Verifone®

V200c

Reference Guide

Verifone Part Number DOC420-004-EN-B, Revision B

P400 Reference Guide

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

Acknowledgments

All other brand names and trademarks appearing in this manual are the property of their respective holders.

Verifone, Inc.
1-800-VERIFONE

www.verifone.com

Verifone Part Number DOC420-004-EN-B, Revision B

CONTENTS

PREFACE 5

Audience. 5
Organization 5
Related Documentation 5
Conventions and Acronyms 6
Conventions 6
Acronym Definitions 7

CHAPTER 1
Overview

Features and Benefits 9
Connectivity 9
Performance 9
Security 10
Form Factor 10
Exceptional Ease of Use. 10
Countertop Performance in a Hand-Over Design 10
True Multi-Application Capability 10

CHAPTER 2
Using the Terminal Keys

Data Entry Modes. 12
The Keypad 12
Function Key Descriptions 12

CHAPTER 3
System Mode

When to Use System Mode 15
Local and Remote Operations 15
Verifying Terminal Status 16
Entering System Mode 16
Exiting System Mode 17
Passwords 18
System Password 18
Default Password 18
System Mode Menus 18
System Mode Procedures. 18
Procedure Description 19
Logging in to System Mode 19
Submenus. 22

CHAPTER 4
File Authentication

Introduction to File Authentication 33
The Verifone Certificate Authority 33
Special Files Used in the File Authentication Process 34
How File Authentication Works 35
Planning for File Authentication 38
Download and Installation. 38
How Signature Files Authenticate Target Files. 39

Determine Successful Authentication 39
Digital Certificates and the File Authentication Process 39
VeriShield File Signing Tool (FST) 43
Signing Files 43
Packaging Tool 44
Downloading Application Files 44

CHAPTER 5
Performing Downloads
Downloads and Uploads 45
Download Methods and Procedures 46
Direct downloads 46
DDL Command Line Syntax 46
DDL Command Line File 47
DDL Example 47
Downloading without an Onboard Application 47
Network Download Utility 48
File Signing and Signature Files 48

APPENDIX A
System Messages
Error Messages 49
Information Messages 54

APPENDIX B
Port Pinouts
V200c Port Pinout Definitions 57
Ethernet Port (LAN) 57
MOD 10 Port (COM1) 57
Telco Port 57
USB Pinout (Host Port) 58
RS-232 Port (COM1) 58
USB Pinout 58
USB Mini-B Pinout 59

APPENDIX C
ASCII Table
The ASCII Table 61

GLOSSARY 63

PREFACE

This guide is the primary source of information for downloading to and maintaining the V200c terminal.

Audience

This guide is useful for anyone configuring the terminal.

Organization

This guide is organized as follows:

Chapter 1, Overview. Provides an outline of the terminal features.

Chapter 2, Using the Terminal Keys. Presents the terminal keys and functions.

Chapter 3, System Mode. Describes password-controlled, System Mode operations, as well as how to use it to perform a variety of test and configuration procedures.

Chapter 4, File Authentication. Focuses on the file authentication module of the VeriShield security architecture and describes how to use the file signing utility, VeriShield File Signing Tool to generate signature files.

Chapter 5, Performing Downloads. Presents procedures for downloading applications and files to the device.

Appendix A, System Messages. Provides descriptions about error and information messages.

Appendix B, Port Pinouts. Provides a list of pinouts for the terminal ports.

Appendix C, ASCII Table. Provides an ASCII table for reference.

Related Documentation

Refer to the following set of documents to learn more about the terminal:

- V200c *Certifications and Regulations Sheet*, VPN DOC420-001-EN
- V200c *Quick Installation Guide*, VPN DOC420-002-EN
- V200c *Installation Guide*, VPN DOC420-003-EN
- V200c *Security Policy*, VPN DOC420-008-EN
- *VOS Programmers Manual,* VPN DOC00501

Conventions and Acronyms

This section describes conventions and acronyms used in this manual.

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	Meaning	Example
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 typeface is used while specifying onscreen text, such as text that you would enter at a command prompt, or to provide an URL.	`RetrieveClearCardData` retrieves the previous swipe's clear track data and places it into the `pstSwipeOut` argument.
NOTE 	The pencil icon is used to highlight important information.	RS-232-type devices do not work with the terminal port.
CAUTION 	The caution symbol indicates possible hardware or software failure, or loss of data.	The terminal is not waterproof or dustproof, and is intended for indoor use only.
WARNING 	The lightning 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
BT	Bluetooth
DUN	Dial-Up Network
ECR	Electronic Cash Registers
EMV	Europay MasterCard and VISA
HSPA	High Speed Packet Access
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MIB	Management Information Block
MRA	Merchandise Return Authorization
MSAM	Micromodule-Size Security Access Module
NFS	Network File System
PAN	Personal Area Network
PED	PIN Entry Device
PCI	Payment and Card Industry
PIN	Personal Identification Number
RJ45	Registered Jack 45
RS-232	Recommended Standard 232
R-UIM	Removable User Identity Module
SAM	Security Access Module
SD	Secure Digital
SIM	Subscriber Identity Module
TFT	Thin Film Transistor
UART	Universal Asynchronous Transmitter/Receiver
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VPN	Verifone Part Number
Wi-Fi	Wireless Fidelity

CHAPTER 1

Overview

This chapter provides a brief description of the V200c terminal.

The V200c offers several communication options, enhanced display, increased processing power and two USB peripheral ports.

The V200c terminal uses a robust, sleek, and highly functional design.

Features and Benefits

The V200c is an all-in-one countertop payment system that provides quick contactless (CTLS), magnetic-stripe card reader (MSR) and smart card (SC) payment processing with a fast internal thermal printer (ITP) and clear color TFT LCD display.

NOTE

Verifone ships variants of the V200c terminals for different markets. Your terminal may have different features described in this section.

Connectivity

- 2 SAM ports (standard size)
- MOD 10 2-in-1 I/O port
- USB port
- Telco port (56K modem)
- Ethernet Port

NOTE

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

Performance

- 600 MHz, 32-bit processor (CPU)
- Increased memory
  - V200c: 128MB RAM, 256MB Flash
  - V200c Plus: 512MB RAM, 512MB Flash
- 2.8-inch QVGA LCD (240RGB x 320 dots)
- Fastest encryption/decryption appliance on the market
- Backlit keypad with tactile and audible feedback.

Security

- PCI PED 4.x approved for debit and other PIN-based transactions
- EMV L1 Type Approval (contact and contactless)
- Tamper-resistant construction, SSL protocols, and VeriShield file authentication
- Supports VeriShield Protect encryption implementations.

Form Factor

- The V200c is ergonomically designed to fit both the traditional countertop and hand-over models.

Exceptional Ease of Use

- Four-way navigation button with two selection keys for UI access.
- The contactless functionality offers a convenient payment option for consumers.
- 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 multiple font-capable integrated thermal printer simplifies paper loading and reduces paper jams. Uses 57 mm wide x 40 mm diameter paper rolls, prints at 30 lines per second (LPS).
- The triple-track, high-coercivity card reader handles most magnetic stripe cards.

Countertop Performance in a Hand-Over 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 V200c ensures uncompromising reliability from Verifone, the worldwide leader in e-payment.

True Multi-Application Capability

- The V200c offers 256 MB while the V200c Plus offers 512 MB of dynamic memory allocation for the operating system, 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.
- V200c units are certified for ISO7816-3, ISO7816-10 and EMV4.3 standards for smart card solutions.
- The VeriShield security architecture meets published specifications for PCI PED and provides sophisticated file authentication to prevent execution of unauthorized software on V200c devices.
- Biometrics and Barcode reader support via MOD 10 connector.

Using the Terminal Keys

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

This section describes how to use the keypad for data entry, which consists of a 12-key Telco-style keypad with three color-coded keys below the keypad. Using these keys you can perform all data entry tasks described in this manual. For added convenience, the keypad is automatically back-lit when you power on the device.

V200c also has navigation keys that allow users to navigate through the menus and select specific operations.

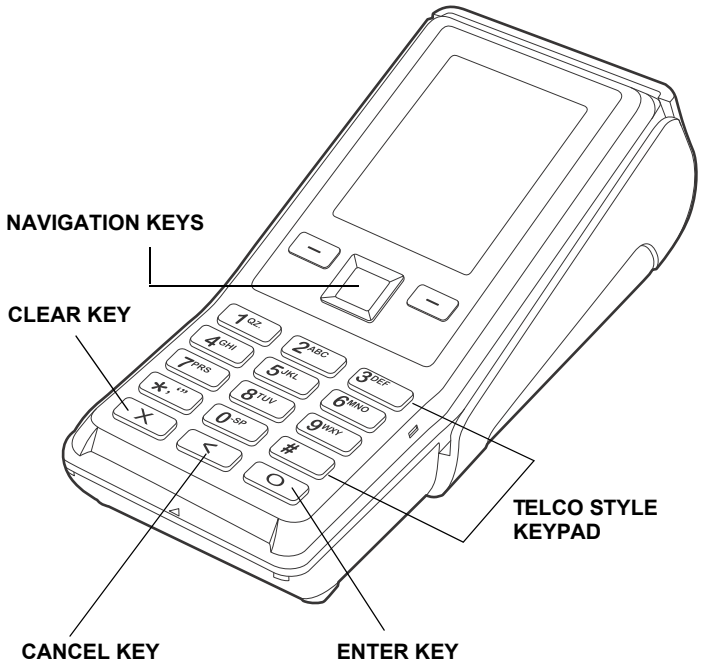


Figure 1 Front Panel Key Arrangement on V200c

Data Entry Modes

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

- **Normal mode:** This is the operating mode where an application program is present in mDRAM and currently running.
- **System mode:** This is a special, password-controlled operating mode for performing a variety configuration procedures that cannot be performed when an application is running.

The application controls how terminal keys process transactions and when you can use specific keys to type characters or respond to prompts.

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 (/).

Alphabetic characters are entered by pressing its corresponding number in the keypad multiple times within a given time. Special characters can be entered by using the asterisk (*) key or the zero number key (0). With the smaller case character selected using the hash key (#), press the asterisk or the zero number key continuously until the desired character is displayed. Some of the special characters may or may not be available when terminal is on System mode.

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 System mode procedure descriptions.

Cancel Key

Pressing the Cancel key in normal mode when the terminal’s application is loaded and running terminates the current function or operation.

In System mode, use Cancel to perform a variety of functions. The most common use of Cancel in System mode is to exit a System mode submenu and return to the main System mode menu. The specific effect of pressing the Cancel key depends on the currently active System mode menu. In the System mode login screen, a special menu can be accessed by pressing the Cancel key — Reboot, Run Apps, Transfer Logs, and System Info can be accessed without logging in or entering any password.

Clear Key

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

In System mode, the specific effect of pressing the Clear key depends on the currently active System mode menu.

Enter Key

In normal mode, the Enter key is generally used in the same way 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 System mode, 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 System mode menu.

Navigation Key

V200c has navigation keys that can be used to navigate through the system mode menus/application menus and select specific operations.

System Mode

This chapter describes *System Mode Operations*. System mode is used exclusively by those responsible for configuring, deploying, and managing on-site terminal installations.

When to Use System Mode

Use the System mode functions to perform different subsets of related tasks:

- **Application programmers**: Configure a development terminal, download development versions of the 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 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 by telephone.

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

Local and Remote Operations

The System mode operations available on a terminal can be divided into the following two categories or types:

- **Local operations**: Addresses a stand-alone unit and do not require communication or data transfers between the unit and another terminal or computer. Perform local System Mode operations to configure, test, and display information about the terminal.
- **Remote operations**: Requires communication between the unit and a host computer (or another terminal) over a telephone line or a cable connection. Perform remote System mode operations to download application software to the terminal, upload software from one terminal to another, or download over the phone line using a modem dongle from VeriCentre or from another download host.

This chapter contains descriptions on how to perform local System mode operations. For information on performing remote operations, such as downloads, refer to Performing Downloads for more information.

Verifying Terminal Status

The device you are using may or may not have an application program running on it. After you have set up the device (refer to V200c *Installation Guide*, VPN - DOC420-003-EN) and the unit is turned on, use the following guidelines to verify terminal status regarding software and current operating mode:

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

Entering System Mode

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

NOTE

Before entering System Mode and selecting the function(s) to perform, verify that the unit has been installed as described in the V200c *Installation Guide*, VPN DOC420-003-EN. Make sure that the unit is connected to a power source and is turned on.

Accessing System Mode

To enter System Mode:

1. Press the '1', '5', '9' keys at the same time.
2. Select preferred login.

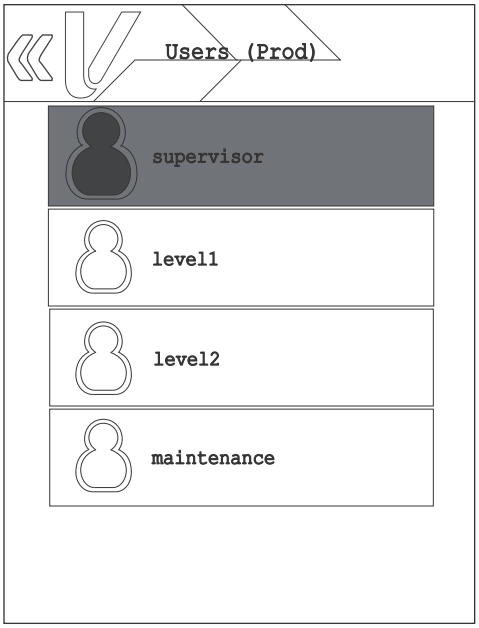


Figure 2 System Mode Login Screen

- Supervisor: Full capability
- Level 1: User defined capability
- Level 2: User defined capability

- Maintenance: Intended for Verifone repair, allows minimal access

NOTE A special menu can be accessed by pressing the Cancel key — Reboot, Run Apps, Transfer Logs, and System Info can be accessed without logging in or entering any password.

3. Once the login has been selected, enter the password. If the password is pre-expired or is pending change, the user must enter the current password and then a new password (pre-defined in the case of a pending password change). The new password must be entered twice for validation. The default System Mode password is:**166831**.
4. If the password is entered correctly, the System Mode idle screen displays. If the password is not entered correctly, the error “password was entered incorrectly” displays and the login screen will be displayed again.

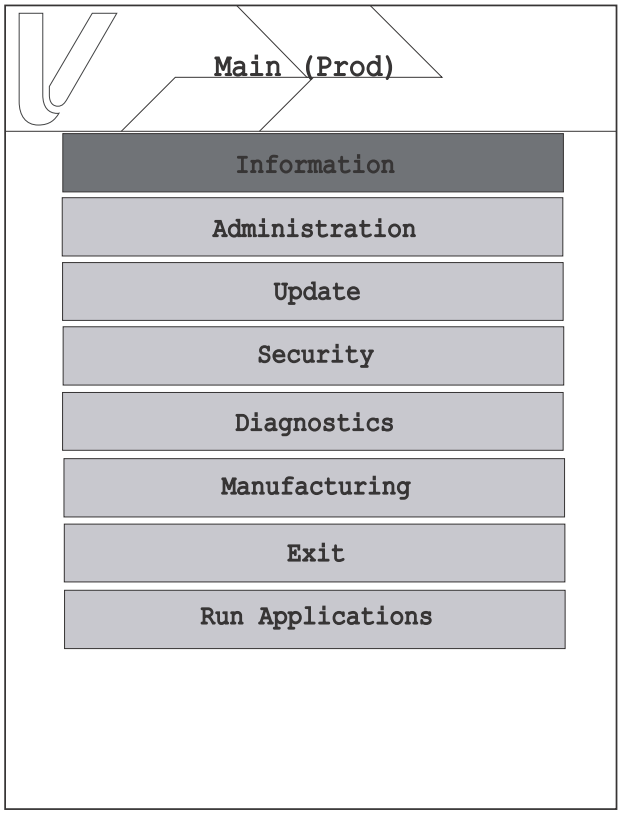


Figure 3 System Mode

Exiting System Mode

After successful completion, some operations automatically exit System mode and restart the device. Other operations require that you manually exit System mode and restart the device by selecting **Log Out** or **Reboot** from the **Exit** submenu.

Passwords

Handle passwords as you would PC passwords.

CAUTION

Without the password, you are unable to access System mode operations and may be prevented from requesting a download, performing remote diagnostics, or changing any of the information already stored in memory. The unit can, however, continue to process transactions in normal mode.

If you change a password but forgot it later on, the user may opt to expire the user passwords. Expiring user passwords clears out ALL user passwords at the same time. Consider advising all users before proceeding with this option.

To expire user passwords, access the Security > Password manager option or contact your local Verifone representative for assistance.

NOTE

Passwords must be in numeric characters only and must be at least seven digits and less than 10 digits in length.

System Password

To prevent unauthorized use of the System mode menus, the unit OS requires a system password each time you enter System mode.

When you key in the system password to enter System mode, an asterisk (*) appears for each character you type. These keys prevent your password from being seen by an unauthorized person.

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.

Default Password

From manufacturing, each file group uses the default password “166831” and entered as follows:

1 6 6 8 3 1, and press **ENTER**

System Mode Menus

Access the submenus by selecting the onscreen panel option. The System mode screen and submenus are shown below.

System Mode Procedures

The procedures in this section explain how to use each of the System mode menu options. Each procedure description starts at a main System mode menu. Each procedure takes you step-by-step through a complete System mode operation in the following sequence:

1. At the idle System mode screen, select an operation using the navigation keys.
2. Complete the operation.

3 Return to the main System mode screen by pressing the back button at the upper left hand portion of the screen or use the red cancel or back keys on your keypad. Scroll through the screen by pressing the onscreen buttons (up, down, and right) or by using the navigation keys.

Procedure Description

Procedure descriptions are arranged in a tabular format.

The Display column 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. For example:

TAMPER

MAINTENANCE REQUIRED - VAT

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 System mode 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 green **ENTER** key to choose the function and display the submenu selected. When editing, pressing **ENTER** will save a newly entered variable.
- Press the yellow **BACK** key to go back to the previous submenu or menu option.
- Press the red **CANCEL** key to exit any submenu without saving changes.

Logging in to System Mode

To enter System Mode after you have turned on the device, follow the procedure described below.

NOTE

On successful completion, some operations automatically exit System mode and restart the device. Other operations require that you exit System mode and restart the device. To manually exit System mode, choose **Exit** from the main menu and then select **Reboot**.

Table 3 Main System Mode User Interface

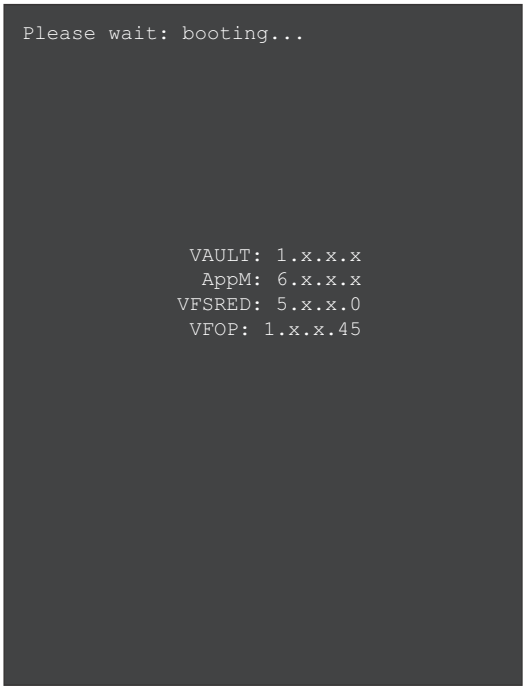
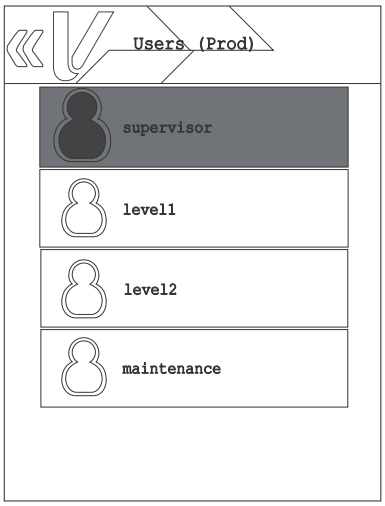
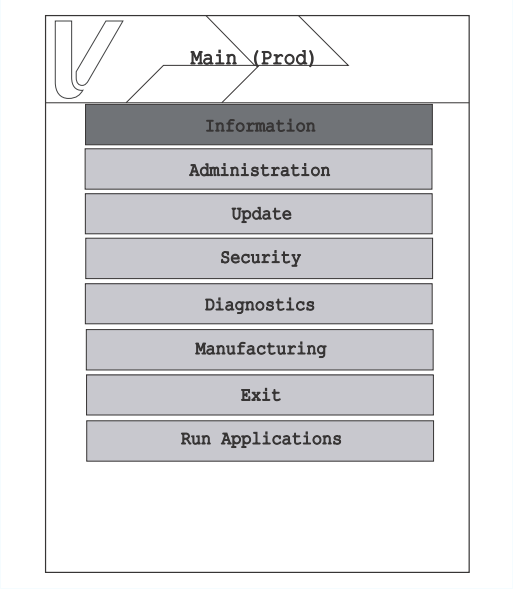
Display	Action
	At startup, the unit displays the Vault, AppM, VFSRED, and VFOP information. These information appear for three seconds, while the device is starting up.

Table 3 Main System Mode User Interface

Display	Action
	The user can choose between the available logins and enter the system password to login.
	The home screen is displayed after successful login.

Submenus

The following submenus are available from the home screen. The user may navigate through the screen using the up, down, right or back keys provided at the top portion of the screen. Use the Navigation Keys when selecting menus and specific options when using V200c.

Table 4 System Mode Submenus

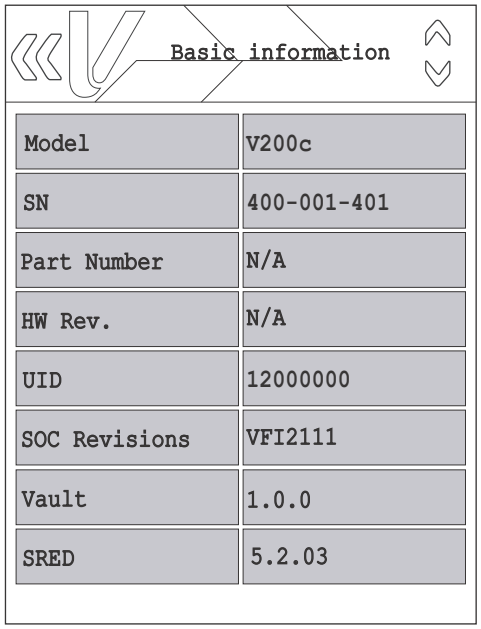
Display	Action
Home > Information> Basic information	
	To view device information, select **Information** from the main System mode menu and then select the **Basic information** panel. Scroll through the screen using the up and down arrow keys provided at the top portion of the screen. The sample screen display shown on the left contains: • Basic Information: Displays basic information such as model, serial number, part number, HW Revision, unit id, SOC Revision, Vault, SRED, Open Protocol, Application Manager version, SBI, RFS version, etc. Critical Values: • Build: Base build release date • Vault Version: Security vault version

Table 4 System Mode Submenus (continued)

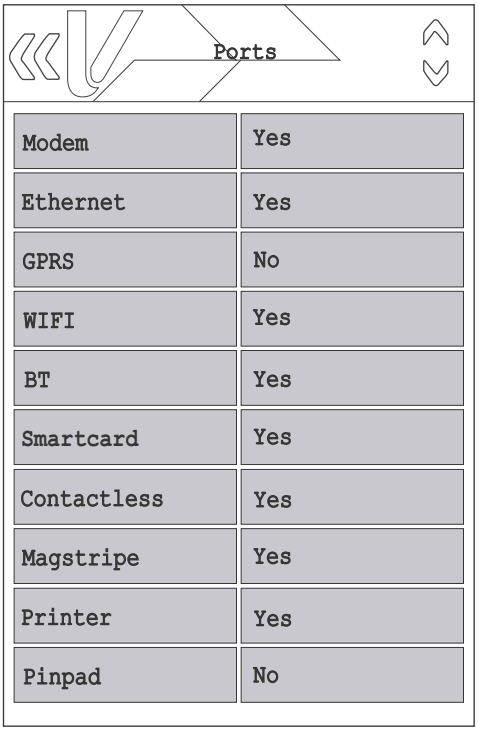
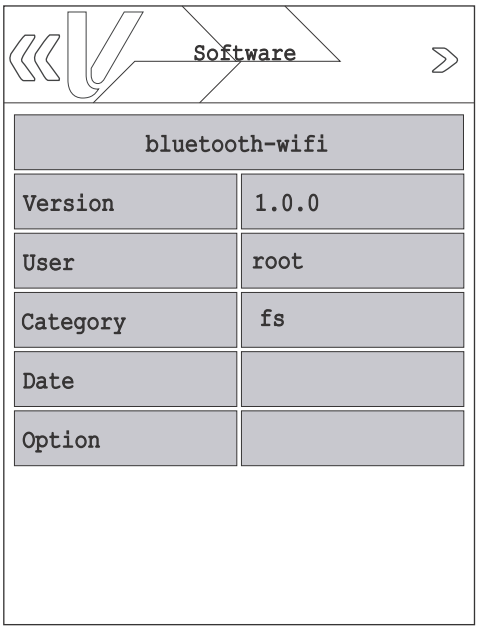
Display	Action
Home > Information > Ports	
	To view device port information, select **Information** from the main System mode menu and then select the **Ports** panel. Scroll through the screen using the navigation keys.
Home > Information > Software	
	To view installed software driver information, select **Information** from the main System mode menu and then select the **Software** panel. Scroll through the screen using the navigation keys.

Table 4 System Mode Submenus (continued)

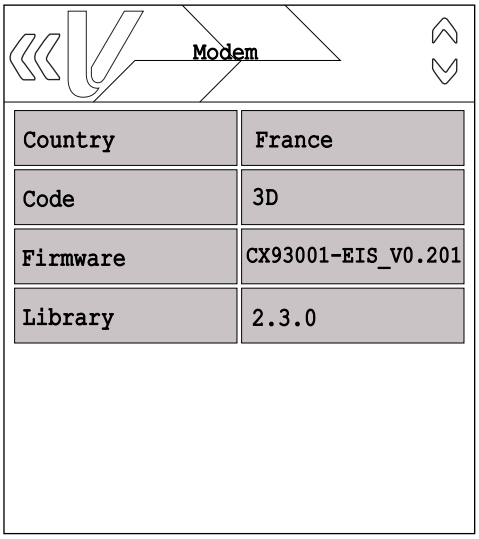
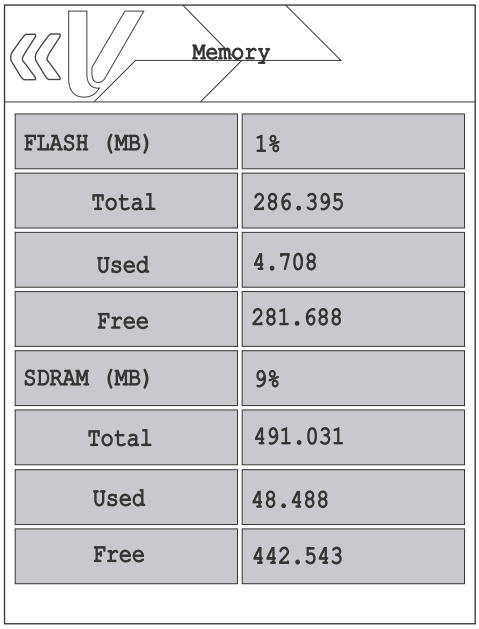
Display	Action
Home > Information > Modem	
	To view modem information, select **Information** from the main System mode menu and then select the **Modem** panel.
Home > Information > Memory	
	To view memory information, select **Information** from the main System mode menu and then select the **Memory** panel. The sample screen provided on the left displays the total, used, and available SDRAM and NAND flash memory.

Table 4 System Mode Submenus (continued)

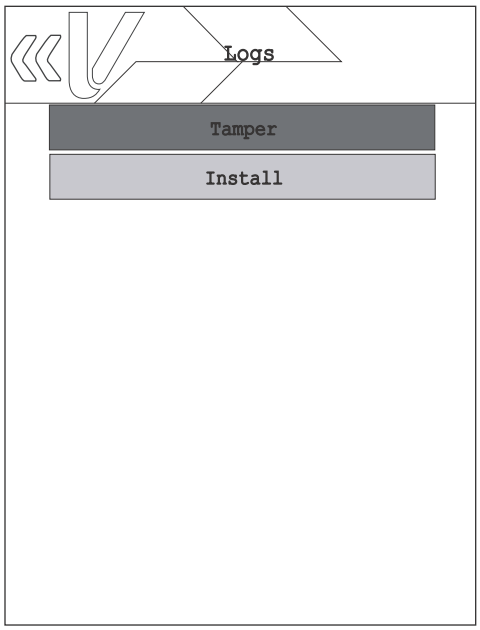
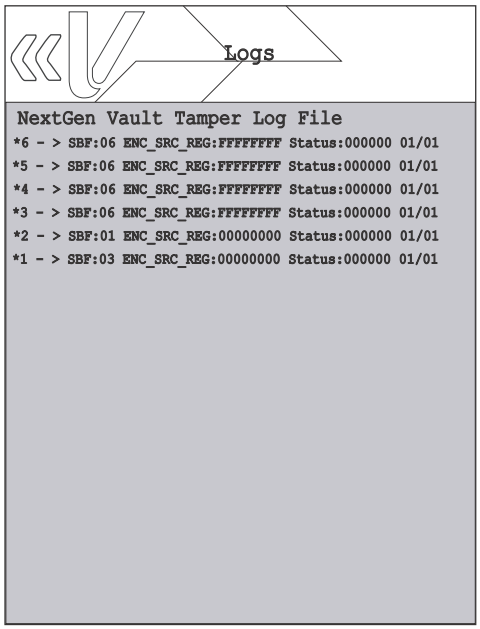
Display	Action
Home > Information > Logs	
	To view logs of tamper and installation history, select **Information** from the main System mode menu and then select the **Logs** panel.
Home > Information > Logs > Tamper	
	Sample Tamper log screen.

Table 4 System Mode Submenus (continued)

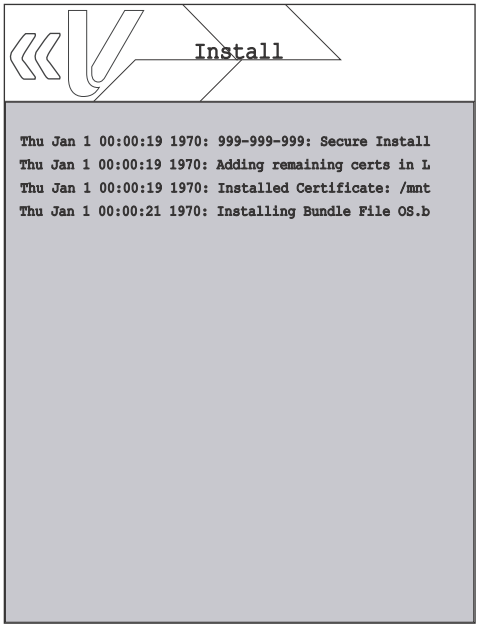
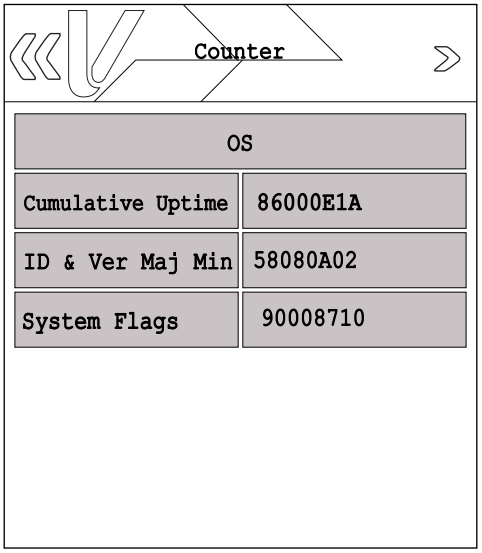
Display	Action
Home > Information > Logs > Install	
	Sample Installation log screen.
Home > Information > Counter	
	To view system counter information, select **Information** from the main System mode menu and then select the **Counter** panel.

Table 4 System Mode Submenus (continued)

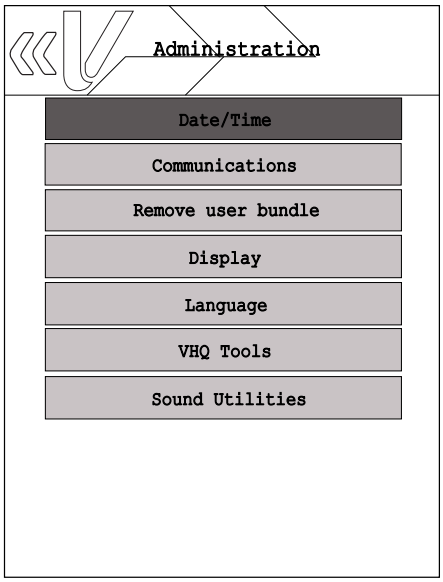
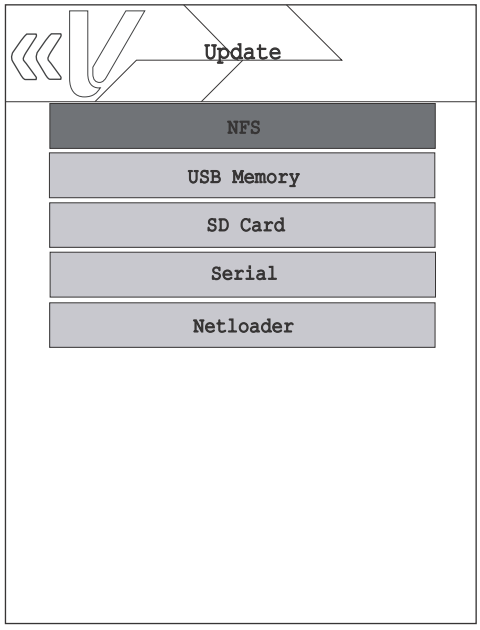
Display	Action
Home > Administration	
	Select the **Administration** panel from the main System mode menu to change the following PINpad settings: To set terminal date and time, select **Date/Time**. To set configuration settings for Ethernet, USB Gadget, Serial, Wi-Fi, iBeacon, USB, or Mini-USB, select **Communications**. To remove user bundle, select **Remove user bundle**. To adjust display brightness, select **Display**. To set or add extra language, select **Language**. To set VHQ configuration, select **VHQ Tools**. To adjust volume, select **Sound Utilities**.
Home > Update	
	To start download or update the device, select **Update** from the main System mode menu, and then select the **Update** panel. The following options will be available: To transfer files via NFS, select **NFS**. To transfer file via the USB memory device, select **USB Memory**. To transfer file via the SD memory device, select **SD Card**. To start download via the Serial port, select **Serial**. The user has the option to select the port and baud rate. Selecting AUTO baud allows the serial port to cycle through the available baud rates until communication is established. Netloader is Verifone's proprietary network based download protocol. To start download/transfer file and command set over IP from the PC client software, select **Netloader**.

Table 4 System Mode Submenus (continued)

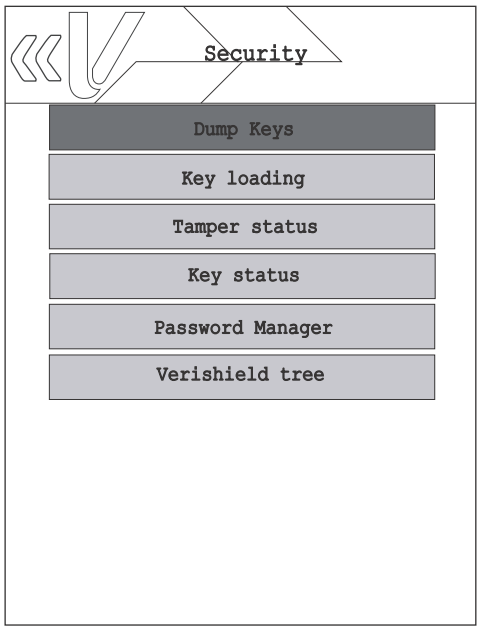
Display	Action
Home > Security	
	From the main System mode menu, select **Security** to perform the following functions. To allow user to dump keys to a storage device, select **Dump Keys**. To enable key loading state, select **Key loading**. After presenting both keyload1 and keyload2 passwords, enable the key loading state that allows data to pass from a serial port to the security module for bank/ADE and VRK keys. To allow user to view the security tamper status, select **Tamper status**. This option displays the current and logged status. To view the key status for Master Session, DUKPT, User, VRK, VSS, Feature Licenses, and ADE, select **Key Status**. To allow user to expire, change, and manage passwords, select **Password Manager**. This option provides option to: Expire: • Users passwords • Keyload passwords Change password for users: • SUPERVISOR - Set SUPERVISOR password for Sysmode. • Level 1 - Set Level 1 password. Subset of SUPERVISOR. • Level 2 - Set Level 1 password. Subset of Level 1. • Maintenance - Set password for maintenance. For repair use only. To view the serial numbers and IDs in the VeriShield Certificate list, select **Verishield tree**. Press Cancel to return to the Security submenu.

Table 4 System Mode Submenus (continued)

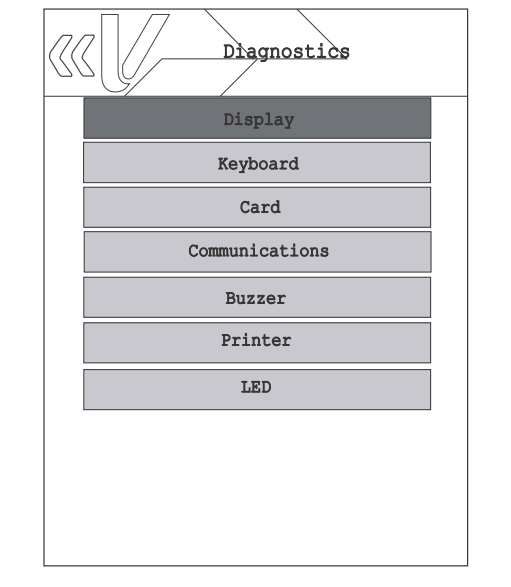
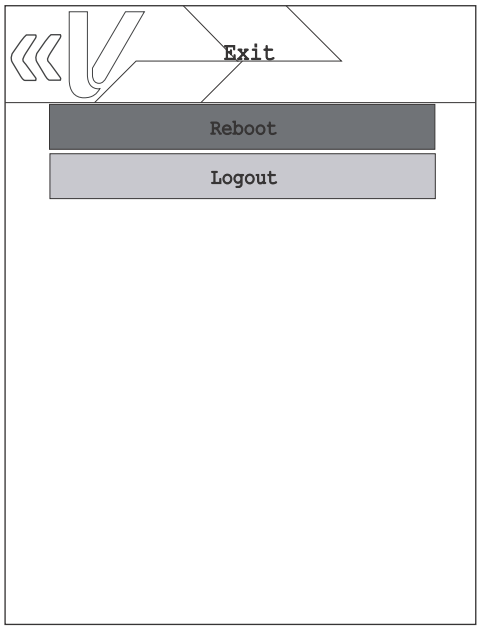
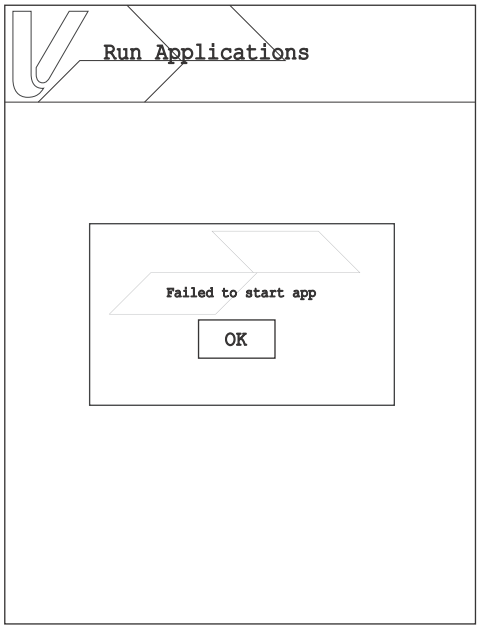
Display	Action
Home > Diagnostics	
	**Diagnostics** option allows user to perform diagnostic procedure on the PINpad display, keyboard, card readers, touch panel, buzzer, LED light, and PINpad connectivity. To perform a diagnostic procedure on the PINpad display, select **Display**. When the diagnostic image is shown on the screen, note the image colors and consistency. The image should appear solid and show no motion. Press enter to go to the next diagnostic step. To test keypad response, select **Keyboard**. Press each key and the keypress will be displayed on the screen. To Test the MSR, SCR, CTLS Reader, select **Card**. • Magnetic Stripe Reader - Swipe a magnetic-stripe card to determine if all three tracks can read the card. All tracks should display GOOD to pass the test. • Smart Card Reader - Determines the state of the smart card reader. If a card is present when the test is run, the first few bytes of the ATR is displayed. For manufacturing test purposes only. • Contactless Reader - The card details are read by placing the card over the display. On a good read, when the card is removed, TEST SUCCESS is reported. To perform test for the available connections, select **Communications**. • Ethernet - Sends a ping to the network gateway over Ethernet. Also allows a unique IP address to be pinged. • Serial - Performs a loopback test to determine the state of the Serial hardware. • Wi-Fi- Performs a ping test. • iBeacon- Allows user to start and stop broadcast, also provides status information. • Modem - Tests modem connection. Connect a phone line to the V200c and then select **Modem** to initialize. Enter the phone number when prompted. The modem then dials the specified number. Press enter to cancel. • USB - Determines the state of the USB hardware. For manufacturing test purposes only.

Table 4 System Mode Submenus (continued)

Display	Action
	To perform a diagnostic procedure on the buzzer, select **Buzzer**. To perform a diagnostic procedure on the printer, insert paper roll into the unit and then select **Printer**. A test receipt is printed and then the unit displays "**PRINTER TEST HAS FINISHED SUCCESSFULLY**". Press enter to go back to the Diagnostics menu. To perform a diagnostic procedure on the keypad LED lights, select **LED**.
Home > Manufacturing	
	To load MIB, select **Manufacturing** panel.

Table 4 System Mode Submenus (continued)

Display	Action
Home > Exit	
	To reboot the device or log off current user profile from System mode, select **Exit**.
Home > Run Applications	
	To run installed applications, select **Run Applications**. A sample screen display is provided here.

CHAPTER 4

File Authentication

This chapter discusses the following VeriShield file authentication security architecture, VeriShield file authentication module, and the organizational infrastructure that supports it.

This chapter also explains how the file authentication process may affect the tasks normally performed by application programmers, deployers, site administrators, or entities authorized to download files to a terminal.

Lastly, this chapter explains how to generate the signature files required to perform downloads and authenticate files on the unit using the file signing utility (see VeriShield File Signing Tool (FST)).

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

Introduction to File Authentication

The unit has a security architecture, called VeriShield, which has both physical and logical components. The logical security component of the VeriShield architecture, which is part of the unit's operating system software, is called file authentication (FA).

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

The Verifone Certificate Authority

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

Special Files Used in the File Authentication Process

The following specially formatted files support the FA process:

- A **digital certificate** (*crt file) is a digital public document used to verify the signature of a file.
- A **digital signature** (*.p7s file) is a piece of information based on both the file and the signer's private cryptographic key. The file sender digitally signs the file using a private key. The file receiver uses a digital certificate to verify the sender's digital signature.
- **Signer private keys** are securely conveyed to clients on smart cards. On V200c, private keys are not kept in files. The secret passwords required by clients to generate signature files, using signer private keys, are sent as PINs over a separate channel such as registered mail or encrypted e-mail.

Digital certificates and signature files, do not need to be kept secure to safeguard the overall security of VeriShield.

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

Table 5 VeriShield File Signing Tool Filename Extensions

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

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

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

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

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

Certificates Contain Keys That Authenticate Signature Files

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

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

NOTE

Only one sponsor certificate is permitted per terminal.

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

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

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

Signer Private Keys Are Issued to Secure the File Signing Process

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

The Verifone CA can also issue additional sets of sponsor and signer certificates, 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 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. Every signature file contains information about the signer private key used to sign it.

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

Certificate Request Process

In this process:

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

This process is presented below:

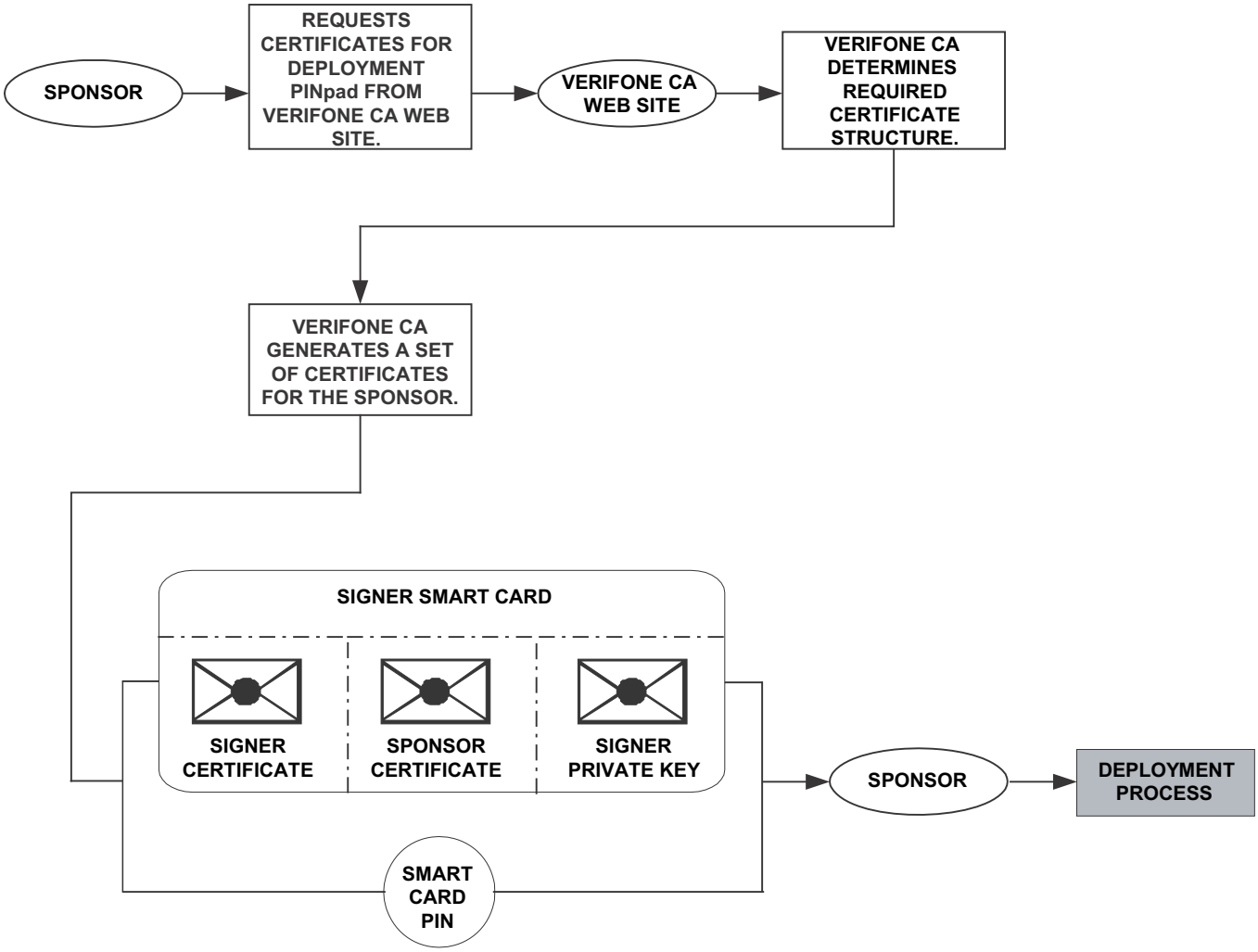


Figure 4 Certificate Request Process

Development Process

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

Deployment Process

In this process:

1. The sponsor provides the application file (from the development process) and the smart card and smart card PIN (from the certificate request process) as inputs to VeriShield.
2. VeriShield unlocks the smart card with the provided PIN, sends the file to be signed to the smart cart that will compute the signature with the resident private key. VeriShield extracts the signature, signer certificate, and sponsor certificate from the smart card.
3. VeriShield uses the extracted data, along with the application file, to create a signature file (*.p7s).
4. VeriShield creates files suitable for downloading from the smart card data.
5. The signature file, the application file, and the extracted signer and sponsor certificates are downloaded into a deployment terminal, where the following actions occur:
   a. When an attempt is made to install an application executable or data file, a matching signature and certificate must be present.
   b. The operating system compares the application file's signature against the values stored in the application file's calculated signature.
6. Each successfully authenticated application file is installed on the terminal (otherwise, the application file is deleted on failed authentication and an error message is displayed.)

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

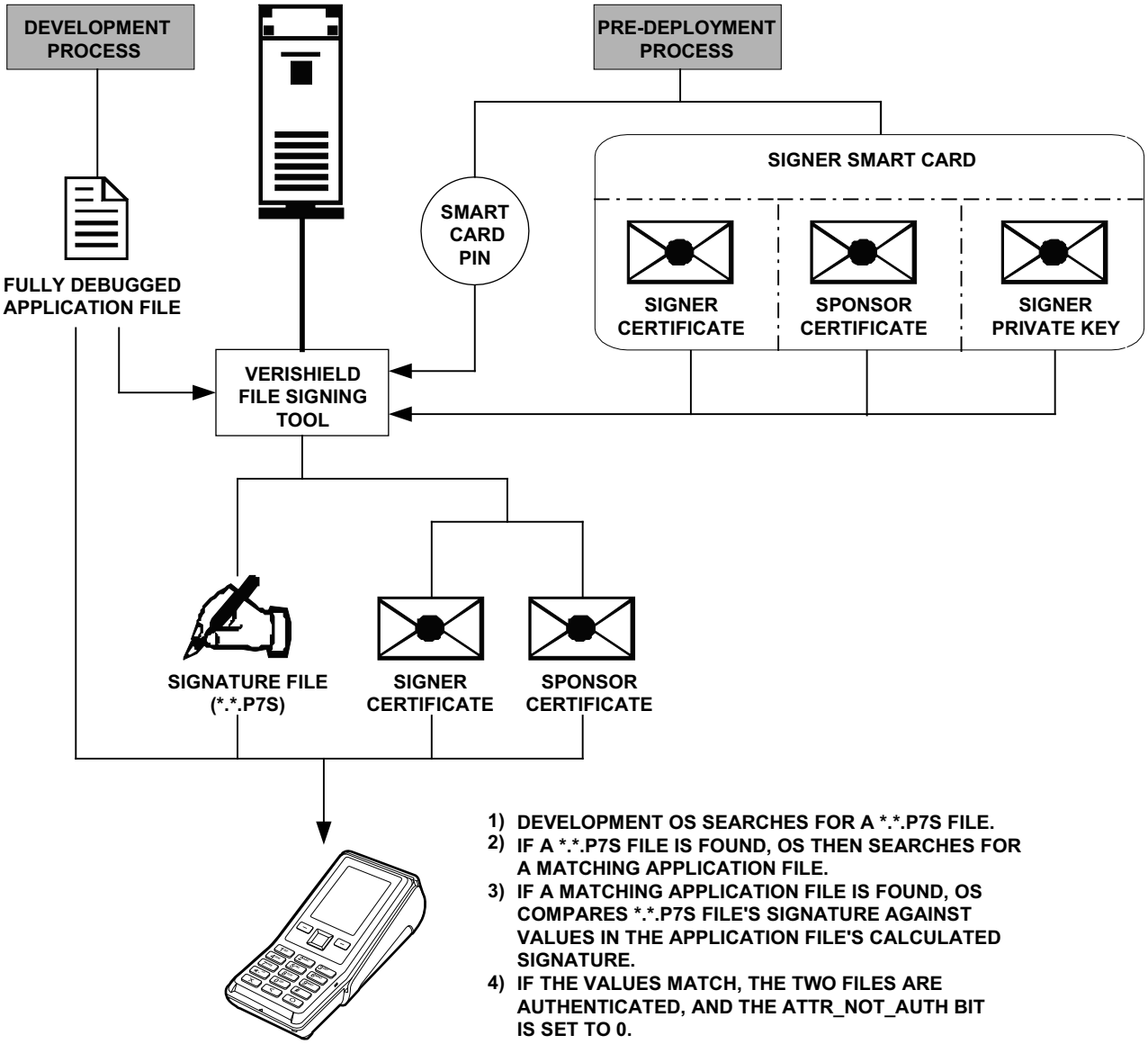


Figure 5 The Development / Deployment Process

Planning for File Authentication

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

Download and Installation

The terminal's Secure Installer plays a critical role on system and application startup as well as authenticating and installing all components; application, system and OS.

The terminal supports the following download mechanisms:

Download Mechanism	Description
Serial Direct	Supported over all serial ports (COM1/COM2/COM3 and USB Serial Gadget
USB/SD	Supported over USB memory devices and micro SD memory
Netloader	Verifone proprietary TCP-IP file transfer
NFS	Network File System

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

How Signature Files Authenticate Target Files

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

Determine Successful Authentication

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

Digital Certificates and the File Authentication Process

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.

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

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

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

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

Adding New Certificates

When you add a new certificate file to a terminal, the system detects it by filename extension (`*.crt`). The device 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 its successfully authentication. The following points explain how certificates are processed:

- If a new certificate is successfully authenticated, the information it contains is automatically stored in the terminal's certificate tree. The corresponding certificate file (`*.crt)` is not retained.

- If the relationship between the new certificate and an existing higher-level certificate cannot be verified, the authentication procedure for the new certificate fails. In this case, the certificate information is not added to the certificate tree and the failed certificate file (usually ~400 bytes) is not retained.

Development Devices

A development device is a device that maintains a set of certificates in its certificate tree. This set of certificates includes a special client certificate called a development signer certificate.

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

Deployment Devices

While the application development process is being completed and while the new application is being tested on a development device, a sponsor can order specific sponsor and signer certificates from the Verifone CA to use to logically secure sponsor and signer privileges when the device is prepared for deployment.

Customer-specific sponsor and signer certificates are usually downloaded to a device 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 6.

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

Ultimately, it is the sponsor decides on how to implement the logical security provided by FA on a field-deployed device. Additional certificates can be obtained from the Verifone CA anytime to implement new sponsor and signer relationships in deployment devices.

Figure 6 illustrates the certificate trees in development and deployment devices.

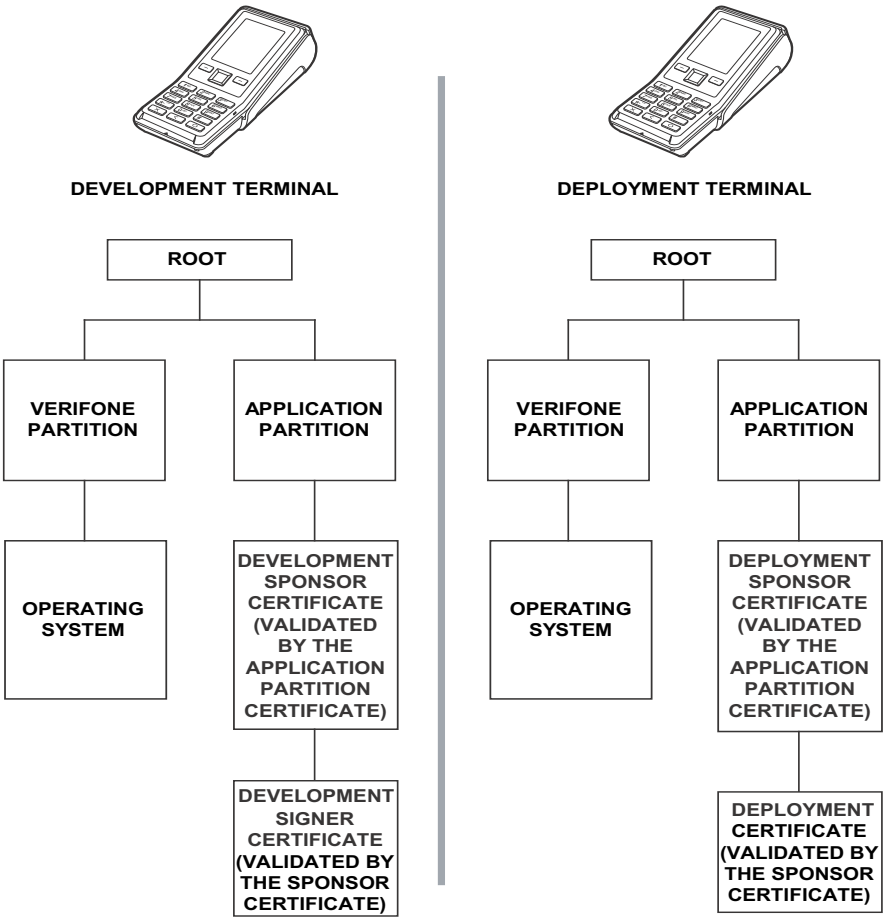


Figure 6 Certificate Trees in Development and Deployment Devices

Permanency of the Certificate Tree

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

Required Inputs to the File Signing Process

The required inputs to the file signing process are:

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

VeriShield File Signing Tool (FST)

The devices are shipped from manufacturer without a development certificate — a development certificate is not available for download.

For development, like for deployment, customers must obtain VeriShield signer cards and use the VeriShield File Signing Tool to sign all executable and other file to be logically protected.

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

Signing Files

To sign files:

1. Log on as Administrator. Launch The VeriShield File Signing tool. In the Windows Start menu, it is typically located under ***All Programs > Verifone > VeriShield > File Signing Tool***.
2. Log in. “Dual logon” is required to sign files.
3. Click “Sign File” and follow the wizard.
4. Click “Next” at the Welcome screen.
5. Select “Sign Files with new settings' and click Next at the settings selection screen.
6. Click “Add” and browse for the file(s) to be signed (DO NOT CHECK the “flash” box. It is for Verix terminals ONLY and may cause authentication failure on V200c terminals).
7. Click “Next” once all files to be signed have been added.
8. Select “Secured” and click “Next” at the security level screen (default is not supported on the V200c terminals).
9. Select the name and location to export the signer certificate file (the sponsor certificate is always exported as SponsorCert.crt in the same location).
10. Click “Sign File” at the “Summary of Settings” screen.
11. Enter first officer PIN.
12. Enter next officer PIN.
13. Click “Close” at the “results” screen.

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

Packaging Tool

Application files are downloaded as packages.

Downloading Application Files

To download a package or packages to the device, the following must be done:

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

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

CHAPTER 5

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 terminal.
- Prepare terminals for deployment.
- Maintain terminal installations in the field.
- Transfer data to/from terminals, terminals (Host), and PC.

In this chapter, information pertaining to file authentication is only discussed in the context of procedures while performing file downloads. See File Authentication for more information.

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

Downloads and Uploads

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

- Using NFS
- Using the ZonTalk Protocol via Serial connection
- Using the Netloader
- Using a local USB memory device / SD device

Refer to sample screen display in Table 4 (Home>Update) for more information.

Serial download can also be done without using an onboard application, please refer to Downloading without an Onboard Application for more infomation.

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

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

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

Download Methods and Procedures

The following methods are available for file and data downloads through the download and upload procedures.

Direct downloads

The usual download utility program is Direct Download (DDL) utility. It is normally available with the device's Developer's Toolkit (DTK), and can be obtained through Verifone. DDL is a subset program of the Verifone VeriTalk download application. It is designed specifically for a direct (RS-232/USB) download from a PC to a device (versus the VeriTalk modem based functionality). As the DDL utility sends files from the PC, the device display shows the progression of the download. The file name is shown on Line 1 of the display with nnn showing the number of blocks downloaded. Line 2 indicates the percent complete of the download where each asterisk represents 10%.

DDL Command Line Syntax

The format of the DDL program is:

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

Features	Description
`-b<baud>`	Specifies the baud rate, for example, • -b300 • -b1200 • -b2400 • -b4800 • -b9600 • -b19200 (default) • -b38400 • -b115200
`-p<port>`	Specifies the PC serial port: • 1 (COM1). The default is -p1 (COM1) • 2 (COM2)
`-i<filename>`	Specifies the name of a binary file to include in the download, for example: `-IBINARY.DAT`.
`-c<delta time>`	Sets the date and time on the terminal to the host PCs date and time. Also, specifies a delta value to add or subtract from the hour, for example, -c+1 specifies the PC's time plus one hour. **Note:** The maximum hour value that can be set is ± 23 hours.
`-X<password>`	Sets the terminal's password.
`-F<filename>`	Processes the contents of the specified file as command line data.

Features	Description
`file 1 [file2...]`	Specifies one or more files to download. Files with the .OUT extension are treated as binary data; all others are assumed text files.
`[config-data]`	Specifies terminal or application environment variables. If the specified variable exists, it is replaced by the new value; otherwise, a new entry is created. For example, the string `*ZR=TERMID` sets the value of the terminal identifier variable to "`TERMID`". **Note:** To remove an existing entry, use an empty string. For example, `*ZT=` " " removes the `*ZT` variable.

DDL Command Line File

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

DDL Example

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

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

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

```
-p2 app.tgz
```

The command line would be:

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

Downloading without an Onboard Application

Use the following procedure to perform a download from a host PC to V200c terminal with no application installed. The terminal must be powered on to begin the procedure.

1. Make all cable connections.
2. Launch the DDL application on the host PC.
3. Enter System mode using a secure password.
4. Select **Update** panel on the main System mode menu.
5. Select **Serial** panel tab to perform direct download to the terminal.
6. Select the COM Port (COM1).
7. Select Baud Rate to start download process.

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

Network Download Utility

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

File Signing and Signature Files

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

System Messages

This appendix describes error and information messages, which are grouped into two categories. 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 terminal is in System Mode. Use the Navigation Keys when selecting menus and specific options.

Table 6 Error Messages

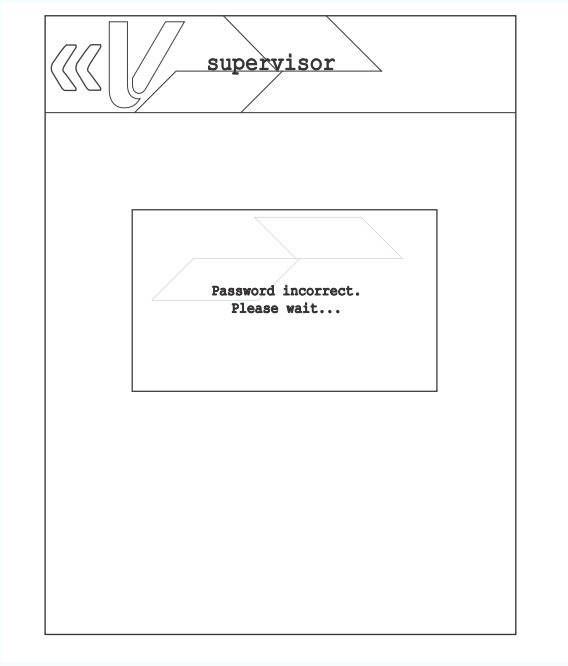
Display	Action
PASSWORD ERRORS	
	Password entered is incorrect. Wait until the login screen is up again and re-enter the password.

Table 6 Error Messages

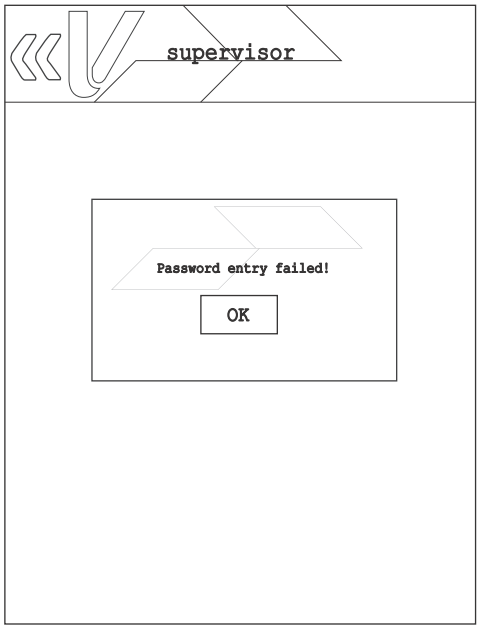
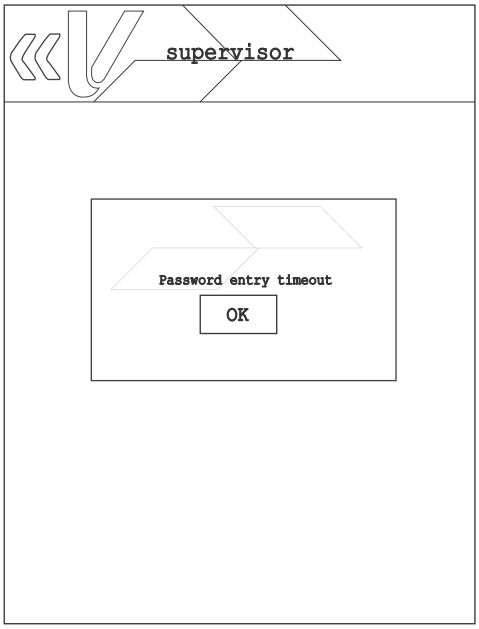
Display	Action
	This error is displayed when entered password does not meet the required number of characters or when the entered password exceeded the number of characters set for the user. Password must be at least seven characters.
	This error appears when the user failed to enter his password within 60 seconds or within the set timeout period. Select **OK** and enter the user password again.

Table 6 Error Messages

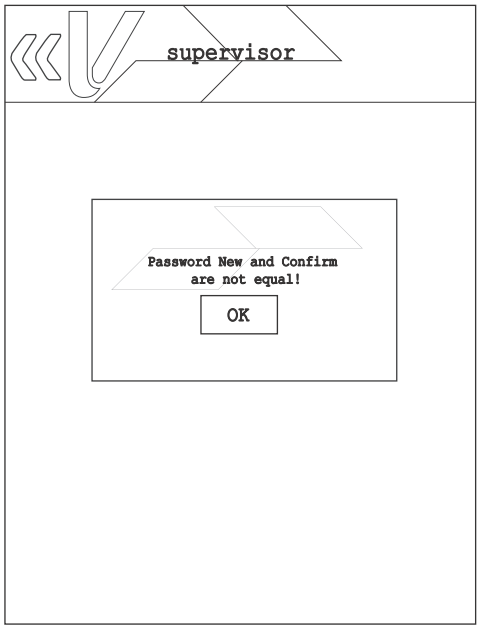
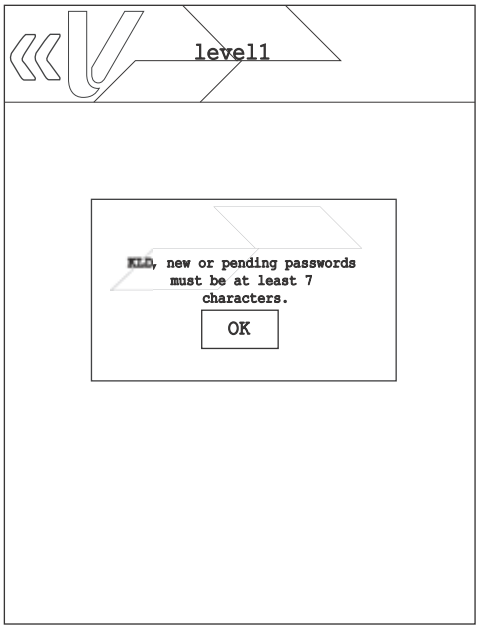
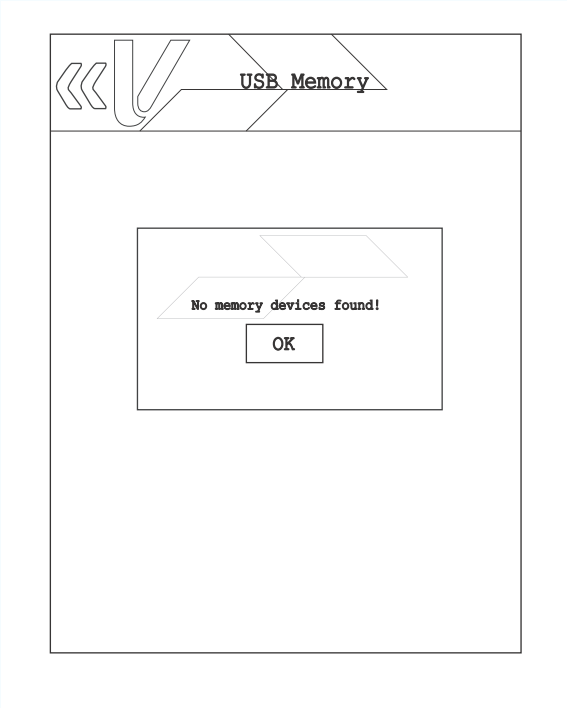
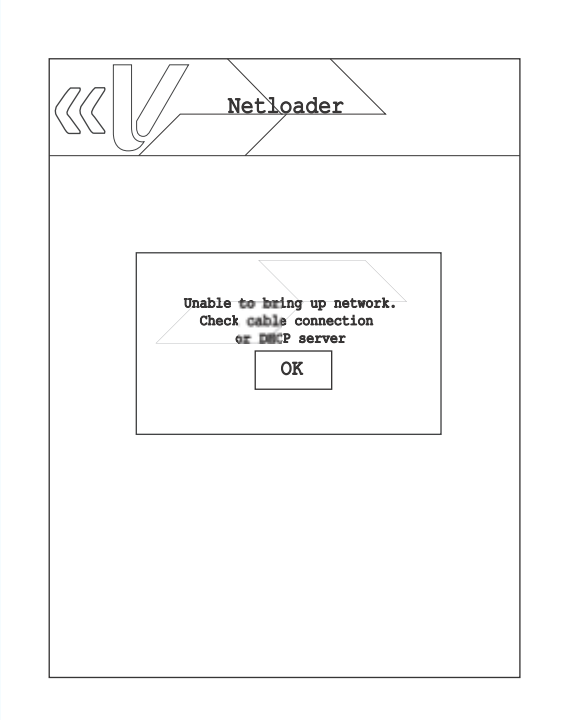
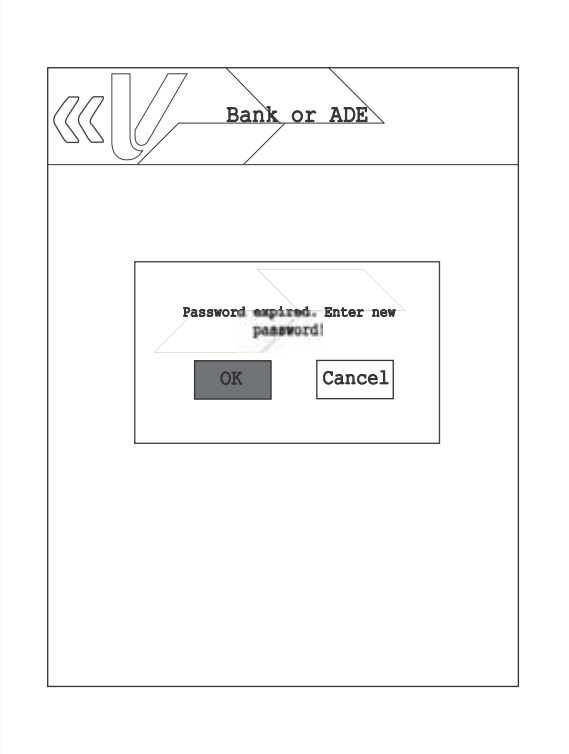
Display	Action
	This error appears when New and Confirm passwords entered do not match. Select **OK** and re-enter your desired user password.
	This error is displayed when the password entered by user did not meet the password requirements. KLD, new, or pending passwords must be at least seven characters. Select **OK** and re-enter password.

Table 6 Error Messages

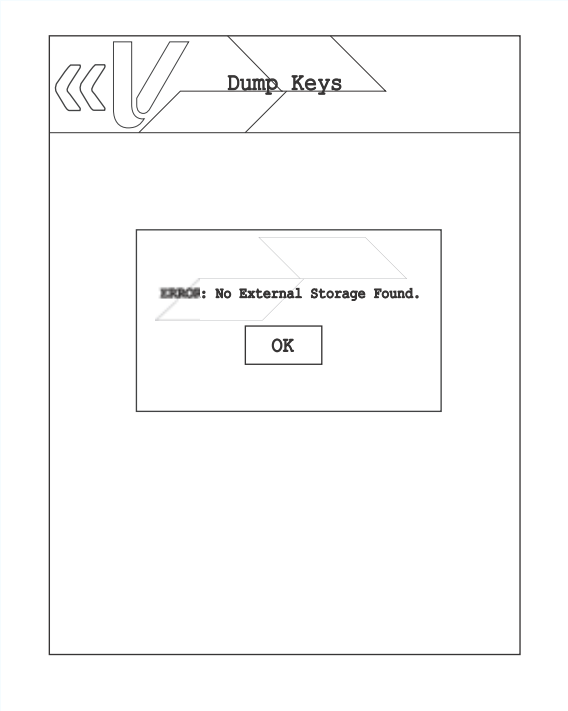
Display	Action
DOWNLOADING ERRORS	
	This error message is displayed when System Mode is unable to detect the USB Memory or SD card. Select **OK** to close the error message. Connect the USB Memory or SD card and try the download/update option again.
	This message is displayed once Netloader is selected and System mode is unable to detect connection to the server. Select **OK** to close the error message, check cable and network connection, then try selecting Netloader again.

SECURITY ERRORS



Key Loading Bank or ADE or VRK error displayed when key loading password has expired.

Select **OK** to close the error message and enter new password.



Key Dump error is displayed when there is no external storage found.

Select **OK** to close the error message and ensure that the external storage is connected to the terminal.

Information Messages

The following information messages may appear when the terminal is in System Mode.

Table 7 Information Messages

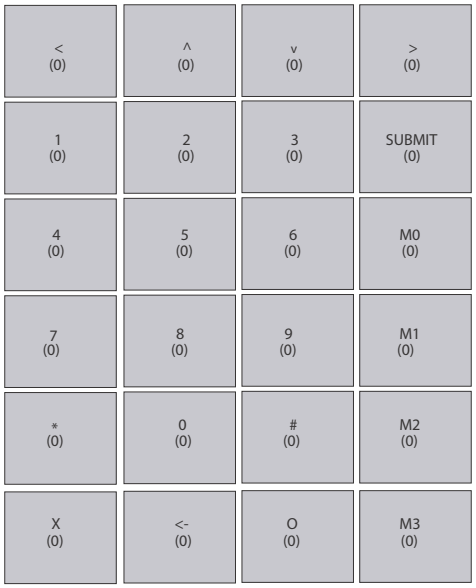
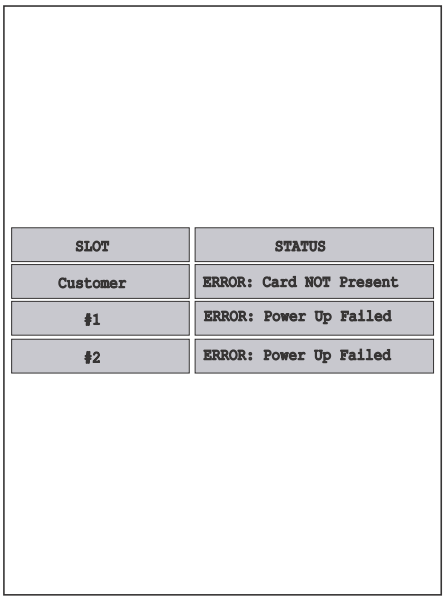
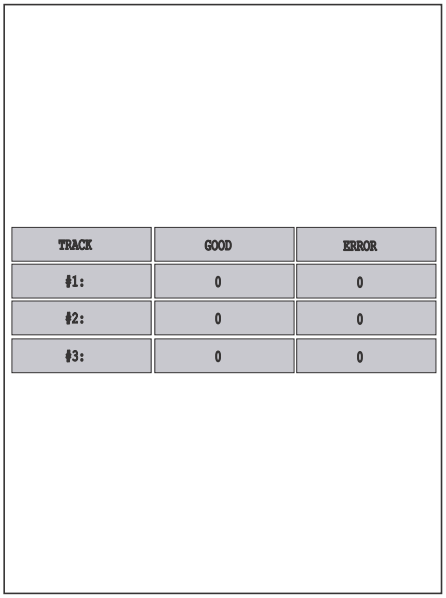
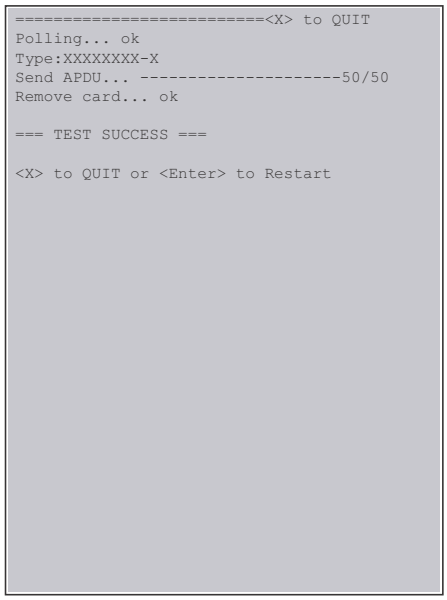
Display	Action
KEYPAD DIAGNOSTICS INFORMATION	
	This screen displays the number of times a key is pressed during a keyboard diagnostics session.
SMART CARD DIAGNOSTICS INFORMATION	
	This screen displays the status of the Smart Card Reader (with no cards inserted).

Table 7 Information Messages (continued)

Display	Action
MAGNETIC CARD DIAGNOSTICS INFORMATION	
	A successful test increments the current value in **GOOD** for each track that reads valid data. For more information about magnetic card error messages, refer to the *VOS Operating System Programmers Manual* -VPN DOC00501.
Contactless DIAGNOSTICS INFORMATION	
	Sample screen display for contactless card.

TRACK	GOOD	ERROR
#1:	0	0
#2:	0	0
#3:	0	0

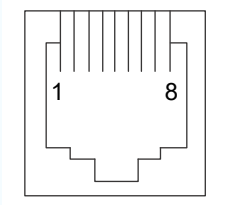
```
==========================<X> to QUIT
Polling... ok
Type:XXXXXXXX-X
Send APDU... ----------------------50/50
Remove card... ok

=== TEST SUCCESS ===

<X> to QUIT or <Enter> to Restart
```

Port Pinouts

V200c Port Pinout Definitions

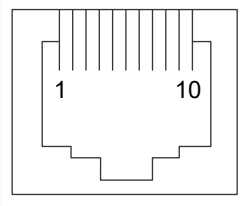
This section contains port pinout tables for the V200c.

Ethernet Port (LAN)



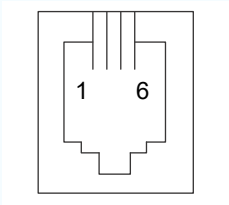
Connector	PIN	Function	Description
	1	TXD+	Transmit data +
	2	TXD-	Transmit data -
	3	RXD+	Receive data +
	4	NC	No connection
	5	NC	No connection
	6	RXD-	Receive data -
	7	NC	No connection
	8	NC	No connection

MOD 10 Port (COM1)



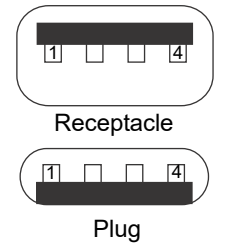
Connector	PIN	Function	Description
	1	VUSB	5 V USB power (500 mA)
	2	PORTPWR	Port power (11.6 V typ., 500 mA)
	3	NC	No connection
	4	NC	No connection
	5	GND	Power ground
	6	RXD	Receive data
	7	TXD	Transmit data
	8	NC	No connection
	9	USB0_DP	USB signal +
	10	USB0_DM	USB signal -

Telco Port



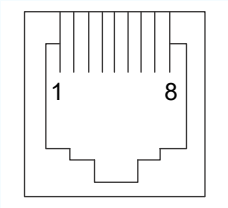
Connector	PIN	Function	Description
	1	NC	No connection
	2	NC	No connection
	3	Tip	Telephone Line
	4	Ring	Telephone Line
	5	NC	No connection
	6	NC	No connection

USB Pinout (Host Port)



Connector	PIN	Function	Description
	1	+5 V	5 V USB Power (600 mA)
	2	DATA-	USB Host Signal -
	3	DATA+	USB Host Signal +
	4	GND	USB ID pin/Ground

RS-232 Port (COM1)

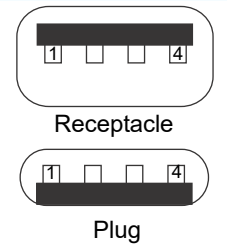


Connector	PIN	Function	Description
	1	Portpwr (9 to12 V DC)	Port power (11.6 V typ., 500 mA)
	2	NC	No connection
	3	NC	No connection
	4	GND	Power ground
	5	RXD	Receive data
	6	TXD	Transmit data
	7	NC	No connection
	8	NC	No connection

NOTE

This RS-232 port is part of the MOD10 cables (VPN CBL420-002-01-A and CBL420-002-02-A).

USB Pinout

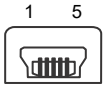


Connector	PIN	Function	Description
	1	+5 V	5 V USB Power (500 mA)
	2	DATA-	USB Host Signal -
	3	DATA+	USB Host Signal +
	4	GND	USB ID pin/Ground

NOTE

This USB Type-A port is part of the MOD10 cable (VPN CBL420-002-01-A).

USB Mini-B Pinout

Connector	PIN	Function	Description
 Receptacle  Plug	1	5 V 0	5 V USB Power
	2	DATA-	USB Device Signal -
	3	DATA+	USB Device Signal +
	4		
	5	GND	USB Ground

NOTE

This USB Mini-B port is part of the MOD10 cable (VPN CBL420-002-02-A).

ASCII Table

The ASCII Table

An ASCII table for the V200c display is presented in Table 8.

Table 8 V200c 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

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

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. ASCII codes are widely used for information interchange in data processing and communication systems.

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.

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

Calendar/clock chip A real-time clock inside the 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 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.

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.

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.

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 memory.

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 terminal is used to enter data and perform operations.

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 terminal, such as a magnetic stripe card reader.

Modem *Modulator/demodulator*. A terminal 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 terminal modem dongle allows communication with a host computer over a dial-up telephone line.

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.

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

RS-232 Also RS-232C. 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.

Serial port A connection point through which digital information is transferred one digital bit at a time. Same as *serial interface*. The terminal has one serial port, available at the multiport connector. The main serial port on a download computer is usually assigned the terminal ID, COM1.

Swipe The action of sliding a magnetic stripe card through a terminal card reader. The 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.

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 terminal, such as the one that is integrated in the terminal.

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.

Volatile memory A type of memory where the contents are destroyed if the power supply to the memory is interrupted. In the terminal applications run from volatile memory, mDRAM. Compare with POS terminal.

Verifone®

Verifone, Inc.
1-800-VERIFONE
www.verifone.com

V200c

Reference Guide

Verifone Part Number DOC420-004-EN-B, Revision B