HEWLETT® PACKARD

HP Encryption Smart Card Security System

User's Guide

Copyright and trademark information

Windows 95 and Windows NT are registered trademarks of the Microsoft Corporation.

Limited warranty

The information contained in this document is subject to change without notice.

Hewlett-Packard Company makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Hewlett-Packard Company shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this document.

In addition to the Limited Warranty Statement provided in the Support and Service booklet, and to the extent permitted by local law, Hewlett-Packard Company expressly disclaims any warranty that this product will be error-free. Hewlett-Packard Company makes no warranty that any data stored or encrypted by this product will be recoverable or accessable, or that access provided by this product will be maintained.

HP Software Product License Agreement

CAREFULLY READ THIS LICENSE AGREEMENT BEFORE PROCEEDING TO OPERATE THIS EQUIPMENT. RIGHTS IN THE SOFTWARE ARE OFFERED ONLY ON THE CONDITION THAT THE CUSTOMER AGREES TO ALL TERMS AND CONDITIONS OF THE LICENSE AGREEMENT. PROCEEDING TO OPERATE THE EQUIPMENT INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE WITH THE TERMS OF THE LICENSE AGREEMENT, YOU MUST NOW EITHER REMOVE THE SOFTWARE FROM YOUR HARD DISK DRIVE AND DESTROY THE MASTER DISKETTES, OR RETURN THE COMPLETE COMPUTER AND SOFTWARE FOR A FULL REFUND.

PROCEEDING WITH CONFIGURATION SIGNIFIES YOUR ACCEPTANCE OF THE LICENSE TERMS.

UNLESS OTHERWISE STATED BELOW, THIS HP SOFTWARE PRODUCT LICENSE AGREEMENT SHALL GOVERN THE USE OF ALL SOFTWARE THAT IS PROVIDED TO YOU, THE CUSTOMER, AS PART OF THE HP COMPUTER PRODUCT. IT SHALL SUPERSEDE ANY NON-HP SOFTWARE LICENSE TERMS THAT MAY BE FOUND ON-LINE, OR IN ANY DOCUMENTATION OR OTHER MATERIALS CONTAINED IN THE COMPUTER PRODUCT PACKAGING.

Note: Operating System Software by Microsoft is licensed to you under the Microsoft End User License Agreement (EULA) contained in the Microsoft documentation.

The following License Terms govern the use of the software:

USE. Customer may use the software on any one computer. Customer may not network the software or otherwise use it on more than one computer. Customer may not reverse assemble or decompile the software unless authorized by law.

COPIES AND ADAPTATIONS. Customer may make copies or adaptations of the software (a) for archival purposes or (b) when copying or adaptation is an essential step in the use of the software with a computer so long as the copies and adaptations are used in no other manner.

OWNERSHIP. Customer agrees that he/she does not have any title or ownership of the software, other than ownership of the physical media. Customer acknowledges and agrees that the software is copyrighted and protected under the copyright laws. Customer acknowledges and agrees that the software may have been developed by a third party software supplier named in the copyright notices included with the software, who shall be authorized to hold the Customer responsible for any copyright infringement or violation of this Agreement.

PRODUCT RECOVERY CD-ROM. If your computer was shipped with a product recovery CD-ROM: (i) The product recovery CD-ROM and/or support utility software may only be used for restoring the hard disk of the HP computer with which the product recovery CD-ROM was originally provided. (ii) The use of any operating system software by Microsoft contained in any such product recovery CD-ROM shall be governed by the Microsoft End User License Agreement (EULA).

TRANSFER OF RIGHTS IN SOFTWARE. Customer may transfer rights in the software to a third party only as part of the transfer of all rights and only if Customer obtains the prior agreement of the third party to be bound by the terms of this License Agreement. Upon such a transfer, Customer agrees that his/her rights in the software are terminated and that he/she will either destroy his/her copies and adaptations or deliver them to the third party.

SUBLICENSING AND DISTRIBUTION. Customer may not lease, sublicense the software or distribute copies or adaptations of the software to the public in physical media or by telecommunication without the prior written consent of Hewlett-Packard.

TERMINATION. Hewlett-Packard may terminate this software license for failure to comply with any of these terms provided Hewlett-Packard has requested Customer to cure the failure and Customer has failed to do so within thirty (30) days of such notice.

UPDATES AND UPGRADES. Customer agrees that the software does not include updates and upgrades which may be available from Hewlett-Packard under a separate support agreement.

EXPORT CLAUSE. Customer agrees not to export or re-export the software or any copy or adaptation in violation of the U.S. Export Administration regulations or other applicable regulation.

U.S. GOVERNMENT RESTRICTED RIGHTS. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013. Hewlett-Packard Company, 3000 Hanover Street, Palo Alto, CA 94304 U.S.A. Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Contents

Understanding the HP Encryption Smart Card Security System

What is the Encryption Smart Card Security System?

The Encryption Smart Card Security System is an accessory for your OmniBook that uses smart card technology to provide smart card protected logon for Windows NT and strong file encryption on Windows NT and Windows 95. The Encryption Smart Card Security System consists of a smart card reader which inserts into a PCMCIA slot on your OmniBook, and a smart card in which to store information that ensures that only you can access your OmniBook and read the files you have chosen to protect.

What is a smart card?

A smart card is a credit-card-sized card which carries a microchip containing memory and a microprocessor. The card's microchip lies beneath gold contact pads and when the card is inserted in a smart card reader, the contents of the microchip can be read and interpreted in a number of ways, depending on the application. A Personal Identification Number (PIN) is normally needed to "unlock" the contents of the microchip, meaning that only the person who knows the PIN can use the card.

What is Encryption?

Encryption is simply taking intelligible data and making it unintelligible by using a mathematical function and a unique key. To return the data to intelligible form, we use the same mathematical function and the same key. Therefore only the holder of the key can take the unintelligible data and make it intelligible.

The type of encryption used in the HP Encryption System provides confidentiality, as no one but the holder of the key can read the data.

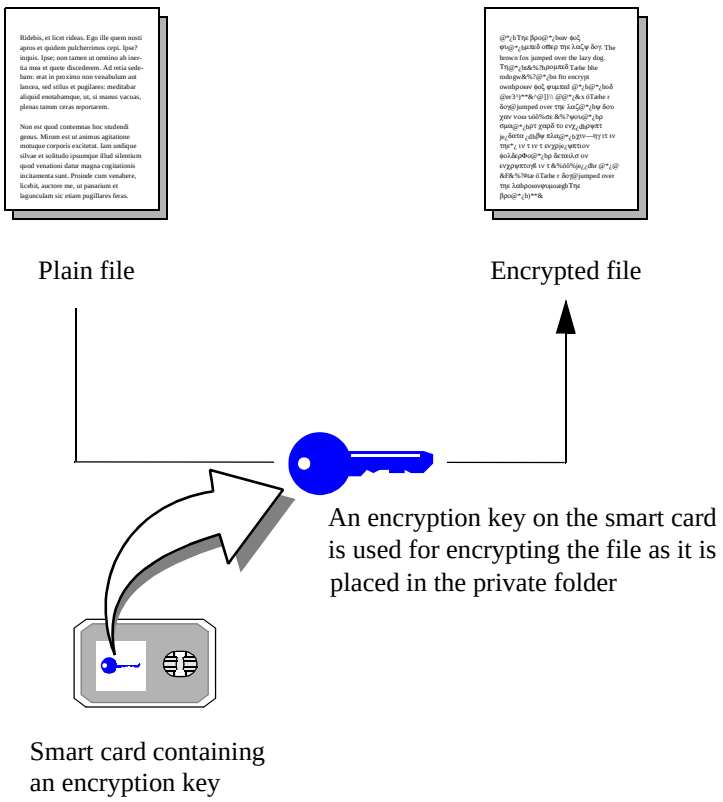
How does the HP Encryption Smart Card Security System work?

The Encryption Smart Card Security System provides two security features:

- Data encryption on your OmniBook's hard drive (Windows 95 and Windows NT).
- Smart card protected logon for Windows NT to prevent unauthorized access to your OmniBook.

Data encryption

When you set up the Encryption Smart Card Security System on your OmniBook, as part of the process you define a Secure folder on your OmniBook, and generate an encryption key that is stored on your smart card. You will also define a PIN which allows only someone with the PIN to use the smart card. When you place a file in the Secure folder with the smart card inserted in the smart card reader, the file is encrypted using a key stored on your smart card. The files in the Secure folder can be accessed only when your smart card is present in the smart card reader and the correct PIN has been provided. This means that for anyone to decrypt and read the files placed in your Secure folder, that person must be in possession of your smart card *and* also know your card's PIN.



Smart card logon with Windows NT

Windows NT offers password-protected logon where you must enter a user name and a password to access your Windows NT account. The Encryption Smart Card Security System increases the security of Windows NT logon by using a smart card in addition to your password. The smart card is registered with your Windows NT logon the first time you log on after the Encryption System software is installed on your OmniBook. Anytime you log on after this, the smart card must be present in a smart card reader inserted in the PCMCIA slot of your OmniBook. When you enter your user name and password, the system reads the smart card in the smart card reader and verifies that the correct smart card is present. If not, then admission to your Windows NT account is denied. Therefore for someone to log on to your Windows NT account, that person must not only know your user name and password, but must also be in possession of your smart card.

Setting up your OmniBook to use a smart card

Checking the package contents

Your Encryption Smart Card Security System package contains:

- 1 PCMCIA smart card reader
- 2 GPK4000 smart cards (one spare card for backup/recovery purposes)
- 1 CD-ROM containing the Encryption Smart Card Security System software
- 1 User's Guide (this manual)

Note that an optional pack of five smart cards is also available as a separate OmniBook accessory (order no. F1613A).

Checking the requirements

To use the Encryption Smart Card Security System, you need:

- An HP OmniBook Model 800, 2000, 3000, 5000, 4100, 7100, Sojourn or later with Microsoft Windows 95 OSR2 or later installed
  or
  An HP OmniBook Model 2100, 3000, 4100, 7100, Sojourn or later with Microsoft Windows NT 4.0 SP3 or later installed (you will need at least 2 NT accounts; one for the NT Administrator and at least one User account for everyday use)
- A CD-ROM drive installed in your OmniBook (note that on certain models of OmniBook, the CD-ROM drive is an option you need to purchase separately)
- 1 free PCMCIA slot on your OmniBook
- At least 5 Mbytes of free space on your hard disk

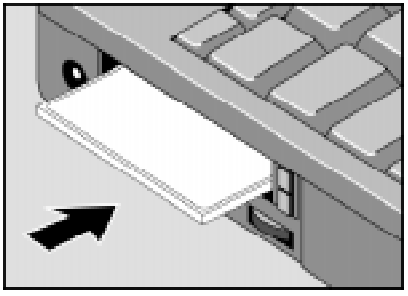
It is also recommended that you have a formatted diskette to hand, to use as a safe place to store the recovery file generated during the smart card initialization process.

Installing the Encryption System software and Smart Card Reader

Note

Before you begin installation, make sure your OmniBook's CD-ROM drive is correctly installed.

1. Start your OmniBook (log on as Administrator for Windows NT). You should have the Windows desktop displayed
2. Insert the HP Encryption System Software CD-ROM into the CD-ROM drive of your OmniBook.
3. Start your Windows program installation utility (Start, Settings, Control panel, Add/Remove Programs) and install the Encryption Smart Card Security System software from the CD-ROM.
   During the installation process you will be asked to install the smart card reader in an available PCMCIA slot in your OmniBook (the smart card reader is installed with the label facing upwards).



   The software will be installed in the `C:\Program Files\Hewlett-Packard\HP Encryption System\` directory by default, but you can specify a different one if you wish.
   Your Secure folder will be `C:\Private` by default, and again, you may change this if you wish.

   Your OmniBook will be restarted when the installation is complete.

If you are using Windows 95, you have now finished the installation. Proceed to "Initializing your smart card and creating a recovery file" on page 10.

For Windows NT users, you are now ready to register the Administrator and User smart cards for use with NT Logon.

Smart card logon with Windows NT

With Windows NT, the Encryption Smart Card Security System provides the additional security feature of smart card logon. This makes the logon procedure more secure as you need both your NT password *and* your smart card during logon. You must register your smart card with your user name and password during the NT logon process. After registration only your smart card can be used with your NT password.

It is recommended to register a smart card for at least 2 different Users; one for your normal User (everyday use) and one for the NT Administrator.

Registering your Administrator smart card for Windows NT logon

With Windows NT, it is highly recommended to register an Administrator smart card for your OmniBook to allow access to the system Administrator account.

In cases where all NT accounts are centrally managed (for example in a corporate environment), registering the Administrator smart card would typically be done by your system Administrator. If you are not part of such an environment, you will need to register an Administrator smart card for yourself.

Your Windows NT documentation will contain additional details on the system Administrator account.

To register an Administrator smart card

Caution

With Windows NT, if you lose your original smart card or it gets damaged or stolen, you will be unable to access your OmniBook unless you have a registered Administrator card.

1. Insert a new smart card in the smart card reader.
2. Log on to your OmniBook using the system Administrator's user name and password.

When you have entered your Administrator's user name and password, a message appears telling you that the card in the reader is now registered for your Administrator's account. You must now use this smart card every time you log on to your Windows NT Administrator's account.

Note

The Administrator smart card allows access to the Windows NT Administrator account and should be used only for administration and recovery purposes (should your original User smart card get lost or damaged). Naturally, the Administrator smart card should be kept in a safe place.

Registering your User smart card for Windows NT logon

To register your User smart card

1 Insert a new smart card in the smart card reader.

Note

This smart card will be the card that you will use for subsequent NT logons. After this card is successfully registered for your NT account, you will be unable to log on to your OmniBook without the card inserted in the smart card reader.

2 Log on to your OmniBook following the normal Windows NT logon procedure.

When you have entered your user name and password, a message appears telling you that the card in the reader is now registered for your User account. You now must use this smart card every time you log on to your Windows NT User account.

This completes the steps necessary to register your smart cards for Windows NT logon.

The first time you log on after installation, you will be in Verification mode.

Verification Mode

When you first set up your HP Encryption System to work with NT, it is put into an insecure “Verification” mode, which allows you to continue to access your OmniBook even if there are problems with accessing your smart card reader or smart card.

This “Verification” mode is only available following first installation, and is only destined to be used until you feel confident that everything is working as it should (especially following a reboot). Once you are confident in the installation and configuration, click on “Secure” in the Verification mode dialog box and the NT Logon installation will be secured.

Note

For security reasons, there is no way to return to this verification mode once you have selected to remove it.

You will now need to initialize each card that you wish to use for file encryption.

Initializing your smart card and creating a recovery file

Purpose of initializing your smart card

Before you can use a smart card to encrypt files, you will need to initialize it. During initialization, an encryption key is generated that is used to encrypt and decrypt your data. This key is stored on your smart card, which means that the encrypted data can be decrypted only when the smart card is inserted in the smart card reader connected to your OmniBook.

The recovery file

As a safety measure, the encryption key generated and stored on your smart card is also copied to a recovery file. If you subsequently lose your smart card, or it gets damaged, this recovery file allows you to load the encryption key that was on your original smart card to a new card, thus enabling you to access and decrypt the files on your OmniBook.

To initialize your smart card

1 Make sure your smart card is inserted in the smart card reader.

2 Open the HP Encryption Smart Card Security System Manager, and select the **Smart Card** tab.

3 In the **Smart Card** page, click on **Initialize** to start the initialization process, and generate your encryption key.

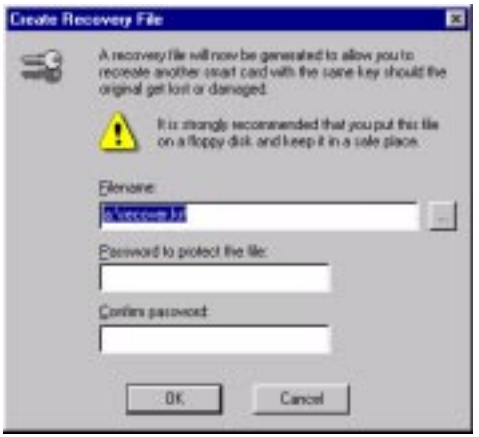
You will now be asked to enter a PIN number for the smart card.

4 Enter an 8-character PIN and confirm the PIN by retyping it exactly in the Confirm PIN field.

Note

Your PIN must be exactly 8 characters long. It is not case sensitive.

5 During the initialization process, you are prompted to define a recovery file and an associated password.
The default directory for the recovery file is on a floppy disk (`a:\`).



If you wish to define another location for the recovery file, click on ... to select another directory.
Then enter the name of the recovery file and the password to prevent unauthorized access to the file.

Caution

The recovery file allows you to create a duplicate smart card to access and decrypt the files in your Secure folder should you lose your original smart card or it gets damaged. For security reasons it is not recommended that you store this file on your OmniBook hard disk. A safe place would be on a floppy disk.

It is also important that you do not forget the password for the recovery file. If this happens, you will be unable to use your recovery file.

6 Click **OK** when you are done.

The encryption key is now generated and stored on your smart card and in the recovery file. You can now use your smart card to encrypt files.

Using your HP Encryption Smart Card Security System

Introduction

When using your HP Encryption Smart Card Security System with the Windows 95 operating system, a smart card must be present to encrypt and decrypt files in your Secure folder. When the card is introduced in the reader a message box will open asking for the PIN. Only when the correct PIN is entered will you be able to access your Secure folder and encrypt and decrypt your files.

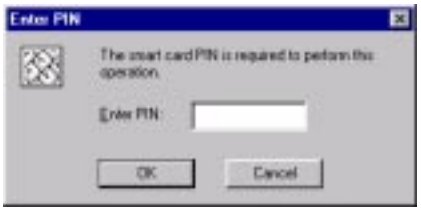
With the Windows NT operating system, in addition to the above, the smart card is required to log on. The PIN is requested, but is not necessary to log on (you can cancel, without stopping the logon). However, only when the correct PIN has been entered will you be able to access your Secure folder and encrypt and decrypt your files.

Getting Information

In the Information page of the HP Encryption System manager, you can easily see where the Secure folder is located. This location was specified during the product installation and cannot be changed. Other information available includes the status of the smart card and smart card reader and the status of the products software components.

Entering the PIN

Each time you insert a new smart card, or remove and insert the same smart card, you will be asked to enter its PIN. When the Encryption System detects the card, it opens a PIN dialog box. Enter the smart card's PIN. Once the PIN has been correctly entered, you will have access to your Secure folder. If a wrong PIN is entered or the smart card is not present, you will not be allowed to access your Secure folder.



Caution

If you type the PIN wrong seven times in a row, the card is locked from further use. This is a security feature to prevent someone from trying to guess your PIN.
See "If you forget your PIN" on page 18.

NT Workstation lock (screen lock)

The Logon tab and page are only accessible when you are logged on as the NT Administrator. The workstation lock is located in the lower part of the Logon page. Check the box to lock the workstation should the session owner's smart card be removed. The workstation can be unlocked only by the smart card that locked it.

Using the Secure Folder

By default, your Secure folder is located in `C:\Private .`

File structure

You can create directories and files within the Secure folder in exactly the same way as outside the Secure folder, as long as your smart card is present, and you have entered the correct PIN.

Storing existing files in the Secure folder

Use your application or file manager to:

- Save as...
- Copy to...
- Move (using drag and drop)

from your normal file structure to your Secure folder. Note that both Save as and Copy to will leave a copy in the unsecure part of your hard disk which presents a potential security risk.

When you Move files out of your Secure folder they will be decrypted.
For security reasons, using Move from the Secure folder is not recommended..

Using an existing file in the Secure folder

Use your application to:

- Open

and then

- Save
- Save as

files stored in your Secure folder.

Deleting a file in the secure folder

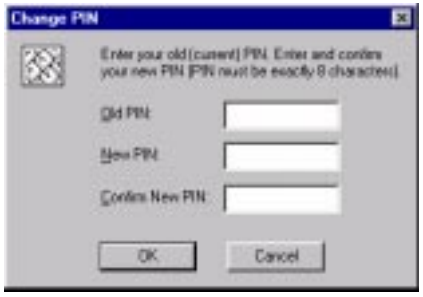
You can use `DELETE` or `SHIFT+DELETE` to remove files from your Secure folder.

Caution For security reasons, deleting files using `DELETE` is not recommended (it will leave a decrypted copy of the file in your Recycle Bin).

Changing your Smart Card's PIN

You can change the PIN of your smart card at any time using the Encryption System Manager. In the center section of the Smart Card page, click on **Change PIN**.

The Change PIN dialog box will open:



In the Change PIN dialog box you are asked for the old PIN and the new PIN (and confirmation). When you have entered this information, click on **OK**. Your PIN will be changed.

If you forget your PIN

If you forget your PIN, you should be aware that seven unsuccessful attempts at entering the PIN will result in your smart card being locked. If your organization does not have a centralized Smart Card Management System (SCMS) and an SCMS Administrator who can unlock your card, your card is now unusable and should be disposed of following your local environmental laws. You will need to create and register a new card as detailed in “Creating a replacement smart card” on page 19.

Creating a replacement smart card

If you lose your smart card

If you lose your smart card or it becomes damaged, you will need to create a replacement smart card to allow you to access and decrypt the files stored in your Secure folder on your OmniBook. The recovery file you created when you initialized your smart card will allow you to create a replacement card. For Windows NT users, you will first need to re-register your smart card for Windows NT Logon.

To create a replacement smart card for use with Windows 95

1 Locate the recovery file (it may be on a diskette).

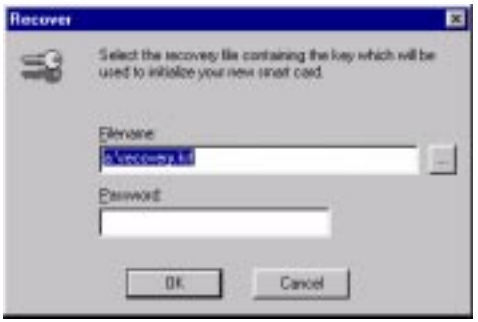
2 Insert a new smart card in the smart card reader.

3 Open the Encryption Smart Card Security System Manager program (if it is not already running) and click on the **Smart Card** tab.

4 If you have stored the recovery file on a floppy disk, insert the diskette into the floppy drive of your OmniBook.

5 Click on **Recover.**

You are now prompted to enter the name of the recovery file and the recovery file password.



6 Click on ... to go to the folder containing the recovery file (or type the full path name in the **filename** field) and enter the password for the recovery file.

7 You will be prompted to enter the (new) PIN for the new smart card.

The same key that was on your original smart card is now loaded in the new smart card, and you can now access and decrypt the files in your Secure folder.

To create a replacement smart card for use with Windows NT

Note

Since you can no longer use your smart card to access your OmniBook, you will need the NT Administrator smart card to regain access.

1 Insert the Administrator smart card in the smart card reader, and log on as the NT Administrator.

2 Open the Encryption System Manager program.

3 Select the **Logon** tab (only accessible by the NT Administrator).

The list of active smart cards and users is now displayed.

4 Click on the user name for which you wish to re-register a new smart card, and then click on the **Allow renewal** button. The card state will change from “Card registered” to “Card renewal allowed”.

5 Log off from your NT Administrator session and remove the NT Administrators smart card from the smart card reader.

6 Insert a new (blank) smart card in the smart card reader. Log on to your OmniBook as the user for which you wish to re-register the new smart card, following the normal Windows NT logon procedure.

7 When you have entered your user name and password, a message appears telling you that the card in the reader is now registered for your user account. You must now use this smart card every time you log on to your Windows NT user

account. (This completes the steps necessary to register your smart card for Windows NT logon).

8 Locate the recovery file (it may be on a diskette).

9 Open the Encryption Smart Card Security System Manager program (if it is not already running) and click on the **Smart Card** tab.

10 If you have stored the recovery file on a floppy disk, insert the diskette into the floppy drive of your OmniBook.

11 Click on **Recover**.

You are now prompted to enter the name of the recovery file and the recovery file password.

12 Click on **...** to go to the folder containing the recovery file (or type the full path name in the **filename** field) and enter the password for the recovery file.

13 You will be prompted to enter the (new) PIN for the new smart card.

The same key that was on your original smart card is now loaded in the new smart card, and you can now access and decrypt the files in your Secure folder.

Troubleshooting

General Troubleshooting tips and tricks

In the case of a problem with your HP Encryption Smart Card Security System, the first place to check is the Information page of the Encryption System Manager.

In this page you will find:

Smart Card Status

The smart card status should be:

- smart card present and correctly initialized

However, if there is a problem, it could be:

- smart card present but badly initialized

  Solution: re-initialize your smart card as detailed in “To initialize your smart card” on page 10

- smart card present but not initialized

  Solution: initialize your smart card as detailed in “To initialize your smart card” on page 9

- no smart card in the reader

  Solution: insert an initialized smart card

Smart Card Reader status

The smart card reader status should be:

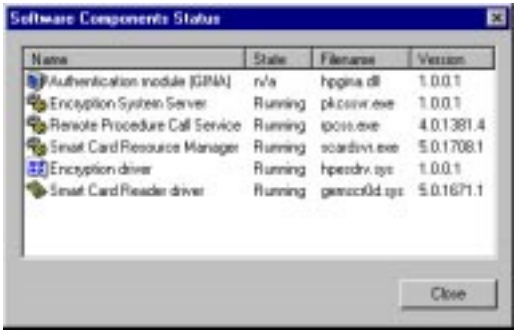
- reader is present and is working correctly

However, in the case of a problem, it could be:

- unable to connect to the smart card reader

  Solution: check the status of all software components as detailed in “Software Components status” below, and follow the directions given in this section. If all seems in order, try rebooting your OmniBook.

Software Components status:



Note

The Authentication module (GINA) is only present in Windows NT installations. It is not present in Windows 95 installations.

The software components status should be:

- Running

(except for the Authentication Module (GINA) which is stateless, and marked n/a)

However, in the case of a problem, it could be:

- Stopped

  Solution: If any components are marked as stopped, you will need to restart them (reboot the OmniBook or start them using the file manager - double click on the file name).

- Missing

  Solution: If any (other than the Remote Procedure Call Service) are marked as missing, you will need to uninstall the Encryption System and then re-install it.

  If the Remote Procedure Call Service is marked as missing, you will need to reinstall it as documented in your Windows 95 or Windows NT Operating System manuals.

If you are still having problems, the next place to check is the smart card reader configuration: go to the Control Panel of your OmniBook, double click on PC Card (PCMCIA) and make sure that the GEMPLUS GPR400 is connected to the correct socket.
If you see “(Empty) - Socket x “: check the reader’s installation and retry.

If you are still having problems, you should try rebooting your OmniBook and check if the problem persists.

Troubleshooting questions and answers

Problem	Explanation	Action
I have lost my smart card	If you are using Windows NT, you will now be unable to log on to your NT account and gain access to your OmniBook.	Contact your system administrator to regain access to your OmniBook using the administrator smart card. Register a new smart card for your NT logon.
	Now you can log on, but you will be still be unable to read the files in your encryption folder.	Use the recovery file to enable your new smart card to decrypt the files you encrypted with your old card.
	If you are using Windows 95, you will be unable to read the files in your encryption folder.	Make a recovery card using the recovery file. See “Creating a replacement smart card” on page 19 for details.
I cannot log on to my NT account	Your smart card is not inserted correctly in the smart card reader, or the reader is not connected correctly to the OmniBook.	Check that the smart card is inserted correctly and check that the reader is inserted correctly.
I could not remember my PIN, I tried to enter it seven times and now my card no longer works	As a security measure to prevent someone who has obtained your smart card from guessing your PIN, you are allowed only seven attempts at entering the correct PIN. If you fail to enter the correct PIN on the seventh attempt your card is locked.	If your organization has a centralized Smart Card Management System (SCMS), see the SCMS Administrator who can unlock your card. If not, your card is now unusable and should be disposed of following your local environmental laws. If you are using Windows NT, you must register a new smart card with your NT logon and then use the recovery file to load the old encryption key on the new card. If you are using Windows 95, use the recovery file to load the old encryption key on the new card.

Problem	Explanation	Action
Access to your Encryption folder is denied	The HP Encryption System Manager is unable to retrieve information stored on the smart card.	Make sure your smart card is properly inserted into the smart card reader and the correct PIN has been entered. If this isn't done, you will not be able to access the secure folder. If you are still unable to access the Secure folder you may have corrupted information on you smart card. Use the recovery procedure detailed in Chapter 3 to recover your smart card.
Files copied into the secure folder don't seem to be encrypted	The smart card you used to move your files into the secure folder is still inserted in the reader, and you still have access to all the files you moved into the secure folder.	Insert another card into the reader and check the content of your files: they should be unreadable.
Encrypted text decrypts badly	The card inserted in the reader is not the one you used to encrypt your files.	Insert the correct card and enter your PIN number to access the secure folder.
I can't delete a file in my Secure folder using DELETE.	For security reasons, deleting files using DELETE is not supported (it would leave a copy in the Recycle Bin).	To delete a file from the Secure folder use SHIFT+DELETE
A message tells me that access to the smart card is denied.	The HP Encryption System Manager is unable to retrieve information stored on the smart card.	Make sure that your smart card reader is properly installed in your OmniBook and that the smart card is properly inserted in the smart card reader. If the error message "Could not access the card reader, please check connection and retry" is displayed, follow the indications given in the message boxes.

If you have questions this manual doesn't answer, you can:
Look at the online help in the HP Encryption System Manager.
Find additional information about this OmniBook accessory on the Internet - visit the Support website at http://www.hp.com/omnibook.
Check with your system administrator, if you have one.
Contact your dealer, or contact Hewlett-Packard - see the OmniBook Support and Service booklet.

Make sure you have the software version number (in the "General" page of the HP Encryption System Manager) and all of the information (including the version of all the installed components) in the "Software Component Status" window of the "Information" page.