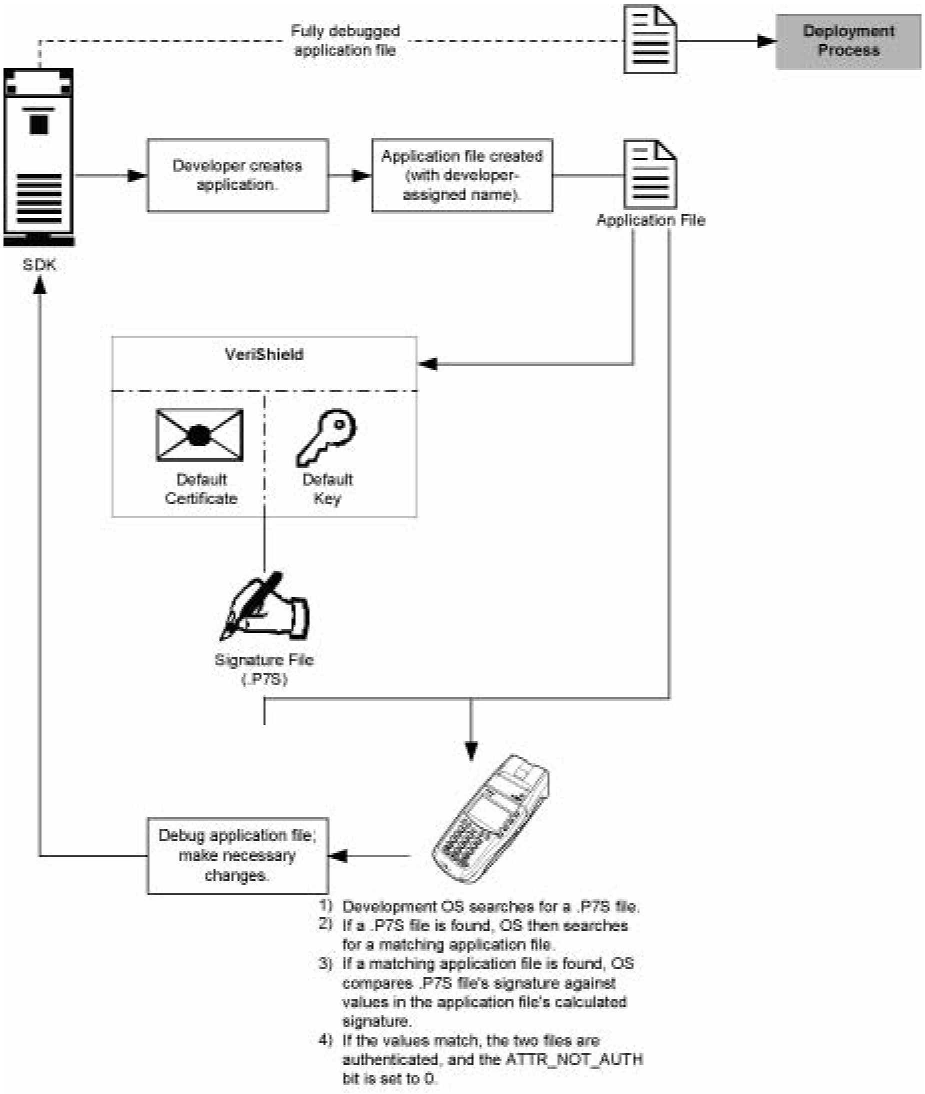

Fully debugged application file
Deployment Process
Developer creates application.
Application file created (with developer-assigned name).
Application File
SDK
VeriShield
Default Certificate
Default Key
Signature File (.P7S)
Debug application file; make necessary changes.

1) Development OS searches for a .P7S file.
2) If a .P7S file is found, OS then searches for a matching application file.
3) If a matching application file is found, OS compares .P7S file's signature against values in the application file's calculated signature.
4) If the values match, the two files are authenticated, and the ATTR_NOT_AUTH bit is set to 0.

Figure 35 The Development Process

Pre-Deployment Process

In this process:

1 A sponsor goes to the VeriFone CA Web site and requests certificates for deployment terminals.

2 Based on information provided by the sponsor through the VeriFone CA Web site, the VeriFone CA determines the required certificate structure.

3 VeriFone CA generates the following items for the sponsor:

a Smart card containing a set of certificates and keys.

b Smart card PIN.

4 VeriFone CA sends the smart card and smart card PIN to the sponsor.

5 The sponsor uses the smart card and smart card PIN as inputs for the deployment process.

Refer to Figure 36 illustrates the pre-deployment process.

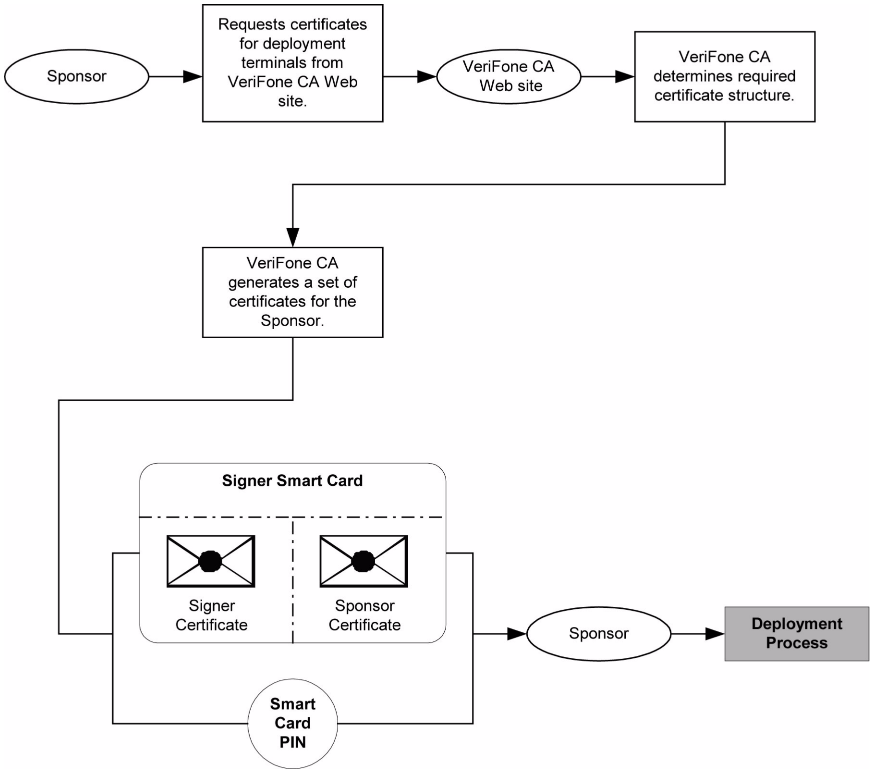

Sponsor
Requests certificates for deployment terminals from VeriFone CA Web site.
VeriFone CA Web site
VeriFone CA determines required certificate structure.
VeriFone CA generates a set of certificates for the Sponsor.
Signer Smart Card
Signer Certificate
Sponsor Certificate
Sponsor
Deployment Process
Smart Card PIN

Figure 36 The Pre-Deployment Process

Deployment Process

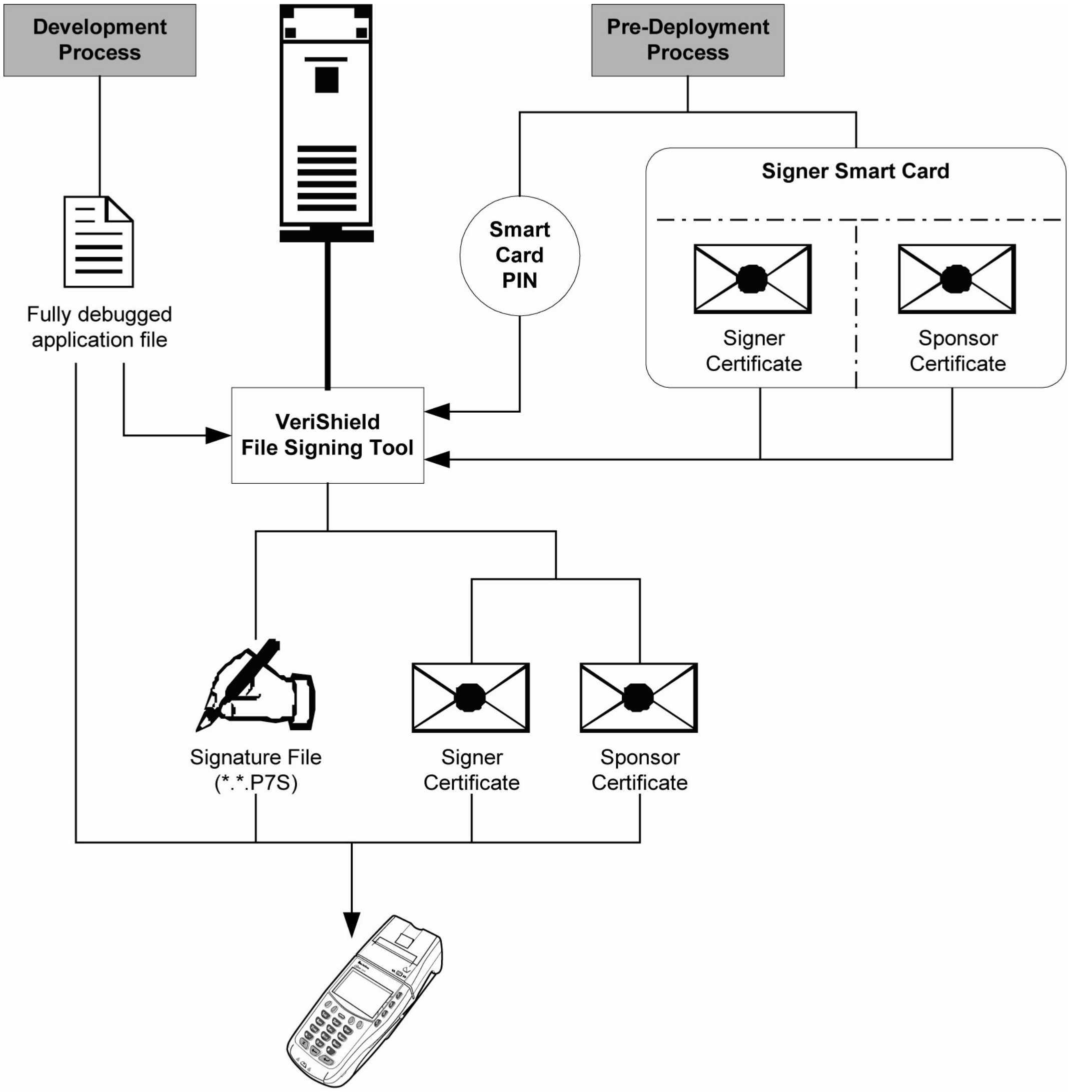
In this process:

1. The sponsor provides the application file (from the development process) and the smart card and smart card PIN (from the pre-deployment process) as inputs to VeriShield.
2. VeriShield extracts the signer key, signer certificate, and sponsor certificate from the smart card.
3. VeriShield uses the extracted data, along with the application file, to create a signature file (*.p7s).
4. VeriShield creates files suitable for downloading from the extracted smart card data.
5. The signature file, the application file, and the extracted signer and sponsor certificates are downloaded into a deployment terminal, where the following actions occur:
   - a The terminal's operating system searches for signature files.
   - b If a signature file is found, the operating system then searches for a matching application file.

- **c** If a matching application file is found, the operating system compares the signature file's signature against the values stored in the application file's calculated signature.
- **d** If the values match, the two files are authenticated and the ATTR_NOT_AUTH bit is set to 0.

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

Figure 37 illustrates the deployment process.



1) Development OS searches for a *.*.P7S file.
2) If a *.*.P7S file is found, OS then searches for a matching application file.
3) If a matching application file is found, OS compares *.*.P7S file's signature against values in the application file's calculated signature.
4) If the values match, the two files are authenticated, and the ATTR_NOT_AUTH bit is set to 0.

Figure 37 The Deployment Process

Planning for File Authentication

File authentication is an integral part of every Omni 3600 terminal. To safeguard the terminal’s logical security, the file authentication module requires that *any executable code file* must be successfully authenticated before the operating system allows it to execute on the terminal.

Authentication Requirements for Specific File Types

For the purposes of file authentication, executable code files include two file types that can be recognized by their filename extensions:

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

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

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

Decide Which Files to Authenticate in a Specific Application

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

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

How (and When) Signature Files Authenticate Their Target Files

Signature files are usually downloaded together with their target application files in the same data transfer operation. This recommended practice lets you specify and confirm the logical security status of the Omni 3600 terminal each time you perform an application download.

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

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

Determine Successful Authentication

To ensure the Omni 3600 terminal's logical security, never assume that a target file was authenticated simply because it downloaded to the Omni 3600 terminal together with its signature file.

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

- **Confirm all downloaded executable files run.** If an executable code file is not successfully authenticated, the operating system does not allow it to execute and run, either following the initial download or on subsequent terminal restarts. The effect of this rule depends on whether or not *all* executable files successfully authenticated:
  - If the executable file that failed to authenticate is the main application (*.out) specified in the CONFIG.SYS *GO variable, the main application is not allowed to run.
  - If the executable that failed to authenticate is a secondary executable (*.out) or shared library (*.lib) used by the main application, the CONFIG.SYS *GO application executes and runs until it issues a function call to that library. When the main application attempts to access a non-authenticated executable, the main application may crash.
- **Visually (and audibly) confirm file authentication during the process.** When the file authentication module is invoked at terminal restart and detects a new signature file, it displays status information on screen indicating success or failure of the authentication of each target file based on its corresponding signature file. (A similar status display also appears on screen when you download digital certificates.)

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

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

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

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

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

Digital Certificates and the File Authentication Process

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

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

Hierarchical Relationships Between Certificates

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

To manage hierarchical relationships between certificates, certificate data is stored in terminal memory in a special structure called a *certificate tree*. New certificates are authenticated based on data stored in the current certificate tree. The data from up to 21 individual related certificates (including root, OS, and other VeriFone-owned certificates) can be stored concurrently in a certificate tree.

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

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

A development set of higher-level certificates is downloaded into each Omni 3600 terminal at manufacture. When you take a new Omni 3600 terminal out of its shipping carton, certificate data is already stored in the terminal's certificate tree. In this just-out-of-the-box condition, the Omni 3600 terminal is called a *development terminal*.

Typically, a sponsor requests an additional set of digital certificates from the VeriFone CA to establish sponsor and signer privileges. This additional set of certificates are then downloaded to the Omni 3600 terminal when the terminal is being prepared for deployment. When this procedure is complete, the Omni 3600 terminal is called a deployment terminal.

Add New Certificates

When you add a new certificate file to an Omni 3600 terminal, the file authentication module detects it by filename extension (*.crt). On restart, the terminal then attempts to authenticate the certificate under the authority of the resident higher-level certificate stored in the terminal's certificate tree or one being downloaded with the new certificate.

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

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

Development Terminals

A development terminal is an Omni 3600 terminal still maintaining the original factory set of certificates in its certificate tree. This set of certificates includes several higher-level system certificates and a special client certificate called a default signer certificate (see Figure 38).

In the development terminal, the level of logical security provided by the file authentication module is minimal, even though applications must still be signed and authenticated before they can run on the terminal. In most application development and test environments, tight security is not required, and the flexibility offered by the Omni 3600 development terminal is more important.

NOTE With the factory set of certificates stored in the terminal memory, *anyone* who has the Omni 3600 SDK and included file signing tool, FILESIGN.EXE, can generate valid signature files for downloading and authenticating files on the Omni 3600 platform.

Deployment Terminals

While the application development process is being completed and while the new application is being tested on a development terminal, a sponsor can order specific sponsor and signer certificates from the VeriFone CA to use to logically secure sponsor and signer privileges when the Omni 3600 terminal is prepared for deployment.

Customer-specific sponsor and signer certificates are usually downloaded to an Omni 3600 terminal as part of the standard application download procedure performed by a deployment service. In this operation, the new sponsor and signer certificates replace the development sponsor certificate that is part of the factory set of certificates, as shown in Figure 38.

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

Ultimately, it is the sponsor's decision how to implement the logical security provided by file authentication on a field-deployed terminal. Additional certificates can be obtained from the VeriFone CA any time, to implement new sponsor and signer relationships in deployment terminals.

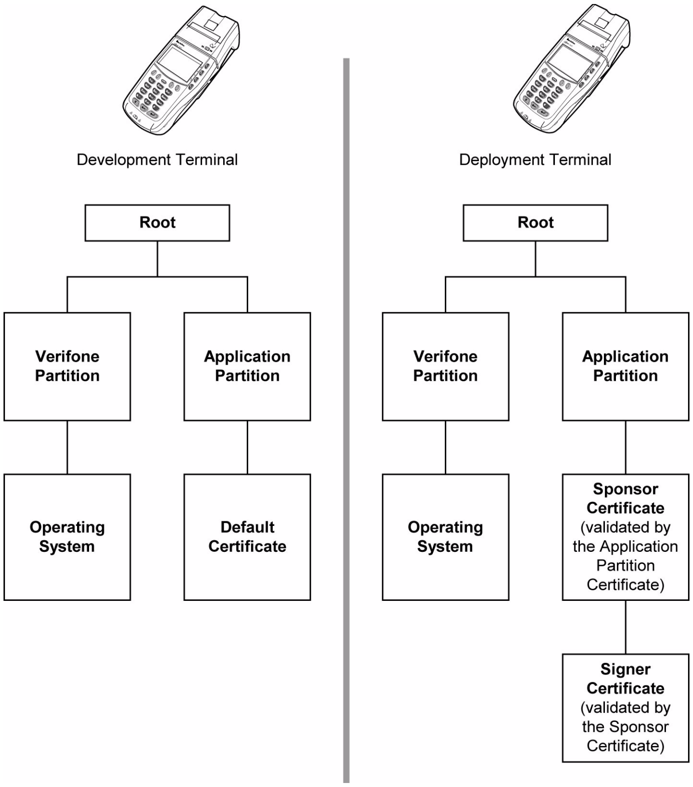


Figure 38 Certificate Trees in Development and Deployment Terminals

Permanency of the Certificate Tree

The data contained in a digital certificate is stored in the terminal's certificate tree when the certificate is authenticated, and the certificate file itself is erased from RAM.

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

Required Inputs to the File Signing Process

The required inputs to the file signing process are somewhat different for development terminals than deployment terminals. The significant differences shown in Table 19.

Table 19 Differences Between Required Inputs

Development Terminals	Deployment Terminals
Manufacturing inputs to the file signing process are included, together with the file signing tool, FILESIGN.EXE, in the Omni 3600 SDK. These inputs make it possible for anyone who has the Omni 3600 SDK to sign and authenticate files.	The required inputs to FILESIGN.EXE must be obtained from the VeriFone CA to logically secure the sponsor and signer privileges for the terminal.
The following two factory inputs are required for the file signing process, in addition to the application files you want to sign and authenticate: • **Default signer certificate**, with the filename K2SIGN.CRT • **Default signer private key**, with the filename K2SIGN.KEY	The following three unique inputs, which are issued at customer request by the VeriFone CA, are required for the file signing process, as well as the application files you want to sign and authenticate: • **Customer signer certificate:** This unique certificate is a required input for FILESIGN.EXE and must be downloaded to the terminal along with the signature files and target application files to authenticate, unless already downloaded to the terminal in a previous operation. • **Customer signer private key:** The VeriFone CA issues this unique, encrypted private key file (*.key) to an authorized signer at the sponsor's request. The signer private key is a required input to FILESIGN.EXE, but does not have to be downloaded to the terminal. • **Customer signer PIN:** The VeriFone CA issues this unique password to an authorized signer at the sponsor's request. The customer signer password is a required input to FILESIGN.EXE, but it does not have to be downloaded to the terminal.
Note: A default signer password is not a required entry when using FILESIGN.EXE to sign files for an Omni 3600 development terminal.	**Note:** The customer sponsor certificate, which authenticates the customer signer certificate, is usually downloaded to the terminal with the customer signer certificate, but it is not a required FILESIGN.EXE input when signing files to be downloaded to, and authenticated on, a deployment terminal.

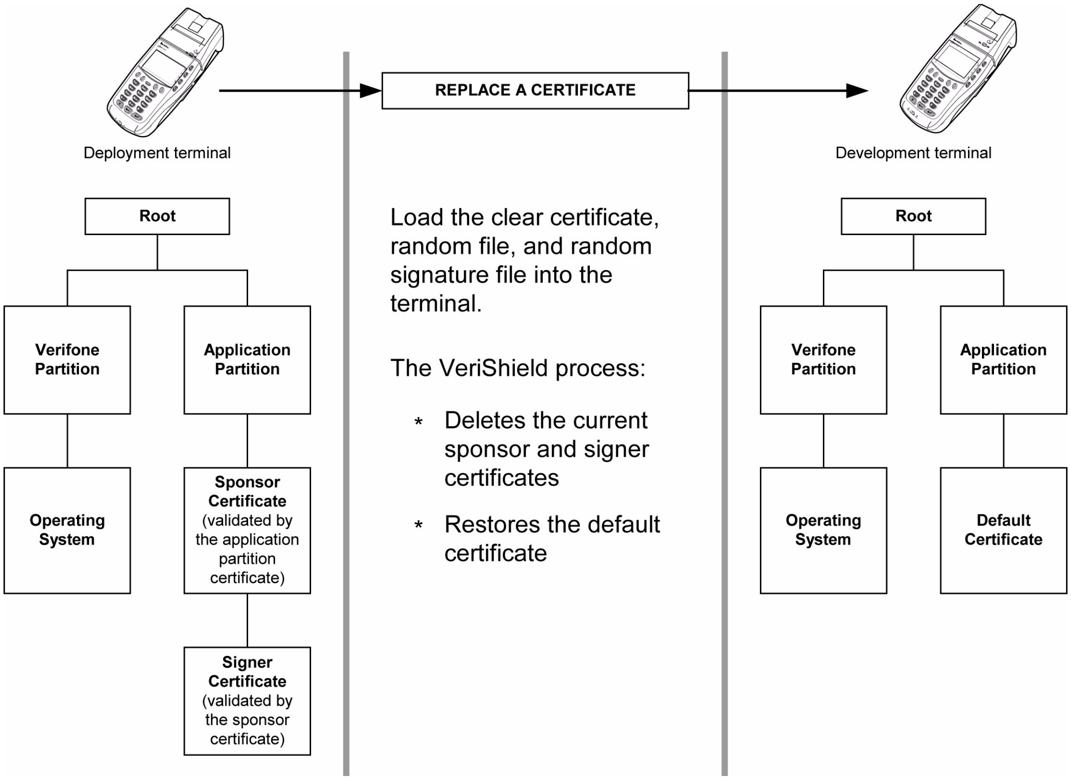
Replace a Sponsor Certificate

A sponsor may need to clear the current sponsor certificate from a terminal so that a new sponsor can load certificates and applications. To do this, the original sponsor must order a "clear" smart card from the VeriFone CA. The clear smart card is specific to the requesting sponsor. It restores a deployment terminal to the development state (refer to Figure 39) by:

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

NOTE

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



Load the clear certificate, random file, and random signature file into the terminal.

The VeriShield process:

- Deletes the current sponsor and signer certificates
- Restores the default certificate

Figure 39 Certificate Replacement Process

File Authentication and the Omni 3600 File System

Application Memory Logically Divided Into File Groups

The memory of an Omni 3600 terminal is logically divided into two main areas, or partitions: One partition is for the operating system and the other partition is reserved for applications. The application partition is further divided into sub-partitions. These sub-partitions are called file groups or GIDs.

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

There are a total of 16 file groups (Figure 40). Group 0 is the name of the operating system partition. Group 1 is reserved for the main application. Groups 2–14 are available for related executable files or secondary applications. Group 15 is *open*, and used for shared files.

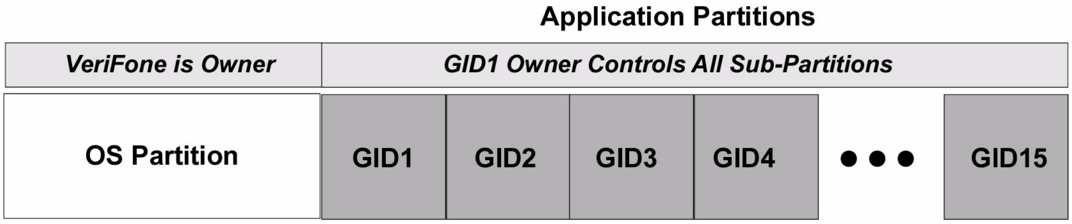


Figure 40 Omni 3600 Application Memory Partitions

NOTE The Omni 3600 operating system only enforces the rule that the main application always be stored in GID1. You can, for example, store a shared library in any file group. Rules for Storing Applications in Specific File Groups states reasons to follow the guidelines previously described for storing applications and libraries in specific file groups.

Rules for Storing Applications in Specific File Groups

Here are some important Omni 3600 file system features, as they relate to storing application files in specific file groups, and how these features affect the file authentication process:

- Most applications consist of more than one executable. For *each* executable to run on the terminal, it must be signed and authenticated.
- Although not enforced by the operating system, it is recommended that only one application be stored per file group in the application partition. Any number of executable files can, however, be stored in a single file group.
- Using the CONFIG.SYS *GO variable, you can specify only one application to automatically execute following a download and terminal restart. The defined application is usually the main application stored in Group 1 and called from the *GO variable in the CONFIG.SYS file in GID1.
- The main application stored in GID1 can access files, secondary applications, or function libraries stored in *any* other file group.
- The application downloaded into GID1 is *always* the primary application for the terminal. This application is owned by the primary terminal sponsor (sponsor A) in cases where there are multiple sponsors.
- The Group 1 application controls any and all secondary applications stored in terminal memory. That is, a secondary application can only be invoked by a RUN command issued by the Group 1 application.
- An application stored in Groups 2–15 can *only* access files stored in its own file group and in Group 15. For example, an application authorized by the sponsor to be authenticated in Group 4 can only access files and libraries stored in Group 4 and Group 15.
- If multiple applications (main and secondary) are to run on the same terminal, each .OUT and/or shared library file must have its own matching signature file.

Because each application is responsible for verifying its own data and prompt files, the other application files should have their own matching signature files. The master .OUT file should validate that these additional signature files are authenticate before the signature files are used.

- If two or more applications are to run on the same terminal, the signature files for the respective applications must be downloaded, together with the corresponding target files, into the specific file group(s) for which the applications are authorized. If an application is downloaded into a group for which is it not authorized, file authentication for that application fails.

  If, for example, Application B is downloaded into GID4, where it is authorized to run, but the signature files for all Application B executable files are downloaded into GID7, file authentication for Application B fails and it is not allowed to run.

- Each certificate contains an attribute to verify if an application is valid for a particular group.

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

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

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

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

If you intend to perform back-to-back downloads, as described in Chapter 4, all signature files *must* be retained in the Omni 3600 terminal's application memory, together with the target application files they authenticate.

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

Restrictions on Downloading Different File Types

A typical application download includes a variety of different file types. There are the following restrictions on how you can download different kinds of files to the Omni 3600 terminal and how files are stored in the file system:

File Type	Restriction
Certificate (*.crt)	*Must* be downloaded into the RAM of the target file group (GID1–GI15) selected in system mode.
Signature (*.p7s)	*Must* be downloaded into the RAM of the target file group (GID1–GID15) that you select in system mode.
Operating system	*Must* be downloaded into Group 1 RAM. When the OS files and related certificates and signature files are authenticated, they are automatically moved from Group 1 RAM into the Group 0 sub-partition, reserved for the operating system.

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

The FILESIGN.EXE File Signing Tool

To generate the signature files required for file authentication, you must sign all executable files and other files to be logically protected, using the FILESIGN.EXE software tool. This section discusses use of this tool, which is included in the Omni 3600 SDK.

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

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

NOTE

The file signing process for operating system files is done for Omni 3600 customers by the VeriFone CA. For operating system updates, VeriFone provides customers with a complete download package that includes all certificates and signature files required for authentication.

FILESIGN.EXE System Requirements

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

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

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

Operating Modes for FILESIGN.EXE

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

- **Command-line mode** (Windows PC DOS shell): Command-line mode is useful for application developers who perform batch file downloads and is convenient when using file download tools provided by VeriFone such as VeriCentre Download Management Module (DMM), ZonTalk 2000, and the direct download utility, DDL.EXE. In command-line mode, you can sign a batch of files in a single operation.
- **Graphical interface mode** (Windows NT or Windows 95): Use the FileSign dialog box (Figure 41) to select the file to sign and assign a name and destination location for the generated signature file on the host computer. When you run the FILESIGN.EXE tool under Windows, you can sign only one file at a time.

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

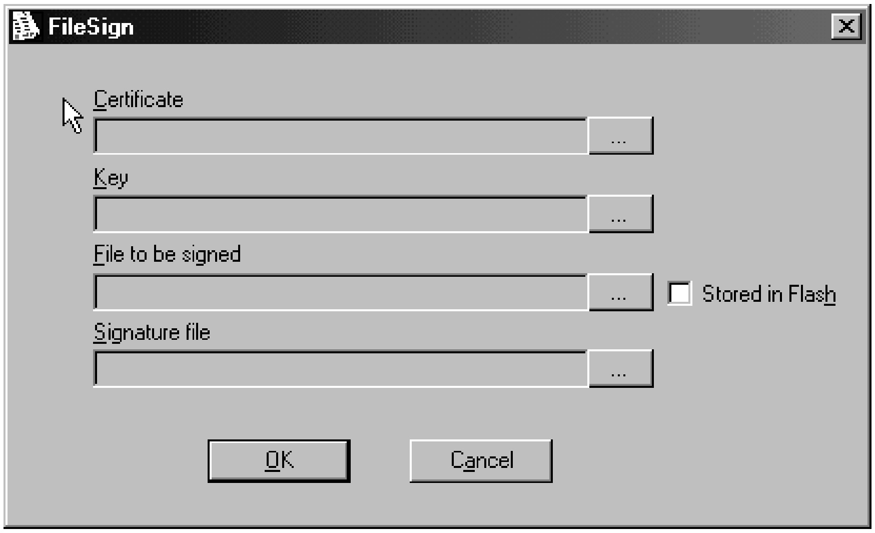


Figure 41 FileSign Dialog Box for FILESIGN.EXE Under Windows

NOTE

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

Command-Line Entries for FILESIGN.EXE

Table 20 lists and describes the *switches* that make up the command-line mode syntax for FILESIGN.EXE.

Table 20 Command-Line Mode Switches for FILESIGN.EXE[a]

Switch	Description	Requirements
-C, -c	Signer certificate file name (*.crt).	Required input for development terminals and deployment terminals. For development terminals, you can use the default signer certificate, K2SIGN.CRT. For deployment terminals, you must use the signer certificate issued by the VeriFone CA.
-K, -k	Signer private key filename (*.key).	Required input for development terminals and deployment terminals. For development terminals, you can use the default signer private key, K2SIGN.KEY. For deployment terminals, you must use the signer private key provided by the VeriFone CA.
-P, -p	Signer password for decrypting the signer private key.	Required input only for deployment terminals. The VeriFone CA issues and securely conveys this password to an authorized signer.
-F, -f	Name of the application file to sign (*.out, *.lib, or other file type).	Required for development terminals and for deployment terminals.
-S, -s	Name of the signature file (*.p7s) for FILESIGN.EXE to generate for the target application file.	Required for development terminals and for deployment terminals.
-L, -l	Specifies to store the target application file to sign and authenticate in the flash (drive F:) file system. If you do not use this switch to specify flash as the target file destination, it is stored by default in the RAM file system (drive I:).	Optional entry. This switch assigns an F: prefix to the name of the *.out or *.lib file to download, and also stores this information in the signature file as part of the special filetype attribute. **NOTE:** Signature files must be downloaded into the target file group's RAM. If the target file is authenticated, the corresponding *.p7s file is moved to the same memory area as the target file it authenticates. For example, if the target file is stored in flash (F:), its *.p7s file is moved into the flash file system. If, however, you set the *FA variable in the file group's CONFIG.SYS file to 0, all signature files are deleted from RAM when file authentication is complete.

[a] The switches described in Table 20 are not case-sensitive and can be entered on the command line in any order.

Command-Line Mode Syntax Example

In the FILESIGN.EXE command-line entry example below, please note that the syntax used applies to an Omni 3600 development terminal with the factory set of certificates, and not to a deployment terminal. The differences are as follows:

- The default signer certificate and default signer key file names that are provided by VeriFone as part of the Omni 3600 SDK are entered on the command line instead of customer-specific customer signer certificate and customer signer private key file names, and
- The switch for signer password (`-P password`) is not used, because a customer signer password is only required to sign and authenticate files for Omni 3600 deployment terminals being prepared for deployment.

Please note also how the command-line mode switches described in Table 20 are used in this example:

```
filesign -L -f file.out -s file.p7s -c k2sign.crt -k k2sign.key
```

- The `-L` switch indicates to store the application file in the flash file system instead of the target group's (default) RAM file system. (The target group for the download must be selected from system mode when the download is performed.)
- The `-f` switch indicates that the application file "`file.out`" must be signed by the FILESIGN.EXE tool.

  Executable files, such as *.out and *.lib files, must always be signed if they are to run on the terminal following a download. Depending on the application's logical security requirements, other types of files, such as data files and font files, may also need to be signed and are authenticated on download.
- The `-s` switch is followed by the name of the signature file to generate, `file.p7s`.
- The `-c` switch is followed by the name of the default signer certificate to use for file authentication with the development terminal, "`k2sign.crt`".
- The `-k` switch is followed by the name of the default signer private key file, `k2sign.key`. A signer private key is a required input to the file signing process for development terminals and for deployment terminals.

FILESIGN.EXE Graphical Interface Mode

When you execute FILESIGN.EXE in the Windows environment, the FileSign dialog box displays (see Figure 41).

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

- Press `ALT-C` or click on the **[...]** button to the right of the "Certificate" field to locate and select the certificate file (*.crt) you want to use to sign the file.
- Press `ALT-K` or click on the **[...]** button to the right of the "Key" field to locate and select the signer private key file (*.key).

- Press `ALT-F` or click on the [**...**] button to the right of the "File to be signed" field to locate and select the application file (*.out, *.lib, or other) to sign. If necessary, you can also modify the filename.

  If you want to store the file in flash memory on download to the terminal, check the "Stored in FLASH" checkbox. This adds the "F:" prefix to the target file name.

- Press `ALT-S` or click on the [**...**] button to the right of the "Signature file" field to enter a filename for the signature file to be generated. The filename extension must always be *.p7s. You can also choose another directory to store the generated signature file.
- When all entries are complete, press `ALT-O` or click the `OK` button to execute FILESIGN.EXE and generate the signature file. Or, press `ALT_A` or click Cancel to exit the FILESIGN.EXE utility.

When the necessary signature files are generated to authenticate the application or applications on the Omni 3600 terminal, you are ready to perform the application download procedure.

For more information about file authentication within the context of specific download procedures, please refer to Chapter 4.

CHAPTER 6

Troubleshooting and Service

This chapter discusses:

- typical problems encountered and their resolution,
- cleaning and maintenance,
- product specifications, and
- where to go for more information.

VeriFone follows stringent quality control standards in the manufacture of Omni 3600 terminals. Each unit that leaves the factory receives numerous tests to ensure quality and reliable operation. However, should you encounter a problem in operation, read this section for possible causes and solutions.

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

NOTE The Omni 3600 terminal comes equipped with tamper-evident labels. Do not, under any circumstance, attempt to disassemble the terminal.

Smart Card

The smart card implementation is a proprietary hardware solution that has no serviceable parts.

System Messages

Appendix A lists all system messages, including informational and error messages, and prompts, that may appear on the Omni 3600 display panel. For an explanation of a message that indicates some terminal malfunction occurred, please refer to the descriptions in Appendix A.

Use Remote Diagnostics to Identify Problems

Certain problems with a specific Omni 3600 terminal can be identified by a computer running a diagnostic test program. The diagnostic computer can be connected directly to a docked terminal by a cable or through a telephone line connection.

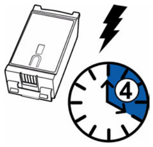
Troubleshooting

The troubleshooting guidelines provided in this section identify various problems and suggest appropriate corrective action(s). If you have problems operating your Omni 3600 terminal, please read through these troubleshooting examples. If the problem persists or if it is not described below, contact your local VeriFone representative for assistance.

Terminal Display Does Not Show Correct or Readable Information

1. Dock the Omni 3600 terminal in a base station.
2. Check all cable connections and verify that the telephone line is properly connected.
3. Recharge or replace the battery.
4. Check display contrast by performing a local diagnostic test of the terminal display in system mode (refer to System Mode Menu 5 in Chapter 3).
5. If the problem persists, contact your local VeriFone representative for assistance.

Smart Battery Will Not Charge



The smart battery must initially receive a *full* charge to set the battery's *charge capacity memory*. Allow the Omni 3600 terminal to remain connected to the power pack for a minimum of 2 hours, maximum of 4 hours to ensure the battery receives a full charge.

Since the smart battery has a 'memory' of its initial charge, this is the maximum charge it will take. If the initial charge was not long enough or insufficient, battery use hours are shortened.

NOTE Conserve battery power by turning the Omni 3600 terminal off when not in use. If the terminal is not to be used for several days, remove the battery from the terminal as it continues to discharge even when the terminal is turned off.

Telephone Line Connection Does Not Work Properly

1. Check the telephone line cord and all telephone connections.
2. If you are using a pass-through (Telset) connection, check that the telephone handset is seated properly in its cradle. Also, check the line using another telephone base unit. If the other telephone works, have the defective telephone repaired or replaced.
3. If you are using a direct (Telco) connection, check the Telco cable by plugging it into a working telephone and listening for a dial tone. If this test does not work, replace the Telco cable. If it is determined that the telephone line is dead, contact your local telephone company to check the status of the line.
4. If the problem persists, contact your local VeriFone representative for assistance.

Printer Does Not Work

1. Check battery status. The printer will not print if there is an insufficient charge remaining in the battery to complete the print operation.
2. Check if the printer is out of paper. Open the paper roll cover and install a new roll of printer paper.
3. Perform a test of the integrated thermal printer as described in Printer Test in Chapter 1.
4. If the problem persists, contact your local VeriFone representative for assistance.

Serial Port Does Not Work

1. The serial port on the back panel of the base station is identified by the "RS232" icon. Check that the device connected to the serial port has power and is functioning properly. If possible, perform a self-test on the device in question.
2. The cable connecting the optional device to the base station serial port may be defective. Try a different serial cable.
3. If the problem persists, contact your local VeriFone representative for assistance.

Terminal Does Not Process Transactions

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

Step 1: *Check the magnetic card reader*

1. Test the magnetic card reader as described in System Mode Menu 5 in Chapter 3.
2. Perform a test transaction using several different magnetic stripe cards to ensure the problem is not a defective card.
3. Make sure you are swiping cards properly. With the Omni 3600 card reader, the black, magnetic stripe on the card should face down, away from the keypad.
4. Process a transaction manually using the keypad instead of the card reader. If the manual transaction works, the problem may be a defective card reader. Contact your VeriFone distributor or service provider.
5. If the manual transaction does not work, proceed to Step 3.

Step 2: *Check the smart card reader*

1. Perform a test transaction using several different smart cards to ensure the problem is not a defective card.
2. Make sure you are inserting the cards properly. With the Omni 3600 smart card reader, the chip on the card should face down and inward.
3. Ensure the MSAM cards are properly inserted and the cardholders are properly secured as described in Install/Replace MSAM Cards in Chapter 1.
4. Process a transaction manually using the keypad instead of the card reader. If the manual transaction works, the problem may be a defective card reader. Contact your VeriFone distributor or service provider.
5. If the manual transaction does not work, proceed to Step 3.

Step 3: *Check the telephone line*

1 Connect to a working telephone and check for a dial tone. If there is no dial tone, replace the Telco cable.

2 If the problem appears to be with the telephone line, check with the party you are trying to call to see if their system is operational. If they are not experiencing difficulties with their line, contact the telephone company and have your line checked.

3 If the telephone line works, contact your local VeriFone representative for assistance.

Keypad Does Not Respond

1 Check the display panel. If it displays the wrong character or nothing at all when you press a key, follow the steps outlined in Terminal Display Does Not Show Correct or Readable Information.

2 If pressing a function key does not perform the expected action, refer to the user documentation for that application to be sure you are entering data correctly.

3 Perform a local diagnostic test of the keyboard in system mode (refer to System Mode Menu 5 in Chapter 3).

4 If the problem persists, contact your local VeriFone representative for assistance.

Cleaning and Care

This section discusses keeping the Omni 3600 terminal and Omni 3600 base clean.

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

CAUTION Never use thinner, acetone, trichloroethylene, or ketone-based solvents — these chemicals can deteriorate plastic or rubber parts.

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

Base Contacts

It is important that the exposed contacts in the docking cradle of the base stay clean and unbent. Gently swab the contacts with alcohol or contact cleaner to remove dirt.

CAUTION Avoid touching the contacts in the raised area in the center of the base. Finger oils tarnish contacts, causing bad connections. If the battery charge state or terminal power LEDs do not light when the terminal is docked or there is a high occurrence of bad or incomplete data transfers, clean the contacts.

Smart Card Reader

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

VeriFone Service and Support

For Omni 3600 terminal or base problems, contact your local VeriFone representative or service provider. Visit www.verifone.com to locate a representative near you.

For Omni 3600 product service and repair information:

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

For Omni 3600 supplies:

- VeriFone Online Store at www.store.verifone.com.
- (USA) VeriFone Customer Development Center, 1-800-837-4366, Monday–Friday, 7 A.M.–8 P.M. mountain time
- (International) Contact your local VeriFone representative

Return a Terminal, Omni 3600 Base, or Smart Battery

Before returning an Omni 3600 terminal, base, or smart battery to VeriFone, you must obtain a Merchandise Return Authorization (MRA) number. The following procedure describes how to return one or more terminals or base for repair or replacement (U.S. customers only):

NOTE International customers, please contact your local VeriFone representative for assistance with your service, return, or replacement.

1 Gather the following information from the printed labels (Figure 42) on the bottom of *each* Omni 3600 terminal and base station you are returning:
   - Product ID, including the model and part number. For example, “OMNI 3600” and “P096-XXX-XX”
   - Serial number (S/N XXX-XXX-XXX)

2 Contact VeriFone:
   - Within the U.S., call VeriFone toll-free at 800-VeriFone (837-4366)
   - Internationally, contact your local VeriFone representative. To locate a representative near you, visit www.verifone.com

3 Select the MRA option from the automated message. The MRA department is open Monday–Friday, 8 A.M.–8 P.M., eastern time.

4 Give the MRA representative the information gathered in Step 1.

If the list of serial numbers is long, you can fax the list, along with the information gathered in Step 1, to the MRA department. Include a telephone number where you can be reached and your fax number.

Please print clearly to the attention of the "VeriFone MRA Dept." and send your fax to 502-329-5947 (U.S.). You will be issued an MRA number and the fax will be returned to you.

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

5 Describe the problem and provide the shipping address to return the repaired or replacement unit.

6 Keep a record of the following items:

- Assigned MRA number(s)
- VeriFone serial number assigned to the Omni 3600 terminal or base station you are returning for service or repair
- Shipping documentation, such as airbill numbers used to trace the shipment
- Model(s) returned (model and part numbers are located on the bottom of each terminal or base station)

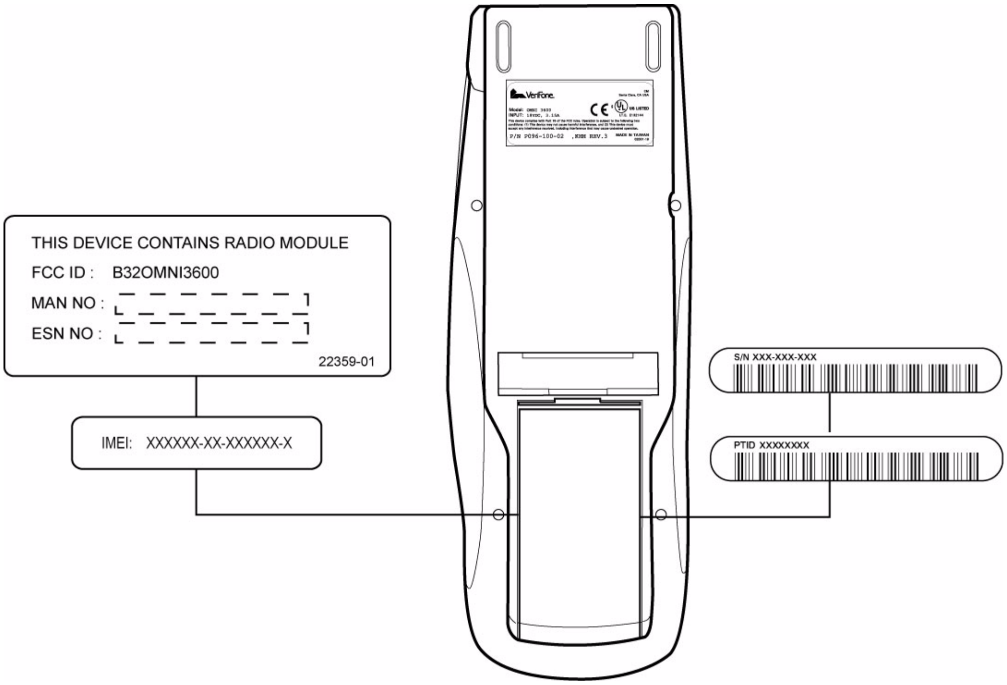


Figure 42 Information Labels on Bottom of Terminal

Specifications

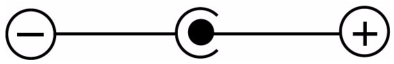
Power Requirements

DC power (all Omni 3600 terminals and base stations): DC: 19VDC; 3.16A

DC power pack (all Omni 3600 terminals and base stations):

- Input: 100–240 V ~ (100–240VAC); 50–60 Hz; 1.5A
- Output: 19VDC; 3.16A

Barrel connector polarity (all Omni 3600 terminals and base stations):



Environmental

Omni 3600 terminal:

- Operating temperature: 0° to 40° C (32° to 104° F)
- Storage temperature: – 18° to + 66° C (0° to 150° F)
- Relative humidity: 15% to 90%; no condensation

Base station:

- Operating temperature: 0° to 55° C (32° to 131° F)
- Storage temperature: – 40° to + 70° C (-40° to 158° F)
- Relative humidity: 15% to 90%; no condensation

Dimensions

- Height: 69 mm (2.72 inches)
- Width: 95 mm (3.74 inches)
- Length: 220 mm (8.64 inches)

Weight

- Terminal weight: 568 g (1.25 lb)
  - with battery installed: 681 g (1.5 lb)
  - with battery and paper roll installed: 710 g (1.56 lb)
- Shipping weight: 1264 g (2.78 lb): The shipping weight for the Omni 3600 terminal includes: shipping carton, one terminal, power pack and cable, one smart battery, paper roll, and one *Quick Installation Guide*.
- Base station weight: 378 g (0.83 lb)
- Shipping weight: 498 g (1.098 lb): The shipping weight for the Omni 3600 base station includes: shipping carton, one base station, one Telco cable, and one *Quick Installation Guide*.

Accessories and Documentation

Accessories and documentation available for the Omni 3600 are listed in this section. When ordering, please refer to the part number on the left.

How to Order

- VeriFone Online Store at www.store.verifone.com
- USA: VeriFone Customer Development Center, 1-800-837-4366, Monday–Friday, 7 A.M.–8 P.M., PST
- International: Contact your local VeriFone representative

Download Cables and Adapters

05651-xx	MOD10-MOD10 (base station-to-base station)
26263-xx	02xxx MOD10-PC DB25F (base station-to-PC)
26264-xx	02xxx MOD10-PC DB9F (base station-to-PC)
22536-01	MOD10 adapter (terminal-to-terminal/PC/telephone)

Cables for Optional Peripherals

07041-xx	MOD10-MDIN9 (CR 600/CR 1000*i* check readers)

Base Station

P096-201-00	Base station

Telco Cable

00124-17	2.1-m (7') telephone line cord, black color, with modular RJ11-type connectors

Antenna

Contact your VeriFone distributor to determine the exact antenna for your Omni 3600 terminal.

22066-XX	Replacement antenna.

Smart Battery

22044-02	12V battery pack

Power Pack

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

22161-01	DC power pack (universal)
21973-01	Power cable (U.S.)

Thermal Printer Paper

CRM0043	Standard-grade thermal printer paper, 57-mm (2.25”) width, 7.62-m (25’) length; single roll

VeriFone Cleaning Kit

02746-01	Cleaning kit

Documentation

22377	*Omni 3600 Quick Installation Guide*
22378	*Omni 3600 Base Station Quick Installation Guide*
22060	*Omni 3600 Installation Guide*
19733	*Verix Operating System Programmer’s Manual*

Appendix A

System Messages

This appendix describes error and information messages that may appear when the Omni 3600 terminal is in system mode. For ease of use, these messages are grouped alphabetically. These messages include those:

- displayed digital certificate and signature file download to the terminal
- processed by the file authentication module
- displayed when using the file compression module of the VeriCentre DMM terminal management and download tool

```
ALREADY DEBUGGING
```

This message displays when DEBUGGER F4 in SYS MODE MENU 4 is selected and the debugging monitor program, DBMON.OUT, is already running on the terminal.

```
APPLICATION
ALREADY RUNNING
PLEASE RESTART
```

This message displays when an attempt was made to invoke a system mode function not allowed to execute while an application is running on the terminal. The requested function is not invoked, and the application continues to run in the background.

Some system mode functions, such as setting the date and time, can be performed in this mode even with the application running in background, and this message does not display. For other system mode functions, such as downloads and RAM or flash clear operations, you must restart the terminal and re-enter system mode *before* the application starts (within three seconds).

To restart the terminal and enter system mode:

1. Press the cancel key until the SYS MODE MENU 1 displays.
2. Select RESTART F4.
3. Enter system mode within three seconds of seeing the VeriFone copyright screen—before the application begins—by simultaneously pressing F2 and F4.

```
DEVICE BUSY
PLEASE RESTART
STAND ALONE
```

This message displays when a system mode function queried an internal device that is busy. This message can also occur if you entered system mode with an application running.

For example, if the application opened the magnetic stripe card reader and you try to invoke the card reader diagnostic through MAG CARD READER F4 in SYS MODE MENU 5, the attempt fails and this message appears.

Restart the terminal and enter system mode before the application starts.

```
DOWNLOAD NEEDED
```

The operating system is unable to start the application specified in the *GO variable for the following reasons:

- No application resident in the terminal.
- The *GO variable is not set in the Group 1 CONFIG.SYS file.
- The application file specified in the *GO variable does not exist in Group 1. (The *GO variable cannot specify an application file stored in a file group other than Group 1.)
- The application or a shared library used by the application either does not exist or is not authenticated. All executables must be authenticated to run on the terminal.
- There is not enough memory available to run the application requested in the *GO variable.

```
FLASH CHKSUM ERROR
```

A corrupt file is detected in the flash file system during terminal start up, after power-on, or during restart. This message may indicate a hardware problem or the error condition may be resolved through another download of the file.

```
LOAD DBMON.OUT
```

The DEBUGGER F4 option in SYS MODE MENU 4 was selected. The debugging monitor program, DBMON.OUT, is included in the SDK, but is not stored in the terminal memory of a factory unit. To use the debugging tool, you must sign, download, and authenticate the DBMON.OUT application.

```
LOAD TERMINAL
MANAGEMENT AGENT
```

This message displays if you select REMOTE DIAGS F2 in SYS MODE MENU 4 and the (optional) Terminal Management Agent (TMA) software is not resident in the Omni 3600 terminal. The TMA software is required to perform remote diagnostics. For more information about support for remote diagnostics, contact your VeriFone service provider.

```
MODL  O3600M
CTRY  GEN
KEYPAD          0
DISPLAY         128064
MAG RDR         3
PRINTER         1
↑    ↓
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3 and press the PF2 key (below the down arrow) two times. This third display, in a series of four, provides the following information about the current terminal configuration:

- MODL: The model number assigned to the terminal on manufacture.
- CTRY: The name or abbreviation (up to 42 characters) of the country of manufacture.
- KEYPAD: A code (0–5) to indicate keypad type.
- DISPLAY: A code (000000, 000001, or xxxyyy) to indicate display unit type.
- MAG RDR: A code (0–4) to indicate magnetic stripe card reader type.
- PRINTER: A code (0 or 1) to indicate that a thermal printer is integrated.

```
PINPAD          1
LIFE            730810
RSET            020829000536
RCNT            198
MODEM CTRY      ?
↑    ↓
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3 and press the PF2 key (below the down arrow) three times. This fourth display, in a series of four, provides the following information about the current terminal configuration:

- PINPAD: A code (0 or 1) to indicate that a PIN pad is integrated.
- LIFE: The number of seconds the terminal has run since first powered on.
- RSET: The date and time when the terminal was last reset, in *yymmddhhmmss* format.
- RCNT: The total number of times the terminal has been reset.
- MODEM CTRY: The current two-digit modem country code setting. For additional information about modem country codes, see the *Verix Operating System Programmer's Manual*.

```
PLEASE TRY AGAIN
```

This message displays if you enter an incorrect system mode password or an incorrect file group password. Repeat the password entry and press the enter key.

```
RAM        1024
FLASH      2048
SERNO      024-546-755
PTID       12443328
PART       P096-100-02
VERS       6
↑   ↓
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3 and press the PF2 key (below the down arrow) to display the next screen. This second display, in a series of four, provides the following information about the current terminal configuration:

- RAM: The RAM (SRAM) size in kilobytes (KB).
- FLASH: The flash memory size in KB.
- SERNO: The serial number assigned to the terminal on manufacture.
- PTID: The permanent terminal ID assigned to the terminal on manufacture. If no PTID is assigned, the default value is “12000000.”
- PART: The part number assigned to the terminal on manufacture.
- VERS: The hardware version number assigned to the terminal on manufacture.

```
RAM CHKSUM ERROR
```

A corrupt file is detected in the RAM file system at terminal start up, after power-on, or during restart. This message may indicate a hardware problem or the error condition may be resolved through another download of the file.

```
RAM FILES     5
 INUSE        31686
 AVAIL        960630
FLASH FILES   1
 INUSE        3232
 AVAIL        1766232
↑   ↓
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3. This first display, in a series of four, provides the following information about the current terminal configuration:

- INUSE: The number of bytes of memory space currently being used in the RAM file system (RAM FILES) or the flash file system (FLASH FILES).
- AVAIL: The number of bytes of memory space currently available in the RAM file system (RAM FILES) or the flash file system (FLASH FILES).

```
RECEIVING NOW
```

In back-to-back downloads, the *Target* (receiving) terminal displays this message on data transfer initiation when pressing the asterisk key (*). To stop the upload, press the cancel key on either terminal (Gold or Target).

```
SYS MODE CLEAR
CLEARING FLASH
PLEASE WAIT
```

This message displays when you select FLASH FILES F4 in SYS MODE MENU 2 and select CLEAR GROUP_nn F2 or CLEAR ALL FILES F3 to clear files from the flash memory of a specific file group (Group 1–15) or from the entire flash memory. This message remains until the files either within the file group or all files in flash are deleted.

If you select CLEAR ALL FILES F3, only application file(s) stored in the flash-based file system—not the files stored in RAM—are erased.

```
SYS MODE CLEAR
CLEARING RAM
PLEASE WAIT
```

This message displays when you select RAM FILES F3 in SYS MODE MENU 2 and select CLEAR GROUP_nn F2 or CLEAR ALL FILES F3 to clear files from the RAM of a specific file group (Group 1–15) or from the entire RAM. This message remains until the files either within the file group or all files in RAM are deleted.

If you select CLEAR ALL FILES F3, only the application file(s) stored in RAM—not the files stored in flash—are erased. If you erase the main application stored in the RAM file system, the terminal displays DOWNLOAD NEEDED after the VeriFone copyright screen on terminal restart.

Note that clearing the RAM does *not* erase the keyed variable settings stored in protected CONFIG.SYS records—that is, in records that start with an asterisk (*).

```
SYS MODE DEFRAG
RECLAIMING FLASH
PLEASE WAIT
```

This message displays when you select FLASH FILES F4, followed by DEFRAG F4 in SYS MODE MENU 2 to perform defragmentation (coalesce) of the flash memory file system. PLEASE WAIT remains displayed during the defragmentation process. On successful completion, the terminal automatically restarts.

```
SYS MODE DOWNLOAD
DOWNLOADING NOW
```

An application is being downloaded to a *receiving* Omni 3600 terminal from a host PC, either directly over a serial cable or by telephone. This message also displays on the Target terminal in a back-to-back download.

The terminal displays a series of asterisks (*) to indicate the progress of the download (each asterisk represents 10% of the file is downloaded). When ten asterisks appear, the data transfer is complete.

```
SYS MODE EDIT

*KEY                    KEY F2
                      VALUE F3
↑  ↓  ←  →
```

This message displays when you select EDIT F3 in SYS MODE MENU 3 to invoke the keyed file editor to edit files (such as, CONFIG.SYS), as follows:

- FILE: Make the appropriate menu selections to select or create a file to edit
- KEY: Search for a specific keyed record
- VALUE: Add a new value for a selected keyed record

```
SYS MODE ERR LOG
TYPE
FRAME
USP
TCB
TIME
```

This information appears when you select ERROR LOG F3 in SYS MODE MENU 4. The following information helps developers interpret the cause of the most recent unrecoverable software error that occurred on the terminal:

- TYPE: The error type code. For a description of error types (codes 2–11), refer to Chapter 3.
- FRAME: The value of the stack frame.
- USP: The value of the user stack pointer.
- TCB: The value of the task control block.
- TIME: The binary-coded decimal clock time when the last error occurred in *yymmddhhmmss* format.

If you report a system error to VeriFone, you may be asked to provide the information displayed in this screen. For detailed information about the error log function and the terms listed above, please refer to the *Verix Operating System Programmer's Manual*.

```
SYS MODE KBD TEST
KEYCODE nn
```

This message displays when you initiate a local diagnostic test of the terminal keyboard through KEYBOARD DIAG F3 in SYS MODE MENU 5. When invoked, the decimal ASCII keycode of each key you press (test) appears to the right of KEYCODE. For example, pressing the 1 key on the terminal keypad displays the corresponding ASCII keycode, 31.

```
SYS MODE PASSWORD
FILE GROUP nn
GROUP nn PASSWORD
```

This message displays when you initiate the procedure for modifying existing system mode passwords through PASSWORDS F4 in SYS MODE MENU 3. Additional menu options display to let you change the password of a file group (F2) or the system mode password (F3).

```
SYS MODE PASSWORD
NEW
AGAIN
PASSWORD CHANGED
```

This message displays when you select PASSWORDS F4 in SYS MODE MENU 3 to modify the existing system mode password.

- NEW: Make the appropriate menu selections to enter the new password.
- AGAIN: Repeat the entry to confirm the new password.
- PASSWORD CHANGED: Displays when the new password is accepted.

```
SYS MODE UPLOAD
UPLOADING NOW
```

In a back-to-back download, the *Gold* (sending) terminal displays this message when you initiate an upload from the receiving terminal. To stop the upload, press the cancel key on either terminal.

```
TRK1:
TRK2:
TRK3:
```

When you invoke a local system mode diagnostic test of the magnetic stripe card reader, status information appears for data track (TRK1, TRK2, and TRK3) on a magnetic stripe card.

To perform this test, select MAG CARD DIAG F4 in SYS MODE MENU 5 and swipe a magnetic stripe card through the card reader:

- NO DATA or VALID DATA: A successful test of the magnetic-stripe card reader displays for each track. Actual data stored on data tracks does not display.
- An error condition generates one of the following error messages for each track with an error:

- NO DATA
- NO START
- NO END
- LRC ERR
- PARITY ERR
- REVERSE END

Press the cancel key to end the local diagnostic test of the card reader.

```
** UNZIP Error n
                 xxxxxx
                 yyyyyy
```

If you are using the file compression module in DMM, information similar to what is shown above appears when an error occurs during file extraction from a downloaded ZIP archive. Note the error number and error codes (xxxxx and yyyyy) and try to download the archive again.

```
UNZIP stuff.zip
    myprog.out
    mydata.txt
    6x8.fon
    10x14.fon
    ...
```

If you are using the file compression module in DMM, information similar to what is shown above appears when a compressed file archive downloaded to the terminal decompresses (unzipped), and the files extracted from the archive.

```
** VERIFYING FILES **
Check Certificate
(or System Certificate)

filename.crt

** Authentic **
(or ---Failed---)
```

This message displays when the file authentication module detects a new digital certificate, together with the filename of the certificate to authenticate, during a download to the Omni 3600 terminal. If the authentication is successful, Authentic displays; otherwise, Failed displays for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated.

This message remains on screen until all new certificates are checked, one by one. In special cases where system certificates are being installed, System Certificate displays instead of Check Certificate.

```
** VERIFYING FILES **
Compare Signature

myfile.p7s
myfile.out

** Authentic **
(or ---Failed---)
```

The file authentication module detected a new signature file, together with the application file for which the signature file was generated, during a download to the Omni 3600 terminal. If the authentication is successful, Authentic displays; otherwise, Failed appears for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated.

This message remains on screen until all new signature files are checked. New digital certificates are always checked first, followed by new signature files, in an uninterrupted process.

APPENDIX B

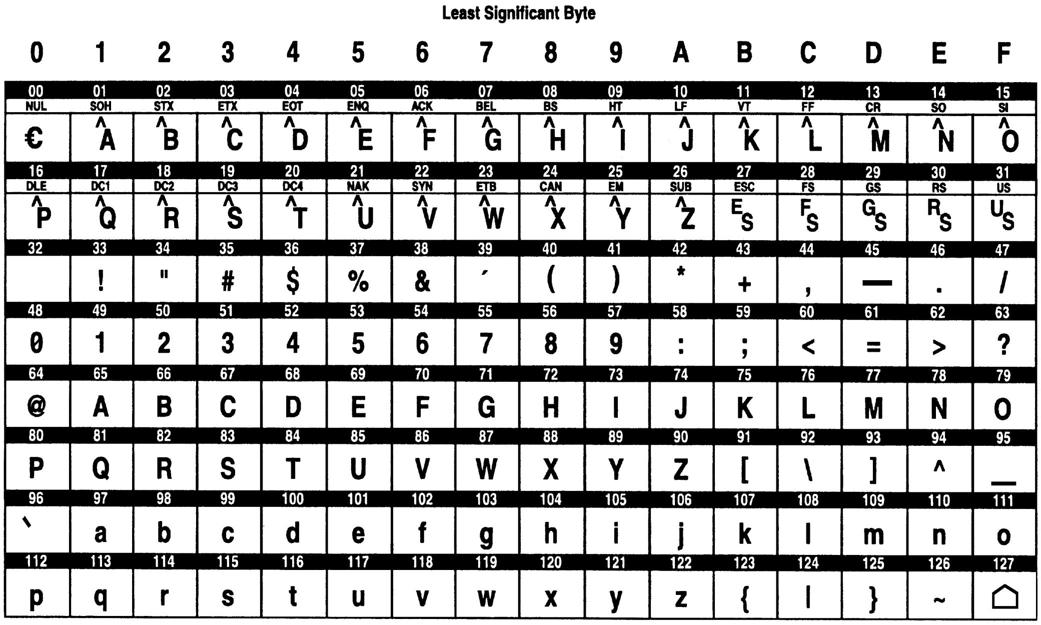
ASCII Table

An ASCII table for the Omni 37xx display is in Figure 43. The table is formatted for quick reference, as follows:

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

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

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



Least Significant Byte

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00 NUL €	01 SOH ^A	02 STX ^B	03 ETX ^C	04 EOT ^D	05 ENQ ^E	06 ACK ^F	07 BEL ^G	08 BS ^H	09 HT ^I	10 LF ^J	11 VT ^K	12 FF ^L	13 CR ^M	14 SO ^N	15 SI ^O
16 DLE ^P	17 DC1 ^Q	18 DC2 ^R	19 DC3 ^S	20 DC4 ^T	21 NAK ^U	22 SYN ^V	23 ETB ^W	24 CAN ^X	25 EM ^Y	26 SUB ^Z	27 ESC ES	28 FS FS	29 GS GS	30 RS RS	31 US US
32	33 !	34 "	35 #	36 $	37 %	38 &	39 ´	40 (	41)	42 *	43 +	44 ,	45 —	46 .	47 /
48 0	49 1	50 2	51 3	52 4	53 5	54 6	55 7	56 8	57 9	58 :	59 ;	60 <	61 =	62 >	63 ?
64 @	65 A	66 B	67 C	68 D	69 E	70 F	71 G	72 H	73 I	74 J	75 K	76 L	77 M	78 N	79 O
80 P	81 Q	82 R	83 S	84 T	85 U	86 V	87 W	88 X	89 Y	90 Z	91 [	92 \	93]	94 ^	95 _
96 `	97 a	98 b	99 c	100 d	101 e	102 f	103 g	104 h	105 i	106 j	107 k	108 l	109 m	110 n	111 o
112 p	113 q	114 r	115 s	116 t	117 u	118 v	119 w	120 x	121 y	122 z	123 {	124 |	125 }	126 ~	127 ⌂

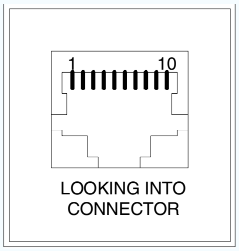
Figure 43 ASCII Table for the Learning Products Template Version 2.1 Display

APPENDIX C

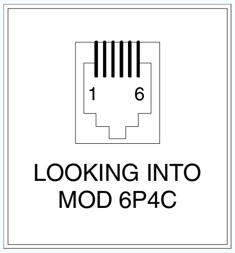
Omni 3600 Base Unit Port Pinouts

The tables in this appendix list pinouts for the Omni 3600 base unit connectors.

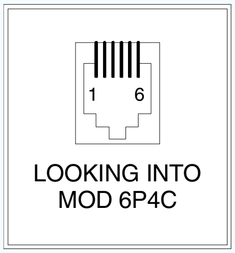
RS232 Port

Connector	Pin	Function	Description
	1	TXCLK	Transmit clock signal
	2	NC	No connection
	3	CD	Carrier detect
	4	DTR	Data terminal ready
	5	GND	Power ground
	6	/RXD	Receive data
	7	/TXD	Transmit data
	8	CTS	Clear to send
	9	RTS	Request to send
	10	RXCLK	Receive clock signal

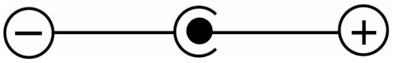
Telco Port

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

Telset Port

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

Barrel Connector Polarity



Glossary

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

Application ID An alphanumeric code that identifies an application program downloaded to a terminal from a download computer. For ZonTalk 2000 application downloads, the application ID is stored in the CONFIG.SYS record which begins with the *ZA key. An Omni 3600 application ID can be up to 21 characters long. For VeriCentre Download Management Module, the application ID, as well as other CONFIG.SYS variables, may differ from those used for ZonTalk 2000.

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

Application prompt The information shown on the terminal's display panel when power is applied to the terminal, assuming that an application program has already been downloaded into the terminal's memory and authenticated by the Omni 3300 file authentication module. The application prompt often contains a graphical logo, and date and time, but it can consist of anything the programmer chooses for that purpose.

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

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

Bar code Optical binary code imprinted on merchandise in retail stores. To support specific applications, an optional bar code reader can be attached to the Omni 3600 to read and process bar codes.

Bar code reader A pencil- or wand-shaped optical scanner used to read bar codes. To read the code, you drag the tip of the bar code reader across the length of the bar code, in a left-to-right or right-to-left direction.

Base station This unit allows the Omni 3600 terminal to obtain land-line connections and perform back-to-back downloads.

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

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

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

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

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

Byte A term developed to indicate a measurable number of consecutive binary digits that are usually operated on as a unit. For the Omni 3600, a byte consists of eight bits. See also Bit.

Calendar/clock chip A microchip inside the Omni 3600 terminal which keeps track of the current date and time.

Card reader Also called *magnetic stripe card reader*. The slot on the right side of the Omni 3600 terminal that automatically reads data stored in the magnetic stripe on the back of a specially-encoded card when you swipe the card through the slot.

Carrier Usually, an analog signal that is selected to match the characteristics of a particular transmission system. The carrier signal on a phone line is modulated with frequency or amplitude variations to allow a terminal to transmit or receive data using a modem. A carrier signal transmits data from a host computer to an Omni 3600 terminal over an analog telephone line.

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

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

CONFIG.SYS file A special keyed file that is stored in terminal memory and which contains system and application configuration parameters. Each record in a CONFIG.SYS file is identified by an alphanumeric search key. In the Omni 3600 file system, there is one password-protected CONFIG.SYS file per file group (Groups 1–15). You can modify CONFIG.SYS records using the keyed file editor. See Keyed file editor.

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

Data Information prepared, often in a particular format, for a specific purpose. Data is to be distinguished from applications or program instructions. In the Omni 3600 terminal, application files and data files can be stored in RAM or flash memory.

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

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

Dedicated line A leased or private telephone line that is used for a particular communications purpose, such as to connect an Omni 3600 base station to a host computer. See Leased line.

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

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

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

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

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

Display The screen on the Omni 3600 terminal that shows numerals, letters, and punctuation symbols in selected fonts, graphics in various formats, information entered from the keypad, as well as system prompts and messages.

Docking/Docked The act of placing a Omni 3600 terminal in the docking cradle of a base station. The following can occur when the Omni 3600 terminal is docked:

- A telephone line connection can be established to transfer data and files and effect downloads
- The smart battery can be recharged (the battery can also be recharged through the terminal)
- You can perform back-to-back downloads by connecting to another base station with a docked terminal

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

DTMF *Dual-tone multi-frequency*. The ordinary dial tone on a telephone line.

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

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

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

Flash memory An area of non-volatile memory where files can be stored. The Omni 3600 also has a RAM-based file system. Files can be stored in RAM (drive `I:`) or in flash (drive `F:`) memory area of any file group (Groups 1–15).

Host computer Also called a *download* computer. The primary or controlling computer in a multiple computer operation. Also, a computer—usually a PC running Windows NT or Windows 95 or 98—used to prepare programs for download to POS terminals. Host computers are also used to process transactions that originate from a distributed network of POS terminals.

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

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

Keyed file character set A limited set of 95 ASCII characters, from 00h to 5Fh (or 0 to 95 decimal), that is used by the Omni 3600 keyed file editor. Although an application program can download all 95 characters in this set, you can only enter 50 of these characters from the terminal keypad: 0–9, A–Z, and 14 special characters.

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

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

Keypad A small keyboard or section of a keyboard containing a smaller number of keys, generally those used in simple calculators. The 16-key core keypad of the Omni 3600 terminal is used to enter data and perform operations.

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

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

Local functions Operations performed at the terminal only and not in interaction with a host computer. For the Omni 3600, local functions such as internal diagnostics are performed in system mode. See Chapter 3.

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

Memory A device or medium that can retain information for subsequent retrieval. The term is most frequently used to refer to the internal storage of a computer (or a terminal) that can be directly addressed by operating instructions. In the Omni 3600, files can be stored in battery-backed RAM or in non-volatile flash memory.

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

Modem *Modulator/demodulator*. A device that converts a digital bit stream into an analog signal to transmit over an analog communication channel (modulation), and converts incoming analog signals back into digital signals (demodulation). The internal modem in the Omni 3600 base station lets the terminal communicate with a host computer over a dial-up telephone line.

Non-volatile memory A memory or storage medium that retains data in the absence of power so that the data is available when power is restored. For the Omni 3600, application files and data files can be stored in battery-backed RAM or non-volatile flash memory, according to the requirements of the application.

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

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

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

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

Password A group of characters that identify a user to the system so that they can gain access to the system or part of that system. Passwords are used to ensure the security of computer systems by regulating the amount of access freedom. The password used to enter system mode is called the *system mode password*. In the Omni 3600 file system, each file group (Groups 1–15) also has its own password.

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

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

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

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

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

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

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

PTID *Permanent terminal ID*. An optional identifier that can be permanently assigned to a VeriFone terminal at the factory, upon customer request. The PTID has two parts: a 2-digit manufacturer ID (12 for VeriFone) and a unique 8-digit terminal ID. If no PTID is assigned, the default PTID value is 1200000000.

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

RAM *Random-access memory*. The type of memory in which storage locations are addressable and can therefore be accessed in any order. In the Omni 3600 terminal, the RAM (or SRAM) is commonly used to store applications and temporary data generated during a transaction.

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

Remote host computer A host computer connected to a Omni 3600 base station over a dial-up telephone line to download files or data, or to process transactions. The opposite of remote is *local*.

RS232 Also RS-232C. A widely used standard interface that covers the electrical connection between data communication equipment, such as a modem, and data terminal equipment, such as a microcomputer or computer terminal. The RS232 interface standard was developed by the EIA (Electronic Industries Association) and is essentially equivalent to the CCITT's V.24 interface.

Scroll To move all or part of the information displayed on a screen up or down, left or right, to allow new information to appear. For the Omni 3600, text that does not fit entirely within the display area can be scrolled to the left or right using the pound (#) and asterisk (*) keys.

Search key Also called *key*. In the Omni 3600, a short character string used by an application to identify a keyed file record stored in CONFIG.SYS file(s). For example, *ZA or *OT. A *keyed file record* consist of two parts: a search key to identify the record, and the variable data stored in the record. See also Keyed file record and CONFIG.SYS file.

Serial port A connection point through which digital information is transferred one digital bit at a time. Same as *serial interface*. The Omni 3600 base station has one serial port, labeled RS232. The main serial port on a download computer is usually assigned the device ID, COM1.

Signature file A digital file with the filename extension *.p7s generated in an industry-standard format by the file signing tool, FILESIGN.EXE. The output of the file signing tool is a signature file in an industry-standard format.

SRAM See RAM.

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

Swipe The action of sliding a magnetic stripe card through a terminal card reader. The Omni 3600 card reader has a bi-directional swipe direction. The user must hold the card so that the magnetic stripe is faces down and towards the printer.

System Mode For the Omni 3600, system mode temporarily disables normal mode operations, allowing you to perform local functions such as downloads, diagnostics, and other operations that cannot be performed while the application program is running.

At startup, the terminal displays a copyright notice screen that shows the version of Omni 3600 system firmware stored in terminal flash memory, the date it was loaded into the terminal, and the copyright notice. This screen appears for three seconds. To enter system mode, simultaneously press the F2 and F4 keys during this three-second period. Pressing any other key(s) during that period resets the copyright notice screen to display an additional three seconds.

See also Local functions and Normal Mode.

System mode password A unique set of characters entered by the user to access the system mode local functions of the terminal. A default password is supplied with each terminal. For the Omni 3600 terminal, the default system password set at manufacture is: Z66831.

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

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

Telephone jack Also, telephone line wall jack. Insert a modular connector into a telephone jack or receptacle. Also, modular-type sockets for connecting telephone line cords. The Omni 3600 base station has two RJ45-type telephone jacks on the back panel: The TELSET jack is used for pass-through connections; the TELCO jack is used for a direct connection to a telephone line wall jack.

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

Terminal Any device capable of sending and receiving data over a data link, such as a telephone line or a RS-232 cable. Some terminals, such as the Omni 3600, can print receipts and display information and graphics on a screen.

Terminal ID An alphanumeric code that identifies a terminal to a download computer. In this way, the download computer can determine what data or application programs to download to that terminal. For ZonTalk 2000 downloads, the Omni 3600 terminal ID is stored in the *ZT record in the CONFIG.SYS file. This variable should not exceed 10 characters in length. Not the same as PTID

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

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

Track 1, 2, or 3 data Information stored on tracks 1, 2, or 3 of a debit or credit card magnetic stripe, which can be read by a magnetic card reader device, such as the one that is integrated in the Omni 3600 terminal.

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

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

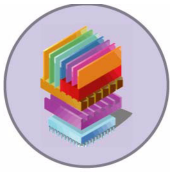
Volatile memory A type of memory where the contents are destroyed if the power supply to the memory is interrupted. When volatile memory, such as SRAM, is used for crucial applications, it is often back up by battery-supplied power. Compare with Non-volatile memory.

Wireless The Omni 3600 terminal a continuous, virtual link through a radio connection to upload transaction data files to and download applications and OS updates from your merchant business processor. This connection is stand-alone, not requiring unit docking. See Docking/Docked.

INDEX

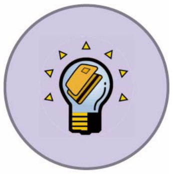
VeriFone, Inc.
2455 Augustine Drive
Santa Clara CA 95054-3002
Tel: 800-VeriFone (837-4366)
www.verifone.com

VERIX
OPERATING
ENVIRONMENT



SOFTPAY
E-PAYMENT
APPLICATION

VERIX
DEVELOPER
TOOLKIT
DEVELOPMENT
TOOLS



VERISHIELD
SECURITY
ARCHITECTURE

OMNI 37XX
HAND-OVER-COUNTER
MULTI-APPLICATION
APPLIANCES

OMNI 33XX
MULTI-APPLICATION
APPLIANCES

OMNI 3600
HAND-HELD
RADIO MODEM
APPLIANCES

Omni 3600

Reference Manual

VERICENTRE
APPLIANCE
MANAGEMENT
SUITE