



## Using the Terminal Keys

Before proceeding to other tasks, familiarize yourself with the operational features of the Omni 3600 terminal keypad to enter data (see [Figure 29](#)). This chapter describes how to use the keypad, including discussions on:

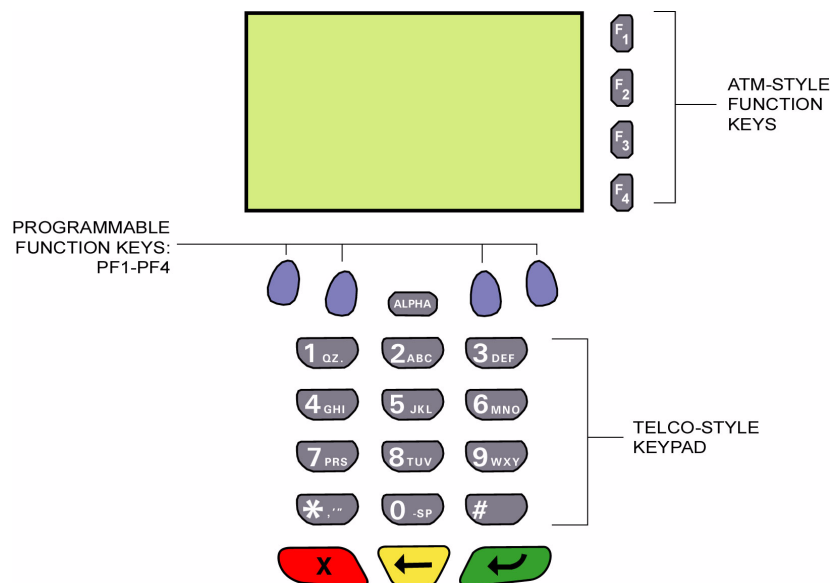
- the 12-key Telco-style keypad,
- the three color-coded keys below the keypad,
- the ALPHA key above the keypad,
- the four ATM-style function keys (F1, F2, F3, and F4) to the right of the display ([Figure 29](#)), and
- the four *programmable* function (PF) keys directly above the keypad.

Using these keys you can perform all data-entry tasks described in this manual. Where a specific key is mentioned, it appears within square brackets (for example, the ALPHA key).

The function keys allow you to navigate through system mode menus and select specific operations.



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



**Figure 29** Front Panel Key Arrangement

## Data Entry Modes

Before you can use the keys on the front panel to enter ASCII characters, the Omni 3600 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.
- **System mode:** 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.

---

### NOTE



If you enter system mode while a terminal application is running in normal mode, system mode preempts the application and takes control of the display and keyboard. The preempted application continues to run in the background, but does not accept user input. The only way to exit system mode is to restart the terminal. For this reason, once you enter system mode, you cannot return to the application in the same session.

If you turn on an Omni 3600 terminal that does not have an application stored in SRAM, the system prompt `DOWNLOAD NEEDED` appears. You can enter system mode by simultaneously pressing F2 and F4, and then entering the password. Once in system mode, you can configure the terminal as required and perform the necessary download.

If you turn on an Omni 3600 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 programmable function (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 system mode may have been changed. If so, you must press a special key combination and then type in the required system password to enter system mode. The behavior of key entries depends on the specific active system mode menu.

---

## The Keypad

The keypad is a 13-key arrangement, consisting of a 12-key Telco-style keypad and the ALPHA key (Figure 29).

---

### NOTE



The system mode functions described in the next section require that you 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 16 special characters: (\*), (,), ('), ("), (-), (.), (#), (%), (:), (!), (+), (@), (=), (&), (space), and (/).

## Function Key Descriptions

The terminal's operating mode and context determine the specific action performed when you press one of the following 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—usually has the same effect as pressing the Esc (escape) key on a PC. That is, it 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.



### 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 on a line.

In system mode, the specific effect of pressing backspace depends on the currently active system mode 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. Use the ALPHA to enter up to 50 different ASCII characters through the following procedure:

- 1 Press the key on the 12-key keypad that shows the letter or symbol you want (for example, use 2 to type 2, A, B, or C). The number (1–9 or 0) or the symbol (\* or #) you pressed now displays.
- 2 Press ALPHA once to display the first letter. Continuing our example, 2 ALPHA displays the letter A.
- 3 Continue pressing 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, you cycle back to the number 2.

---

#### 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, "222222..." displays

---

If two or more characters display on the Omni 3600 screen, pressing ALPHA changes the last character on the line to the next letter, number, or symbol in the key sequence. For example:

Current display: A5C*2	
ALPHA	A5C*A
ALPHA	A5C*B
ALPHA	A5C*C
ALPHA	A5C*2

Table 2 provides additional examples of how to use the ALPHA key to select ASCII characters from the 12-key Telco-style keypad.

**Table 2 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 3 lists all the ASCII characters you can type using the ALPHA key and the Telco keypad.

**Table 3 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]	+
* , ' "	*	,	'	"
# <sup>a</sup>	#	!	:	@

a. The # key also supports four 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.



In system mode, use ALPHA to key in the default system password, to enter a new system password, and for entering alpha characters.



### 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 system mode, press the enter key to begin a selected procedure, step forwards or backwards in a procedure, and confirm data entries. The specific effect of the enter key depends on the currently active system mode menu.

## Programmable Function (PF) Key Descriptions

The row of four PF keys directly above the keypad (Figure 29) 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.

The PF keys are also used to toggle through system mode menus. These keys are functioning when arrows appear in the display screen above the associated key, indicating the key's can be used as follows:

- PF1    ↑      Move to the previous menu or screen
- PF2    ↓      Move to the next menu or screen
- PF3    ←      Scroll left
- PF4    →      Scroll right





# System Mode

This chapter describes a category of terminal functions called *system mode operations*, including discussions on:

- system mode entry,
- initiating local and remote operations,
- passwords,
- file groups, and
- system mode menus.

System mode is used exclusively by those responsible for configuring, deploying, and managing Omni 3600 terminal installations in the field.

## When to Use System Mode

Use system mode functions to perform different subsets of related tasks:

- **Application programmers:** To configure a development terminal, download versions of the Omni 3600 application program you are developing, and test and debug the application until validated and ready to download to other terminals.
- **Deployers of Omni 3600 terminals to end-user sites:** To perform the specific tasks required to deploy a new Omni 3600 terminal in the field, including configuring the terminal, downloading application software, and testing the terminal prior to deployment.
- **Terminal administrators or site managers:** To 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 your job, select the appropriate system mode menu(s) and execute the corresponding procedure(s).

## Local and Remote Operations

The system mode operations available on an Omni 3600 terminal can be divided into the following two categories or types:

- **Local operations:** Address a standalone terminal and do not require communication or data transfers between the terminal and another terminal or computer. Perform local system mode operations to configure, test, and display information about the terminal.
- **Remote operations:** Require communication between the terminal 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, and perform diagnostics over a telephone line.

This chapter contains descriptions on how to perform local system mode operations. For information performing remote operations, such as downloads, refer to [Chapter 4](#).

## Verifying Terminal Status

The Omni 3600 terminal you are working with may or may not have an application program running on it. After you have set up the terminal ([Chapter 1](#)) 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. From this point, press F2 and F4 to enter system mode and perform the required download.
- If an application program is loaded into terminal RAM or flash, an application-specific application prompt appears. The application is running and the terminal is in normal mode. If all installation steps are complete, the terminal can process transactions.

## Entering System Mode

To prevent the unauthorized use of system mode menus, the Omni 3600 terminal firmware requires a system password each time you enter system mode. The default, factory set system password is “Z66831.” Use the following key sequence to enter this password:

1 ALPHA ALPHA 6 6 8 3 1 [↵]

After entering the correct password, the terminal enters system mode and displays the first system mode main menu, SYS MODE MENU 1. You can now toggle through all seven system mode main menus.

### NOTE



It is recommended to enter system mode only on system startup or terminal restart.

If you enter system mode while an application is running, system mode suspends the application and takes control of the display and keyboard. The application idles in the background, but no longer accepts user inputs. You cannot return to the application during that session, only after a restart. In addition, an application running in the background may deny access to certain system mode functions.

## File Groups

The Omni 3600 operating system implements a file system in volatile, battery-backed RAM and non-volatile flash memory. Files are assigned to one of 15 groups for access control. Groups are similar to directories on a computer 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 Omni 3600 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 through 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 through 15 are empty until they are filled through a download to the Omni 3600 terminal.

For more information on managing file groups, refer to the *Verix Programmer's Manual* (VeriFone P/N 19733).

## Passwords



**CAUTION** If you change a password and then forget it, there is no password recovery method. 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 terminal can, however, continue to process transactions in normal mode.

If you forget or lose the system password to your terminal, please contact your local VeriFone representative for assistance.

### System Password

In SYS MODE MENU 3, you can select a procedure to change the default password to a unique and more secure password. Once you set a new system password, be sure to secure a copy of the new password.

A valid system password may consist of one to ten alphanumeric characters. You can change the system password at any time, provided you know what the current password is.

When you key in the system password to enter system mode, an asterisk (\*) appears on the display 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

From manufacture, each file group uses the default password "Z66831," entered as:

1 ALPHA ALPHA 6 6 8 3 1, and press [↵]



This default password is the same as the password for system mode entry, which is set in the CONFIG.SYS entry \*SMPW.

## System Mode Menus

The seven main system mode menus are listed in [Table 4](#).

**Table 4 System Mode Menus**

SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑ ↓
SYS MODE MENU 3 CONFIG INFO F2 EDIT F3 PASSWORDS F4 ↑ ↓	SYS MODE MENU 4 REMOTE DIAGS F2 ERROR LOG F3 DEBUGGER F4 ↑ ↓
SYS MODE MENU 5 SCREEN DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4 ↑ ↓	SYS MODE MENU 6 IPP DIAG F2 IPP KEYLOAD F3 PRINTER DIAG F4 ↑ ↓
SYS MODE MENU 7 BATTERY STATUS F2 ↑	

On successful entry of the system password, SYS MODE MENU 1 appears.

To return to a previous menu, press the PF1 key (below the up arrow). To go to the next menu, press the PF2 key (below the down arrow). To return to the main system mode menu and cancel any changes, press the cancel key.

Each menu has items to select; sometimes these items contain submenus or a series of prompts. When prompted to enter alphabetic or special characters, use the procedure described in [Chapter 2](#).

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.

## System Mode Procedures

The procedures in this section explain how to use each of the system mode menus listed in [Table 4](#). 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 When a main system mode menu appears, select an operation by pressing the appropriate key.
- 2 Complete the operation.
- 3 Return to the main system mode menu.

**NOTE**



Before entering system mode and selecting the function(s) to perform, please verify that you have completely installed the Omni 3600 as described in [Chapter 1](#), that the terminal is connected to a power source, and that the terminal is turned on.

Procedure descriptions are arranged in the following tabular format:

Display	Action
Submenu	

The *Display* column indicates what appears on the terminal display 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 font and in 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, (Application Prompt), in which the normal font is used, and text is typed in initial caps.

The *Action* column provides a procedure 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 procedure evoked from a main menu screen. A description of that procedure immediately follows the Submenu row. The following keys have the same function from all submenus:



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



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

**Enter and Exit System Mode**

To enter system mode after you have turned on the Omni 3600 terminal, follow the procedure described in [Table 5](#).



**NOTE** On successful completion, some operations automatically exit system mode and restart the terminal. Other operations require that you exit system mode and restart the terminal. To manually exit system mode, select RESTART F4 in SYS MODE MENU 1.

**Table 5 Enter System Mode**

Display	Action
<p>VERIFONE OMNI 3600<sup>a</sup> Q80000XX 4/10/01 VERIX</p> <p>COPYRIGHT (C) 1997-2003 VERIFONE, INC. ALL RIGHTS RESERVED Battery 95%</p>	<p>At startup, the terminal displays a copyright notice screen that shows the terminal model number, the version of the Omni 3600 system firmware stored in the terminal's flash memory, the date the firmware was loaded into the terminal, the copyright notice, and battery charge remaining.</p> <p>This screen appears for three seconds, during which time you can enter system mode by simultaneously pressing F2 and F4.</p> <p>You can extend the display period of this screen by pressing any key during the initial three seconds. Each key press extends the display period an additional three seconds.</p>
<p>(Application Prompt) or DOWNLOAD NEEDED</p>	<p>If an application already resides on the terminal, an application-specific prompt displays. If no application resides on the terminal, the following message displays:</p> <p>DOWNLOAD NEEDED</p> <p>To enter system mode from this screen, simultaneously press F2 and F4.</p>

**Table 5** Enter System Mode (continued)

Display	Action
SYSTEM MODE ENTRY PASSWORD -----	<p>If an application prompt appeared in Step 2 and you chose to enter system mode you are prompted to type the system password.</p> <p>If DOWNLOAD NEEDED appeared in Step 2, use the default password "Z66831." This password is entered as:</p> <p>1 ALPHA ALPHA 6 6 8 3 1, and press [↵]</p> <p>Use the backspace [←] key to delete the entry and correct any mistakes. If you enter an incorrect password, the terminal exits the SYSTEM MODE ENTRY screen. Verify your password and re-enter it.</p> <p>To quit this operation and return to the application prompt or DOWNLOAD NEEDED screen, press the cancel key.</p>
SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	<p>SYS MODE MENU 1 is the first menu to display. To toggle through to the other six menus, press the PF2 key or [↵] until you reach the desired menu.</p>

a. May have the letter G for GSM radio, P for GPRS radio, or C for CDMA radio.

## System Mode Menu 1

In this menu you can adjust the display contrast, set the terminal clock, and exit system mode.

**Table 6** System Mode Menu 1

Display	Action
SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	<p>To adjust the display contrast, select CONTRAST F2. To set the date and time, select CLOCK F3.</p> <p>To restart the terminal, select RESTART F4.</p> <p>To toggle to system mode menu 2, press PF2 or [↵].</p>
CONTRAST F2	
SYS MODE CONTRAST CONTRAST UP F2 CONTRAST DOWN F3 ↑	<p>Select CONTRAST UP F2 to increase display contrast or CONTRAST DOWN F3 to decrease display contrast. To return to the main menu and save your changes, press [↵].</p>

**Table 6** System Mode Menu 1 (continued)

Display	Action
<b>CLOCK F3</b>	
<p><b>Note:</b> The terminal clock is battery-backed to retain date and time settings when the terminal is shut off.</p>	
<pre> SYS MODE CLOCK                 YEAR: 2003                 MONTH: 02                 DAY: 22                 ↑   ↓           </pre>	<p>This example shows February 22, 2001.</p> <p>To set YEAR, press F2 and type a four-digit number for the current year. To set MONTH, press F3 and type a two-digit number for the current month (between 01–12). To set DAY, press F4 and type a two-digit number for the current day (between 01–31).</p> <p>To save your changes and return to SYS MODE MENU 1, press the PF1 key. To set the time, go to</p> <p><b>Note:</b> The terminal only accepts entries in the format and range specified above. Errors are not highlighted; <i>you must ensure each entry is correct</i>. To correct a mistake, press the field's function key (for example, F2 for YEAR) and type a new entry.</p>
<pre> SYS MODE CLOCK                 HOUR: 17                 MINUTE: 32                 ↑           </pre>	<p>This example shows 5:32 P.M.</p> <p>To set HOUR, press F2 and type a two-digit number between 00–23 (using the twenty-four hour clock). To set MINUTE, press F3 and type a two-digit number between 01–59.</p> <p><b>Note:</b> The terminal only accepts entries in the format and range specified above. Errors are not highlighted; therefore, <i>you must ensure each entry is correct</i>. To correct a mistake, press the field's function key (for example, F2 for HOUR) and type a new entry.</p> <p>To return to the previous menu to set the date, press the PF1 key. To save your changes and return to SYS MODE MENU 1, press enter.</p>
<pre> RESTART F4           </pre>	<p>Select RESTART F4 to exit system mode and restart the terminal.</p>

## System Mode Menu 2

In this menu, you can accomplish full or partial downloads to your terminal, clear RAM files, and clear flash files.



### NOTE

Before performing a download to flash memory in an initialized terminal (one that contains an application), reclaim all available flash space. Unlike RAM, unused flash and duplicate flash information are not automatically reclaimed during a download. To reclaim this space perform a defrag operation from system mode (refer to the procedure [FLASH FILES F4](#), in [Table 7](#)). This operation makes all files in flash contiguous. You must also clear some or all flash memory if your terminal does not have enough space for the impending download.

You cannot perform download, clear, and defragment operations if you entered system mode while an application is running. If you see the message APPLICATION ALREADY RUNNING, PLEASE RESTART, press the cancel key and restart the terminal from system mode menu 1. When you see the copyright notice screen, enter system mode within 3 seconds (before the application begins).

**Table 7 System Mode Menu 2**

Display	Action
SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑          ↓	<p>To download an application to your terminal, select DOWNLOAD F2. To clear RAM files, select RAM FILES F3. To clear flash files, select FLASH FILES F4.</p> <p>To return to the previous system mode menu, press the PF1 key.</p> <p>To return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.</p> <p>To toggle to SYS MODE MENU 3, press the PF2 key or [↵].</p>
<b>DOWNLOAD F2</b>	
SYS MODE FILE FILE GROUP _1	<p>Type the number of the file group (1 for the primary application; between 1–15 for other applications) to perform the download. (Refer to <a href="#">Chapter 4</a> for detailed download instructions and information.)</p> <p>After you type a file group number, press [↵].</p>
SYSTEM MODE FILE GROUP NN PASSWORD -----	<p>To continue, enter the required password. If you enter an incorrect password, the following message appears:</p> <p>SYS MODE PASSWORD PLEASE TRY AGAIN</p> <p>Press [↵]. Verify your password and re-enter it.</p>
SYS MODE DOWNLOAD FULL F3 PARTIAL F4 ↑	<p>For a full download, select FULL F3. For a partial download, select PARTIAL F4. (Refer to <a href="#">Chapter 4</a> for detailed download instructions and information.)</p> <p>To return to the main menu, press the PF1 key.</p>
SYS MODE DOWNLOAD MODEM F2 COM1 F3 WIRELESS F4 ↑          ↓	<p>Select a download mode: MODEM F2, COM1 F3, or WIRELESS F4.</p> <p>To return to the main menu without saving your selection, press the cancel key.</p>
SYS MODE DOWNLOAD ***----- DOWNLOADING NOW	<p>The terminal is ready to receive a download. During the download, a line of asterisks appears that shows percentage of completion. Each asterisk equals approximately 10% of the download.</p> <p>You can cancel a download by pressing the cancel key during the download; doing so restarts your terminal.</p>

Table 7 System Mode Menu 2 (continued)

Display	Action
<b>RAM FILES F3</b>	
SYS MODE RAM CLEAR GROUP _1 F2 CLEAR ALL FILES F3	<p>To clear a file group's RAM files, type the file group number (1–15) and press F2. To correct a mistake, press [←] to delete the number, and type a new entry. CONFIG.SYS protected records that begin with * or # are retained when you clear a RAM file group.</p> <p>To clear the RAM of all file groups, select CLEAR ALL FILES F3. This operation also clears the CONFIG.SYS files from all groups except Group 1. Records that begin with * or # in Group 1 are retained.</p> <p><b>Note:</b> If you have not previously entered a group's password in this session, the terminal prompts for the group's password prior to clearing that group's RAM files.</p>
SYSTEM MODE FILE GROUP NN PASSWORD -----	<p>To continue, enter the required password. If you enter an incorrect password, the following message appears:</p> <p>SYS MODE PASSWORD PLEASE TRY AGAIN</p> <p>Press [↵]. Verify your password and re-enter it.</p>
SYS MODE CONFIRM CANCEL F3 CONFIRM F4	<p>To cancel the operation, select CANCEL F3.</p> <p>To continue the operation, select CONFIRM F4. After the operation is complete, you return to the main menu.</p>
<b>FLASH FILES F4</b>	
SYS MODE FLASH CLEAR GROUP _1 F2 CLEAR ALL FILES F3 DEFRAG 0 F4	<p>To clear a file group's flash files, type the file group number (1–15) and press F2. To correct a mistake, press [←] to delete the number, and type a new entry.</p> <p>To clear the flash files of all file groups, press F3. If you have not previously entered a group's password in this session, the terminal prompts you for the group's password prior to clearing that group's flash files.</p> <p><b>CAUTION!</b> Clearing all flash files erases the application program from your terminal. A new application download is then required.</p> <p>To defragment flash files, press F4, then skip to SYS MODE CONFIRM of this procedure.</p> <p>The number displayed beside DEFRAG is the total amount of space, in bytes, to reclaim in the defrag operation.</p>



**Table 7 System Mode Menu 2 (continued)**

Display	Action
SYSTEM MODE FILE GROUP NN PASSWORD -----	To continue, enter the required password. If you enter an incorrect password, the following message appears: SYS MODE PASSWORD PLEASE TRY AGAIN Press [↵]. Verify your password and re-enter it.
SYS MODE CONFIRM  CANCEL F3 CONFIRM F4	To cancel the operation, select CANCEL F3. To continue the operation, select CONFIRM F4. After the operation is completed, you are returned to the main SYS MODE MENU 2 screen.  If you selected DEFRAG in SYS MODE FLASH and select CONFIRM F4 here, you are taken to SYS MODE DEFRAG.
SYS MODE CLEAR CLEARING FLASH PLEASE WAIT	This operation may take a few seconds. If you have cleared all flash files, the terminal displays DOWNLOAD NEEDED on restart.  If after clearing selected flash files you experience difficulties with your application, you may have accidentally deleted a flash file that the CONFIG.SYS file in File Group 1 uses. This type of error usually generates the error message RUN FAILED when trying to execute the application; you must restore the required File Group 1 flash file.
SYS MODE DEFRAG RECLAIMING FLASH PLEASE WAIT	This message indicates the flash files are being defragmented; this operation may take a few seconds.  On successful completion, the terminal automatically restarts.

**System Mode Menu 3**

In this menu, you can view terminal configuration information, edit the CONFIG.SYS or another keyed file, and change system mode and file group passwords.



Some application program downloads automatically reset the system password.

**Table 8 System Mode Menu 3**

Display	Action
<pre> SYS MODE MENU 3           CONFIG INFO F2           EDIT F3           PASSWORDS F4           ↑   ↓ </pre>	<p>To view terminal configuration information, select CONFIG INFO F2. To edit the CONFIG.SYS or another keyed file, or to set the country code for your terminal's modem, select EDIT F3. (For more information, refer to the <a href="#">Edit Keyed Files</a> section that follows this main menu description.)</p> <p>To change the system mode and file group passwords, select PASSWORDS F4. The file groups and system mode all use a default password that is pre-set at the factory: Z66831. It is entered as: 1 ALPHA ALPHA 6 6 8 3 1 and press [↵].</p> <p>To return to the previous system mode menu, press the PF1 key.</p> <p>To return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.</p> <p>To toggle to the system mode menu 4, press the PF2 key or [↵].</p>
<b>CONFIG INFO F2</b>	
<pre> SYS MODE CONF RAM FILES   3 INUSE      728 AVAIL      481056 FLASH FILES 0 INUSE       0 AVAIL      786424           ↓ </pre>	<p>This screen shows the number of kilobytes in use and that available for RAM and flash.</p> <p>To continue, press the PF2 key.</p>
<pre> SYS MODE CONF RAM        512 FLASH     1024 SERNO     K2-0001 PTID      12000000 PART      P096-100-02 VERS      A           ↑   ↓ </pre>	<p>This screen shows configuration information specific to your terminal:</p> <ul style="list-style-type: none"> <li>• Total kilobytes of RAM memory</li> <li>• Total kilobytes of flash memory</li> <li>• Serial number</li> <li>• Permanent terminal identification number (PTID)</li> <li>• Terminal part number</li> <li>• Terminal hardware version number</li> </ul> <p>Your terminal's screen may vary depending on your terminal's model and the operating system version installed.</p> <p>To return to the previous menu, press the PF1 key; to continue, press the PF2 key.</p>

**Table 8 System Mode Menu 3 (continued)**

Display	Action
<pre> SYS MODE CONF MODL      OMNI3600 CTRY      US KEYPAD    0 DISPLAY   128064 MAG RDR   0 PRINTER   1 ↑           </pre>	<p>This screen shows additional configuration information specific to your terminal:</p> <ul style="list-style-type: none"> <li>• Model number</li> <li>• Country of manufacture</li> <li>• Keypad type (0 = Telco, 1 = calculator, 2 = Singapore)</li> <li>• Display unit type</li> <li>• Magnetic stripe card reader type</li> <li>• Whether or not a thermal printer is integrated into the terminal (where 0 = No, 1 = Yes)</li> </ul> <p>To return to the previous menu, select the PF1 key; to continue, select the PF2 key.</p> <p>To return to the main menu, press the cancel key.</p>
<pre> SYS MODE CONF PINPAD    0 LIFE      73525 RSET 971117023334 RCNT      29 MODEM CTRY? ↑           </pre>	<p>This screen shows additional configuration information specific to your terminal:</p> <ul style="list-style-type: none"> <li>• Whether or not a PIN pad device is integrated into the terminal (where 0 = No, 1 = Yes)</li> <li>• Number of seconds the terminal has run (LIFE)</li> <li>• Last reset date and time, in YYMMDDHHMMSS format (where YY = year, MM = month, DD = day, HH = hour, MM = minute, and SS = second)</li> <li>• Number of times the terminal has been reset (RCNT)</li> <li>• Modem country code (not applicable on this model)</li> </ul> <p>To return to the previous menu, select the PF1 key; to return to the main menu, press the cancel key.</p>
<b>EDIT F3</b>	
<pre> SYS MODE FILE FILE GROUP _1           </pre>	<p>To search for keyed records in a particular file group, type the appropriate group number and press [↵].</p> <p>If you cannot locate a particular keyed record, it may be stored in another file group. To search for keyed records in another file group, return to the main menu by pressing the cancel key, then type the appropriate group number and press [↵].</p> <p>To correct a mistake, press [←] to delete the number, and type the new entry.</p>
<pre> SYSTEM MODE FILE GROUP NN PASSWORD -----           </pre>	<p>To continue, enter the required password. If you enter an incorrect password, the following message appears:</p> <pre> SYS MODE PASSWORD PLEASE TRY AGAIN           </pre> <p>Press [↵]. Verify your password and re-enter it.</p>

**Table 8** System Mode Menu 3 (continued)

Display	Action
<pre>SYS MODE EDIT FILE CONFIG.SYS_</pre>	<p>To edit the CONFIG.SYS file, press [↵].</p> <p><b>Note:</b> In this menu, you can create a new keyed file or edit an existing one. First, use [←] to clear any previous key name from the display. Then, type the key name, press [↵], and skip to the SYS MODE EDIT VALUE screen below.</p>
<pre>SYS MODE EDIT KEY (KEY NAME)----- -----</pre>	<p>To create or search for a keyed record, use [←] to clear any previous key name from the display. Then, type the key name, press [↵], and skip to Step 5b of this procedure.</p> <p>To scroll through the search keys, press [↵], or use the PF1 or PF2 keys to scroll the up and down respectively, as needed.</p> <p>To scroll through keyed records, press either the PF3 or the PF4 key, below the Left and Right arrows respectively, as needed.</p>
<pre>SYS MODE EDIT           (KEY NAME)  KEY F2           (KEY VALUE) VALUE F3 ↑   ↓   ←   →</pre>	<p>To scroll through the search keys, press [↵]. Or use the PF1 or PF2 keys to scroll the up and down respectively, as needed.</p> <p>To manually enter another key name, select KEY F2 and use [←] to clear the previous key name from the display. Then, type the appropriate key name and press [↵].</p> <p>To scroll through the displayed key value, press either the PF3 or the PF4 key, below the Left and Right arrows respectively, as needed.</p> <p>To edit a key value, select VALUE F3 and proceed to the next step.</p>
<pre>SYS MODE EDIT VALUE (Value)----- -----</pre>	<p>To create or edit a key value, use [←] to clear any previous key value from the display. Then, type the new key value and press [↵].</p>
<pre>SYS MODE EDIT (Key name)  KEY F2 (Key value)VALUE F3 ↑   ↓   ←   →</pre>	<p>To exit SYS MODE EDIT after completing your edit operations, press the cancel key twice.</p>

**Table 8 System Mode Menu 3 (continued)**

Display	Action
<b>PASSWORDS F4</b>	
SYS MODE PASSWORD FILE GROUP _1 F2 SYS MODE ENTRY F3	<p>To change the password of File Group 1, select FILE GROUP _1 F2. Then, go to SYSTEM MODE FILE GROUP NN PASSWORD below.</p> <p>To change the password of another file group, type the appropriate file group number and press F2. Then, go to SYSTEM MODE FILE GROUP NN PASSWORD below.</p> <p>To correct a mistake, press [←] to delete the number, and type the new entry.</p> <p>To change the system password, select SYS MODE ENTRY F3. Then, skip to SYS MODE PASSWORD NEW below.</p> <p><b>Note:</b> Some application program downloads automatically reset the system mode password.</p>
SYSTEM MODE FILE GROUP NN PASSWORD -----	<p>Type the current password for the selected file group and press [↵].</p> <p>If you enter an incorrect password, the following message appears:</p> <p>SYS MODE PASSWORD PLEASE TRY AGAIN</p> <p>Press [↵]. Verify your password and re-enter it.</p>
SYS MODE PASSWORD NEW-----	Type the new password and press [↵]. To correct a mistake, press [←] to delete the number, and then type the new entry.
SYS MODE PASSWORD AGAIN-----	The terminal requests that you verify the new password. Retype the new password and press [↵].
SYS MODE PASSWORD PASSWORD CHANGED	The new password is now in effect. To exit this screen, press [↵]. You are returned to the main menu.

**NOTE**



When entering any password, an asterisk (\*) appears on the display 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 ALPHA does not cause additional asterisks to appear. Secure a copy of every password to ensure it is not forgotten or lost.

**Edit Keyed Files**

A *keyed* file is a collection of individual records, which contain ASCII data and are identified by unique search keys. You can edit the ASCII data directly from the terminal keypad using the terminal's built-in keyed file editor. Each record has two parts: a key name and a key value. The search key is a variable-length string, or *key name*, that identifies the record. The information assigned to the search key is contained in a separate variable-length string, or *key value*.

For example, in CONFIG.SYS, the ZonTalk key for the application serial ID number is \*ZT. 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 [.] to scroll through the search keys instead of entering the characters \*ZT through the keypad.

**NOTE**



For a complete list of the ASCII characters supported by the Omni 3600, as well as their decimal and hexadecimal equivalents, please refer to [Appendix B](#).

**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 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 are all other CONFIG.SYS files, and records of other files. These records are deleted when RAM is cleared.

**Editing CONFIG.SYS with an External Editor**

You can create and edit the CONFIG.SYS files of Omni 3600 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 *ZonTalk 2000<sup>®</sup> Reference Manual*, the *Verix Programmer's Manual*, 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.

**System Mode  
Menu 4**

In this menu you can view the error log and perform application debugging operations.

**Table 9 System Mode Menu 4**

Display	Action
<pre> SYS MODE MENU 4       REMOTE DIAGS F2       ERROR LOG F3       DEBUGGER F4 ↑      ↓ </pre>	<p>REMOTE DIAGS: This function is reserved for future use with TMM.</p> <p>To return to the previous system mode menu, press the PF1 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key; to move to the next system mode menu, press the PF2 key or [-].</p>
<p><b>ERROR LOG F3</b></p>	
<pre> SYS MODE ERR LOG TYPE  0000 FRAME 00800698       008002BA       F1000002       00A00000 ↑      ↓ </pre>	<p>The error log screens display internal diagnostic information about the most recent unrecoverable software error. If you report a terminal problem, you may be asked to provide this information.</p> <p>This first screen displays the following: TYPE (Error Type) FRAME (Stack Frame)</p> <p>After making any notations, press the PF2 key to view additional error log information.</p>
<pre> SYS MODE ERR LOG USP   2491ED57 TCB   00000000 TIME  010329053144 ↑ </pre>	<p>This screen displays the following: USP (User Stack Pointer) TCB (Task Control Block) TIME (binary-coded, decimal system, clock time of the error in the format <i>yymmddhhmmss</i>, where <i>yy</i> = year, <i>mm</i> = month, <i>dd</i> = day, <i>hh</i> = hour, <i>mm</i> = minute, and <i>ss</i> = second)</p> <p>After taking desired notes, press the PF1 key to view the previous screen or press the cancel key to return to the main menu.</p> <p>DEBUGGER F4: This selection starts the application program's debug monitor, if installed, on the selected file group.</p> <p>The <i>Verix Operating System Programmer's Manual</i> fully documents debug operations. For more information on debugging your terminal, contact your terminal supplier.</p>

## System Mode Menu 5

In this menu you can test the display panel, keyboard, and magnetic stripe card reader.

**Table 10 System Mode Menu 5**

Display	Action
SYS MODE MENU 5 SCREEN DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4 ↑     ↓	<p>To test the display panel, select SCREEN DIAG F2. To test the keyboard, select KEYBOARD DIAG F3. To test the magnetic card reader, select MAG CARD DIAG F4.</p> <p>To return to the previous system mode menu, press the PF1 key; to toggle through to SYS MODE MENU 6, press the PF2 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.</p>
<b>SCREEN DIAG F2</b>	<p>When you select F2, you should see a completely dark screen. Press [↵] to completely clear the screen.</p> <p>To stop the test and return to the main menu, press the cancel key.</p>
<b>KEYBOARD DIAG F3</b>	
SYS MODE KBD TEST KEYCODE NN	<p>This screen displays the decimal ASCII keycode for each key you press. The value displayed corresponds to the actual key pressed. Other values assigned to keys (for example, "Q", "Z", and "." are assigned to [1]) are software dependent.</p> <p>To test the keyboard, press some keys and check that they match their ASCII keycodes (for example, [1] displays keycode 31). For more ASCII keycodes, refer to the ASCII table in <a href="#">Appendix B</a>.</p> <p>To stop the test and return to the main menu, press either the cancel key or [↵].</p>
<b>MAG CARD DIAG F4</b>	
SYS MODE TRK 1:VALID DATA TRK 2:VALID DATA TRK 3:VALID DATA	<p>To test the magnetic-stripe card reader, swipe a magnetic-stripe card through it.</p> <p>A successful test displays VALID DATA for each track that read valid data. An error generates one of the following error messages for each track with an error:</p> <p>NO DATA            NO START            NO END            LRC ERR            PARITY ERR            REVERSE END</p> <p>For more information about magnetic card error messages, refer to the <i>Verix Programmer's Manual</i>.</p> <p>To stop the test and return to the main menu, press the cancel key.</p>



## System Mode Menu 6

In this menu you can run integrated PIN pad (IPP) diagnostics, check the IPP key loading mode, display printer information, and run printer tests.

**Table 11 System Mode Menu 6**

Display	Action
<pre> SYS MODE MENU 6       IPP DIAG F2       IPP KEY LOAD F3       PRINTER DIAG F4 ↑      ↓           </pre>	<p>To test the IPP, select IPP DIAG F2. To test the IPP key load, select IPP KEY LOAD F3. To run printer diagnostics and test the printer, select PRINTER DIAG F4.</p> <p>To return to the previous system mode menu, press the PF1 key; to toggle through to SYS MODE MENU 7, press the PF2 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.</p>
<b>IPP DIAG F2</b>	
<pre> INTERNAL PIN PAD MEMORY TEST PASSED IPP6 0PGP021 12/99 B6 SN: 00000000000000000000 BAUD: 1200          RESET F3 MODE: VISA                                 EXIT F4           </pre>	<p>When you select F2, the INTERNAL PIN PAD screen appears and the diagnostic test begins. The firmware version and download date, IPP serial number, baud rate, and mode display.</p> <p>To reset the IPP, press F3; to exit the test and return to SYS MODE MENU 6, press F4 or the cancel key.</p>
<b>IPP KEY LOAD F3</b>	
<pre> INTERNAL PIN PAD KEY LOADING MODE BYTES SENT 0 BYTES RCVD 0                                 END F4           </pre>	<p>Select this mode when using SecureKit or programming from your PC to inject keys into your terminal. The terminal must be docked to inject keys using these tools. In this mode, a pipe is opened through COM1 to the IPP to allow key loading.</p> <p>Press the cancel key to stop the key load session; press F4 when finished with the key load.</p>
<b>PRINTER DIAG F4</b>	
<pre> PRINTER ID      M VERSION         0LIT002C STATUS          20                                 TEST F3                                 PAPER FEED F4           </pre>	<p>When you select F4, the firmware ID and version, and the printer status appear.</p> <p>Press F3 to run the printer test. A print sample begins that uses approximately 30.5 cm (12") of paper. This allows you to test the print quality and adjust your code for print optimization.</p> <p>See the <i>Verix Programmer's Manual</i> for specifics on application development and the internal thermal printer.</p> <p>Press F4 to run approximately 5 cm (2") of paper through the printer without printing. To exit this screen, press the cancel key.</p>

## System Mode Menu 7

In this menu you can check the status of the smart battery.

**Table 12 System Mode Menu 7**

Display	Action
SYS MODE MENU 7 BATTERY STATUS F2  ↑	Press F2 to bring up the state of the battery.
BATTERY STATUS F2	
BATTERY STATUS FULL CHARGE      1680 REMAINING        93% 1556 VOLTAGE            8161 STATUS             00C0	When you select F2, the BATTERY STATUS screen appears. The full charge state of the smart battery displays in mA hours. The remaining charge capacity and state (in mA hours) displays. The voltage capacity displays in mV. A hex value stating the status of the smart battery displays.



# 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 Omni 3600 terminal.
- Prepare Omni 3600 terminals for deployment.
- Maintain Omni 3600 terminal installations in the field.
- Transfer data to/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 Omni 3600 terminal can perform downloads when docked with the base station.

---

### NOTE



Wireless downloads can only be performed on Omni 3600 models connected to a GSM network.

---

The base station contains ports that allow the Omni 3600 terminal to connect to a network, telephone line, or perform back-to-back downloads. See [Download Methods](#).

---

## Downloads and Uploads

In downloads, data transfers from a sending system to a receiving system. 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 three operations to program, deploy, transfer data files from, and support Omni 3600 terminals:

- *Host* computer downloads: Applications, operating systems and associated files transfer from a host PC to a Omni 3600 terminal
- *Back-to-back* downloads: Applications and associated files transfer from one Omni 3600 terminal to another Omni 3600 terminal
- *Wireless* downloads: Applications, operating systems or OS updates, and data files transfer between your wireless service provider and a Omni 3600 terminal

## Download Methods

The following four methods are available for file and data downloads through the Omni 3600 download and upload procedures:

- **Direct downloads:** Files and/or data transfer directly from the sending system (a host computer) to the receiving system (an Omni 3600 terminal docked on the base station or connected using the MOD10 adapter). A special cable (PN 056051-00) connects the RS-232 serial ports of the two systems.
- **Downloads by telephone:** Files and data transfer over a telephone line from the sending system (a host computer) to the receiving system (an Omni 3600 terminal docked on the base station). The modem of the sending host computer, and the internal modem of base station are connected by a telephone line connection. Data transfers into the Omni 3600 terminal through the docking port contacts on the base unit.
- **Back-to-back downloads:** Files and data transfer from a docked, sending Omni 3600 terminal to a docked receiving Omni 3600 terminal. A special cable (PN 056051-00) connects the RS-232 serial ports of the two base stations. Two undocked terminals can also be connected with the MOD10 adaptor.
- **Wireless downloads (Omni 3600 GSM models only):** Files and data transfer over your wireless system provider's network. The Omni 3600 terminal does not need to be docked in the base station for this type of download. Large downloads can take a long time. It is recommend that the unit be connected to the power pack during this process.

---

**NOTE**

The Omni 3600 terminal can complete the first three types of downloads listed above only when docked in the base station. The base unit contains the ports to make the required wired connections (RS-232 and modem).

---

## Download Tools

Three software tools are available from VeriFone for performing downloads.

---

**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 three software tools are for performing direct downloads and downloads by telephone from a host computer to an Omni 3600 terminal:

- **VeriCentre Download Management Module (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 Omni 3600 operating system supports file decompression for archives created using DMM.

- **ZonTalk 2000:** PC-based software tool to manage applications and data for VeriFone. In addition to being a database and communications management tool, ZonTalk 2000 automates application downloads and updates to terminal records.
- **DDL.EXE (Direct Download Utility):** Download files and data from a development system or other host computer directly to an Omni 3600 terminal over a serial cable connection. DDL.EXE is a 32-bit, Windows 95 program included in the VDTK (Verix 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 system mode, is handled by the OS software and firmware of the sending and receiving Omni 3600 terminals.

## Download Content

In general, you can download files *and* data to an Omni 3600 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 Omni 3600 terminal during the manufacture. If necessary, download newer versions during application development, when preparing for deployment, or to terminals in the field.

- **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.

Omni 3600 applications can be developed by VeriFone, customers, or third parties on customer request. One or more applications must be downloaded to the Omni 3600 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 Omni 3600 terminal is *file authentication*. For an executable to run on an Omni 3600 terminal, it must be authenticated by the VeriShield file authentication module.

**NOTE**

For a 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 an Omni 3600 terminal, including

CONFIG.SYS variables, passwords for accessing protected system mode functions, the current date and time, the modem country code setting, and so on (refer to [Chapter 3](#)).

## Full and Partial Downloads

When preparing to initiate a download procedure, you must choose either a *full* or *partial* download and the COM 1 port, through the system mode menu options (refer to [Chapter 3](#)). Depending on the type of files you are downloading and the download method you are using, there are some restrictions on if a full or partial download is permitted.

The various types of full and partial download procedures are listed and described in [Table 13](#).

**Table 13** Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full application download	<p>An entire application, including all executables and data files, transfers from one system to another in a single operation.</p> <p>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.</p> <p>Following a full application download, the terminal restarts and the file authentication module is invoked. If application files are authenticated, the application executes.</p>	<ul style="list-style-type: none"> <li>• Direct downloads</li> <li>• Telephone downloads</li> <li>• Back-to-back downloads</li> <li>• Wireless downloads<sup>a</sup></li> </ul>
Partial application download	<p>A subset of application executables, font files, and/or data files transfer from one system to another to modify or update an existing application.</p> <p>Files related to file authentication and terminal configuration settings can be included in a partial application download. During this process, RAM is <i>not</i> cleared.</p> <p>Following a partial application download, the terminal does not restart and returns control to system mode or the issuing application.</p> <p>The file authentication module is not invoked, nor is the application allowed to execute, until the terminal is manually restarted from within system mode.</p>	<ul style="list-style-type: none"> <li>• Direct downloads</li> <li>• Telephone downloads</li> <li>• Wireless downloads<sup>a</sup></li> </ul> <p><b>Note:</b> Partial back-to-back downloads are <i>not</i> supported.</p>

**Table 13** Types of Full and Partial Downloads (continued)

Download Type	Description and Effects	Download Methods Supported
Full operating system download	<p>An <i>entire</i> OS version transfers from a host PC to the Omni 3600 terminal.</p> <p>Files related to file authentication and terminal configuration settings can be included in a full OS download. During this process, RAM is cleared.</p> <p>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.</p> <p>Application files stored in the memory area where the OS downloads (Group 1) are erased.</p>	<ul style="list-style-type: none"> <li>• Direct downloads</li> <li>• Telephone downloads</li> <li>• Wireless<sup>a</sup></li> </ul> <p>Full back-to-back OS downloads are <i>not</i> supported</p>
Partial operating system download	<p>Either an <i>entire</i> or a <i>partial</i> OS version transfers from a host PC to the Omni 3600 terminal.</p> <p>Files related to file authentication and terminal configuration settings can be included in a partial OS download.</p> <p>Following a partial OS download, the terminal does not restart and returns control to system mode or the issuing application.</p> <p>The file authentication module is not invoked, and the new OS is not processed until you manually restart the terminal from within system mode. If the new OS is authenticated, it then updates (replaces) the existing OS.</p> <p>Application files stored in the memory area the OS downloaded into (Group 1) are retained.</p>	<ul style="list-style-type: none"> <li>• Direct downloads</li> <li>• Telephone downloads</li> <li>• Wireless<sup>a</sup></li> </ul> <p>Partial back-to-back operating system downloads are <i>not</i> supported.</p>

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

Here are a few more points on downloads:

- The most common download procedure is a full (complete) application download.
- Partial application downloads are useful when developing and testing new applications.
- Full OS downloads are usually performed by VeriFone at the factory and, on occasion, by those who deploy terminals or in the field 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 an Omni 3600 terminal and then return control to the main application.

- Full downloads restart the terminal; partial downloads return control to system mode 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.

## Omni 3600 Download Differences

---

To help you plan download tasks and explain how the download procedures for Omni 3600 terminals may differ from those you may be accustomed to using for other POS terminals, some information on the following related topics is included in this chapter:

- Support for multiple applications
- Use of RAM and flash memory
- Redirection of files during application downloads
- File authentication requirements

### Support for Multiple Applications

The Omni 3600 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 Omni 3600 terminal uses a system of file groups to store and manage multiple applications, as well as operating system files, in such a way that the data integrity of each application is ensured and that applications do not interfere with each another (see [File Groups, page 38](#)).

### How the File System Supports Multiple Applications

The application memory partition of the Omni 3600 terminal is divided into 15 logically-defined sub-partitions called file groups or *GIDs*. These groups are called 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. You select the target file group for the download using system mode menu options and by entering a file group password.

Usually, one application is stored in one file group. An application can, however, 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 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.

### The 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 Omni 3600 operating system controls *physical* access to GIDs 1–15 using password-protected system mode functions.

To download data into a specific file group, you must first enter system mode and choose the target group by making the appropriate menu selections. Then, you must enter the correct password for that file group.

Each file group has its own CONFIG.SYS file. The CONFIG.SYS settings of the target group you select are always used as the system parameters for the download operation you are performing.

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

- If GID1 is selected as the target group in system mode, 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 Omni 3600 application memory partition has two separate file systems:

- RAM (battery-backed volatile memory, also called SRAM), drive name I:
- Flash (non-volatile memory), drive name F:

The fact that there are 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 which 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 system mode. 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.

To redirect files during a download procedure, see the following sections.

### Defragment Flash For Application Downloads

Before you perform an application download, you may need to defragment terminal flash memory. For information on performing this system mode operation, see [Table 7, page 45](#).

To ensure the best result when performing back-to-back downloads, you may need to defragment the flash memory on the receiving terminals. A system mode procedure is also available for clearing the RAM or flash memory, either entirely or for a specific file group, to prepare an Omni 3600 for a *clean* download.

---

**NOTE**

The flash defragment operation is not necessary for an Omni 3600 terminal just out of the box. In this case, the terminal flash file system is still in its factory-new condition.

---

### Redirection of Files During Application Downloads

You can download application files into RAM or flash memory. By default, files that you download to a specific file group are stored in the RAM of that group. To store a file in flash of that file group, you must provide instructions to redirect the file to flash as part of the procedure.

There are two methods you can use to redirect files during an application download, depending on the download tool you are using:

- If you are using Download Manager or ZonTalk 2000, 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 further described in the following sections.

## Manually Redirecting Files to Flash Memory

To manually redirect files to flash memory for Download Manager or ZonTalk 2000 application downloads, you must create one or more files on the download computer with the special file name, SETDRIVE.x, where, x is the name of the drive (memory area) to download files to:

- Drive name I: is RAM: This is the system mode default for downloads.
- Drive name 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 RAM of the target group to flash 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 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 the following files 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 flash of GID1. 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. Together, the zero-length SETDRIVE.x and SETGROUP.n files allow you flexibility to store files as required in 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 telephone, and only using the Download Manager or ZonTalk 2000 download tools (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 system mode setting for performing downloads. Using the system mode 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 system mode. If no number is added to the SETGROUP filename, SETGROUP.1 (GID1) is assumed.

### Restrictions on File Redirection

The Omni 3600 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 Omni 3600 file system, only two schemes are available for redirecting files during a batch application download:
  - If, using system mode menu options, you select Group 1 (default) as the target group for the download, files can be redirected to any other file group, including GID15.
  - If, using system mode menu options, you 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 the shared library, COMN.LIB, 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 Omni 3600 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: (RAM, default) or F: (flash), and/or

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

where, group number is 1-15.

For example, the following 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 download 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 13, page 60](#)):

- For full OS downloads, the redirection of OS files into Group 0 is performed automatically, after the terminal restart, 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 system mode 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 minutes, 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 terminal. 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 the signature file authenticates is stored in flash, the signature file is moved to flash only after the target file is successfully authenticated.

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 provided a general introduction to the file authentication process. Now we become more task-oriented and see how the file authentication process affects how to perform the various download procedures.

### Required Certificates and Signature Files

Here are some important points to remember about how certificates and signature files relate to application download procedures:

- Before an executable file can be downloaded to and be allowed to run on an Omni 3600 terminal, the file must be digitally signed on the download computer using the file signing tool, FILESIGN.EXE. The result of this procedure is a signature file recognized by its \*.p7s file name extension.
- A signature file must be downloaded together 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 together 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 is required by an application that consists of 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) required to authenticate both application files and operating system files must always be downloaded into 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 the 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.

### The File Authentication Process During an Application Download

In the following example of a typical file authentication process, it is assumed that we:

- are downloading an application to prepare an Omni 3600 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.
- generated a signature file for each executable that comprises the application on the download computer using FILESIGN.EXE, 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 Omni 3600 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 processed. This process continues in random order until all certificates are authenticated.

When a certificate file in the processing list is authenticated, the “Authenticated” message displays below the corresponding filename. If it fails to be authenticated, the “Failed” message displays for five seconds and the terminal beeps three times (see [Figure 30](#)). The routine then resumes processing and continues until all certificates are successfully processed.

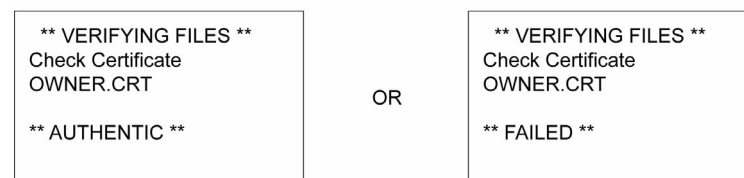


The processing routine gives you both visible and audible indications if a specific certificate successfully authenticates. The file authentication module does not halt the process if a certificate fails to authenticate, but continues to the next step: authenticating signature files.

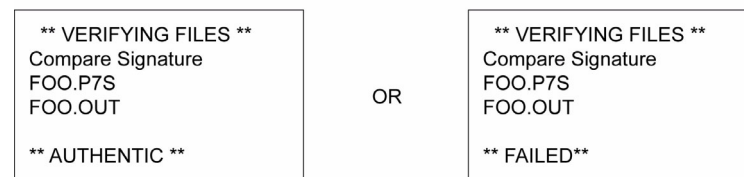
If one or more certificates fail to authenticate, the ensuing file authentication process based on signature files probably also fails, with the result that an application is not authenticated and is not allowed to execute on the terminal.

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



Step 2: Authenticate Signature Files



**Figure 30 Display Prompts During the File Authentication Process**

5 Signature files are processed next (after certificate files). The file authentication module calls the signature checking routine one time 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, the “AUTHENTIC” message displays and the target file’s ATTR\_NOT\_AUTH bit is set to 1.
- If the authentication process fails, the “FAILED” message displays for five seconds and the terminal beeps three times (see Figure 30). 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 RAM or flash.

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

The processing routine gives you visible and audible indications of if a specific signature file successfully authenticates. 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 deleted or redirected as required, the terminal restarts and the \*GO application executes.

### File Group Permissions

Now, consider how file authentication controls *who* (which business entity) can store application files in which file groups in the Omni 3600 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 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 Omni 3600 file system.

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

Chapter 5 discussed how signer certificates are required inputs to FILESIGN.EXE 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 system mode, the files you download are not authenticated for the target group you selected 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 Omni 3600 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.



Operating system files can only be transferred to an Omni 3600 terminal using a PC-to-terminal download procedure, either direct or by telephone. OS files cannot be downloaded to an Omni 3600 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, and
  - A signature file generated by the VeriFone CA under the authority of a higher-level OS *partition sponsor certificate*, called VFI.P7S. 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.
- You *must* download the entire OS package into Group 1 RAM. If you select a target group other than Group 1, the operation fails.
- Before you initiate an OS download, either full or partial, ensure enough memory space is available in Group 1 RAM to temporarily store the OS files and that any application files can also be stored in Group 1.
- If you have selected a *full* OS download in system mode, the terminal restarts automatically 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 you select a *partial* OS download, the operating system returns control to system mode after the download completes. To process the new OS, you must *manually* restart the terminal by selecting the appropriate system mode

menu option. In a partial OS download operation, application files stored in Group 1 are not erased.

- When you initiate the OS download, the OS file authentication progress displays 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 [Figure 30, page 71](#).
- While the new OS is being processed, there is no visible indication on the terminal display of progress. When the new OS is processed (this usually takes a few minutes), 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 docked Omni 3600 terminals, the file authentication process on the receiving terminal is similar to an application download from a host computer to a standalone Omni 3600 terminal. There are, however, 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 system mode 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 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 the same 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 the following:
  - 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 displays 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, including:

- the number and size of application files,
- the number of certificates and signature files, and
- if you are using the file compression feature of Download Manager 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, you can 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; in back-to-back downloads, memory on both the sending and receiving terminal.
- 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 you perform a download, use system mode menu selections to clear the entire RAM and/or flash or the RAM 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 refer to the *Verix Operating System Programmer's Manual* (VeriFone part number 19733).

### Effect of Downloads on Existing Files and Data

When you download application files and data to an Omni 3600 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 to remember:

- 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) together 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 (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 system mode 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 *system mode* password in a separate, securely-controlled operation.

- 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. System mode 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 again in a subsequent operation, together with the certificates and signature files required to authenticate them.

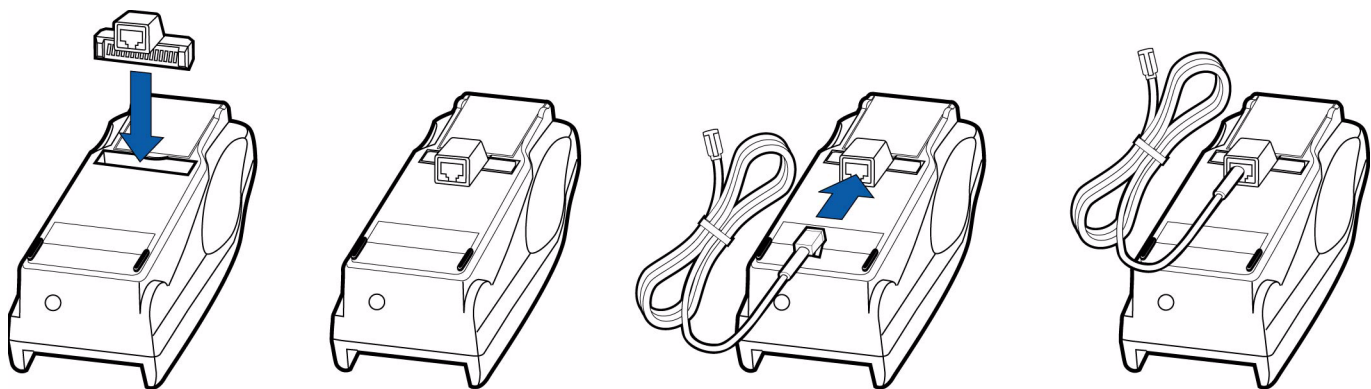
## Set Up the Download Environment

The first step in performing a download to an Omni 3600 terminal is to establish the physical communication link between the sending and receiving system required to support the desired download method:

- 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 base station of the docked receiving Omni 3600 terminal, or through the MOD10 adapter (PN 22536-01) directly to a receiving Omni 3600 terminal.

Two cables are available from VeriFone to support direct downloads: one for computers with DB25-type serial connectors (PN 26263-02) and another for DB9-type connectors (PN 26264-01). Both of these cables have a 10-pin RJ45 modular plug on one end for the terminal-side connection.

The MOD10 adapter allows direct cable connections to an *undocked* Omni 3600 terminal. [Figure 31](#) shows how to install the MOD10 adapter.



**Figure 31** Connecting the MOD10 Adapter

- 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 base station of the docked receiving Omni 3600 terminal.

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 port of the base stations between the docked sending and docked receiving Omni 3600 terminals, or between two Omni 3600 terminals directly connected by cable through two MOD10 adapters.

A special cable is required for back-to-back downloads (PN 056051-00). This cable has two 10-pin RJ45 modular plugs on each end to establish the base station-to-base station connection.

### **Cable Connection for Direct Downloads**

There are two cables and one adapter for direct downloads:

- DB25 serial connector (PN 26263-02)
- DB9 connector (PN 26264-01)
- MOD10 adapter (PN 22536-01)

The following steps describe how to establish the cable link between the sending host computer and the receiving Omni 3600 terminal (see [Figure 32](#)):

- 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 RJ45 connector on the other end of the download cable to the RS-232 port on the back panel of the base station of the docked Omni 3600 terminal, or to the MOD10 adapter installed in an undocked Omni 3600 terminal (see [Figure 33](#)).



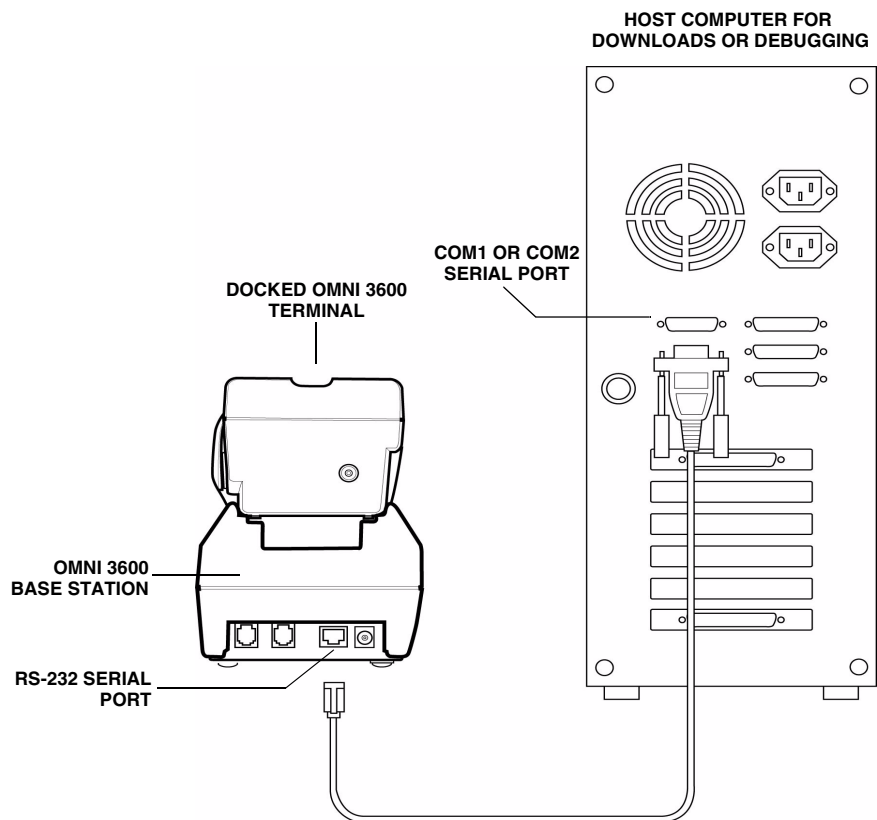


Figure 32 Serial Cable Connection for Direct Downloads

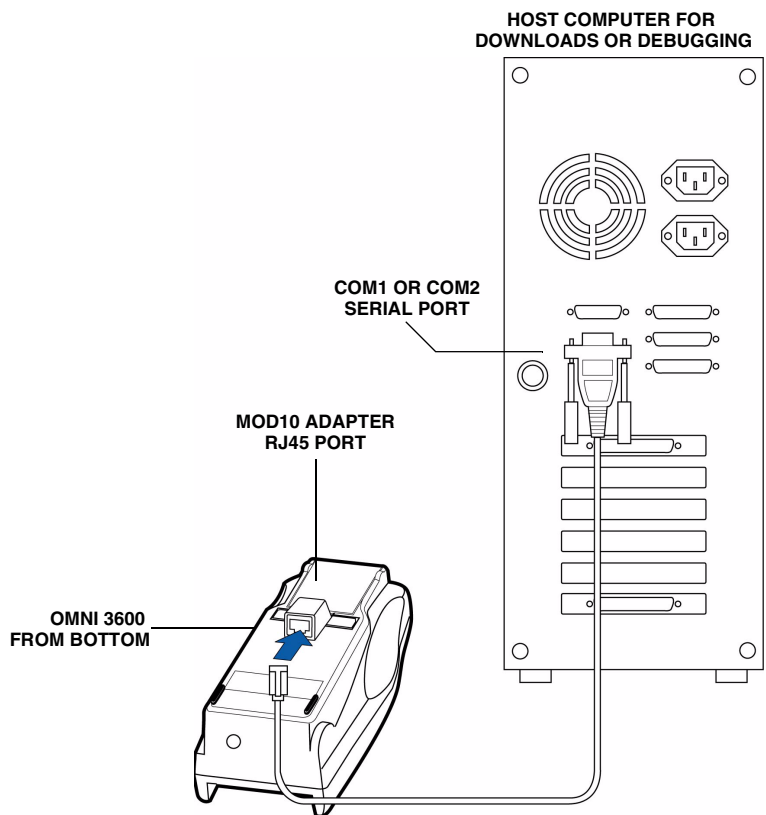


Figure 33 Serial Cable Connection using the MOD10 Adapter

### Telephone Line Connection for Telephone Downloads

To set up the telephone line connection for application or OS downloads between a host computer and a docked Omni 3600 terminal:

- 1 Confirm proper configuration of the dial-up telephone line and modem connection on the host computer and
- 2 Confirm the parameters for the download by telephone are set in the download tool.
- 3 Confirm that the base station of the docked receiving Omni 3600 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 docked receiving terminal.

### Connections for Back-to-Back Downloads

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

- 1 Insert the RJ45 modular connector on one end of the download cable (PN 056051-00) into the RS-232 port of the base station of the docked sending terminal.
- 2 Insert the RJ45 connector on the other end of the cable into the RS-232 port on the back panel of the base station of the docked receiving terminal.

To prepare for a back-to-back application download for terminals using MOD10 adapters:

- 1 Insert the RJ45 modular connector on either end of the download cable into the port of each MOD10 adapter installed in the two terminals.

### Direct Application Downloads

This section provides procedures for direct downloads.

#### Hardware Checklist

- The cable to connect the download computer serial port (COM1 or COM2) to the RS-232 serial port (COM1) of the base station of the docked Omni 3600 terminal, or
- The MOD10 adapter and cable to connect the download computer serial port (COM1 or COM2) directly to the Omni 3600 terminal

#### Software Checklist

- Download Manager, ZonTalk 2000, or DDL.EXE running on the host computer.
- The application file to download (full or partial) resides on 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 docked receiving terminal are stored in memory or they reside on the host computer and download together with the application files.
- All required signature files (\*.p7s) generated using FILESIGN.EXE, reside 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.
- To avoid accidental overwrites, ensure that file names and CONFIG.SYS variables to download are correct in relation to those stored in memory of the docked receiving terminal.
- The required system mode and file group passwords are available to make the system mode menu selections required to prepare the docked receiving terminal to receive the application download.
- Sufficient memory space exists in RAM of the target group so that it can accept the entire download package, including certificates, signature files, and all data files.
- Use the system mode menu options to clear the entire RAM or flash or specific file groups on the receiving terminal (as necessary). Perform a flash defragment (coalesce) 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 system mode operations, refer to [Chapter 3](#).

**NOTE**



Download, clear, and defragment operations cannot proceed in system mode if an application is executing. If you see the message DEVICE BUSY, PLEASE RESTART STAND ALONE, press the cancel key and restart the terminal from SYS MODE MENU 1. When you see the VeriFone copyright screen, enter system mode within 3 seconds (before the application starts).

**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 15](#) describes how to perform a direct application download from a host download computer into the Group 1 application memory area of a docked Omni 3600 deployment terminal.

Steps described in the *Action* column are performed directly on the docked Omni 3600 terminal. Notes provided in this column indicate and explain actions you must perform on the host computer.



The five steps listed in [Table 15](#) 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 14](#) are assumed to be completed.

**Table 14 Common Steps to Start a Download**

Step	Display	Action
1	VERIFONE OMNI Q80000XX 01/10/01 K2 *K2*  COPYRIGHT (C) 1997-2003 VERIFONE, INC. ALL RIGHTS RESERVED	<p>When the terminal restarts, a copyright screen displays that shows the version of Omni 3600 system firmware stored in the terminal's flash EPROM, the date the firmware was loaded into the terminal, and the copyright.</p> <p>This screen displays for three seconds, during which time you can enter system mode by simultaneously pressing F2 and F4.</p> <p>To extend the display period of this screen, press any key during the initial three seconds. Each key press extends the display period an additional three seconds.</p>
2	(Application Prompt) or DOWNLOAD NEEDED	<p>If an application already exists on the receiving terminal, the application starts and the application prompt displays. Otherwise, the DOWNLOAD NEEDED message displays.</p> <p>To enter system mode, simultaneously press F2 and F4.</p>
3	SYSTEM MODE ENTRY PASSWORD -----	<p>Enter the system mode password.</p> <p>If an application already resides on the terminal, a unique system mode password may already exist. In this case, type that password and press enter to confirm your entry.</p> <p>If DOWNLOAD NEEDED displayed in step 2, enter the default password, "Z66831". To type this password on the keypad, enter: 1 ALPHA ALPHA 6 6 8 3 1, and then press enter.</p> <p>If you enter an incorrect password, the message, PLEASE TRY AGAIN displays. Reenter the password.</p> <p>To correct a typing mistake, press [←] to delete the entry, and retype your entry. To end the password entry session and return to the display shown in Step 2, press the cancel key.</p>

**Table 14 Common Steps to Start a Download** (continued)

Step	Display	Action
4	SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	When the system mode password is accepted, the terminal enters system mode and SYS MODE MENU 1 displays.  To display additional system mode menus, press the PF2 key located on the terminal just below the on-screen down arrow. You can also press the enter key to toggle to the next menu.  To perform any type of download operation, press the enter key one time when SYS MODE MENU 1 displays to move to SYS MODE MENU 2.
	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑ ↓	When SYS MODE MENU 2 displays, press F2 to select the DOWNLOAD menu option.  To return to SYS MODE MENU 1, press the PF1 key located on the terminal keypad just below the on-screen up arrow. To return to SYS MODE MENU 1 and cancel the download procedure from within SYS MODE MENU 2, press the cancel key.

**Table 15 Direct Application Download Procedure**

Step	Display	Action
1	SYS MODE FILE FILE GROUP _1	Enter the target file group for the download. File Group _1 (Group 1) displays as the default selection. To select Group 1 as the target file group, press enter; 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	SYSTEM MODE FILE GROUP _1 PASSWORD -----	Enter the password of the selected file group. For example, if Group 1 is the target group, the GROUP_1 PASSWORD message as shown at left displays.  To continue, enter the required file group password and press enter to confirm your entry.
3	SYS MODE DOWNLOAD  FULL F3 PARTIAL F4 ↑	Select if the download operation is FULL or PARTIAL. To perform a full application download, press F3; to perform a partial download, press F4.  To return to SYS MODE MENU 2, press the PF1 key.
4	SYS MODE DOWNLOAD MODEM F2 COM1 F3 COM2 F4 ↑ ↓	Select the terminal port to use for the data transfer from the host computer to the docked receiving terminal. (To display additional menu options, press the PF2 key.)  For a direct application download, always select the COM1 menu option by pressing F3. When you press F3, the docked terminal is ready to receive the application download from the host computer.
5	SYS MODE DOWNLOAD ***** DOWNLOADING NOW	To initiate the download, execute the proper command(s) in the download tool running on the host computer. The data transfer operation starts, and the status messages shown at left display on the terminal screen.  The progress of the download is indicated by a series of ten asterisks (each asterisk indicates 10% of the download is complete). When the last asterisk displays, the direct download is complete.  You can stop the download operation at any time by pressing the cancel key. The terminal restarts automatically.

**Table 15** Direct Application Download Procedure (continued)

Step	Display	Action
6	<p><b>**VERIFYING FILES**</b> CHECK CERTIFICATE  (FILENAME.CRT)  <b>**AUTHENTIC**</b>  or else  --- FAILED ---</p>	<p>When the download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal begins to check for new certificate files (*.crt) and signature files (*.p7s) included in the download. These special files then process, one at a time; certificates are processed first, then signature files.</p> <p>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 displays directly below the certificate filename. If file authentication fails for a specific certificate, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate.</p> <p>The authentication process then continues to the next certificate until all new certificates are authenticated.</p>
7	<p><b>**VERIFYING FILES**</b> COMPARE SIGNATURE  FILENAME.P7S FILENAME.OUT  <b>**AUTHENTIC**</b>  or else  --- FAILED ---</p>	<p>The file authentication module proceeds to authenticate any new signature files downloaded with the OS files.</p> <p>When the signature file authentication routine starts, the status display shown at left informs you of the progress of the authentication process.</p> <p>If file authentication succeeds for a specific signature file, the "AUTHENTIC" message displays directly below the filename of the signature file. If file authentication fails for a specific signature file, the "FAILED" message displays 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.</p> <p>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.</p>
8	<p>(Application Prompt) or DOWNLOAD NEEDED</p>	<p>If the downloaded application successfully authenticated, the corresponding application prompt or logo displays on restart.</p> <p>The terminal can now process transactions.</p> <p><b>Note:</b> The message DOWNLOAD NEEDED appears if:</p> <ul style="list-style-type: none"> <li>• The *GO variable is not set.</li> <li>• *GO does not specify an application is present.</li> <li>• The application did not authenticate (invalid or missing *.p7s file).</li> <li>• The application uses shared libraries that are missing or were not authenticated (invalid or missing *.p7s files).</li> </ul> <p><b>Note:</b> 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. You must then repeat the direct download procedure using the correct certificates and/or signature files.</p>

## Direct Operating System Downloads

This section presents procedures for direct downloads.

### Hardware Checklist

- The cable to connect the download computer serial port (COM1 or COM2) to the base station of the docked Omni 3600 “RS232” serial port (COM1) (refer to [Cable Connection for Direct Downloads](#)), or
- The MOD10 adapter and cable to connect the download computer serial port (COM1 or COM2) directly to the Omni 3600 terminal.

### Software Checklist

- Download Manager, ZonTalk 2000, or DDL.EXE running on the host computer.
- The complete OS version to download resides on host computer.
- Determine 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 system mode and the new OS does not process until you manually initiate a terminal restart from system mode.
- 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).
  - A signature file, called VFI.P7S, for the OS update. This signature file is generated by VeriFone CA using the high-level OS certificates for the Omni 3600 platform.
  - A file called VFI.PED. This file is an encrypted list of the new OS files.
  - One or more digital certificates (\*.crt) download with the OS update.

All new OS files, including VFI.P7S, VFI.PED, all certificate files, and any other files in the download package provided by VeriFone CA, must download together into Group 1 RAM.

- The required system mode and file group passwords are available to make the system mode menu selections required to prepare the receiving terminal to receive the OS 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 system mode menu options to clear the entire RAM or the RAM of Group 1 on the receiving terminal (as necessary).

**NOTE**

Download, clear, and defragment operations cannot proceed in system mode if an application is executing. If you see the message `DEVICE BUSY, PLEASE RESTART STAND ALONE`, press the cancel key and restart the terminal from `SYS MODE MENU 1`. When you see the copyright screen, enter system mode within three seconds (before the application begins).

### 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 system mode and does not erase application files from 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 are authenticated 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 are processed, they are moved out of the Group 1 RAM into the Group 0 area of the Omni 3600 file system.

### Direct Operating System Download Procedure

The procedure in [Table 16](#) describes how to perform a direct operating system download from a host computer into the Group 1 RAM of a docked Omni 3600 terminal.

Steps are performed directly on the Omni 3600 terminal. Notes provided in the Action column indicate actions to perform on the download computer side of the data transfer.

**NOTE**

In [Table 16](#) and in the following procedures, only method-specific steps are included. For a description of the first five steps required to enter system mode and display `SYS MODE MENU 2`, please refer to [Table 14](#).



**Table 16** Direct Operating System Download Procedure

Step	Display	Action
1	SYS MODE FILE FILE GROUP _1	Enter the target file group for the download. File Group _1 (Group 1) is the default. Operating system files must <i>always</i> download into Group 1. This is the default group number in system mode.  To select Group 1 as the target file group, press enter.
2	SYSTEM MODE FILE GROUP _1 PASSWORD -----	Enter the password of the selected file group (Group 1) and press enter to confirm your entry.
3	SYS MODE DOWNLOAD  FULL F3 PARTIAL F4  ↑	Select the OS download operation: FULL or PARTIAL.  To perform a full OS download, press F3; to perform a partial OS download, press F4.  To return to the previous system mode menu, press PF1.
4	SYS MODE DOWNLOAD  MODEM F2 COM1 F3 COM2 F4  ↑ ↓	Select the terminal port to use for the data transfer from the host computer to the docked receiving terminal. (To display additional menu options, press PF2.) For a direct OS download, always select the COM1 menu option by pressing F3.  When you press F3, the terminal is ready to receive the OS download from the host computer.
5	SYS MODE DOWNLOAD *****  DOWNLOADING NOW	Initiate the download by executing the proper command(s) in the download tool running on the host computer (when the receiving terminal is prepared to receive the direct OS download). The data transfer operation starts and status messages display on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk indicates 10% of the download has completed).  When the last asterisk displays, the direct download is complete.  To stop the download operation, press the cancel key. The terminal restarts automatically.
6	**VERIFYING FILES** CHECK CERTIFICATE  (FILENAME.CRT)  **AUTHENTIC**  or else  --- FAILED ---	When the OS download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal then checks for new certificate (*.crt) and signature (*.p7s) files included in the download. It processes these special files one at a time; certificates are processed first, then signature files.  When the file authentication module is invoked, the progress of the file authentication process displays. If file authentication succeeds for a specific certificate, the "AUTHENTIC" message displays directly below the certificate filename. If file authentication fails for a specific certificate, the "FAILED" message displays 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.

**Table 16** Direct Operating System Download Procedure (continued)

Step	Display	Action
7	<p><b>**VERIFYING FILES**</b>                      COMPARE SIGNATURE</p> <p>FILENAME.P7S                      FILENAME.OUT</p> <p><b>**AUTHENTIC**</b></p> <p>or else</p> <p>--- FAILED ---</p>	<p>The file authentication module proceeds to authenticate new signature files downloaded with the OS files. When the signature file authentication routine begins, the progress of the authentication process displays. If file authentication succeeds for a specific signature file, the "AUTHENTIC" message displays directly below the filename of the signature file. If file authentication fails for a specific signature file, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate.</p> <p>The authentication process proceeds to the next signature file until all signature files are validated. When file authentication is complete, the terminal either restarts automatically and begins processing the new OS (full download) or it returns control to system mode (partial download).</p> <p>If you are performing a partial download, the terminal does not restart until manually initiated by pressing F4 in SYS MODE MENU 1. If an application resides on the terminal following the OS download, it executes and starts running on restart.</p> <p><b>Note:</b> Because a full OS download clears the RAM, all terminal applications and related certificate and signature files must download to the terminal when performing this type of download.</p>
8	<p>(Application Prompt)                      or                      DOWNLOAD NEEDED</p>	<p>If you performed a full OS download, the DOWNLOAD NEEDED prompt displays.</p> <p>At this point, you can perform a direct application download on the receiving terminal.</p> <p>If you performed a partial OS download and manually restarted the terminal, the application residing in the terminal (if any) executes. The application prompt displays on terminal restart, after OS processing, and the application starts running.</p>

**Download by Telephone**

The procedure to perform an application or OS download by telephone is similar to that of direct application (see [Table 15](#)) and direct operating system downloads (see [Table 16](#)).

**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 docked receiving Omni 3600 terminal, as described in [Telephone Line Connections, page 28](#).

**Software Checklist**

- Download Manager or ZonTalk 2000 installed and running on the host computer. (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 ZonTalk 2000 may include the following:
  - Dial-up numbers used to established 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 ZonTalk 2000, please refer to the user documentation supplied by VeriFone with these software products.

### Telephone Downloads Procedure

Press F2 (step 4 in [Table 17](#)) to select the MODEM port on the receiving terminal when the port selection options display (SYS MODE MENU 2). When you press F2, the internal modem in the base station of the receiving Omni 3600 terminal dials the host computer to request the download. When the host computer accepts the call, the download procedure is initiated by the host.

**Table 17 Download by Telephone Procedure**

Step	Display	Action
1	SYS MODE FILE FILE GROUP _1	Enter the target file group for the download. File Group _1 (Group 1) is the default. Operating system files must <i>always</i> download into Group 1. This is the default group number in system mode.  To select Group 1 as the target file group, press enter.
2	SYSTEM MODE FILE GROUP _1 PASSWORD -----	Enter the password of the selected file group (Group 1) and press enter to confirm your entry.
3	SYS MODE DOWNLOAD  FULL F3 PARTIAL F4  ↑	Select the OS download operation: FULL or PARTIAL.  To perform a full OS download, press F3; to perform a partial OS download, press F4.  To return to the previous system mode menu, press PF1.
4	SYS MODE DOWNLOAD  MODEM F2 COM1 F3 COM2 F4  ↑ ↓	Select the terminal port to use for the data transfer from the host computer to the docked receiving terminal. (To display additional menu options, press PF2.)  For a download by telephone, you <i>must</i> select the MODEM F2 menu option. When you press F2, the docked terminal can receive the download from the host computer over the Telco port telephone line connection.
5	SYS MODE DOWNLOAD *****  DOWNLOADING NOW	Initiate the download by executing the proper command(s) in the download tool running on the host computer. The data transfer operation then starts, and status messages display on the terminal screen.  The progress of the download is indicated by a series of ten asterisks (each asterisk represents 10% of the completed download). When the last asterisk displays, the direct download is complete.  You can stop the download operation by pressing the cancel key. The terminal restarts automatically.

**Table 17 Download by Telephone Procedure (continued)**

Step	Display	Action
6	<p><b>**VERIFYING FILES**</b>                      CHECK CERTIFICATE                        (FILENAME.CRT)    <b>**AUTHENTIC**</b>                        or else                        --- FAILED ---</p>	<p>When the OS download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal then checks for new certificate (*.crt) and signature (*.p7s) files included in the download. It processes these special files one at a time; certificates are processed first, then signature files.</p> <p>When the file authentication module is invoked, the progress of the file authentication process displays. If file authentication succeeds for a specific certificate, the "AUTHENTIC" message displays directly below the certificate filename. If file authentication fails for a specific certificate, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate.</p> <p>The authentication process then continues to the next certificate until all new certificates are checked.</p>
7	<p><b>**VERIFYING FILES**</b>                      COMPARE SIGNATURE                        FILENAME.P7S                      FILENAME.OUT    <b>**AUTHENTIC**</b>                        or else                        --- FAILED ---</p>	<p>The file authentication module proceeds to authenticate new signature files downloaded with the OS files. When the signature file authentication routine begins, the progress of the authentication process displays. If file authentication succeeds for a specific signature file, the "AUTHENTIC" message displays directly below the filename of the signature file. If file authentication fails for a specific signature file, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate.</p> <p>The authentication process proceeds to the next signature file until all signature files are validated. When file authentication is complete, the terminal either restarts automatically and begins processing the new OS (full download) or it returns control to system mode (partial download).</p> <p>If you are performing a partial download, the terminal does not restart until manually initiated by pressing F4 in SYS MODE MENU 1. If an application resides on the terminal following the OS download, it executes and starts running on restart.</p> <p><b>Note:</b> Because a full OS download clears the RAM, all terminal applications and related certificate and signature files must download to the terminal when performing this type of download.</p>
8	<p>(Application Prompt)                      or                      DOWNLOAD NEEDED</p>	<p>If you performed a full OS download, the DOWNLOAD NEEDED prompt displays.</p> <p>At this point, you can perform a direct application download on the receiving terminal.</p> <p>If you performed a partial OS download and manually restarted the terminal, the application residing in the terminal (if any) executes. The application prompt displays on terminal restart, after OS processing, and the application starts running.</p>

## Back-to-Back Application Downloads

This section presents procedures for back-to-back terminal downloads.


### Hardware Checklist

- The correct serial cable connects the RS-232 ports of the base stations of the docked sending and receiving Omni 3600 terminals (refer to [Connections for Back-to-Back Downloads](#)), or
- The MOD10 adapter and cable to connect the download computer serial port (COM1 or COM2) directly between the two Omni 3600 terminals.
- Verify 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 version of the sending and receiving terminals must be identical or very similar.
- One or more complete, authenticated, application programs are stored in 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 you initiate the download procedure, remember to select Group 1 as the target file group on both the sending and receiving terminals. The required system mode and file group passwords must also be available to make the required system mode 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 your desired settings.
- 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 system mode 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.

**NOTE**

Download, clear, and defragment operations cannot proceed in system mode if an application has already started. If you see the message DEVICE BUSY, PLEASE RESTART STAND ALONE, press the Cancel (  ) key and then restart the terminal from system mode Menu 1. When you see the copyright notice screen, enter system mode within three seconds (before the application begins).

### 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 RAM of the receiving terminal.
- All CONFIG.SYS records and settings on the receiving terminal—protected and non-protected—are replaced with those of the sending terminal. Ensure that these are correct on the sending terminal 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.
- The OS software on the receiving terminal is not affected by a back-to-back application download. (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* Omni 3600 terminal (transfers application files to the *Target* Omni 3600 terminal).
- 2 Downloading application files from the Gold terminal to a properly configured Target terminal.

#### Prepare Gold Terminal (PC-to-Terminal)

- 1 Configure a PC for an application download operation to the Gold terminal:
  - Set the \*FA variable (if present in the application) to 1.
  - Ensure all certificates, \*p7s files, applications, and other required files are present.
  - Ensure the download is exactly what you want your Target terminals to receive.
- 2 Configure the Gold terminal to receive an application download from a PC:
  - From SYS MODE MENU 2, set Group 1 and the COM1 port to receive the download.
- 3 Connect a cable between the RS-232 serial ports of the PC and the base station of the docked Gold terminal, or to a MOD10-equipped Gold terminal.

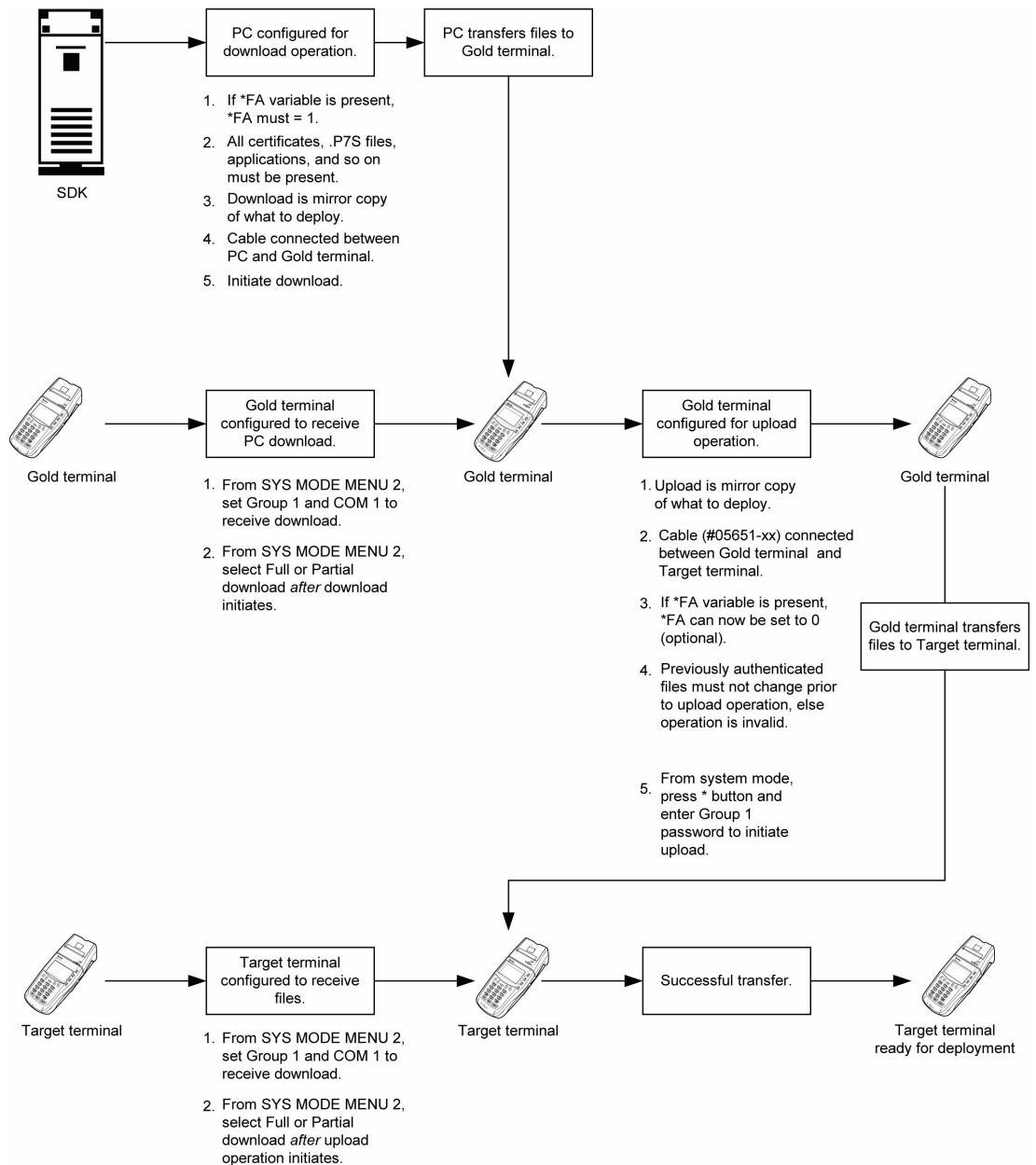
- 4 Initiate the file transfer on the PC.
- 5 From SYS MODE MENU 2 on the Gold terminal, select either a full or a partial download.

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 1, you can reset it to 0. For more information on the \*FA variable, refer to the *Verix Programmer's Manual* (PN 19733).
  - Ensure 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 docked Target terminal to receive an application download from the Gold terminal:
  - From SYS MODE MENU 2, set Group 1 and the COM1 port to receive the file transfer.
- 3 Connect a cable between the RS-232 serial ports of the base stations of the docked Gold and Target terminals, or between the MOD10-equipped Gold and Target terminals.
- 4 From any system mode menu on the Gold terminal, press [\*] and enter the GID1 password to initiate the file transfer.
- 5 From SYS MODE MENU 2 on the deployment terminal, select either a full or a partial download. The Gold terminal begins to transfer files to the Target terminal.

Figure 34 illustrates these two phases and how they relate to each other.



**Figure 34 Back-To-Back Download Process**

The procedure in [Table 18](#) steps you through a back-to-back application download from a docked sending Omni 3600 terminal (Gold) to a docked receiving Omni 3600 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 18](#) 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. However, the Gold terminal displays DOWNLOAD INCOMPLETE before returning to SYS MODE MENU 2.

- You are performing a *full* download.

**Table 18 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 base stations. Dock each terminal and allow each terminal to boot up. After boot up, the Target terminal displays DOWNLOAD NEEDED.	
2	Press F2+F4 to enter system mode.	
3	Enter system mode password (factory default is 1 ALPHA ALPHA 6 6 8 3 1 <sup>a</sup> ) and press the enter key.	
4	Press the ↓ key (PF2) to access the SYS MODE MENU 2 screen.	
5	Press the * (asterisk) key and press the Enter [↵] key. You are prompted to reenter the system mode password. UPLOADING NOW displays.	Press F2, DOWNLOAD, to enter download mode.
6		Press enter key at the next SYS MODE DOWNLOAD screen to select FILE GROUP_1 (default displayed) as the target file group.
7		Press F3, FULL, at the next SYS MODE DOWNLOAD screen. Full downloads are required in back-to-back downloads.
8		Select F3 (COM1) at next SYS MODE DOWNLOAD screen. DOWNLOADING NOW displays.
<p>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 SYS MODE MENU 2. 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 loaded. Allow the Target terminal to complete file authentication and reboot the terminal.</p> <p>The Gold terminal is ready to perform another download. An application-specific menu displays after the Target terminal completes the reboot.</p>		

a. Z66831; 1 ALPHA ALPHA = the character, Z.





# File Authentication

This chapter:

- introduces the file authentication module of the VeriShield security architecture, and the organizational infrastructure that supports this feature.
- explains how the file authentication process may affect the tasks normally performed by application programmers, terminal deployers, site administrators, or by entities authorized to download files to an Omni 3600 terminal.
- describes how to use the file signing utility, FILESIGN.EXE, to generate the signature files that are required to perform downloads and authenticate files on the Omni 3600 terminal.

In [Chapter 4](#), the topic of file authentication is also discussed in the context of specific file download procedures.

## Introduction to File Authentication

The Omni 3600 terminal has a new type of security architecture, developed by VeriFone. This architecture, called VeriShield, 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, or simply, file authentication.

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 an Omni 3600 terminal to logically secure access to the terminal by controlling who is authorized to download application files to that terminal. It proves and verifies the

- file's origin
- sender's identity
- integrity of the file's information

## **The 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 Omni 3600 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 FILESIGN.EXE tool, you can recognize the special file types that support the file authentication process by their 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 Omni 3600 clients — either internally within VeriFone or externally to sponsors.

All certificates that are issued by the VeriFone CA for the Omni 3600 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 files and target files for them 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.

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

To establish the logical security of applications to download to an Omni 3600 terminal, the designated signer uses the signer private key issued them by the VeriFone CA as a required input to the file signing tool, FILESIGN.EXE. Every signature file contains information about the signer private key used to sign it.

When a signature file generated using a signer private key downloads to the Omni 3600 terminal, if it is successfully authenticated 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 file signing software tool FILESIGN.EXE creates a signature file for each application file to authenticate.
- 2 **Pre-deployment:** An optimal certificate structure is determined, and the necessary certificates and keys created.
- 3 **Deployment:** The development and pre-deployment processes, once complete, are used in combination to prepare a terminal for deployment.

### Development Process

In this process:

- 1 The application developer creates an application file.
- 2 The developer assigns a name to the application file.

- 3** The application file becomes a required input for the FILESIGN.EXE tool (included in the SDK).
- 4** The default certificate (K2SIGN.CRT) and default key (K2SIGN.KEY) included in the SDK are inputs for the FILESIGN.EXE tool.
- 5** Using the application file, default certificate, and default key, FILESIGN.EXE creates a signature file (\*.p7s).
- 6** The signature file and the original application file are loaded into a development terminal, where the following actions occur:
  - a** 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 two files are authenticated, and the ATTR\_NOT\_AUTH bit is set to 0.
- 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 35 illustrates the development process.