HP ProtectTools Embedded Security Guide

Document Part Number: 364876-001

May 2004

This guide provides instructions for using the software that allows you to configure settings for the HP ProtectTools Embedded Security chip.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

⚠ **WARNING:** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

△ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

HP ProtectTools Embedded Security Guide

First Edition (May 2004)

Document Part Number: 364876-001

Contents

HP ProtectTools Embedded Security

HP ProtectTools Embedded Security

The HP ProtectTools Security Manager is the software that allows you to configure settings for the HP ProtectTools Embedded Security. The Manager is an interface (shell) that points to the various options available in the Embedded Security software. HP ProtectTools Embedded Security is the software suite that includes the Personal Secure Drive (PSD), encryption/TPM chip interface, security migration, archive creation, and password control.

Requirements

In order to use the security features, the following tools are required:

- HP ProtectTools Embedded Security software
- HP ProtectTools Security Manager software
- HP ProtectTools Embedded Security chip installed on the computer

For information on setting up the Embedded Security solution, see "Setup Procedures" on page 8 later in this chapter.

Basic ProtectTools Embedded Security Concepts

This section contains high-level information on concepts you should understand in order to use HP ProtectTools Embedded Security and HP ProtectTools Security Manager.

HP ProtectTools Embedded Security Chip

The Embedded Security chip is a hardware component that offers security and encryption features and provides a tamper-proof storage area for protecting public and private keys. The chip is factory-installed and should not be accessed or removed except by HP authorized service providers.

Personal Secure Drive

One feature of Embedded Security is the Personal Secure Drive (PSD). The PSD is a virtual drive that is created during the HP ProtectTools Embedded Security User initialization process. It provides a protected storage area for sensitive data. The PSD allows you to create and access files and folders, just like other drives.

Access to the PSD requires both physical access to the computer on which the PSD resides and the PSD password. When you enter your PSD password, the PSD becomes visible and the files become available for use. The files remain accessible until you log off, at which time the PSD automatically hides its presence. PSDs cannot be accessed from a network.

The PSD stores the keys used to encrypt files on the HP ProtectTools Embedded Security chip, ensuring the data is protected from unauthorized users and is “locked” to the computer. This means that the protected data can only be accessed on the target computer.

Email

Secure email is another significant feature of Embedded Security. It allows users to share information confidentially and to be certain that the authenticity of the information is maintained during transfer. Secure email allows you to:

- Select a public key certificate issued by a Certification Authority (CA).
- Digitally sign messages.
- Encrypt messages.

HP ProtectTools Embedded Security and HP ProtectTools Security Manager enhance secure email functionality by providing additional protection for the key used to encrypt, decrypt, and digitally sign messages. They enhance the security of email when the following email clients are used:

- Microsoft Outlook Express (version 4 or higher)
- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Netscape Messenger 4.79
- Netscape Messenger 7.0

For instructions on using email clients, refer to the HP ProtectTools Embedded Security Email Integration Help.

Enhanced Encrypted File System (EFS)

EFS is the file encryption service offered by Microsoft Windows 2000 and Windows XP Professional. EFS provides data privacy by offering the following functionality:

- Encryption of files by the user when stored on a disk
- Quick and easy access to encrypted files
- Automatic (and transparent) encryption of data
- Ability for the system administrator to recover data encrypted by another user

HP ProtectTools Embedded Security and HP ProtectTools Security Manager enhance the EFS by providing additional protection for the key used to encrypt and decrypt data.

For more information on EFS, refer to the operating system online Help.

Users and Administrators

Users

Users have basic access to Embedded Security and may:

- send and receive encrypted email
- encrypt files and folders
- initialize personal Basic User key
- create, delete, or modify personal user account within the embedded security
- configure, create, use, and delete individual PSD

Administrators

Administrators initialize the Embedded Security solution on a computer and may:

- configure the local machine and user policies of Embedded Security
- prepare user keys and certificates for migration
- change the Embedded Security owner password
- disable and enable Embedded Security
- authorize destination computers for user key and certificate migration
- recover data that was stored and encrypted using Embedded Security

For more information on Embedded Security users and administrators, refer to the operating system online Help. For more information on Embedded Security owners, refer to the HP ProtectTools Embedded Security Help.

Digital Certificates

Digital certificates are a form of electronic “keys” that confirm the identity of an individual or company. Keys are numbers or strings of characters known only to the sender and/or recipient. A digital certificate authenticates the digital certificate owner by providing a digital signature that attaches to email sent by the owner of the digital certificate.

A digital certificate is issued by a Certification Authority (CA) and contains the following information:

- Owner's public key
- Owner's name
- Expiration date of the digital certificate
- Serial number of the digital certificate
- Name of the CA that issued the digital certificate
- Digital signature of the CA that issued the digital certificate

Digital Signature

A digital signature displays the name of the CA issuing the digital certificate. It is used to:

- verify the identity of the sender of a digital document.
- certify that the contents were not modified after the sender digitally signed the document.

For more information on digital signatures, refer to the operating system online Help.

Public Key and Private Key

Asymmetric cryptography, which is a method used by Embedded Security to encrypt information, requires the use of 2 keys, a public key and a private key.

A public key can be freely distributed to many users, whereas a private key is held by only one user.

For example, to send encrypted email, User A would use the public key (freely available) from User B to encrypt the contents of the email sent to User B. Since User B has sole possession of his private key, he is the only one that can decrypt the contents of the email sent from User A.

Public key-enabled technology allows you to transmit private information over public networks, use digital signatures to ensure the authenticity of your email, and provides authentication between a server and a client.

Emergency Recovery

The Emergency Recovery Archive, created by the administrator during Embedded Security setup, is a file that stores sensitive information about the computer, its users, and the private keys used to protect encrypted or private data. In the case of a system failure, this sensitive information is required to restore access to protected data.

An Emergency Recovery Token, also created by the administrator during Embedded Security setup, is a file that stores the keys used to protect the data in the Emergency Recovery Archive. The token is required to access the archive. The access to the Emergency Recovery Token is protected by a password. This password is required in case the Embedded Security system needs to be restored.

Policies

Policies are rules that govern the behavior of a computer or software. The system administrator generally specifies security policies to ensure consistent use of Embedded Security within an organization. The two types of security policies are machine policies and user policies.

Machine Policies

Machine policies are rules governing the overall behavior of Embedded Security as it relates to a specific computer.

User Policies

User policies are rules governing the rights of the user of Embedded Security.

For more information on machine and user security policies, refer to the HP ProtectTools Embedded Security Help.

Setup Procedures

Follow these steps to enable and initialize the Embedded Security chip through the Computer Setup utility in the system BIOS:

CAUTION: To prevent a security risk, HP recommends that a person authorized by your organization immediately initialize the Embedded Security chip (see step 4). Failure to initialize the Embedded Security chip could result in an unauthorized user, a computer worm, or a virus taking ownership of the system.

✎ Because the chip configurations are enabled and changed through Computer Setup, the BIOS administrator password must be established in Computer Setup before the chip configurations can be accessed.

Enabling the Chip

1. Turn on or restart the computer. If you are in Microsoft Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the F10 key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. Use the up or down arrow key to select the language. Press **Enter** to enter Computer Setup.

   For navigation instructions, press **F1**.

4. Use the left or right arrow key to select the **Security** menu, then use the up or down arrow key to select **Setup Password**. Press **Enter**, enter and confirm a new setup password, and press **F10** to accept.

✎ Type carefully; for security reasons, the characters typed do not appear on the screen.

5. In the **Security** menu, use the up or down arrow key to select **Embedded Security Device**, then press **Enter**.
6. If the selection in the dialog box is **Embedded Security Device–Disable**, use the left or right arrow key to change it to **Embedded Security Device–Enable**.
7. Press **F10** to accept the changes to the Embedded Security configuration.
8. To save your preferences and exit Computer Setup, press **F10** to go to **Save Changes and Exit**. Press **Enter**, then press **F10** to confirm.

Initializing the Embedded Security Chip

✎ In most cases, the IT System Administrator initializes the Embedded Security chip.

1. Right-click the **HP ProtectTools** icon in the system tray, then left-click **Embedded Security Initialization**.

   The **HP ProtectTools Embedded Security Initialization Wizard** appears.
2. Click **Next**.
3. Type and confirm a Take Ownership password, then click **Next**.

✎ Type carefully; for security reasons, the characters typed do not appear on the screen.

4. Click **Next** to accept the default Recovery archive location.
5. Type and confirm an Emergency Recovery Token password, then click **Next**.

6. Click **Browse** and select the appropriate destination.

△ **CAUTION:** The Emergency Recovery Token Key is used to recover encrypted data in the event of a computer or embedded security chip failure. The data cannot be recovered without the key. (The data still cannot be accessed without the Basic User password.) Store this Key in a safe place.

7. Click **Save** to accept the location and the default file name, then click **Next**.
8. Click **Next** to confirm settings before the Security Platform is initialized.

△ **CAUTION:** A message may be displayed to say that the Embedded Security features are not initialized. Do not click in the message; this is addressed later in the procedure and the message will close after a few seconds.

9. If the user account is to be set up now, make sure the **Start Embedded Security User Initialization Wizard** check box is selected. Click **Finish**.

Setting Up a User Account

Setting up a user account:

- produces a Basic User key that protects encrypted data
- sets up a PSD for storing encrypted files and folders

△ **CAUTION:** Safeguard the Basic User password. Encrypted data cannot be accessed or recovered without this password.

To set up a Basic User account and enable the user security features:

1. If the **Embedded Security User initialization Wizard** is not open, right-click the **HP ProtectTools** icon in the system tray, then left-click **Embedded Security User Initialization**.

   The **Embedded Security User initialization Wizard** appears.
2. Click **Next**.
3. Type and confirm a Basic User Key password, then click **Next**.

✎ Type carefully; for security reasons, the characters typed do not appear on the screen.

4. Click **Next** to confirm settings.
5. Select the appropriate Security Features and click **Next**.
6. Click **Next** to skip Help files.
7. If more than one Encryption Certificate exists, click the appropriate certificate.

   Click **Next** to apply the Encryption Certificate.
8. Configure the PSD with appropriate settings and click **Next**.
9. Configure the PSD again with appropriate settings and click **Next**.

✎ The minimum size of the PSD is 50 MB; the maximum size is 2,000 MB.

10. Click **Next** to confirm settings.

✎ Depending on the size of the PSD, the computer could take a few minutes to process the confirmation.

11. Click **Finish**.
12. Click **Yes** to restart the computer.

Commonly Performed Tasks

This section discusses basic tasks that are most often performed by a user and an owner.

User Tasks

Basic user tasks include setting up the PSD, encrypting files and folders, and sending and receiving email by encryption and/or digital signatures.

Using the PSD

To use the PSD, enter your PSD password. The PSD becomes visible and the files are decrypted. The PSD may be used like any other drive.

When you are finished using the PSD, log off properly. The PSD automatically hides its presence.

Encrypt Files and Folders

When working with EFS in Windows 2000 and Windows XP Professional, consider the following:

- Only files and folders on NTFS partitions can be encrypted. (Files and folders on FAT partitions cannot be encrypted.)
- System files and compressed files cannot be encrypted, and encrypted files cannot be compressed.
- Temporary folders should be encrypted, as temporary files are potentially of interest to attackers.
- A recovery policy is automatically set up when users encrypt a file or folder for the first time. This ensures that users who lose their certificates and private keys are able to use a recovery agent to decrypt their data.

To encrypt files and folders:

1. Select the file or folder you want to encrypt.
2. Right-click the mouse or Touchpad.
3. Click **Encrypt**.
4. Click either **Apply changes to this folder only** or **Apply changes to this folder, subfolder and files**.
5. Click **OK**.

Send and Receive Email by Encryption and/or Digital Signatures

For instructions on digitally signing and encrypting email, refer to the email client online Help.

✎ To use secure email, you must first configure the email client to use a digital certificate that is created with Embedded Security. If a digital certificate is not available, you must obtain one from a Certification Authority. For instructions on configuring your email and obtaining a digital certificate, refer to the email client online Help.

To send an encrypted email message, you will need a copy of the recipient's public key or encryption certificate. (The certificate contains a copy of the recipient's public key.)

Microsoft Outlook uses the recipient's public key to encrypt your email; therefore you are not requested to insert your private key. However, you do need your private key to read an encrypted email because the decryption requires the private key that corresponds to the public key used to encrypt the email.

Administrator Tasks

The administrator can perform a number of tasks, some of which are described below. For more information, refer to the HP ProtectTools Embedded Security Help.

Migrate Keys through the Computer Security Migration Wizard

Migration is an advanced administrator task that allows the management, restoration, and transfer of keys and certificates.

The first step of migration is the authorization, setup, and management of the migration process. Once authorization is complete, the user exports and imports keys and certificates from the source computer to the destination computer.

For details on migration, refer to the HP ProtectTools Embedded Security Help.

Recover Information

In the event of chip failure or reset:

- The Emergency Restore Wizard can be used to recover data from the PSD.
- The PSD also supports recovery by using a recovery agent, which is a mechanism similar to Encryption File Systems (EFS).

  To determine if you have a registered recovery agent on the computer, click **Start > All Programs > Administrator Tools > Local Security Policy > Public Key Policies > Encrypted Data Recovery Agents**.

For more information, refer to the operating system online Help.

✎ Windows XP Professional does not automatically create a registered recovery agent. Follow the operating system instructions for setting up the registered recovery agent.

To recover data, the registered recovery agent must have the digital certificate and the keys. You should export the data recovery certificate and private key to disc, store them in a safe place, and delete the data recovery private key from the computer. The only person who can recover data is the person who has physical access to the data recovery private key.

Restore the Embedded Security Chip to the original factory settings through Computer Setup

CAUTION: This task releases ownership of the Embedded Security chip. Once ownership is released, anyone can initialize the Embedded Security chip.

Restoring the Embedded Security chip to its original factory settings may result in data loss if you have encrypted files.

To return the Embedded Security chip to its original factory settings:

1. Turn on or restart the computer. If you are in Microsoft Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the F10 key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. If necessary, enter the setup password and press **Enter**.
4. Use the up or down arrow key to select the language. Press **Enter** to enter Computer Setup.

   For navigation instructions, press **F1**.
5. If the Security setup password has not been set, one must be set now. Use the left or right arrow key to select the **Security** menu, then use the up or down arrow key to select **Setup Password**. Press **Enter**, enter and confirm a new setup password, and press **F10** to accept.

✎ Type carefully; for security reasons, the characters typed do not appear on the screen.

6. In the **Security** menu, use the up or down arrow key to select **Embedded Security Device**, then press **Enter**.
7. Use the up or down arrow key to move to **Reset to Factory Settings–Do Not Reset**. Press the left or right arrow key *once*.

   A message is displayed stating: **Performing this action will erase all security keys. Data loss may occur. Press any key to continue.**

   Press **Enter**.
8. The selection will now read **Reset to Factory Settings–Reset**. Press **F10** to accept the change.
9. To save the changes and exit Computer Setup, press **F10** to go to **Save Changes and Exit**. Press **Enter**, then press **F10** to confirm.
10. Turn the computer off and back on.

Your preferences are set when you exit Computer Setup and take effect when the computer is turned off and back on; a restart is not effective.

Best Practices

HP recommends following these guidelines when using Embedded Security.

- An IT security administrator should set up the BIOS administrator password in Computer Setup and initialize the Embedded Security chip before distributing the computer to users.
- An IT security administrator should set up the Emergency Recovery Archive during the process of setting up the Embedded Security solution and encourage users to save and backup data regularly. In case of system failure, this is the only way to recover encrypted data. The Emergency Recovery Archive and Emergency Recovery Token should be stored separately.
- Encrypt folders instead of individual files so that temporary files that are created during editing are encrypted as well.
- Encrypt sensitive data on computers that are members of a domain. This protects against compromise of data through offline cryptographic attacks.

- Regularly back up the entire server that stores server-based encrypted data. This ensures that in the event of data recovery, the profiles that include decryption keys can also be restored.
- If you are encrypting file types that are monitored by System Restore, put the files on a volume that is not monitored by System Restore.
- The system does not support multiple levels of encryption. For example, a user should not store an EFS encrypted file in the PSD, nor try to encrypt a file already stored in the PSD.

Frequently Asked Questions

How do I know my computer has an HP ProtectTools Embedded Security chip?

The chip is a hardware component built into the system. The component will be listed in Device Manager.

Where do I get the HP ProtectTools Embedded Security software?

Download the software, drivers, and online Help by visiting the HP Web site at http://www.hp.com/products/security.

Can the HP ProtectTools Embedded Security software be uninstalled? How?

Yes. The software is uninstalled using the standard Windows software removal process. Before uninstalling, user-specific protected data should be saved. Without saving, the data is lost. The final step in uninstalling is to disable the chip in the computer BIOS via the Computer Setup utility. Once HP ProtectTools Embedded Security is uninstalled, the only way to disable the chip is through Computer Setup (**F10**).

1. Turn on or restart the computer. If you are in Microsoft Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the F10 key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. If necessary, enter the setup password and press **Enter**.
4. Use the up or down arrow key to select the language. Press **Enter** to enter Computer Setup.

   For navigation instructions, press **F1**.
5. If the Security setup password has not been set, one must be set now. Use the left or right arrow key to select the **Security** menu, then use the up or down arrow key to select **Setup Password**. Press **Enter**, enter and confirm a new setup password, and press **F10** to accept.

✎ Type carefully; for security reasons, the characters typed do not appear on the screen.

6. In the **Security** menu, use the up or down arrow key to select **Embedded Security Device**, then press **Enter**.
7. If the selection in the dialog box is **Embedded Security Device–Enable**, use the left or right arrow key to change it to **Embedded Security Device–Disable**.
8. Press **F10** to accept the changes to the Embedded Security configuration.
9. To save the preferences and exit Computer Setup, press **F10** to go to **Save Changes and Exit**. Press **Enter**, then press **F10** to confirm.

Troubleshooting

My Embedded Security is not working. What should I do?

1. Right-click the **HP ProtectTools** icon in the system tray, then left-click **Manage Embedded Security**.
2. Click **Embedded Security > Info > Self Test**.

Also check under **Embedded Security State, Chip, Owner** and **User**.

I restored my system after a crash. What should I do now?

CAUTION: In most cases, the IT System Administrator performs this procedure. Permanent data loss can result if the procedure is not performed properly.

To recover data after replacement of the ProtectTools chip, you must have the following:

- SPEmRecToken.xml-the Emergency Recovery Token Key
- SPEmRecArchive.xml-hidden folder, default location: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools passwords
  - ❑ F10 Setup
  - ❑ Take Ownership
  - ❑ Emergency Recovery Token
  - ❑ Basic User

1. Turn on or restart the computer. If you are in Microsoft Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the F10 key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. If necessary, enter the setup password and press **Enter**.
4. Use the up or down arrow key to select the language. Press **Enter** to enter Computer Setup.

   For navigation instructions, press **F1**.
5. If the Security setup password has not been set, one must be set now. Use the left or right arrow key to select the **Security** menu, then use the up or down arrow key to select **Setup Password**. Press **Enter**, enter and confirm a new setup password, and press **F10** to accept.

✎ Type carefully; for security reasons, the characters typed do not appear on the screen.

6. In the **Security** menu, use the up or down arrow key to select **Embedded Security Device**, then press **Enter**.
7. If only one selection, **Embedded Security Device–Disable**, is available, go to step 13.
8. If two selections are available:
   a. Use the up or down arrow key to move to **Reset to Factory Settings–Do Not Reset**. Press the left or right arrow key *once*.

      A message is displayed stating: **Performing this action will erase all security keys. Data loss may occur. Press any key to continue.**

   b. Press **Enter**.

      The selection will now read **Reset to Factory Settings–Reset**.
9. Press **F10** to accept the change.

10. To save the changes, press **F10** to go to **Save Changes and Exit**. Press **Enter**, then press **F10** to confirm.
11. Turn off the computer.

✎ Power must be turned off for the chip to reset.

12. Go to step 1.
13. If the selection in the dialog box is **Embedded Security Device–Disable**, use the left or right arrow key to change it to **Embedded Security Device–Enable**.
14. Press **F10** to accept the changes to the Embedded Security configuration.
15. To save the changes, press **F10** to go to **Save Changes and Exit**. Press **Enter**, then press **F10** to confirm.
16. After Windows opens, right-click the **HP ProtectTools Embedded Security** icon in the system tray, then left-click **Embedded Security Initialization**.
17. Select the check box: **I want to restore the existing Embedded Security**, then click **Next**.
18. Type and confirm the original Take Ownership password. Click **Next**.
19. Click **Do not create a recovery archive**, then click **Next**.

△ **CAUTION:** Creating a new archive results in total loss of data by overwriting the archive required for this restoration.

20. Click **Yes** to proceed without creating a recovery archive.
21. Click **Next** to confirm settings.
22. Click **Browse** and locate the emergency archive; the default location is: C:\Documents and Settings\ All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
23. Click **Open** and **Next**.

24. Click **Browse** and locate the Recovery token created during the initial **HP ProtectTools Embedded Security Initialization**, click the token, and click **Open**.
25. Enter Token password and click **Next**.
26. Select the machine name and click **Next**.
27. Click **Next** to confirm settings.

    If an announcement appears that the restore failed, return to step 1. Carefully check passwords, token location and name, and archive location and name.
28. If the user account is to be set up now, make sure the **Start Embedded Security User Initialization Wizard** check box is selected. Click **Finish**.

✎ Steps 29 through 41 restore the Basic User Keys. These steps must be repeated for each user.

29. If the **Embedded Security User initialization Wizard** is not open, right-click the **HP ProtectTools Embedded Security** icon in the system tray, then left-click **Restore Embedded Security Features**.

    The **Embedded Security User Initialization Wizard** appears.
30. Click **Next**.
31. Click **Recover your basic user key** and click **Next**.
32. Select a user, type the original Basic User Key password for that user, then click **Next**.
33. Click **Next** to confirm settings and accept the default recovery data location.
34. Select the appropriate Security Features and click **Next**.
35. Click **Next** to bypass help files.
36. If more than one Encryption Certificate exists, click the appropriate certificate.

    Click **Next** to apply the Encryption Certificate.
37. Click **I want to change my Personal Secure Drive settings** where appropriate and click **Next**.

38. Confirm the Security Features and click **Next**.
39. Confirm the Settings and click **Next**.
40. Enter the PSD password and click **OK**.
41. Click **Finish** and **Yes** to restart.

△ **CAUTION:** Safeguard the Basic User password. Encrypted data cannot be accessed or recovered without this password.

Glossary

Certification Authority (CA)—a service that issues the certificates required to run a public key infrastructure.

Cryptography—the practice and study of encryption and decryption; encoding data so that it can only be decoded by specific individuals. A system for encrypting and decrypting data is a cryptosystem. These usually involve an algorithm for combining the original data ("plaintext") with one or more "keys"-numbers or strings of characters known only to the sender and/or recipient. The resulting output is known as "cipher text."

Cryptographic Service Provider (CSP)—a provider or library of cryptographic algorithms that can be used in a well-defined interface to perform particular cryptographic functions.

Decryption—any procedure used in cryptography to convert cipher text (encrypted data) into plaintext.

Digital Certificates—electronic credentials that confirm the identity of an individual or a company by binding the identity of the digital certificate owner to a pair of electronic keys that are used to sign digital information.

Digital Signature—feature used to verify the identity of the sender of a digital document and certify that the contents were not modified after the sender signed the document.

Emergency Recovery Archive—the archive is a protected storage area that allows the re-encryption of basic user keys from one platform owner key to another.

Encryption—i.e., algorithm, cryptography; any procedure used in cryptography to convert plaintext into cipher text in order to prevent unauthorized recipients from reading that data. There are many types of data encryption and they are the basis of network security. Common types include Data Encryption Standard and public-key encryption.

Encryption File System (EFS)—a system that encrypts all files and subfolders within the selected folder.

Migration—a task that allows the management, restoration, and transfer of keys and certificates.

Personal Secure Drive (PSD)—provides a protected storage area for sensitive data.

Public Key Infrastructure (PKI)—a standard that defines the interfaces for creating, using, and administering certificates and cryptographic keys.

Trusted Platform Module (TPM)—provides hardware level of security to data. Built into the system, the Embedded Security chip can check the system integrity and authenticate third-party users who access the platform, while still remaining under complete control of its primary user.