the certificate tree, the file authentication process for signature files can proceed.



Step 1: Authenticate Certificate File

```
   ** VERIFYING FILES **
Check Certificate
OWNER.CRT

** AUTHENTIC **
```

OR

```
   ** VERIFYING FILES **
Check Certificate
OWNER.CRT

** FAILED **
```

Step 2: Authenticate Signature Files

```
   ** VERIFYING FILES **
Compare Signature
FOO.P7S
FOO.OUT

** AUTHENTIC **
```

OR

```
   ** VERIFYING FILES **
Compare Signature
FOO.P7S
FOO.OUT

** FAILED **
```

Figure 33 Display Prompts During the File Authentication Process

5 Signature files are now processed (after certificate files). The file authentication module calls the signature checking routine once for each new signature file it detects. Each `*.p7s` file is checked as it is detected; a list is not built and multiple processing passes are not required.

- If a signature file is authenticated, ***AUTHENTIC*** is displayed and the target file is flagged authentic.
- If the authentication process fails, ***FAILED*** is displayed for five seconds and the terminal beeps three times (see Figure 33). The routine then continues processing the next signature file until all newly detected signature files are checked.
- If a signature file fails to authenticate and its target file is an executable code file, such as `*.out` or `*.lib`, the executable is not allowed to run on the terminal on terminal restart.

For data files, font files, and any other files that require authentication to meet the application's design specification, the application must ensure that these files successfully authenticate.

While a signature file is being processed, it remains stored in the RAM file system of the target file group. The target application file may be redirected immediately on download to the RAM or flash.

When the signature file successfully authenticates its target file, it is automatically moved to the same file system and file group as the target file it authenticates (that is, if `*FA = 1`).

The processing routine gives visible and audible indications when a specific signature file authenticates successfully. The file authentication module does not halt the process if a signature file fails to authenticate, but continues to the next step, storing the downloaded files in their final locations in the terminal file system.

6 Certificate files and signature files are retained in the RAM file system until the file authentication process is complete. These special files are then either deleted or automatically redirected to another file system or file group, as previously described.

When an application file is authenticated, the operating system sets the file's read-only attribute to protect it from being modified while stored in terminal memory. This is also true for a signature file retained in terminal memory. When a signature file is assigned the read-only attribute, it is no longer detected as a new signature file by the file authentication module on terminal restart.

7 When all certificates and signature files are processed and special files are deleted or redirected as required, the terminal restarts and the `*GO` application executes.

File Group Permissions

This section discusses how file authentication controls *who* (which business entity) can store application files in which file groups in the VX 520 file system.

By inserting zero-length `SETDRIVE.x` and `SETGROUP.n` files into a download list, you can specify which drive (*x* = `I:` RAM or `F:` flash) and in which group (*n* = 1–15) to store an application file. In addition to this file redirection protocol, the file authentication module controls which files are allowed, under the authority of the signer certificate used to sign them, to be stored in which file groups in the VX 520 file system.

For example, if the terminal owner specifies storing a *loyalty* application in GID2, the information is encoded in the sponsor and signer certificates and issued by the VeriFone CA for that terminal.

Chapter 5 discusses how signer certificates are required inputs to the VeriShield File Signing Tool when preparing a deployment terminal. Each signature file generated under that signer certificate contains a logical link that allows the application to authenticate and run on the terminal *only* if the signature files and corresponding target files are downloaded into the target GID.

Although you *can* store files in any file group simply by selecting the target group in terminal manager, the files downloaded are not authenticated for the selected target group unless they are properly signed under the authority of the sponsor and signer certificates issued for that terminal.

Download an Operating System Update Provided by VeriFone

Because the operating system software for the VX 520 is developed and controlled by VeriFone for its customers, VeriFone provides the necessary certificates and signature files to ensure the authenticity and integrity of the operating system update as part of the download package.

NOTE

Operating system files can only be transferred to a VX 520 terminal using a PC-to-terminal download procedure, either direct or by telephone. OS files cannot be downloaded to a VX 520 terminal in a back-to-back operation.

The file authentication procedure for OS downloads is much the same as application downloads, with the following exceptions:

- VeriFone provides all files required for the OS download, including:
  - The operating system files (such as `Q.out`, `1.out`, and `2.out`).
  - An encrypted list of the new files, called `VFI.PED`.
  - A signature file generated by the VeriFone CA under the authority of a higher-level OS *partition sponsor certificate*, called VFI.crt. The file authentication logic on the receiving terminal uses this signature file to confirm the origin and authenticity of the encrypted list of files, `VFI.PED`.
- The entire OS package must download into Group 1 RAM. If you select a target group other than Group 1, the operation fails.

- Before initiating an OS download, either full or partial, ensure that enough memory space is available in Group 1 RAM to temporarily store the OS files, verify that any application files can also be stored in Group 1.
- If a *full* OS download was selected in Verix Terminal Manager, the terminal automatically restarts and the new OS is processed and replaces the existing OS. In this download operation, all application files stored in Group 1 are automatically erased.
- If a *partial* OS download was selected in terminal manager, the operating system returns control to terminal manager after the download completes. To process the new OS, you must *manually* restart the terminal by selecting the appropriate terminal manager menu option. In a partial OS download operation, application files stored in Group 1 are not erased.
- When the OS download is initiated, the OS file authentication progress is displayed on the screen as new certificates are authenticated and added to the terminal's certificate tree, and as signature files for corresponding OS files are detected and authenticated, as shown in Table 33.
- While the new OS is being processed, there is no visible indication on the terminal display of the progress of processing. When the new OS is processed (this usually takes a few moments), the terminal restarts automatically and the OS download procedure is complete.

CAUTION If the power supply to the receiving terminal is accidentally cycled during an operating system download procedure, the terminal may permanently lock up. In that case, return the terminal to VeriFone for service.

File Authentication for Back-to-Back Application Downloads

When performing a back-to-back application download between two VX 520 terminals, the file authentication process on the receiving terminal is similar to an application download from a host computer to a standalone VX 520 terminal. There are some important differences to take into account:

- Only a *full* application download is supported for back-to-back data transfers. You cannot perform partial back-to-back application downloads.
- Before you can initiate the back-to-back download, you must enter terminal manager in *both terminals*, select Group 1 as the target group for both terminals, and enter all required passwords.
- All signature files required to authenticate the download application(s) must reside in the memory of the sending terminal. They *must not be deleted* through the `*FA` variable being cleared to 0 on previous downloads.
- Any sponsor and signer certificates downloaded to and authenticated on the sending terminal are stored in the certificate tree of that terminal. When you perform a back-to-back download, certificate files are reconstructed from the data present in the sending unit's certificate tree.

- All certificates transfer to Group 1 RAM on the receiving terminal, except for the highest-level *platform root certificate*, which can never be transferred to another terminal.
- When certificates are detected by the file authentication module of the receiving terminal, they are processed exactly as in a direct download: All certificates are checked one by one and, on authentication, are added to the certificate tree of the receiving terminal. Then, all signature files are checked.
- Downloaded certificates (receiving terminal) must synchronize with the certificate data present in the certificate tree.

  "Synchronized" means that the certificate tree of the receiving terminal can be no more than one revision out-of-sync with the certificate tree on the sending terminal or the files on the receiving terminal do not successfully authenticate. In this case, the term *revision* refers to any generic change to the current sponsor and signer certificates stored in the certificate tree of a deployment terminal.
- When the back-to-back download completes and all certificates and signature files authenticate, the receiving terminal restarts. If the name of the `*GO` application is specified in the Group 1 `CONFIG.SYS` file of the receiving terminal, the application executes and the application prompt or logo is displayed on the terminal.

Timing Considerations Due to the Authentication Process

The file authentication process takes some time. The total amount of time required depends on a number of factors:

- The number and size of application files.
- The number of certificates and signature files.
- Whether the file compression feature of Download Manager is being used to perform the download.

Here are a few additional considerations that may affect the total elapsed time required to complete the download operation:

- Because additional processing steps are required, an operating system download takes longer to complete than an application download (several minutes as opposed to a few seconds).
- The download order of a batch of certificate files may affect total processing time. Digital certificates are validated in a looping process where the validation process cycles as many times as necessary to establish the proper relationship and position of a given certificate in the certificate tree that exists in the terminal.

  To optimize the authentication process, download certificates in a higher-level-certificates-first order. This way, they process faster than a random order download.

Optimize Available Memory Space for Successful Downloads

One certificate file or signature file requires approximately 400 bytes of memory space. The application designer must account for the extra memory required to download and store these special files.

When planning your download procedure, carefully consider the total amount of memory space required to store certificates and signature files *and* the application files. In some cases, a considerable number of 400-byte signature files reside in terminal memory at any given time. Here are some general guidelines to follow:

- Know the size of available memory (RAM and flash) of the receiving terminal; also in back-to-back downloads, know the size of available memory on both the sending and receiving terminals.
- Know in advance how application files are redirected to RAM or flash and to file groups other than the target group.
- Defragment flash memory before performing a download to optimize the available space in the flash file system.
- Before performing a download, use the Verix Terminal Manager menu selections to clear the entire RAM and/or flash of a specific file group, as necessary, to ensure proper use of available memory in the target group.

Support for File Compression

For information regarding file compression, refer to the *Verix V Operating System Programmers Manual* (VPN 23230).

Effect of Downloads on Existing Files and Data

When downloading application files and data to a VX 520 terminal, an important consideration is the effect of download procedure on existing application files, files used in the file authentication process, and terminal configuration settings stored in `CONFIG.SYS` files in the receiving terminal. Here are some important points:

- If a file already exists in the target file group, the existing file is replaced with the new file of the same name. (Files in separate file groups can have identical names).
- Always download executable files (and any other files to logically protect under VeriShield file authentication) with the certificates and signature files required to authenticate them.
- In full or partial application downloads, all `CONFIG.SYS` records on the receiving terminal, both protected and non-protected (that is, beginning with * or #), are retained. New `CONFIG.SYS` variables included in the download package, including the `*GO` variable, selectively replace existing variables with the same key name in the `CONFIG.SYS` file of the target group.

- All current passwords are retained on the receiving terminal during an application or operating system download (direct, by telephone, and back-to-back). This includes the terminal manager password and file group passwords. If required, you can replace existing *file group* passwords with new values as part of the data transfer operation.

NOTE

Always modify the *Verix Terminal Manager* password in a separate, securely-controlled operation. Ensure that this password is retained in a secure place.

- For back-to-back application downloads, clear the RAM and flash of the receiving terminal before initiating the download. All application files stored on the receiving terminal, including `CONFIG.SYS` settings, are replaced by those of the sending terminal. Verix Terminal Manager and file group passwords are retained on the receiving terminal.
- For full operating system downloads, Group 1 RAM is cleared as part of the operation and any application files stored in GID1 are erased. In this case, previously downloaded and authenticated applications must be downloaded in a subsequent operation, together with the certificates and signature files required to authenticate them.

Set Up the Download Environment

The first step in performing a download to a VX 520 terminal is to establish the physical communication link between the sending and receiving systems required to support the following download methods:

- **Direct serial cable connection for direct application and OS downloads:** The link is between the COM1 port of a download computer (PC) and the COM1 port on the receiving VX 520 terminal.

  Two special cables are available from VeriFone to support direct downloads: one for computers with DB-25-type serial connectors (VPN 26263-02) and another for DB-9-type connectors (VPN 26264-01). Both of these cables have a 10-pin RJ-45 modular plug on one end for the terminal-side connection.

- **Telephone line connection for application or OS downloads by telephone:** The link is from the modem connection of a host computer to the integrated modem direct in the receiving terminal (see Figure 34).

  For this type of download operation, a standard telephone line cord with modular Telco connectors is required.

- **Direct serial cable connection for back-to-back application downloads:** The link is between the RS-232 ports of the sending and receiving VX 520 terminals.

  A special cable is required for back-to-back downloads (VPN 05651-00). This cable has two 10-pin RJ-45 modular plugs on each end to establish the terminal-to-terminal connection.

Cable Connection for Direct Downloads

There are two cables for direct downloads:

- DB-25 serial connector (VPN 26263-02)
- DB-9 connector (VPN 26264-01)

The following steps describe how to establish the cable link between the sending host computer and the receiving VX 520 terminal (see Figure 34):

1. Connect the DIN-type connector on one end of the cable to the COM1 (or COM2) serial I/O port on the download computer.
2. Connect the RJ-45 connector on the other end of the download cable to the RS-232 port on the back panel of the VX 520 terminal.

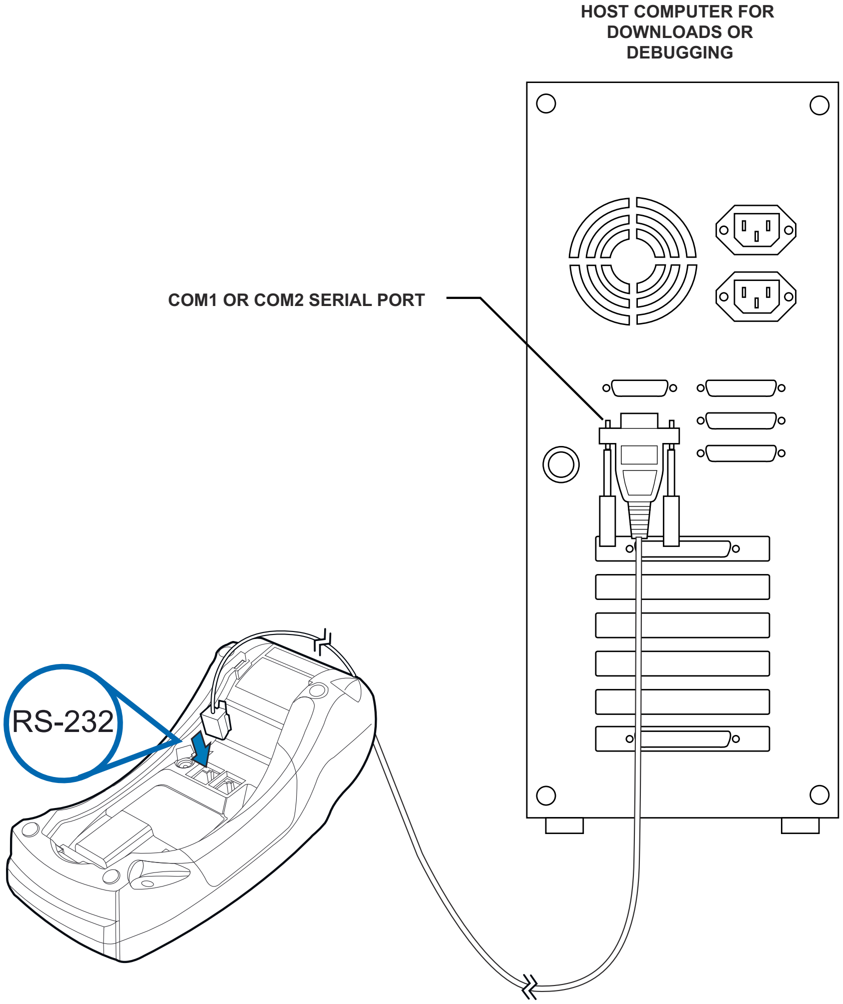


Figure 34 Serial Cable Connection for Direct Downloads

Telephone Line Connection for Telephone Downloads

To set up the telephone line connection for application or OS downloads between a host computer and a VX 520 terminal:

1. Confirm proper configuration of the dial-up telephone line and modem connection on the host computer.

2. Confirm that the parameters for the download by telephone are set in the download tool.
3. Confirm that the receiving VX 520 terminal has a direct telephone line connection.
4. Ensure that the correct keyed variables used to control downloads by telephone are stored in the `CONFIG.SYS` file of the target file group on the receiving terminal.

Cable Connection for Back-to-Back Application Downloads

To prepare for a back-to-back application download:

1. Insert the RJ-45 modular connector on one end of the download cable (VPN 05651-00) into the RS-232 port of the sending terminal.
2. Insert the RJ-45 connector on the other end of the cable into the RS-232 port on the back panel of the receiving terminal.
3. Power up both terminals.

Common Steps to Start a Download

After setting up the appropriate cable connections, power up the terminal and initiate the downloading session. Table 17 guides you through the common steps when initiating a download. Procedures specific to a download type is discussed in the later sections.

Table 17 Common Steps to Start a Download

Step	Display	Action
1	**VERIFONE VX 520 QT00E20B 12/22/2009 Verix COPYRIGHT 1997-2009 VERIFONE ALL RIGHTS RESERVED**	At startup, the terminal displays a copyright notice screen that shows the terminal model number, the OS version of the VX 520 stored in the terminal's flash memory, the date the firmware was loaded into the terminal, and the copyright notice. This screen appears for three seconds, during which time you can enter Verix Terminal Manager by simultaneously pressing F2 and F4. You can extend the display period of this screen by pressing any key during the initial three seconds. Each keypress extends the display period an additional three seconds.

Table 17 Common Steps to Start a Download

Step	Display	Action
3	**<application prompt>** **DOWNLOAD NEEDED** **<error message>**	If an application already resides on the terminal, an application-specific prompt is displayed. If no application resides on the terminal or an application error is detected, the following message is displayed: **DOWNLOAD NEEDED** For more information on startup errors, see STARTUP ERRORS. To enter Verix Terminal Manager from this screen, simultaneously press F2 and F4. **Note:** The terminal will automatically download the file `VERIFONE.ZIP` from a USB flash drive without the user having to go through Verix Terminal Manager under the following conditions: • The USB flash drive is connected before the terminal is turned on. • The USB flash drive is inserted when the initial **DOWNLOAD NEEDED** message is displayed. In both cases, the **USB DOWNLOAD COMPLETE** message will appear on the terminal screen after the `VERIFONE.ZIP` file has been downloaded.
4	**TERMINAL MGR ENTRY** **Please Enter Password** __________	If an application prompt appeared and you chose to enter terminal manager, you are prompted to type the system password. If **DOWNLOAD NEEDED** appeared, use the default password "1, Alpha, Alpha, 66831." Use ← to delete the entry and correct any mistakes. If you enter an incorrect password, the terminal exits the **VERIX TERMINAL MGR ENTRY** screen. Verify your password and reenter it. To quit this operation and return to the application prompt or **DOWNLOAD NEEDED** screen, press ✕.

Table 17 Common Steps to Start a Download

Step	Display	Action
5	**VERIX TERMINAL MGR** **1> Restart** **2> Edit Parameters** **3> Download** **4> Memory Usage** **5> RAM Directory** **6> Flash Directory** ↓ ↑ ↓	The first of three **VERIX TERMINAL MGR** menus is displayed. To toggle through to the other two menus, press the PF1 and PF2 keys. To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the PF3 button then press the enter key. Use the PF4 key to scroll up the menu options. Select **3> DOWNLOAD**to start a download session.

Direct Application Downloads

This section provides the hardware and software checklist needed for direct application downloads. The procedure for direct application downloads is also discussed.

Hardware Checklist

- □ The correct cable connects the download computer serial port (COM1 or COM2) to the RS-232 serial port (COM1) of the VX 520 terminal (refer to Cable Connection for Direct Downloads).

Software Checklist

- □ Download Manager, VeriCentre, or `DDL.EXE` running on the host computer.
- □ The application file to download (full or partial) is located on the host computer.
- □ The correct keyed record variables exist in the `CONFIG.SYS` file(s) of the file group(s) to store the application files.
- □ Certificate files (`*.crt`) required for file authentication on the receiving terminal are stored in memory or they are located on the host computer, and must download with the application files.
- □ All required signature files (`*.p7s`) generated using the VeriShield File Signing Tool are located on the host computer. One signature file downloads for each executable (`*.out` or `*.lib`) to run on the terminal.
- □ The filenames in the batch download list on the host computer indicate which application files to redirect to flash and file groups other than the target group.
- □ Ensure that filenames and `CONFIG.SYS` variables to download are correct in relation to those stored in the memory of the receiving terminal to avoid accidental overwrites.
- □ The required terminal manager and file group passwords are available to make the required terminal manager menu selections and to prepare the receiving terminal to receive the application download.
- □ Sufficient memory space exists in the RAM of the target group so that it can accept the entire download package, including certificates, signature files, and all data files.

❑ Use the terminal manager menu options to clear the entire RAM or flash or specific file groups on the receiving terminal (as necessary). Perform a flash defragment (merge) operation to optimize the flash file system (as necessary, the application itself can issue a function call to defragment the flash on restart after the download.) For more information on terminal manager operations, refer to Chapter 4, Verix Terminal Manager.

Checklist for Effects on Files and Settings in the Receiving Terminal

❑ Protected records in the `CONFIG.SYS` file(s) of the receiving terminal — keyed records that begin with * or # — are not erased.

❑ The bootloader, OS, and other firmware on the receiving terminal are not modified as a result of the application download.

❑ The certificate tree that exists on the receiving terminal is not modified unless one or more new certificate files are downloading to the terminal. When new certificates are authenticated on the receiving terminal, the data they contain is stored in the certificate tree and the certificate files are deleted from the RAM of the target group.

Direct Application Download Procedure

The procedure in Table 18 describes how to perform a direct application download from a host download computer into the Group 1 application memory area of a VX 520 deployment terminal.

Steps described in the *Action* column are performed directly on the VX 520 terminal. Notes provided in this column indicate and explain actions you must perform on the host computer.

NOTE The eight steps listed in Table 18 are required for all download and upload procedures. In each of the following procedural tables, step numbering starts at 1 to indicate the unique steps of the specific download method. In subsequent procedures, only the method-specific steps are documented; the five steps in Table 17 are assumed to be complete.

Table 18 Direct Application Download Procedure

Step	Display	Action
1	**VERIX TERMINAL MGR** **GROUP ID: nn**	Enter the target file group for the download. **FILE GROUP _1** (Group 1) is displayed as the default selection. **Note:** File Group 1 is reserved for the operating system. Try using a different file group when downloading additional applications. For more information on operating system downloads, see Direct Operating System Downloads. To select a file group other than Group 1, type the one or two-digit number of the desired file group (2–15) for the download.
2	**TERMINAL MGR ENTRY** **Please Enter Password** ____________	Enter the password of the selected file group. For example, if Group 2 is the target group, the **GROUP _2 PASSWORD** message is displayed. **Note:** If you have not previously entered a group's password in this session, the terminal prompts for the group's password prior to downloading applications. To continue, enter the required password. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↵. Verify your password and reenter it.
3	**VTM DOWNLOAD MGR** **1> Full dnld** **2> Partial dnld**	Select whether to run a full or partial download. **Note:** If you selected **1> FULL DNLD** on a single application download, a screen will appear warning you that all existing files in the selected group will be deleted. Press F3 to cancel or F4 to continue downloading an application. If you selected **1> FULL DNLD** on a multiple application download, you will be prompted to clear the existing application on the currently selected group. Select **1> YES** to continue or **2> NO** to cancel downloading applications.

Table 18 Direct Application Download Procedure

Step	Display	Action
4	**VTM DOWNLOAD MGR Gnn** **1> Modem** **2> COM1** **3> COM2** **4> SD Card** **5> Memory Stick** **6> TCPIP** ↓ ↑ ↓	Select **2> COM1** for a direct application download. When you press 2, the terminal is ready to receive the application download from the host computer. Press the PF1 key to view more system download modes.
	VTM DOWNLOAD MGR Gnn **1> USB Dev** **2> COM6** ↑ ↑ ↓	
5	**VTM DOWNLOAD MGR Gnn** *****_______** **DOWNLOADING NOW**	Initiate the download by executing the proper command(s) in the download tool running on the host computer. The data transfer operation starts, and the status messages are displayed on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk indicates that 10% of the download is complete). When the last asterisk is displayed, the download is complete. If you performed a full download, the terminal restarts automatically. Otherwise, you must restart the terminal manually by selecting **RESTART** on the first menu of **VERIX TERMINAL MGR**. If an application resides on the terminal following the download, it executes on restart.

Table 18 Direct Application Download Procedure

Step	Display	Action
6	****VERIFYING FILES**** **CHECK CERTIFICATE** **FILENAME.CRT** ***AUTHENTIC*** ****VERIFYING FILES**** **COMPARE SIGNATURE** **FILENAME.P7S** **FILENAME.OUT** ***FAILED***	On startup, the file authentication module authenticates any new signature files downloaded with the OS files. When the signature file authentication routine starts, the status display informs you of the progress of the authentication process. If file authentication succeeds for a specific signature file, the "**AUTHENTIC**" message is displayed directly below the filename of the signature file. If file authentication fails for a specific signature file, the "**FAILED**" message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate. The authentication process then proceeds to the next signature file until all signature files are validated. When all new signature files are authenticated, the terminal restarts, and the application specified in the `*GO` variable or the default application in Group 1 executes and starts running on the terminal.
7	**<application prompt>** **DOWNLOAD NEEDED** **<error message>**	If the downloaded application successfully authenticates, the corresponding application prompt or logo is displayed upon restart. The terminal can now process transactions. **Note:** The message **DOWNLOAD NEEDED** appears if: • The `*GO` variable is not set. • `*GO` does not specify that an application is present. • The application did not authenticate (invalid or missing `*.p7s` file). • The application uses shared libraries that are missing or were not authenticated (invalid or missing `*.p7s` files). If one or more executables in the application fail to successfully authenticate, the application may not run. If the application attempts to access an unauthenticated executable or library, it may crash. Repeat the Direct Application Download Procedure using the correct certificates and/or signature files. For more information on startup errors, see STARTUP ERRORS.

Direct Operating System Downloads

This section provides the hardware and software checklist needed for direct operating system downloads. The procedure for direct operating system downloads is also discussed.

Hardware Checklist

- ❑ The correct cable connects the download computer serial port (COM1 or COM2) to the RS-232 serial port (COM1) of the VX 520 terminal (refer to Cable Connection for Direct Downloads).

Software Checklist

- ❑ Download Manager, VeriCentre, or DDL.EXE running on the host computer.
- ❑ The complete OS version to download is located on the host computer.
- ❑ Select full or partial download of the OS. In a full OS download, the terminal restarts automatically and the new OS is processed, replacing the existing OS. In a partial OS download, the terminal returns to terminal manager and the new OS does not process until you manually initiate a terminal restart from terminal manager.
- ❑ The correct keyed record variables for the download exist in the `CONFIG.SYS` files of Group 1. (OS files must always download into GID1 RAM). The required variables can also be written into the `CONFIG.SYS` file as part of the download operation.
- ❑ The following files provided by VeriFone CA for full OS downloads must reside on the host computer:
  - The new OS version or OS update (`Q*.out`, `1*.out`, `2*.out`, `3*.out`, `4*.out`, `5*.out`, `6*.out`).
  - A signature file called `VFI.p7s` for the OS update. This signature file is generated by the VeriFone CA using the high-level OS certificates for the VX 520 platform.
  - A file called `VFI.PED`. This file is an encrypted list of the new OS files.
- ❑ The required terminal manager and file group passwords are available to make the required terminal manager menu selections to prepare the receiving terminal to receive the application download.
- ❑ Sufficient memory space exists in the Group 1 RAM to accept the OS download package including certificates, signature files, and all data files.
- ❑ Use the terminal manager menu options to clear the entire RAM or flash or the RAM of Group 1 on the receiving terminal (as necessary).

Checklist for Effects on Files and Settings in the Receiving Terminal

- ❑ A full OS download replaces the existing OS and erases all application files from the Group 1 RAM.
- ❑ A partial OS download returns control of the terminal to terminal manager and does not erase application files from the Group 1 RAM.
- ❑ Protected records in the `CONFIG.SYS` file(s) of the receiving terminal — keyed records that begin with * or # — are not erased.

- An OS download does not overwrite terminal configuration settings, including the current date and time, passwords, and modem country code. If required, you can download new terminal configuration settings together with the OS files.
- The certificate tree that exists on the receiving terminal is not modified unless one or more new certificate files required to authenticate the new OS are being downloaded to the terminal. When new certificates authenticate on the receiving terminal, the data they contain is stored in the certificate tree and the certificate files are deleted from the Group 1 RAM.
- The certificates and signature files required to authenticate the new OS are processed by the file authentication module of the receiving terminal the same as application files.
- When the terminal restarts and the new OS files process, they are moved out of the Group 1 RAM into the Group 0 area of the VX 520 file system.

Direct Operating System Download Procedure

The procedure in Table 19 describes how to perform a direct operating system download from a host computer into the Group 1 RAM of a VX 520 terminal.

Steps described in the *Action* column are performed directly on the VX 520 terminal. Notes provided in this column indicate and explain actions you must perform on the host computer.

NOTE In Table 19 and in the following procedures, only method-specific steps are included. For a description of the steps required to enter terminal manager and display the first menu of **VERIX TERMINAL MGR**, refer to Table 17.

Table 19 Direct Operating System Download Procedure

Step	Display	Action
1	**VERIX TERMINAL MGR** **GROUP ID: nn**	**FILE GROUP: _1** (Group 1) is automatically displayed on the screen. **Note:** Operating system files must *always* download into Group 1. This is the default group number in terminal manager. Press ↵ to select Group 1.
2	**VERIX TERMINAL MGR EDIT** **GROUP nn PASSWORD** __________	Enter the password for Group 1 and press ↵ . If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ← and type in a valid password. Press ↵ to confirm the newly entered password.

Table 19 Direct Operating System Download Procedure

Step	Display	Action
3	**VTM DOWNLOAD MGR** **1> Full dnld** **2> Partial dnld**	Select a full or partial OS download. To return to the first **VERIX TERMINAL MGR** menu, press x.
4	**VTM DOWNLOAD MGR Gnn** **1> Modem** **2> COM1** **3> COM2** **4> SD Card** **5> Memory Stick** **6> TCPIP** ↓ ↑ ↓	Select **2> COM1** for a direct application download. When you press 2, the terminal is ready to receive the application download from the host computer.
5	**VTM DOWNLOAD MGR Gnn** *******_______ **DOWNLOADING NOW**	Initiate the download by executing the proper command(s) in the download tool running on the host computer. The data transfer operation starts, and the status messages are displayed on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk indicates that 10% of the download is complete). When the last asterisk is displayed, the download is complete. If you performed a full download, the terminal restarts automatically. Otherwise, you must restart the terminal manually by selecting **1> RESTART**on the first **VERIX TERMINAL MGR** menu. If an application resides on the terminal following the download, it executes on restart.

Table 19 Direct Operating System Download Procedure

Step	Display	Action
6	****VERIFYING FILES**** **CHECK CERTIFICATE** **FILENAME.CRT** ***AUTHENTIC***	When the OS download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal begins to check for new certificate (`*.crt`) and signature (`*.p7s`) files included in the download. These special files then process one at a time; certificates process first, then signature files.
	****VERIFYING FILES**** **COMPARE SIGNATURE** **FILENAME.P7S** **FILENAME.OUT** ***AUTHENTIC***	When the file authentication module is invoked, the status display informs you of the progress of the file authentication process. If file authentication succeeds for a specific certificate, the ***AUTHENTIC*** message is displayed directly below the certificate filename. If file authentication fails for a specific certificate, the ***FAILED*** message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate.
		The authentication process then continues to the next certificate until all new certificates are checked.
7	**<application prompt>**	When all new signature files are authenticated, the terminal restarts and begins processing the new OS (full download) or it returns control to terminal manager (partial download).
	DOWNLOAD NEEDED **<error message>**	Because a full OS download clears the RAM, all terminal applications, related certificates, and signature files must download to the terminal when performing this type of download.

Download by Telephone

The procedure to perform an application or OS download by telephone is similar to that of direct application (see Table 18) and direct operating system downloads (see Table 19).

Hardware Checklist

□ Set up the dial-up telephone line and modem connection on the host computer.

□ Set up the direct telephone line connection on the receiving VX 520 terminal, as described in Telephone Line Connection for Telephone Downloads.

Software Checklist

□ Download Manager or VeriCentre running on the host computer.

Note: `DDL.EXE` can only be used for direct downloads.

□ The information required to control the download by telephone is stored in the `CONFIG.SYS` file of the target group selected on the receiving terminal. Required settings for Download Manager and VeriCentre may include the following:

- Dial-up numbers to establish the telephone line connection
- Baud rate settings for the data transfer
- Terminal ID
- Application ID
- Operating system name or serial number

NOTE

For detailed information about the setup requirements and download procedures for Download Manager and VeriCentre, refer to the user documentation supplied by VeriFone with these software products.

Telephone Download Procedure

Select the modem port (step 4 in Table 20) on the receiving terminal when the port selection options are displayed. The internal modem in the receiving VX 520 terminal dials the host computer to request the download. When the host computer accepts the call, the host initiates the download procedure.

Table 20 Download by Telephone Procedure

Step	Display	Action
1	**VERIX TERMINAL MGR** **GROUP ID: nn**	**FILE GROUP: _1** (Group 1) is automatically displayed on the screen. **Note:** Operating system files must *always* download into Group 1. This is the default group number in terminal manager. Press ↵ to select Group 1.

Table 20 Download by Telephone Procedure

Step	Display	Action
2	**VERIX TERMINAL MGR EDIT** **GROUP nn PASSWORD** ____________	Enter the password for Group 1 and press ↵. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ← and type in a valid password. Press ↵ to confirm the newly entered password.
3	**VTM DOWNLOAD MGR** **1> Full dnld** **2> Partial dnld**	Select a full or partial OS download. To return to the first **VERIX TERMINAL MGR** menu, press ✕.
4	**VTM DOWNLOAD MGR Gnn** **1> Modem** **2> COM1** **3> COM2** **4> SD Card** **5> Memory Stick** **6> TCPIP** ↓ ↑ ↓	Select **1> MODEM** for a telephone procedure download.
5	**VTM DOWNLOAD MGR Gnn** ***ZP HOST PHONE NUM** ________________	If `*ZP` (host phone number) is not defined, you must enter valid phone number (up to 32 characters long) and press ↵.
6	**VTM DOWNLOAD MGR Gnn** ***ZT TERMINAL ID** ________________	If `*ZT` (terminal ID used by VeriCentre) is not defined, you must enter a valid terminal ID (up to 15 characters long) and press ↵.

Table 20 Download by Telephone Procedure

Step	Display	Action
7	**VTM DOWNLOAD MGR Gnn** ***ZA APPLICATION ID** ________	If `*ZA` (application ID) is not defined, you must enter a valid application ID (up to 10 characters long) and press ↵ .
8	**VTM DOWNLOAD MGR Gnn** ***ZA= nnnn** ***ZP= nnnn** ***ZR= nnnn** ***ZT= nnnn** **1> EDIT** **2> START**	You can view the specified values on the confirmation screen. Select **1> EDIT** to go back and modify the specifications or **2> START** to begin the download.
9	**VTM DOWNLOAD MGR Gnn** **GID: nn** **APP ID: nnnn** **STATUS: DOWNLOADING** *******________	The progress of the download is indicated by a series of ten asterisks (each asterisk indicates that 10% of the download is complete). If the download is successful, the message **DOWNLOAD DONE** is displayed. If you performed a full download, the terminal restarts automatically. Otherwise, you must restart the terminal manually by selecting **1> RESTART** on the first **VERIX TERMINAL MGR** menu. If an application resides on the terminal following the download, it executes on restart. If an error occurs during connection or download, an error message is displayed. For more information on downloading errors, see DOWNLOADING ERRORS.

Table 20 Download by Telephone Procedure

Step	Display	Action
10	**VERIFYING FILES** COMPARE SIGNATURE FILENAME.P7S FILENAME.OUT *AUTHENTIC* **VERIFYING FILES** COMPARE SIGNATURE FILENAME.P7S FILENAME.OUT *FAILED*	On startup, the file authentication module on the receiving terminal begins to check for new certificate (`*.crt`) and signature (`*.p7s`) files included in the download. These special files then process one at a time; certificates process first, then signature files. When the file authentication module is invoked, the status display informs you of the progress of the file authentication process. If file authentication succeeds for a specific certificate, the ***AUTHENTIC*** message is displayed directly below the certificate filename. If file authentication fails for a specific certificate, the ***FAILED*** message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate. The authentication process then continues to the next certificate until all new certificates are checked.
9	<application prompt> DOWNLOAD NEEDED *GO FILE NOT FOUND	If the downloaded application successfully authenticates, the corresponding application prompt or logo is displayed upon restart. The terminal can now process transactions. **Note:** The message **DOWNLOAD NEEDED** appears if: • The `*GO` variable is not set. • `*GO` does not specify that an application is present. • The application did not authenticate (invalid or missing `*.p7s` file). • The application uses shared libraries that are missing or were not authenticated (invalid or missing `*.p7s` files). If one or more executables in the application fail to successfully authenticate, the application may not run. If the application attempts to access an unauthenticated executable or library, it may crash. Repeat the Download by Telephone Procedure using the correct certificates and/or signature files. For more information on startup errors, see STARTUP ERRORS.

Back-to-Back Application Downloads

This section provides the hardware and software checklist needed for back-to-back application downloads. The procedure for back-to-back terminal downloads is also discussed.

Hardware Checklist

- ❑ The correct serial cable connects the RS-232 ports of the sending and receiving VX 520 terminals (refer to Cable Connection for Back-to-Back Application Downloads).
- ❑ Verify that the RAM size on the receiving terminal is large enough to receive files uploaded from the sending terminal. If the RAM on the sending terminal is 512 KB, the RAM on the receiving terminal must be at least 512 KB.

Software Checklist

- ❑ The firmware versions of the sending and receiving terminals must be identical or very similar.
- ❑ One or more complete and authenticated application programs are stored in the GIDs 1–15, RAM or flash of the sending terminal. In this type of operation, *all* files stored in application memory of the sending terminal download to the receiving terminal.
- ❑ Before initiating the download procedure, remember to select Group 1 as the target file group on both the sending and receiving terminals. The required terminal manager and file group passwords must also be available to make the required terminal manager menu selections on both terminals.
- ❑ The current `CONFIG.SYS` variables, date and time, and other terminal configuration settings on the sending terminal are those downloaded to the receiving terminal. Ensure that the desired settings are correct.
- ❑ All signature files required to authenticate the application files being downloaded to the receiving terminal are present in the RAM or flash file system of the sending terminal.
- ❑ The certificate tree of the sending and receiving terminal must be synchronized. That is, there can be no more than one revision difference between the certificate data currently stored in the memory of the sending and receiving terminals.
- ❑ If application files are downloaded to the receiving terminal in previous operations, use the terminal manager menu options to clear the RAM and flash file systems of the receiving terminal before you initiate the back-to-back download procedure. This ensures a clean download.

Checklist for Effects on Files and Settings in the Receiving Terminal

- ❑ A back-to-back application download overwrites existing applications, libraries, or any other files stored in the RAM of the receiving terminal.
- ❑ All `CONFIG.SYS` records and settings on the receiving terminal—protected and non-protected—are replaced by those of the sending terminal. Ensure that these records and settings on the sending terminal are correct before initiating the download.
- ❑ Passwords on the receiving terminal are retained.
- ❑ Certificates and signature files downloaded to the receiving terminal, together with application files, must be processed by the file authentication module on the receiving terminal on terminal restart after the back-to-back download completes.
- ❑ The OS software on the receiving terminal is not affected by a back-to-back application download.

  Note: OS files cannot be downloaded in a back-to-back operation.
- ❑ An application upload does not overwrite the existing certificate tree on the receiving terminal. Any downloaded certificate files are authenticated and then added to the tree.

Back-to-Back Application Download Procedure

The back-to-back application download process consists of two main phases:

1. Preparing a *Gold* VX 520 terminal (transfers application files to the *Target* VX 520 terminal).
2. Downloading application files from the Gold terminal to a properly configured Target terminal.

Prepare Gold Terminal (PC-to-Terminal)

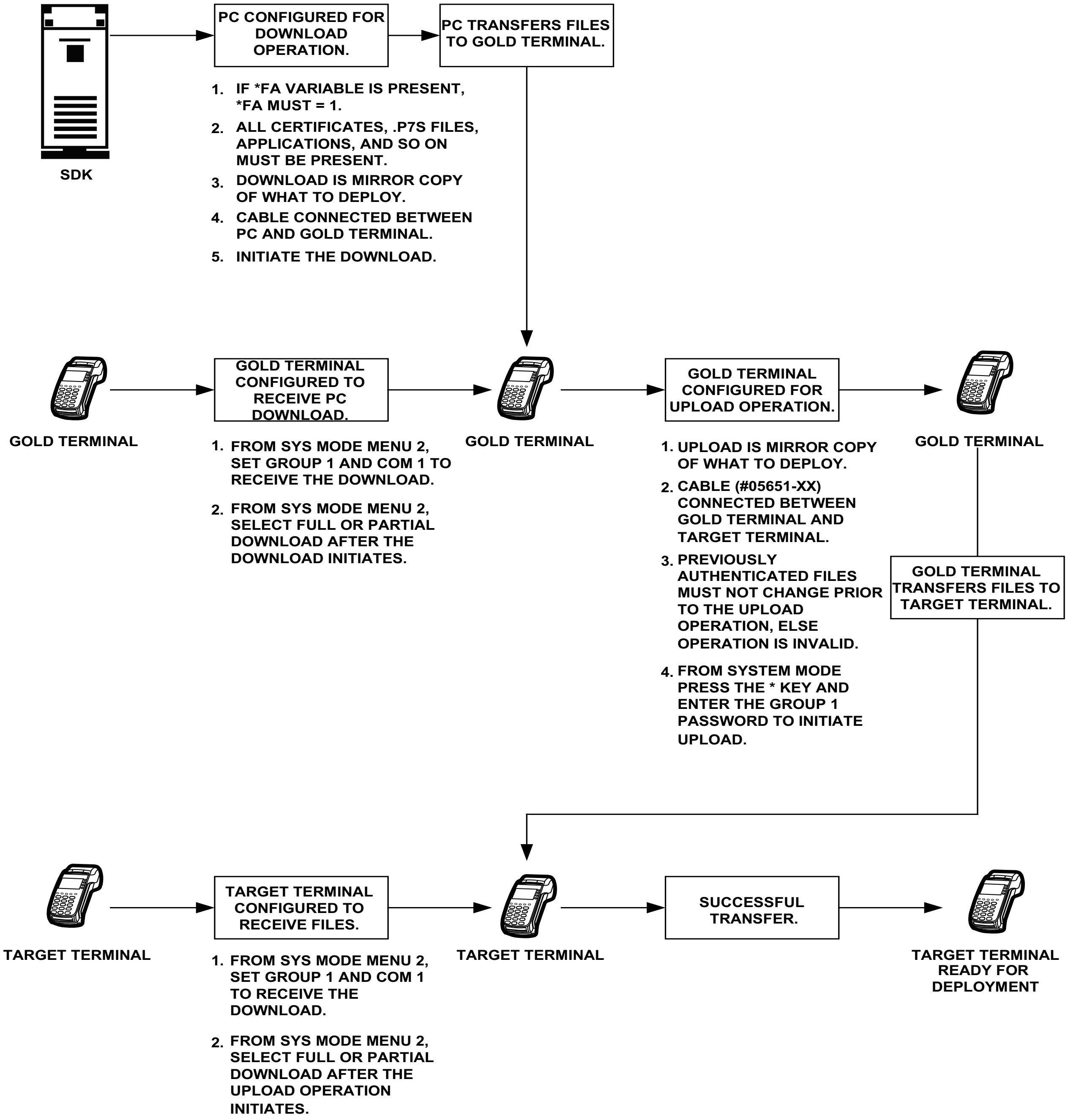
1. Configure the host PC for an application download operation to the Gold terminal:
   - Set the `*FA` variable (if present in the application) to 1.
   - Ensure that all certificates, `*p7s` files, applications, and other required files are present.
   - Ensure that the download is exactly what you want your Target terminal to receive.
2. Configure the Gold terminal to receive an application download from a PC:
   - From **VERIX TERMINAL MGR MENU 2**, set Group 1 and COM1 as the port to receive the download.
3. Connect a cable between the RS-232 serial ports of the PC and the Gold terminal.
4. Initiate the file transfer on the PC.
5. From **VERIX TERMINAL MGR MENU 2** on the Gold terminal, select either a full or a partial download.

The PC transfers files to the Gold terminal.

Download Application Files to Target Terminal

1. Configure a Gold terminal for an application download operation to a deployment terminal:
   - If the `*FA` variable (if present in the application) is set to 0, you can reset it to 1. For more information on the *FA variable, refer to the *Verix V Programmers Manual* (VPN 23230).
   - Ensure that the download is exactly what you want your Target terminals to receive.
   - Ensure that previously authenticated files are not changed prior to the file transfer operation.
2. Configure the Target terminal to receive an application download from the Gold terminal. Select **DOWNLOAD F3** from **VERIX TERMINAL MGR MENU 1**. Set Group 1 enter the group password.
3. Select **SINGLE-APP F3** or **MULTI-APP F4** from the **VERIX TERMINAL MGR DOWNLOAD** menu. Specify whether to perform a full or partial download then select COM1 as the receiving port.
4. Connect a cable (VeriFone part number 05651-xx) between the RS-232 serial ports of the Gold and Target terminals.
5. From any terminal manager menu on the Gold terminal, press [`*`] and enter the GID1 password to initiate the file transfer.

Figure 35 illustrates these two phases and how they relate to each other.


SDK
PC CONFIGURED FOR DOWNLOAD OPERATION.
PC TRANSFERS FILES TO GOLD TERMINAL.
GOLD TERMINAL
GOLD TERMINAL CONFIGURED TO RECEIVE PC DOWNLOAD.
GOLD TERMINAL
GOLD TERMINAL CONFIGURED FOR UPLOAD OPERATION.
GOLD TERMINAL
GOLD TERMINAL TRANSFERS FILES TO TARGET TERMINAL.
TARGET TERMINAL
TARGET TERMINAL CONFIGURED TO RECEIVE FILES.
TARGET TERMINAL
SUCCESSFUL TRANSFER.
TARGET TERMINAL READY FOR DEPLOYMENT

1. IF *FA VARIABLE IS PRESENT, *FA MUST = 1.
2. ALL CERTIFICATES, .P7S FILES, APPLICATIONS, AND SO ON MUST BE PRESENT.
3. DOWNLOAD IS MIRROR COPY OF WHAT TO DEPLOY.
4. CABLE CONNECTED BETWEEN PC AND GOLD TERMINAL.
5. INITIATE THE DOWNLOAD.

1. FROM SYS MODE MENU 2, SET GROUP 1 AND COM 1 TO RECEIVE THE DOWNLOAD.
2. FROM SYS MODE MENU 2, SELECT FULL OR PARTIAL DOWNLOAD AFTER THE DOWNLOAD INITIATES.

1. UPLOAD IS MIRROR COPY OF WHAT TO DEPLOY.
2. CABLE (#05651-XX) CONNECTED BETWEEN GOLD TERMINAL AND TARGET TERMINAL.
3. PREVIOUSLY AUTHENTICATED FILES MUST NOT CHANGE PRIOR TO THE UPLOAD OPERATION, ELSE OPERATION IS INVALID.
4. FROM SYSTEM MODE PRESS THE * KEY AND ENTER THE GROUP 1 PASSWORD TO INITIATE UPLOAD.

1. FROM SYS MODE MENU 2, SET GROUP 1 AND COM 1 TO RECEIVE THE DOWNLOAD.
2. FROM SYS MODE MENU 2, SELECT FULL OR PARTIAL DOWNLOAD AFTER THE UPLOAD OPERATION INITIATES.

Figure 35 Back-To-Back Download Process

The procedure in Table 21 walks you through a back-to-back application download from a sending VX 520 terminal (Gold) to a receiving VX 520 terminal (Target).

Back-to-back downloads require that one terminal, the *Gold* terminal, be loaded with the required applications. The receiving terminal is the *Target* terminal. The procedure in Table 21 assumes the following:

- The Target terminal has no applications loaded.
- There is enough memory in the Target terminal to complete the download.

NOTE The Target terminal does not display an error message if there is not enough memory to complete the download. The Gold terminal displays **DOWNLOAD INCOMPLETE** before returning to **VERIX TERMINAL MGR MENU 2**.

- You are performing a *full* download.

Table 21 Back-to-Back Application Download Procedure

Step	Gold Terminal	Target Terminal
1	Connect a MOD10 cable (P/N 05651-XX) between the RS-232 ports of the terminals. Allow each terminal to boot up. After boot up, the Target terminal displays **DOWNLOAD NEEDED**.	
2	Press F2+F4 to enter Verix Terminal Manager.	
3	Enter the terminal manager password (factory default is “1, Alpha, Alpha, 66831”) and press the enter key.	
4	Press the * (asterisk) key, then press ↵. You are prompted to reenter the terminal manager password. **UPLOADING NOW** is displayed.	Press **DOWNLOAD** to enter download mode.
5		Press ↵ at the next **VERIX TERMINAL MGR DOWNLOAD** screen to select **FILE GROUP_1** (default displayed) as the target file group.
6		Select **FULL DNLD** at the next **VERIX TERMINAL MGR DOWNLOAD** screen. Full downloads are required in back-to-back downloads.
8		Select (COM1) in the next **VERIX TERMINAL MGR DOWNLOAD** screen. **DOWNLOADING NOW** is displayed.
	Both terminals display a status indicator, where each dash represents a 10% increment of the download. Ensure that the Gold terminal displays **UPLOAD COMPLETE** before returning to the second **VERIX TERMINAL MGR** menu. This is when the Gold terminal might display an error message if problems occurred during the download process. The Target terminal begins to validate all files. Allow the Target terminal to complete file authentication and reboot the terminal. The Gold terminal is ready to perform another download. An application-specific menu is displayed after the Target terminal completes the reboot.	

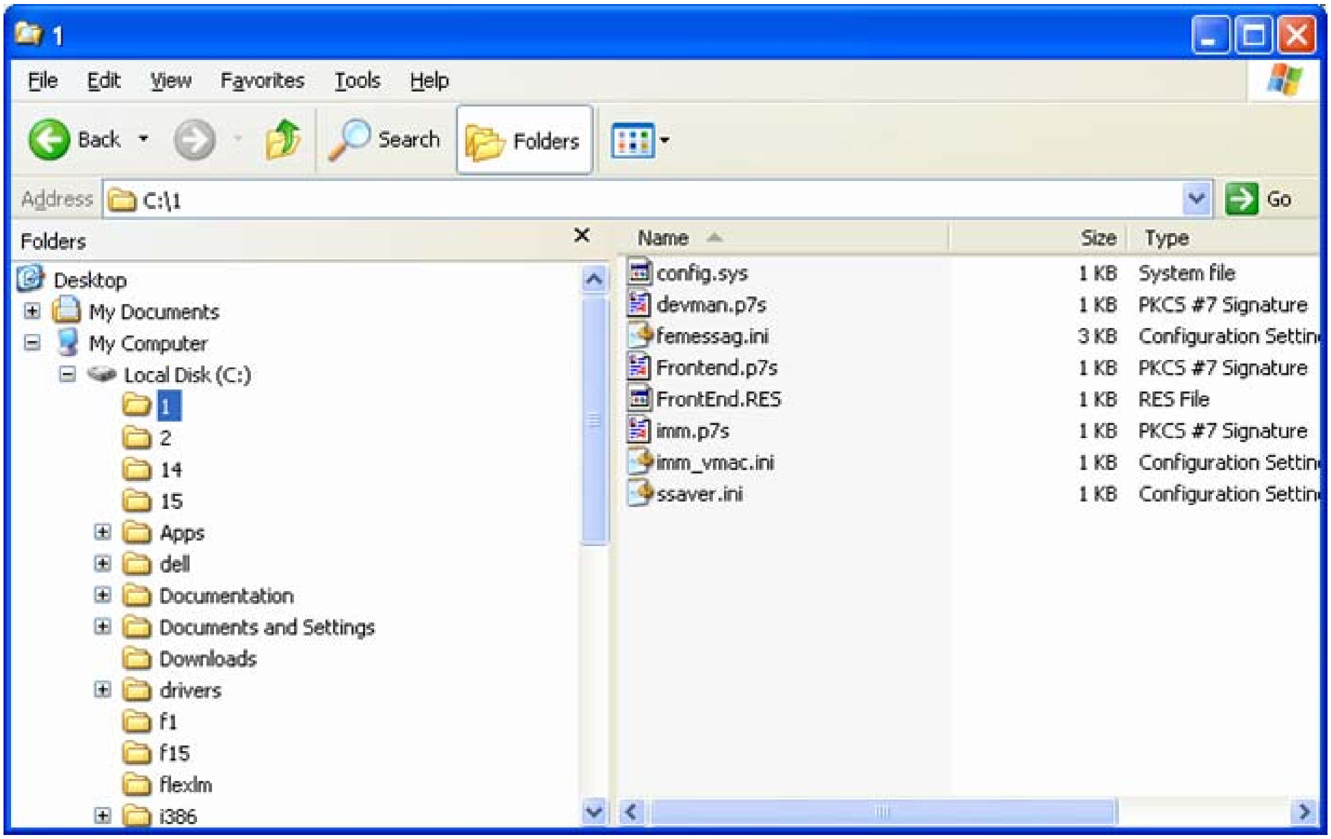
Download from a USB Flash Drive

The procedure provided in Table 22 guides you through the process of downloading multiple applications from a USB flash drive.

Before you begin, make sure that the USB device is properly inserted in the terminal's USB port and the `VeriFone.zip` file resides in the device. `VeriFone.zip` is the only filename recognized by the system as a downloadable file. For more information on how to build a `VeriFone.zip` file, see Build a VeriFone.zip File

Build a VeriFone.zip File

To build a multiple-application `.zip` file (`VeriFone.zip`), you must first create folders on your root drive (`C:`) representing the specific groups on the terminal (Figure 36). All Group 1 files MUST be in unzipped download formats, while other group folders can contain standard pre-compressed `.zip` files.

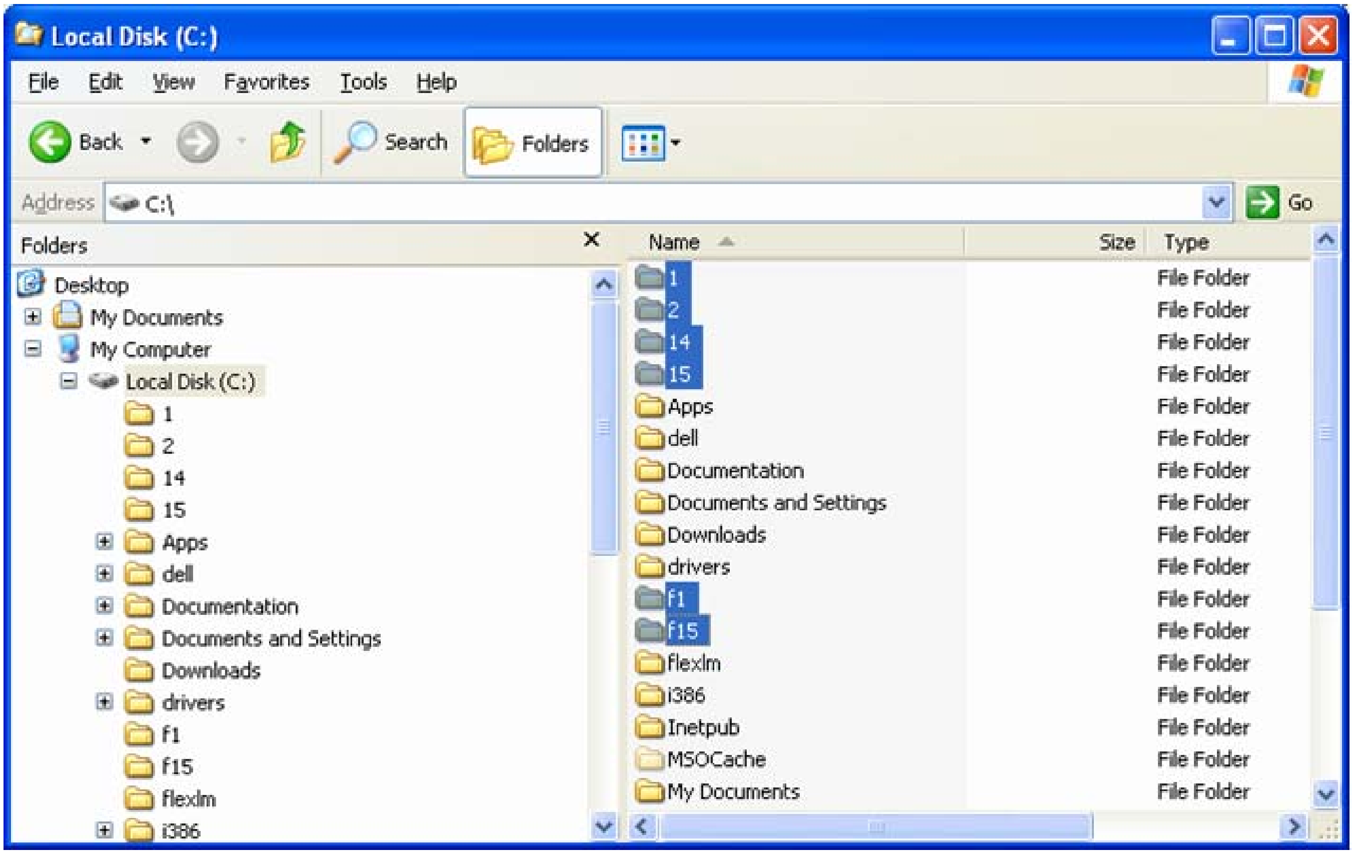


Address C:\1

Name	Size	Type
config.sys	1 KB	System file
devman.p7s	1 KB	PKCS #7 Signature
femessag.ini	3 KB	Configuration Settin
Frontend.p7s	1 KB	PKCS #7 Signature
FrontEnd.RES	1 KB	RES File
imm.p7s	1 KB	PKCS #7 Signature
imm_vmac.ini	1 KB	Configuration Settin
ssaver.ini	1 KB	Configuration Settin

Figure 36 Create GID-Specific Folders

Each RAM folder should contain a `CONFIG.SYS` file of parameters for applications running in that GID (Figure 37).



Address C:\

Name	Size	Type
1		File Folder
2		File Folder
14		File Folder
15		File Folder
Apps		File Folder
dell		File Folder
Documentation		File Folder
Documents and Settings		File Folder
Downloads		File Folder
drivers		File Folder
f1		File Folder
f15		File Folder
flexlm		File Folder
i386		File Folder
Inetpub		File Folder
MSOCache		File Folder
My Documents		File Folder

Figure 37 Config.sys File Inside a GID Folder

Use the following instructions to build a `CONFIG.SYS` downloadable file:

1. Open Notepad and create a `.txt` file containing parameter and value pairs.
2. Run the Variable Length Record (VLR) utility to convert the text file to a downloadable file format (`vlr -c input.file output.file`).

After creating a `CONFIG.SYS` downloadable file, move the created file to the proper folder. Then, create a new `.zip` file named `VeriFone.zip` on your root drive and move all the required GID folders into the `.zip` file. Make sure that **Save Full Path Info** is selected. Transfer the `VeriFone.zip` file into a flash drive and you are ready start downloading the applications into a terminal.

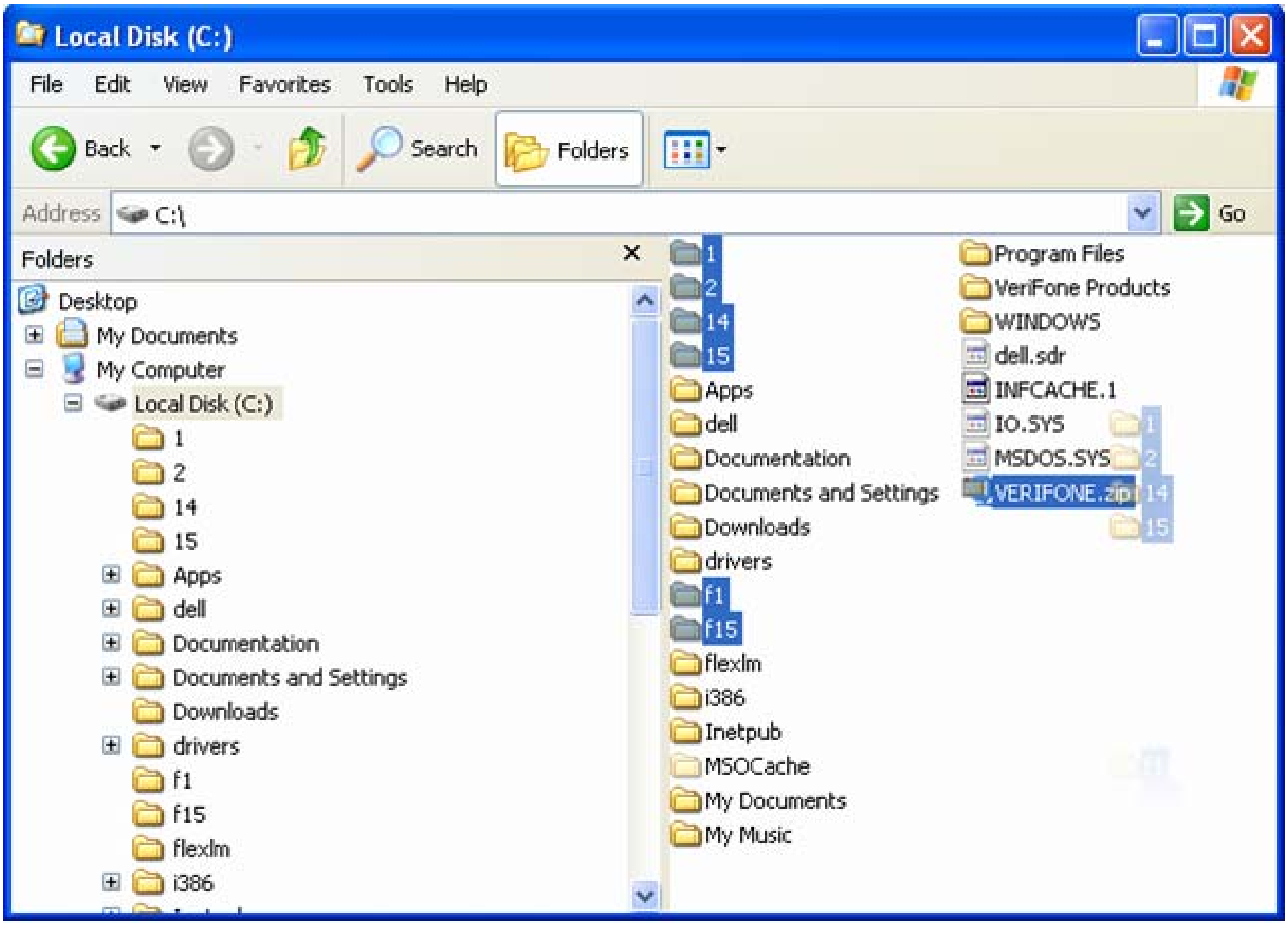


Figure 38 Moving GID files to VERIFONE.zip file

USB Flash Drive Download Procedure

To begin downloading from a USB flash drive, insert the flash drive into the USB port of the VX 520 terminal and follow the instructions on Table 22.

Table 22 USB Flash Drive Download Procedure

Step	Display	Action
1	**VERIX TERMINAL MGR** **DOWNLOAD** **GROUP ID: nn**	Enter the target file group for the download. **FILE GROUP _1** (Group 1) is displayed as the default selection. **Note:** File Group 1 is reserved for the operating system. Try using a different file group when downloading additional applications. For more information on operating system downloads, see Direct Operating System Downloads. To select a file group other than Group 1, type the one or two-digit number of the desired file group (2–15) for the download.
2	**VERIX TERMINAL MGR** **DOWNLOAD** **GROUP n PASSWORD** ____________	Enter the password of the selected file group. For example, if Group 2 is the target group, the **GROUP _2 PASSWORD** message is displayed. **Note:** If you have not previously entered a group's password in this session, the terminal prompts for the group's password prior to downloading applications. To continue, enter the required password. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press ↵. Verify your password and reenter it.
3	**VERIX TERMINAL MGR** **DOWNLOAD Gnn** **1> SINGLE-APP** **2> MULTI-APP**	Select **1> SINGLE-APP** to download a single application. Select **2> MULTI-APP** to download multiple applications.

Table 22 USB Flash Drive Download Procedure

Step	Display	Action
4	**VERIX TERMINAL MGR** **DOWNLOAD Gnn** **1> Full dnld** **2> Partial dnld**	Select whether to run a full or partial download. **Note:** If you selected **1> FULL DNLD** on a single application download, a screen will appear warning you that all existing files in the selected group will be deleted. Press F3 to cancel or F4 to continue downloading an application. If you selected **1> FULL DNLD** on a multiple application download, you will be prompted to clear the existing application on the currently selected group. Select **1> YES** to continue or **2> NO** to cancel downloading applications.
5	**VERIX TERMINAL MGR** **DOWNLOAD Gnn** **1> MODEM** **2> COM1** **3> TCPIP** ↑ ↓	On the next screen, press the PF1 key to go to the next menu.
6	**VERIX TERMINAL MGR** **DOWNLOAD Gnn** **1> COM2** **2> USB FLASH MEMORY** ↑	Select **2> USB FLASH MEMORY** to download from a USB flash drive. When you press 2, the terminal is ready to receive the download from the connected USB device.
7	**VERIX TERMINAL MGR** **DOWNLOAD Gnn** **DOWNLOAD FROM USB** **FLASH MEMORY DEVICE** **1> CANCEL DOWNLOAD** **2> CONTINUE**	Select **2> CONTINUE** to begin the download.

Table 22 USB Flash Drive Download Procedure

Step	Display	Action
8	**VERIX TERMINAL MGR** **DOWNLOAD Gnn** **USB DOWNLOAD COMPLETE**	The terminal will automatically download the file `VeriFone.zip` from the USB flash drive. **USB DOWNLOAD COMPLETE** appears on the terminal screen after a successful download. If you performed a full download, the terminal restarts automatically. Otherwise, you must restart the terminal manually by selecting **1> RESTART** on **VERIX TERMINAL MGR MENU 1**. If an application resides on the terminal following the download, it executes on restart.
9	****VERIFYING FILES**** **CHECK CERTIFICATE** **FILENAME.CRT** ***AUTHENTIC*** ****VERIFYING FILES**** **COMPARE SIGNATURE** **FILENAME.P7S** **FILENAME.OUT** ***FAILED***	On startup, the file authentication module authenticates any new signature files downloaded with the OS files. When the signature file authentication routine starts, the status display informs you of the progress of the authentication process. If file authentication succeeds for a specific signature file, the ***AUTHENTIC*** message is displayed directly below the filename of the signature file. If file authentication fails for a specific signature file, the ***FAILED*** message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate. The authentication process then proceeds to the next signature file until all signature files are validated.
		When all new signature files are authenticated, the terminal restarts, and the application specified in the `*GO` variable or the default application in Group 1 executes and starts running on the terminal.

Table 22 USB Flash Drive Download Procedure

Step	Display	Action
8	**<application prompt>** **DOWNLOAD NEEDED** **<error message>**	If the downloaded application successfully authenticates, the corresponding application prompt or logo is displayed upon restart. The terminal can now process transactions. **Note:** The message **DOWNLOAD NEEDED** appears if: • The *GO variable is not set. • *GO does not specify that an application is present. • The application did not authenticate (invalid or missing *.p7s file). • The application uses shared libraries that are missing or were not authenticated (invalid or missing *.p7s files). If one or more executables in the application fail to successfully authenticate, the application may not run. If the application attempts to access an unauthenticated executable or library, it may crash. Repeat the Direct Application Download Procedure using the correct certificates and/or signature files. For more information on startup errors, see STARTUP ERRORS.

CHAPTER 7

Specifications

This chapter discusses power requirements, dimensions, and other specifications of the VX 520 terminal.

Power

VX 520 terminal: 9.3V DC; 4.0 A

NOTE The VX 520 uses an 18-watt wall-mount power supply as a standard power source. An optional 36-watt power supply may also be used for all other variants of the VX 520. However, the VX 520 GPRS requires the 36-watt power supply to optimize battery charging.

DC Power Pack

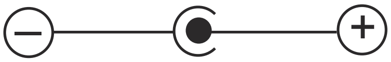
36-watt power supply

UL, ITE listed, LPS power supply:

a Input rated: 100 - 240V AC, 50/60 Hz

b Output rated: 9.3V DC 4.0 A

Barrel connector polarity:



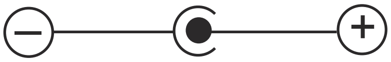
18-watt power supply

UL, ITE listed, LPS power supply:

a Input rated: 100 - 240V AC, 50/60 Hz

b Output rated: 8V DC 2.25 A

Barrel connector polarity:



CAUTION Using an incorrectly rated power supply may damage the terminal or cause it not to work as specified. Ensure that the power supply being used to power the terminal matches the requirements specified on the bottom of the terminal.

Temperature

- Operating temperature: 0° to 40° C (32° to 104° F)
- Storage temperature: -20° to + 60° C (-4° to 140° F)
- Relative humidity: 5% to 85%; no condensation

External Dimensions

- Length: 203 mm (7.9 in)
- Width: 87 mm (3.4 in)

NOTE VeriFone ships variants of the VX 520 terminal for different markets. Your terminal may have a different configuration. The basic processes described in this guide remain the same, regardless of terminal configuration.

CHAPTER 8

Maintenance

The VX 520 terminal has no user-maintainable parts.

Clean the Terminal

To clean the terminal, use a clean cloth slightly dampened with water and a drop or two of mild soap. For stubborn stains, use alcohol or an alcohol-based cleaner.

CAUTION

Never use thinner, trichloroethylene, or ketone-based solvents – they may cause deterioration of plastic or rubber parts.

Do not spray cleaners or other solutions directly onto the keypad or terminal display.

Smart Card Reader

Do not attempt to clean the smart card reader. Doing so may void any warranty. For smart card reader service, contact your VeriFone distributor or service provider.

CHAPTER 9

VeriFone Service and Support

For terminal problems, contact your local VeriFone representative or service provider.

For product service and repair information:

- USA – VeriFone Service and Support Group, 1-800-VeriFone (837-4366), Monday - Friday, 8 A.M. - 8 P.M., Eastern time
- International – Contact your VeriFone representative

Return a Terminal for Service

Before returning a VX 520 terminal to VeriFone, you must obtain an MRA number. The following procedure describes how to return one or more VX 520 terminals for repair or replacement (U.S. customers only).

NOTE

International customers are advised to contact their local VeriFone representative for assistance regarding service, return, or replacement of terminals.

To return a terminal for service

1 Get the following information from the printed labels on the bottom of *each* VX 520 terminal to be returned:

- Product ID, including the model and part number. For example, “VX 520” and “Pxxx- xxx-xx,” “Mxxx-xx-xx-xxx,” or “2xxxx-xx”
- Serial number (S/N xxx-xxx-xxx)

2 Obtain the MRA numbers by completing one of the following:

a Call VeriFone toll-free within the United States at 1-800-VeriFone and follow the automated menu options.

- Select the MRA option from the automated message. The MRA department is open Monday to Friday, 8 A.M.–8 P.M., Eastern Time.
- Give the MRA representative the information you gathered in Step 1. If the list of serial numbers is long, you can fax the list, along with the information gathered in Step 1, to the MRA department at 727-953-4172 (U.S.).

b Address a fax to “VeriFone MRA Dept.” with the model and part number(s)

- Include a telephone number where you can be reached and your fax number.

c Complete the Inquiry Contact Form at http://www.verifone.com/aboutus/contact/contact_form.cfm.

- Address the Subject box with to “VeriFone MRA Dept.”
- Reference the model and part number in the Note box.

NOTE

One MRA number must be issued for each VX 520 terminal you return to VeriFone, even if you are returning several of the same model.

3 Describe the problem(s).

4 Provide the shipping address where the repaired or replacement unit must be returned.

5 Keep a record of the following items:

- Assigned MRA number(s).
- VeriFone serial number assigned to the VX 520 terminal you are returning for service or repair (terminal serial numbers are located on the bottom of the unit).
- Shipping documentation, such as air bill numbers used to trace the shipment.
- Model(s) returned (model numbers are located on the VeriFone label on the bottom of the VX 520 terminal).

Accessories and Documentation

VeriFone produces the following accessories and documentation for the VX 520 terminal. When ordering, please refer to the part number in the left column.

- VeriFone online store at *www.store.verifone.com*
- USA – VeriFone Customer Development Center, 800-VeriFone (837-4366), Monday - Friday, 7 A.M. - 8 P.M., Eastern time
- International – Contact your VeriFone representative

Power Pack

Contact your local VeriFone distributor to determine which power pack or power cord fits your needs.

VPN PWR258-001-01-A	36W power supply
VPN WIR30017	AC power cord (US)

NOTE

The VX 520 uses an 18-watt wall-mount power supply as a standard power source. An optional 36-watt power supply may also be used for all other variants of the VX 520. However, the VX 520 GPRS requires the 36-watt power supply to optimize battery charging.

Connectors

VPN 26263-02	DB-25-type serial connectors
VPN 26264-01	DB-9-type connectors
VPN 05651-00	Back-to-back download cable

Thermal Printer Paper

VPN PPR 268-001-01-A	38 mm (1.49 in) diameter, 57 mm (2.24 in) wide
VPN PPR 252-001-01-A	49 mm (1.93 in) diameter, 57 mm (2.24 in) wide

NOTE VeriFone ships variants of the VX 520 terminal for different markets. Your terminal may have a different printer configuration and use one or the other of the printer paper types.

Supplementary Hardware

STA252-001-01-A	Swivel stand
STA252-005-01-A	Wall-mount stand

VeriFone Cleaning Kit

VPN 02746-01	Cleaning kit

Telephone Line Cord

VPN CBL000-001-01-A	2.1-meter (7-foot) telephone line cord, black, with modular RJ-11-type connectors

Documentation

VPN DOC252-001-EN	*VX 520 Certifications and Regulations*
VPN DOC252-002-EN	*VX 520 Quick Installation Guide*
VPN DOC252-003-EN	*VX 520 Installation Guide*
VPN DOC252-021-EN-A	*VX 520 GPRS Certifications and Regulations*
VPN DOC252-022-EN-A	*VX 520 GPRS Quick Installation Guide*
VPN 23230	*Verix V Operating System Programmers Manual*
VPN DOC00301	*Verix eVo Volume I: Operating System Programmers Manual*
VPN DOC00302	*Verix eVo Volume II: Operating System and Communication Programmers Manual*
VPN DOC00303	*Verix eVo Volume III: Operating System Programming Tools Reference Manual*

CHAPTER 10

Troubleshooting Guidelines

The troubleshooting guidelines provided in the following section are included to assist you to successfully install and configure your VX 520 terminal. If you have problems operating your VX 520 terminal, please read through these troubleshooting examples.

If the problem persists even after performing the outlined guidelines or if the problem is not described below, contact your local VeriFone representative for assistance. Typical examples of malfunction you may encounter while operating your VX 520 terminal and steps you can take to resolve them are listed.

NOTE The VX 520 terminal comes equipped with tamper-evident labels. The VX 520 contains no user serviceable parts. Do not, under any circumstance, attempt to disassemble the terminal. Perform only those adjustments or repairs specified in this guide. For all other services, contact your local VeriFone service provider. Service conducted by parties other than authorized VeriFone representatives may void any warranty.

CAUTION Using an incorrectly rated power supply may damage the terminal or cause it not to work as specified. Use only a VeriFone-supplied power pack with the correct output ratings. Before troubleshooting, ensure that the power supply being used to power the terminal matches the requirements specified on the bottom of the terminal. (See Chapter 7 Specifications for detailed power supply specifications) Obtain the appropriately rated power supply before continuing.

Blank Display

When the terminal display screen does not show correct or clearly readable information:

- Check terminal power connection.
- Remove and reapply power to the terminal.
- Check all cable connections and verify that the telephone line is properly connected.
- If the problem persists, contact your local VeriFone service provider.

Terminal Does Not Dial Out

If the terminal does not dial out:

- Check the telephone line connections.
- Check that the telephone line is working by plugging it into a working telephone and listening for a dial tone.
- Replace the telephone cable that connects the terminal with a cable you know is working correctly.
- If the problem persists, contact your local VeriFone service provider.

Printer Paper Jam

If paper jams inside the printer:

- Open the paper roll cover.
  - Remove the damaged paper from the paper roll and clear the feed mechanism.
  - Install a roll of printer paper, as described in Installing the Paper Roll in the Printer.
  - If the problem persists, it may be due to poor paper quality. Install a new roll of higher-quality paper.

WARNING

Poor-quality paper may jam the printer. To order high-quality VeriFone paper, refer to Accessories and Documentation.

Keypad Does Not Respond

If the keypad does not respond properly:

- Check the terminal display. If it displays the wrong character or nothing at all when you press a key, follow the steps outlined in Transactions Fail To Process.
- If pressing a function key does not perform the expected action, refer to the user documentation for that application to ensure you are entering data correctly.
- If the problem persists, contact your local VeriFone representative.

Peripheral Device Does Not Work

If any peripheral device (PIN Pad or smart card reader) does not work properly:

- Check the power cord connection to the peripheral device.
- Check that the device connected to the proper port has power and is functioning properly. If possible, perform a self-test on the device in question.
- The cable connecting the optional device to the terminal serial port may be defective. Try a different serial cable. See Connecting Optional Devices.
- If the problem persists, contact your local VeriFone representative.

Transactions Fail To Process

There are several reasons why the terminal may not be processing transactions. Use the following steps to troubleshoot failures.

Check the Magnetic Card Reader

- Perform a test transaction using one or more different magnetic stripe cards to ensure the problem is not a defective card.
- Ensure that you are swiping cards properly. With the card reader, the black magnetic stripe on the card should face down and inward, toward the keypad and must be inserted from the top of the terminal.
- Process a transaction manually, using the keypad instead of the card reader. If the manual transaction works, the problem may be a defective card reader.
- If the manual transaction does not work, proceed to Check the Telephone Line.
- Contact your VeriFone distributor or service provider.

Check the Smart Card Reader

- Perform a test transaction using several different smart cards to ensure the problem is not a defective card.
- Ensure that the card is inserted correctly and that the card is not removed prematurely.
- Ensure the MSAM cards are properly inserted in the cardholders and that the cardholders are properly secured (see Installing/Replacing MSAM Cards).
- If the manual transaction does not process, proceed to Check the Telephone Line.
- Contact your VeriFone distributor or service provider.

Check the Telephone Line

- Disconnect the telephone line from the terminal and connect it to a working telephone to check for a dial tone. If there is no dial tone, replace the telephone cable.
- If the problem appears to be with the telephone line, check with the party you are trying to call to see if their system is operational. If they are not experiencing difficulties with their line, contact the telephone company and have your line checked.
- If the telephone line works, contact your local VeriFone representative for assistance.

Printer Does Not Print

If the printer does not work properly:

- Check terminal power connection.
- Check if the printer is out of paper and that the roll is properly installed. Open the paper roll cover and install a new roll of printer paper or ensure that the roll is feeding from the bottom.
- Verify that the printer roller and paper roll dust cover are properly installed.
- If the problem persists, contact your VeriFone distributor or service provider.

Terminal Display Does not Show Correct or Readable Information

- Connect the terminal in to a known-good power supply (if you have one) to see if this clears the problem.
- If the problem persists, contact your local VeriFone representative for assistance.

Terminal Does Not Start

Make sure you press the **ENTER** key for approximately 3 seconds, until the unit lights up.

APPENDIX A

System Messages

This appendix describes two categories of error and information messages. For ease of use, these messages are grouped alphabetically in each of these two categories.

These messages include the following:

- Digital certificate displays and signature file downloaded to the terminal.
- File authentication module processes.
- File compression module use messages from the VeriCentre DMM terminal management and download tool.

Error Messages

The following error messages may appear when the VX 520 terminal is in Verix Terminal Manager.

Table 23 Error Messages

Display	Action
COMPRESSION MODULE ERROR	
**** UNZIP Error n xxxxxx yyyyyy**	If you are using the file compression module in DMM, information similar to what is shown above appears when an error occurs during file extraction from a downloaded ZIP archive. Note the error number and error codes (xxxxx and yyyyy) and try to download the archive again.
DEBUGGER ERRORS	
ALREADY DEBUGGING	The debugger has already been invoked.

Table 23 Error Messages

Display	Action
LOAD DBMON.OUT	The `DBMON.OUT` debugging monitor program is included in the SDK, but is not stored in the terminal memory of a factory unit. To use the debugging tool, you must sign, download, and authenticate the `DBMON.OUT` application.
DOWNLOADING ERRORS	
VERIX TERMINAL MGR **DOWNLOAD Gnn** **TCP/IP NOT PRESENT**	This error only occurs on a VX 520 terminal when downloading through TCP/IP. An application that supports the TCP stack does not exist.
VERIX TERMINAL MGR **DOWNLOAD Gnn** **NO *ZTCP VARIABLE**	This error only occurs on a VX 520 terminal when downloading through TCP/IP. An application that supports the TCP stack does not exist.
VERIX TERMINAL MGR **DOWNLOAD Gnn** **GID: nn** **APP ID: nnnn** **STATUS: CONNECTING** **<error message>**	The following error message may occur while connecting to a host during a modem or wireless download: • **NO LINE** - Your phone line is currently being used. • **NO DIAL TONE** - Your phone line has no dial tone. • **NO CARRIER** - The terminal could not establish a connection with the host. • **LOST CARRIER** - The carrier was lost during connection. • **BUSY** - The host is currently busy. • **NO ENQ FROM HOST** - The host did not send an ENQ (Enquiry).

Table 23 Error Messages

Display	Action
VERIX TERMINAL MGR DOWNLOAD Gnn GID: nn APP ID: nnnn STATUS: DOWNLOADING <error message>	The following error message may occur while connecting to a host during a modem or wireless download: • **BAD RX COMM -** The terminal received too many bad packets. • **BAD TX COMM -** The host received too many bad packets. • **LOST CARRIER -** The carrier was lost during download. • **NO RESP FROM HOST -** The terminal timed out waiting for a packet from the host.
EDIT PARAMETERS ERROR	
GID nn: NOT EMPTY <parm name> NOT FOUND CANCEL F3 ADD VARIABLE F4	You entered an invalid parameter name. Select **CANCEL F3** to go back to the parameter editor or **ADD VARIABLE F4** to add the entered parameter name as a new variable.
PASSWORD ERRORS	
VERIX TERMINAL MGR PASSWORD Gnn PLEASE TRY AGAIN	You entered an invalid GID password. Press ↵ or ✕ and enter a valid password.
VERIX TERMINAL MGR PASSWORD ERROR: PASSWORD MUST BE 5 TO 10 CHARACTERS	When changing passwords, this screen appears when you enter an invalid new password length. Press ↵ or ✕ and enter a password with the appropriate length of five to ten characters.
PRINTER DIAGNOSTICS ERRORS	
PRINTER ID P VERSION 0PRED1A1 STATUS 22 NO PAPER TEST F3 PAPER FEED F4	**NO PAPER** is displayed when you select **TEST F3** or **PAPER FEED F4** and there is no paper installed in the printer.

Table 23 Error Messages

Display	Action
PRINTER ID P **VERSION 0PRED1A1** **STATUS 22** **PRINTER BUSY** **TEST F3** **PAPER FEED F4**	When you select **TEST F3** or **PAPER FEED F4** from the printer diagnostics screen, terminal manager first checks if the printer is currently active. If it is, **PRINTER BUSY** is displayed.
REMOTE DIAGNOSTICS ERROR	
LOAD TERMINAL MANAGEMENT AGENT	The (optional) Terminal Management Agent (TMA) software is not resident in the VX 520 terminal. The TMA software is required to perform remote diagnostics. For more information about support for remote diagnostics, contact your VeriFone service provider.
SMART CARD DIAGNOSTICS ERRORS	
TEST NOT SUPPORTED	This message appears if the terminal does not support ICC devices. Therefore, a SAM card diagnostics session cannot be performed. Press any key to go back to the main menu.
SAM nn **POWER UP: FAILED**	This screen is displayed when there is no SAM card inserted in the selected slot.
NO SYNC DRIVERS INSTALLED	This screen is displayed if sync drivers are not installed in the terminal. Therefore, a sync drivers test cannot be performed. Press any key to go back to the smart card diagnostics screen.

Table 23 Error Messages

Display	Action
STARTUP ERRORS	
DOWNLOAD NEEDED **<error message>**	The following error messages may occur if a defect is found on the *GO variable. *GO is a variable in the CONFIG.SYS file and is the first thing that runs on startup if available. • **NO *GO VARIABLE** - There is no *GO environment variable in the group one CONFIG.SYS file. • ***GO NOT FOUND** - The *GO variable is set but the executable file is missing. • ***GO NOT AUTHENTICATED** - The *GO variable is set but the executable file is not authenticated. • **NOT ENOUGH MEMORY** - The *GO variable is set but there is not enough memory to execute the file. • **INVALID *GO VARIABLE** - This is the defalut error condition. The system could not run the *GO variable eventhough it is set, authenticated, and enough memory is available to execute the file.
FLASH CHKSUM ER Gnn	A corrupt file is detected in the flash file system during terminal start up, after power on, or during restart. This message may indicate a hardware problem; the error condition may be resolved through another download of the file.
RAM CHKSUM ERROR Gnn	A corrupt file is detected in the RAM file system at terminal start up, after power-on, or during restart. This message may indicate a hardware problem; the error condition may be resolved through another download of the file.
****VERIFYING FILES**** **COMPARE SIGNATURE** **FILENAME.P7S** **FILENAME.OUT** ***FAILED***	This message appears on screen when the file authentication module fails to authenticate a new signature file. ***FAILED*** appears for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new signature files are checked. New digital certificates are always checked first, followed by new signature files, in an uninterrupted process.

Table 23 Error Messages

Display	Action
****VERIFYING FILES**** **CHECK CERTIFICATE** **FILENAME.CRT** ***FAILED***	This message appears on screen when the file authentication module fails to authenticate a new digital certificate. ***FAILED*** is displayed for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new certificates are checked, one by one. In special cases where system certificates are being installed, **SYSTEM CERTIFICATE** is displayed instead of **CHECK CERTIFICATE**.

Information Messages

The following information messages may appear when the VX 520 terminal is in terminal manager.

Table 24 Information Messages

Display	Action
DOWNLOADING INFORMATION	
VERIX TERMINAL MGR **UPLOAD** **I:CONFIG.SYS** ******______** **UPLOADING NOW**	During a back-to-back download session, this screen appears on the Gold terminal indicating that an application is being uploaded to the Target terminal.
VERIX TERMINAL MGR **DOWNLOAD Gnn** ******______** **DOWNLOADING NOW**	During a back-to-back download session, this screen appears on the Target terminal indicating that an application is being downloaded from the Gold terminal.
VERIX TERMINAL MGR **DOWNLOAD Gnn** **GID: nn** **APP ID: nnnn** **STATUS: DOWNLOADING** *****______**	An application is being downloaded to a *receiving* VX 520 terminal from a host PC via telephone. The terminal displays a series of asterisks (*) to indicate the progress of the download (each asterisk represents 10% of the download). When ten asterisks appear, the data transfer is complete.

Table 24 Information Messages

Display	Action
VERIX TERMINAL MGR DOWNLOAD Gnn UNIT RECEIVE MODE ***_______	An application is being downloaded to a *receiving* VX 520 terminal from a host PC directly over a serial cable. The terminal displays a series of asterisks (*) to indicate the progress of the download (each asterisk represents 10% of the download). When ten asterisks appear, the data transfer is complete.
VERIX TERMINAL MGR DOWNLOAD Gnn UNIT RECEIVE MODE WAITING FOR DOWNLOAD	This screen indicates that the terminal is ready for download and is waiting for a response from the host.

Table 24 Information Messages

Display	Action
ERROR LOG	
VERIX TERMINAL MGR ERR LOG **TYPE 1** **TASK 2** **TIME 060302201212** **CPSR 40000010** **PC 00000004** **LR 70448B23** **ADDR 27FFFFEF9**	The following information helps developers interpret the cause of the most recent unrecoverable software error that occurred on the terminal: This first screen displays the following: • **TYPE** (error type), where the error type code is: • 1 = Data abort: attempt to access data at an invalid address. • 2 = Program abort: attempt to execute code at an invalid address. • 3 = Undefined abort: attempt to execute an illegal instruction. • **TASK** (task number): indicates type of task that was currently executed: • 1 = Verix Terminal Manager • 2 = First user task • **TIME** (time of crash): clock time of the error in the format *YYMMDDhhmmss*, where *YY* = year, *MM* = month, *DD* = day, *hh* = hour, *mm* = minute, and *ss* = second. • **CPSR** (Current Program Status Register): contains the processor and state condition code. • **PC** (Program Counter): holds the execution address. • **LR** (Link Register): holds the return address of the function call. **Note:** LR may not always contain the current return address. • **ADDR** (fault address): contains the illegal address that the application was trying to access. If you report a system error to VeriFone, you may be asked to provide the information displayed on this screen. For detailed information about the error log function and the terms listed above, please refer to the Verix eVo OS Programmers Manual (VPN DOC00301).

Table 24 Information Messages

Display	Action
INTERNAL PIN PAD DIAGNOSTICS INFORMATION	
INTERNAL PIN PAD **MEMORY TEST PASSED** **IPP8 EMUL01A 07/05 OD** **SN: 246021114A009999** **BAUD: 1200 RESET F3** **MODE: VISA** **EXIT F4**	After an internal PIN pad diagnostic session, the firmware version and download date, IPP serial number, baud rate, and mode are displayed.
KEYBOARD DIAGNOSTICS INFORMATION	
VERIX TERMINAL MGR KBD TEST **KEYCODE nn**	This screen displays the hexadecimal ASCII keycode for each key you press during a keyboard diagnostics session. The value displayed corresponds to the actual key pressed. Other values assigned to keys are software dependent.
MAGNETIC CARD DIAGNOSTICS INFORMATION	
VERIX TERMINAL MGR **TRK 1:VALID DATA** **TRK 2:VALID DATA** **TRK 3:VALID DATA**	When you invoke a local terminal manager diagnostic test of the magnetic stripe card reader, status information appears for the data tracks (TRK1, TRK2, and TRK3) on the card. A successful test displays **VALID DATA** for each track that reads valid data. An error generates one of the following error messages for each track with an error: • **NO DATA** • **NO START** • **NO END** • **LRC ERR** • **PARITY ERR** • **REVERSE END** For more information about magnetic card error messages, refer to the Verix eVo OS Programmers Manual (VPN DOC00301).
MEMORY INFORMATION	
MEMORY USAGE **RAM FILES nnnn** **INUSE nnnn** **AVAIL nnnn** **FLASH FILES nnnn** **INUSE nnnn** **AVAIL nnnn**	This screen displays how much RAM and flash memory is used and how much is available. • **INUSE -** Closest estimate of used memory (in KB). • **AVAIL -** Lowest number of free memory (in KB).

Table 24 Information Messages

Display	Action
RAM DIRECTORY Gnn <filename> 36 MM/DD/YY - <filename> 36 MM/DD/YY - <filename> 36 MM/DD/YY - PRINT	The following screens display the contents of the RAM and flash directories. If there are no files inside a RAM or flash directory, **<EMPTY>** is displayed.
FLASH DIRECTORY Gnn <filename> 36 MM/DD/YY - <filename> 36 MM/DD/YY - <filename> 36 MM/DD/YY - PRINT	
ALL RAM AND FLASH CLEARED	This screen indicates that all RAM and flash data within a GID is deleted.
ALL RAM AND FLASH CLEAR COALESCING FLASH	This screen indicates that all RAM and flash data within all GIDs is deleted and the flash memory is being merged.
PASSWORD INFORMATION	
VERIX TERMINAL MGR PASSWORD Gnn PASSWORD CHANGED	This message confirms that you have successfully changed a GID password or the system password.

Table 24 Information Messages

Display	Action
PRINTER DIAGNOSTICS INFORMATION	
PRINTER ID P **VERSION 0PRED1A1** **STATUS 22** **TEST F3** **PAPER FEED F4**	This screen displays the printer ID, firmware version, and the printer status appear. See the Verix eVo OS Programmers Manual (VPN DOC00301) for specifics on application development and the internal thermal printer.
PRINTER ID P **VERSION 0PRED1A1** **STATUS 22** **NO PAPER** **TEST F3** **PAPER FEED F4**	**NO PAPER** is displayed when you select **TEST F3** and there is no paper installed in the printer.
SMART CARD DIAGNOSTICS INFORMATION	
VOYAGER VER 02000007 **DRV VER 070125165914** **PHILIP VER 2.0 6/06** **SMART CARD TEST F3** **LIST SYNC DRIVERS F4**	This screen displays system and driver information and the number of SAM card slots available.
CUSTOMER CARD **POWER UP: PASSED** **GET ATR: PASSED** **READ TEST: PASSED** **WRITE TEST: PASSED** **READ VERIFY TEST: PASS** **ALL TESTS: PASSED**	When a SAM card is tested, the following information is displayed.

Table 24 Information Messages

Display	Action
STARTUP INFORMATION	
VERIFONE VX 520 **QT00E20B** **12/22/2009 Verix** **COPYRIGHT 1997-2009** **VERIFONE** **ALL RIGHTS RESERVED**	At startup, the terminal displays a copyright notice screen that shows the terminal model number, the OS version of the VX 520 stored in the terminal's flash memory, the date the firmware was loaded into the terminal, and the copyright notice. This screen appears for three seconds, during which time you can enter Verix Terminal Manager by simultaneously pressing F2 and F4. You can extend the display period of this screen by pressing any key during the initial three seconds. Each keypress extends the display period an additional three seconds.
VERIFONE VX 520 **QT00E20B** **12/22/2009 Verix** **COPYRIGHT 1997-2009** **VERIFONE** **ALL RIGHTS RESERVED**	If some other certificate is loaded by a reseller (e.g., bank), the fourth line on the startup screen is left blank.
VERIFONE VX 520 **QT00E20B** **12/22/2009 Verix** ****TAMPER**** **COPYRIGHT 1997-2009** **VERIFONE** **ALL RIGHTS RESERVED**	If an attempt to break into the terminal's system has been made, the message ****TAMPER**** is displayed in place of the certificate on the startup screen. The terminal will remain in this state until the condition has been remedied.
****VERIFYING FILES**** **COMPARE SIGNATURE** **FILENAME.P7S** **FILENAME.OUT** ***AUTHENTIC***	This message appears on screen when the file authentication module successfully authenticates a new signature file. ***AUTHENTIC*** appears for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new signature files are checked. New digital certificates are always checked first, followed by new signature files, in an uninterrupted process.

Table 24 Information Messages

Display	Action
VERIFYING FILES CHECK CERTIFICATE FILENAME.CRT *AUTHENTIC*	This message appears on screen when the file authentication module successfully authenticates a new digital certificate. ***AUTHENTIC*** is displayed for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new certificates are checked, one by one. In special cases where system certificates are being installed, **SYSTEM CERTIFICATE** is displayed instead of **CHECK CERTIFICATE**.
TERMINAL INFORMATION	
VERIX TERMINAL MGR TERM INFO SERNO 711-656-340 PTID 12000000 PART M251553306AP1 REV 1 OS VER QA000819 ↓	The following screens show configuration information specific to your terminal: • **SER NO -** serial number • **PTID -** permanent terminal identification number • **PART -** terminal part number • **REV -** terminal hardware version number • **OS VER -** operating system version
VERIX TERMINAL MGR TERM INFO MODL 05150 CTRY GEN KEYPAD 0 DISPLAY 128064 MAG RDR 3 PRINTER 1 ↑ ↓	• **MODL -** model number • **CTRY -** country of manufacture • **KEYPAD -** keypad type (0 = Telco, 1 = calculator, 2 = Singapore, 6 = EBS100) • **DISPLAY -** display unit type • **MAG RDR -** magnetic stripe card reader type • **PRINTER -** shows if a thermal printer is integrated with the terminal (0 = No, 1 = Yes)
VERIX TERMINAL MGR TERM INFO PINPAD 1 LIFE 7195425 RSET 070208170926 RCNT 6658 TAMPER DETECTED N ↑ ↓	• **PINPAD -** whether or not a PIN Pad device is integrated into the terminal (0 = No, 1 = Yes) • **LIFE -** number of seconds the terminal has run • **RSET -** last reset date and time, in YYMMDDHHMMSS format (YY = year, MM = month, DD = day, HH = hour, MM = minute, and SS = second) • **RCNT -** number of times the terminal has been reset either through application control, a terminal manager request, or a power cycle • **TAMPER DETECTED -** indicates whether the terminal has been tampered (N = No, Y = Yes)

Table 24 Information Messages

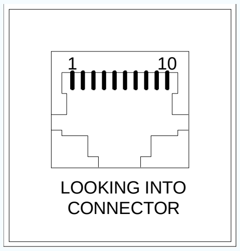
Display	Action
VERIX TERMINAL MGR TERM INFO **MDM TYPE 22** **VER B305xx00yy00zz00** **MODEM CTRY 89** **I1 042** **I3 CX81802-V32** ↑ ↓	• **MDM TYPE** - determines the modem type (0 = none, 4 = 14.4 modem, 22 = modem/ethernet combo) • **VER** - shows the modem firmware patch (B3 = Banshee modem, 05xx = firmware patch version, yy = country profile code, zz = country profile major version) • **MODEM CTRY** - shows 12-bytes of factory-deefined country variant data • **I1** - shows the modem firmware version • **I3** - shows the modem manufacturer’s hardware version
VERIX TERMINAL MGR TERM INFO **CERT 234000** **HEAP 772** **STACK 1700** **NEXT CERT F3** ↑	• **CERT** - shows the first certificate • **HEAP** - displays the memory designation used by the OS • **STACK** - shows the memory set aside for the OS stack. This is where the terminal stores data for running tasks like all the parameters from the call Select **NEXT CERT F3** to view other certificates.

Appendix B

Port Pinouts

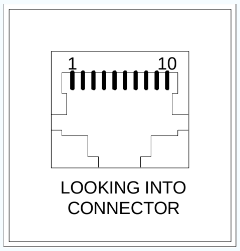
The tables in this appendix list pinouts for the VX 520 terminals.

PIN Pad Serial Port

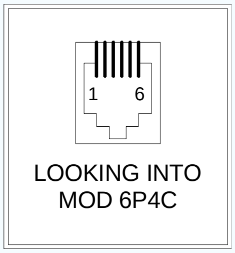
Connector	PIN	Function	Description
	1	NC	No connection
	2	VPINpad	+9V DC regulated power[a]
	3	NC	No connection
	4	NC	No connection
	5	GND	Power ground
	6	/RXD	Receive data
	7	/TXD	Transmit data
	8	NC	No connection
	9	NC	No connection
	10	NC	No connection

[a] Maximum 450 mA.

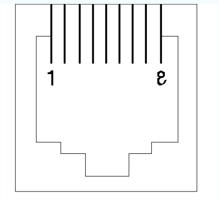
RS-232 Port

Connector	PIN	Function	Description
	1	NC	No connection
	2		9V
	3	NC	No connection
	4	NC	No connection
	5	GND	Power ground
	6	/RXD	Receive data
	7	/TXD	Transmit data
	8	CTS	Clear to send
	9	RTS	Request to send
	10	NC	No connection

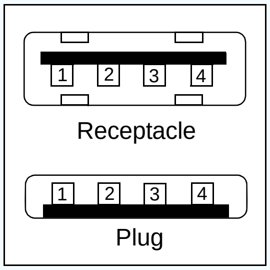
Telco Port

Connector	PIN	Function	Description
	1	NC	No connection
	2	NC	No connection
	3	Tip	Telephone line
	4	Ring	Telephone line
	5	NC	No connection
	6	NC	No connection

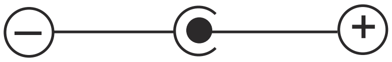
Ethernet Port

Connector	PIN	Function	Description
	1	TXD+	Transmit data +
	2	TXD-	Transmit data -
	3	RXD+	Receive data +
	4	NC	No connection
	5	NC	No connection
	6	RXD-	Receive data -
	7	NC	No connection
	8	NC	No connection

USB Pinout

Connector	PIN	Function	Description
	1	USB_5V_EXT	5V USB Power (200mA)
	2	nUSB_DEVICE	USB Device Signal -
	3	pUSB_DEVICE	USB Device Signal +
	4	GND	USB Ground

DC Input Jack Polarity



APPENDIX C

ASCII Table

ASCII Values

The following section shows the ASCII table for the VX 520 display.

Table 25 VX 520 Display ASCII Table

Dec	Hex	ASCII	Dec	Hex	ASCII	Dec	Hex	ASCII	Dec	Hex	ASCII
0	00	NUL	32	20	SP	64	40	@	96	60	'
1	01	SOH	33	21	!	65	41	A	97	61	a
2	02	STX	34	22	"	66	42	B	98	62	b
3	03	ETX	35	23	#	67	43	C	99	63	c
4	04	EOT	36	24	$	68	44	D	100	64	d
5	05	ENQ	37	25	%	69	45	E	101	65	e
6	06	ACK	38	26	&	70	46	F	102	66	f
7	07	BEL	39	27	'	71	47	G	103	67	g
8	08	BS	40	28	(	72	48	H	104	68	h
9	09	HT	41	29	)	73	49	I	105	69	i
10	0A	LF	42	2A	*	74	4A	J	106	6A	j
11	0B	VT	43	2B	+	75	4B	K	107	6B	k
12	0C	FF	44	2C	,	76	4C	L	108	6C	l
13	0D	CR	45	2D	-	77	4D	M	109	6D	m
14	0E	SO	46	2E	.	78	4E	N	110	6E	n
15	0F	SI	47	2F	/	79	4F	O	111	6F	o
16	10	DLE	48	30	0	80	50	P	112	70	p
17	11	DC1	49	31	1	81	51	Q	113	71	q
18	12	DC2	50	32	2	82	52	R	114	72	r
19	13	DC3	51	33	3	83	53	S	115	73	s
20	14	DC4	52	34	4	84	54	T	116	74	t
21	15	NAK	53	35	5	85	55	U	117	75	u
22	16	SYN	54	36	6	86	56	V	118	76	v
23	17	ETB	55	37	7	87	57	W	119	77	w
24	18	CAN	56	38	8	88	58	X	120	78	x
25	19	EM	57	39	9	89	59	Y	121	79	y
26	1A	SUB	58	3A	:	90	5A	Z	122	7A	z
27	1B	ESC	59	3B	;	91	5B	[	123	7B	{
28	1C	FS	60	3C	<	92	5C	\	124	7C	|
29	1D	GS	61	3D	=	93	5D	]	125	7D	}
30	1E	RS	62	3E	>	94	5E	^	126	7E	~
31	1F	US	63	3F	?	95	5F	_	127	7F	DEL

APPENDIX D

Keypress Scan Codes

Keypress Scan Codes Table

The following section shows the Keypad Scan Code table for the VX 520.

Table 26 Keypress Scan Codes

Key	Scan Code	Notes
1	0xB1	‘1’ with high order bit set
2	0xB2	‘2’ with high order bit set
3	0xB3	‘3’ with high order bit set
4	0xB4	‘4’ with high order bit set
5	0xB5	‘5’ with high order bit set
6	0xB6	‘6’ with high order bit set
7	0xB7	‘7’ with high order bit set
8	0xB8	‘8’ with high order bit set
9	0xB9	‘9’ with high order bit set
*	0xAA	‘*’ with high order bit set
0	0xB0	‘0’ with high order bit set
#	0xA3	‘#’ with high order bit set
CANCEL	0x9B	ESC with high order bit set
BKSP	0x88	BS with high order bit set
BKSP (long key press)	0x8E	SO with high order bit set
ALPHA	0x8F	SI with high order bit set
ENTER	0x8D	CR with high order bit set
F1	0xFA	‘z’ with high order bit set
F2	0xFB	‘{‘ with high order bit set
F3	0xFC	‘|’ with high order bit set
F4	0xFD	‘}’ with high order bit set
F5	0xEF	Vx670 only, ‘o’ with high order bit set
PF1	0xE1	‘a’ with high order bit set
PF2	0xE2	‘b’ with high order bit set
PF3	0xE3	‘c’ with high order bit set
PF4	0xE4	‘d’ with high order bit set

Dual Keypress

When certain pairs of keys are pressed, the console driver detects it and returns a combined scan code. There are two restrictions to this event:

- One of the pair of keys must be from column three of the physical keypad above (control chars: d, cancel, bksp, clear, enter), otherwise the first key scanned of the pair is returned as a single key.
- The second key must be a numeric key (‘0’ -’9’). Scan codes for control characters and any other key are undefined.

Dual keypresses are debounced for the same period as single keys (2 scans in a row) and do not auto repeat. The scan codes returned for dual keypresses are shown in the table below:

Table 27 Dual Keypress Scan Code

Key Pair	Scan Code
‘d’ + ’0’..’9’	0xd0..0xd9
Cancel + ‘0’..’9’	0xc0..0xc9
Bksp/Clear + ‘0’..’9’	0xa0..0xa9
Alpha + ‘0’..’9’	0xf0..0xf9
Enter + ‘0’..’9’	0xe0..0xe9

NOTE

Some dual keypresses return codes overlap with the normal single keypress return codes. Specifically, dual keypress ENTER-1 through ENTER-4 overlap with single keypress 'a' through 'd', and CLEAR-3 overlaps with the single '#' keypress.

The special keypairs F2-F4 and Enter-7 are used to enter Verix Terminal Manager. These are the only dual keypresses that do not follow the two restrictions outlined in this section.

Auto-repeating Keys

If you hold down a key, after a short debounce the console posts an `EVT_KBD` event and passes the key’s return code to the keybuffer. If the user continues to hold the key for another 750 msec, then auto-repeat begins. At this point, another event and key code are returned to the application. After this initial repeat, if the same key is still held, the event and key code returns every 100 msec that the key is being held.

NOTE

Dual keypresses do not auto-repeat.

When you hold down the BACKSPACE key, it changes from 0x88 to 0x8E and does not autorepeat.

GLOSSARY

Access Code A code number dialed to gain access to a telephone line, such as dialing the number 9 to reach an outside line.

Application ID An alphanumeric code that identifies an application program downloaded to a terminal from a download computer. For ZonTalk 2000 application downloads, the application ID is stored in the `CONFIG.SYS` record which begins with the *ZA key. A VX 520 application ID can be up to 21 characters long. For VeriCentre Download Management Module, the application ID, as well as other `CONFIG.SYS` variables, may differ from those used for ZonTalk 2000.

Application program The ordered set of programmed instructions by which a computer performs an intended task or series of tasks.

Application prompt The information shown on the terminal's display panel when power is applied to the terminal, assuming that an application program has already been downloaded into the terminal's memory and authenticated by the file authentication module. The application prompt often contains a graphical logo, and date and time, but it can consist of anything the programmer chooses for that purpose.

ASCII Abbreviation for *American Standard Code for Information Interchange*. A 7-bit code (with no parity bit) that provides a total of 128 bit patterns (see ASCII Table). ASCII codes are widely used for information interchange in data processing and communication systems.

Back-to-back application download The process of copying the contents of one terminal's application memory to another terminal's application memory. A terminal-to-terminal application upload require that the sending and receiving terminal be connected to each other by a serial cable. The same operation as a *terminal-to-terminal* application upload.

Baud The number of times per second that a system, especially a data transmission channel, changes state. The state of a system may represent a bit, digit, or symbol. For a POS terminal, the baud rate indicates the number of bits per second that are transmitted or received by the terminal's serial ports or modem.

Bit Short for *binary digit*. Either of the two digits 0 and 1 in the binary number system. Also, a unit of information equal to one binary decision. The bit is the smallest unit of storage and hence of information in any binary system within a computer.

Block A collection of data units such as words, characters, or records (generally more than a single word) that are stored in adjacent physical positions in memory or on a peripheral storage device. A block can therefore be treated as a single unit for reading, writing, and other data communication operations.

Boot loader Also called a *bootloader* or *bootstrap loader*. A short program, stored in flash, that allows the terminal to continue operating during an operating system download procedure, until the new operating system is downloaded into terminal memory.

Buffer A temporary memory area for data, normally used to accommodate the difference in the rate at which two devices can handle data during a transfer.

Byte A term developed to indicate a measurable number of consecutive binary digits that are usually operated on as a unit. For the VX 520, a byte consists of eight bits. See also Bit.

Calendar/clock chip A real-time clock inside the VX 520 terminal which keeps track of the current date and time.

Card reader Also called *magnetic stripe card reader*. The slot on the right side of the VX 520 terminal that automatically reads data stored in the magnetic stripe on the back of a specially-encoded card when you swipe the card through the slot.

Carrier Usually, an analog signal that is selected to match the characteristics of a particular transmission system. The carrier signal on a phone line is modulated with frequency or amplitude variations to allow a terminal to transmit or receive data using a modem. A carrier signal transmits data from a host computer to a VX 520 terminal over an analog telephone line.

Certificate Also called a *digital certificate*. A digital document or file that attests to the binding of a public key to an individual or entity, and that allows verification that a specific public key does in fact belong to a specific individual.

Character An element of a given character set. The smallest unit of information in a record. A letter, numeral, or other symbol to express information.

CONFIG.SYS file A special keyed file that is stored in terminal memory and which contains system and application configuration parameters. Each record in a `CONFIG.SYS` file is identified by an alphanumeric search key. In the VX 520 file system, there is one password-protected `CONFIG.SYS` file per file group (Groups 1–15). You can modify `CONFIG.SYS` records using the keyed file editor. See Keyed file editor.

CPU Abbreviation for *central processing unit*. The principal operating part of a computer system that controls the interpretation and execution of instructions stored in memory.

Data Information prepared, often in a particular format, for a specific purpose. Data is to be distinguished from applications or program instructions. In the VX 520 terminal, application files and data files can be stored in RAM or flash memory.

Data entry The process of using a keyboard, card reader, or other device to input data directly into a system.

Data packet A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a composite whole through a packet switching network. Any message that exceeds the maximum size is partitioned and carried as several packets. Data packets are formed by the controller in the sending data terminal and the data is extracted and reassembled by the controller at the receiving end.

Dedicated line A leased or private telephone line that is used for a particular communications purpose, such as to connect a VX 520 terminal to a host computer. See Leased line.

Default A value, parameter, option, or attribute that is assigned by the program or system when another has not been assigned by the user.

Delete To remove a record, field, or item of data.

Diagnostics Techniques employed for detection and isolation of malfunctions and errors in programs, systems, and devices. In a diagnostic test, a program or routine is run to detect failures or potential failures. These tests and routines help detect and isolate problems in a terminal or peripheral device.

Dial-up line A standard public telephone line. The switching equipment on a dial-up line requires that one party dial the other party before a connection can be made.

Direct download The process of transferring files and/or data from a download computer to a terminal over a serial cable connection and in a local, as opposed to a remote, system environment.

Display The backlit LCD screen on the VX 520 terminal that shows numerals, letters, and punctuation symbols in selected fonts, graphics in various formats, information entered from the keypad, as well as system prompts and messages.

Download To transfer files or data from a host computer or sending terminal over a communication link to a receiving terminal.

DTMF *Dual-tone multi-frequency*. The tones used on a touch-tone telephone.

File authentication A process through which one proves and verifies the origin of a file, the identity of the sender, and the integrity of the information it contains.

Firmware System software, including the operating system, boot loader, default display font, and system messages, stored in terminal flash memory.

Fixed prompt A system prompt or message stored as part of system firmware in terminal memory. Fixed prompts appear on the terminal display to alert the user to specific system occurrences or malfunctions, and to prompt the user to enter specific information or select options.

Flash memory An area of non-volatile memory where files can be stored. The VX 520 also has a RAM-based file system. Files can be stored in RAM (drive `I:`) or in flash (drive `F:`) memory area of any file group (Groups 1–15).

Host computer Also called a *download* computer. The primary or controlling computer in a multiple computer operation. Also, a computer used to prepare programs for download to POS terminals. Host computers are also used to process transactions that originate from a distributed network of POS terminals.

Input The process of entering data into a processing system or a peripheral device such as a terminal, or the data that is entered.

Interface A common boundary between two systems, devices, or programs. Also, to interact with a device.

Keyed file character set A limited set of 96 ASCII characters, from 00h to 5Fh (or 0 to 95 decimal), that is used by the VX 520 keyed file editor. Although an application program can download all 95 characters in this set, you can only enter 50 of these characters from the terminal keypad: 0–9, A–Z, and 14 special characters.

Keyed file editor A keyed file editor lets you create new records or modify existing records stored in a keyed file such as `CONFIG.SYS`. See CONFIG.SYS file.

Keyed file record ASCII data, or variables, stored in the terminal's `CONFIG.SYS` file(s). A keyed file record consist of two parts: a search key that identifies the record, and the data or variable stored in the record. See CONFIG.SYS file.

Keypad A small keyboard or section of a keyboard containing a smaller number of keys, generally those used in simple calculators. The 16-key core keypad of the VX 520 terminal is used to enter data and perform operations.

Leased line A private telephone line leased from the phone company. See Dedicated line.

Line cord A telephone-type cord with modular plugs on each end to connect the terminal to a dial-up telephone line.

Local functions Operations performed at the terminal only and not in interaction with a host computer. For the VX 520, local functions such as internal diagnostics are performed in terminal manager. See Chapter 4, Verix Terminal Manager.

Manual transaction A transaction involving the manual entry of account information from the terminal keypad instead of automatic entry of the information from a reading device, such as a magnetic stripe card reader.

Memory A device or medium that can retain information for subsequent retrieval. The term is most frequently used to refer to the internal storage of a computer (or a terminal) that can be directly addressed by operating instructions. In the VX 520, files can be stored in battery-backed RAM or in non-volatile flash memory.

Messages Words and symbols appearing on the display screen which inform the user of the terminal of the result of a process, or if an error has occurred. The term "prompt" is used when the displayed message is requesting the user to enter information or to select an option.

Modem *Modulator/demodulator*. A device that converts a digital bit stream into an analog signal to transmit over an analog communication channel (modulation), and converts incoming analog signals into digital signals (demodulation). The VX 520 terminal's internal modem allows communication with a host computer over a dial-up telephone line.

Non-volatile memory A memory or storage medium that retains data in the absence of power so that the data is available when power is restored. For the VX 520, application files and data files can be stored in battery-backed RAM or non-volatile flash memory, according to the requirements of the application.

Normal Mode The operating mode for normal transaction processing. The main application (downloaded and authenticated) starts and displays an application prompt, indicating that the terminal is in normal mode. In this mode, the terminal is ready to process transactions. See Chapter 4, Verix Terminal Manager.

Packet A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a composite whole through a packet switching network. Any message that exceeds the maximum size is partitioned and carried as several packets.

Packet-switched networks Networks of computers or computing devices in which communication resources are allocated dynamically on a variety of levels to multiple communicating entities. Messages between entities are partitioned into segments, or packets, with a fixed maximum size.

Parameter A variable that is usually assigned a constant value for a specific subroutine, procedure, or function. Parameters stored in terminal memory or in the `CONFIG.SYS` file(s), enable a host or download computer to identify to terminal configuration.

Password A group of characters that identify a user to the system so that they can gain access to the system or part of that system. Passwords are used to ensure the security of computer systems by regulating the amount of access freedom. The password used to enter terminal manager is called the *Verix Terminal Manager password*. In the VX 520 file system, each file group (Groups 1–15) also has its own password.

PC Abbreviation for personal computer. Usually, PC refers to an IBM-compatible personal computer.

Peripheral device In a computer system, any equipment that provides the processing unit with outside communication. Typical peripheral devices for a POS terminal include PIN Pads and check readers.

Port An opening or connection that provides electrical or physical access to a system or circuit. Also, a connection point with associated control circuitry that allows I/O devices to be connected to the internal bus of a microprocessor.

POS terminal A terminal used at the *point of sale*, which is usually at a merchant site where a customer pays for goods or services received. Information concerning the sale can be entered into the terminal and transmitted to a remote host computer for verification and processing.

Power pack A unit for transforming and converting electrical power from one AC voltage level to another AC voltage level, or from AC to DC, for electronic devices.

Prompt A short message, sent from a process to a user, indicating that the process expects the user to input data. For example, a prompt appears on the terminal display asking the user to enter specific information. See Messages.

Protocol An agreement that governs the procedures used to exchange information between cooperating entities. For example, protocols govern the format and timing of messages exchanged between devices in a communication system, such as between a terminal and a host computer.

PTID *Permanent terminal ID*. An optional identifier that can be permanently assigned to a VeriFone terminal at the factory, upon customer request. The PTID is an eight digit number, consisting of a two digit manufacturer's ID (12 for VeriFone), followed by a six digit terminal ID. If no PTID is assigned to the unit then, the default value 12000000 is used.

Pulse dialing A method of telephone dialing that specifies a phone number by the number of electrical pulses sent.

RAM *Random-access memory*. The type of memory in which storage locations are addressable and can therefore be accessed in any order. In the VX 520 terminal, the RAM (or SRAM) is commonly used to store applications and temporary data generated during a transaction.

The RAM is battery-backed, meaning that if power is turned off, data stored in this area of volatile memory is not lost. Application files and data can also be stored in the non-volatile flash memory system. By default, files downloaded to the terminal are stored in the RAM of the target file group(s). The RAM file system is called drive `I:`. See Flash memory.

Remote host computer A host computer connected to a VX 520 terminal over a dial-up telephone line to download files or data, or to process transactions. The opposite of remote is *local*.

RS-232 A widely used standard interface that covers the electrical connection between data communication equipment, such as a modem, and data terminal equipment, such as a microcomputer or computer terminal. The RS-232 interface standard was developed by the EIA (Electronic Industries Association) and is essentially equivalent to the CCITT's V.24 interface.

Scroll To move all or part of the information displayed on a screen up or down, left or right, to allow new information to appear. For the VX 520, text that does not fit entirely within the display area can be scrolled to the left or right using the pound (#) and asterisk (*) keys.

Search key Also called *key*. In the VX 520, a short character string used by an application to identify a keyed file record stored in `CONFIG.SYS` file(s). For example, *ZA or *OT. A *keyed file record* consist of two parts: a search key to identify the record, and the variable data stored in the record. See also Keyed file record and CONFIG.SYS file.

Serial port A connection point through which digital information is transferred one digital bit at a time. Same as *serial interface*. The VX 520 terminal has one serial port, labeled RS-232. The main serial port on a download computer is usually assigned the device ID, COM1.

Signature file A digital file with the filename extension *.p7s generated in an industry-standard format by the VeriShield File Signing Tool. The output of the file signing tool is a signature file in an industry-standard format.

SRAM See RAM.

Subroutine A software routine that can be part of another routine. When a main routine calls a subroutine, program control is transferred to the subroutine. When the subroutine is completed, control reverts to the instruction in the main routine immediately following the subroutine call.

Swipe The action of sliding a magnetic stripe card through a terminal card reader. The VX 520 card reader has a bi-directional swipe direction. The user must hold the card so that the magnetic stripe is faces in and towards the keyboard.

Verix Terminal Manager For the VX 520, terminal manager temporarily disables normal mode operations, allowing you to perform local functions such as downloads, diagnostics, and other operations that cannot be performed while the application program is running.

At startup, the terminal displays a copyright notice screen that shows the version of VX 520 system firmware stored in terminal flash memory, the date it was loaded into the terminal, and the copyright notice. This screen appears for three seconds. To enter terminal manager, simultaneously press the F2 and F4 keys during this three-second period. Pressing any other key(s) during that period resets the copyright notice screen to display an additional three seconds.

See also Local functions and Normal Mode.

Verix Terminal Manager password A unique set of characters entered by the user to access the terminal manager local functions of the terminal. A default password is supplied with each terminal. For the VX 520 terminal, the default system password is: “1, Alpha, Alpha, 66831”.

To prevent unauthorized access, change the default password to a confidential password on terminal deployment. Store the new password in a safe place, as it is impossible to restore the terminal default password without sending the unit to VeriFone for service.

Telephone download The process of transferring an application program and/or data from a remote host or download computer to a terminal over a telephone line.

Telephone jack Also, telephone line wall jack. Insert a modular connector into a telephone jack or receptacle. Also, modular-type sockets for connecting telephone line cords. The VX 520 terminal has a TELCO RJ-45-type telephone jack on the back panel used for a direct connection to a telephone line wall jack.

Telephone line The standard telephone wiring connecting your phone or terminal to a local or private telephone company.

Terminal Any device capable of sending and receiving data over a data link, such as a telephone line or a RS-232 cable. Some terminals, such as the VX 520, can print receipts and display information and graphics on a screen.

Terminal ID An alphanumeric code that identifies a terminal to a download computer. In this way, the download computer can determine what data or application programs to download to that terminal. For ZonTalk 2000 downloads, the VX 520 terminal ID is stored in the *ZT record in the `CONFIG.SYS` file. This variable should not exceed 10 characters in length. Not the same as PTID

Terminal-to-terminal application upload The process of copying the application memory contents of one terminal to the application memory of another terminal. A terminal-to-terminal application upload requires that the terminals be connected to each other by a serial cable. See also Back-to-back application download.

Tone dialing Also called *touch-tone dialing*. A method of telephone dialing that uses different pitched tones to specify a phone number. See also DTMF.

Track 1, 2, or 3 data Information stored on tracks 1, 2, or 3 of a debit or credit card magnetic stripe, which can be read by a magnetic card reader device, such as the one that is integrated in the VX 520 terminal.

Transaction An exchange of data resulting in a transfer of goods, services, value, and/or information between two parties.

Variable A string of characters that denotes some value stored within the computer and that can be changed during execution. A variable may be internal to a program, in which case it is held in memory, or external if the program must perform an input operation to read its value. See Parameter.

Volatile memory A type of memory where the contents are destroyed if the power supply to the memory is interrupted. When volatile memory, such as SRAM, is used for crucial applications, it is often back up by battery-supplied power. Compare with Non-volatile memory.

INDEX

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

VX 520

Reference Guide

VeriFone Part Number DOC252-004-EN-B, Revision B