IBM® Client Security Solutions

Client Security Software Version 5.3 User's Guide

IBM® Client Security Solutions

Client Security Software Version 5.3 User's Guide

Note

Before using this information and the product it supports, be sure to read Appendix B, "**Notices and Trademarks**," on page 53.

First Edition (May 2004)

Contents

Preface

This guide contains information about using Client Security Software on IBM network computers, also referred to as IBM clients which contain IBM embedded Security Chips.

The guide is organized as follows:

″Chapter 1, “Introduction”″ contains a brief outline of basic security concepts, an overview of the applications and components that are included in the software, and a description of Public Key Infrastructure (PKI) features.

″Chapter 3, “CSS Credential Roaming,”″ contains information about how to use IBM Client Security Software to protect sensitive files and folders.

″Chapter 4, “Instructions for the client user,”″ contains instructions about different tasks that the client user performs when using Client Security Software. This chapter includes instructions about how to use UVM logon protection, the Client Security screen saver, secure e-mail and the User Configuration Utility.

″Chapter 5, “Troubleshooting,”″ contains helpful information for solving problems you might experience while using the instructions provided in this guide.

″Appendix A, “Password and passphrase information,”″ contains passphrase criteria that can be applied to a UVM passphrase and rules for administrator passwords.

″Appendix B, “**Notices and Trademarks**,”″ contains legal notices and trademark information.

Who should read this guide

This guide is intended for Client Security end users (client users). Client Security Software must be installed and set up on your computer before you can use the information in this guide. Knowledge of using digital certificates and using logon and screen saver programs is required.

How to use this guide

Use this guide to set up the Client Security screen saver, change UVM passphrases and Windows passwords, and use Client Security cryptographic capabilities on Microsoft and Netscape applications. This guide is a companion to the *Client Security Software Installation Guide*, *Using Client Security with Tivoli Access Manager*, and *Client Security Software Administrator's Guide*.

Some information provided in this guide is also provided in the *Client Security Software Administrator's Guide*. The *Administrator's Guide* is intended for security administrators who will install and set up Client Security Software on IBM clients.

This guide and all other documentation for Client Security can be downloaded from the http://www.pc.ibm.com/us/security/index.html IBM Web site.

Additional information

You can obtain additional information and security product updates, when available, from the http://www.pc.ibm.com/us/security/index.html IBM Web site.

Chapter 1. Introduction

Select ThinkPad™ and ThinkCentre™ computers are equipped with built-in cryptographic hardware that work together with downloadable software technologies to provide a powerful level of security in a client PC platform. Collectively this hardware and software is called the IBM Embedded Security Subsystem (ESS). The hardware component is the IBM Embedded Security Chip and the software component is the IBM Client Security Software (CSS).

Client Security Software is designed for IBM computers that use the IBM Embedded Security Chip to encrypt files and store encryption keys. This software consists of applications and components that enable IBM client systems to use client security features throughout a local network, an enterprise, or the Internet.

The IBM Embedded Security Subsystem

The IBM ESS supports key-management solutions, such as a Public Key Infrastructure (PKI), and is comprised of the following local applications:

- File and Folder Encryption (FFE)
- Password Manager
- Secure Windows logon
- Multiple, configurable authentication methods, including:
  - Passphrase
  - Fingerprint
  - Smart Card

In order to effectively use the features of the IBM ESS a security administrator must be familiar with some basic concepts. The following sections describe basic security concepts.

The IBM Embedded Security Chip

The IBM Embedded Security Subsystem is the built-in cryptographic hardware technology that provides an extra level of security to select IBM PC platforms. With the advent of this security subsystem, encryption and authentication processes are transferred from more vulnerable software and moved to the secure environment of dedicated hardware. The increased security this provides is tangible.

The IBM Embedded Security Subsystem supports:

- RSA3 PKI operations, such as encryption for privacy and digital signatures for authentication
- RSA key generation
- Pseudo random number generation
- RSA-function computation in 200 milliseconds
- EEPROM memory for RSA key pair storage
- All Trusted Computing Group (TCG) functions defined in TCG Main Specification version 1.1
- Communication with the main processor through the Low Pin Count (LPC) bus

IBM Client Security Software

IBM Client Security Software comprises the following software applications and components:

- **Administrator Utility:** The Administrator Utility is the interface an administrator uses to activate or deactivate the embedded Security Subsystem, and to create, archive, and regenerate encryption keys and passphrases. In addition, an administrator can use this utility to add users to the security policy provided by Client Security Software.
- **Administrator Console:** The Client Security Software Administrator Console enables an administrator to configure a credential roaming network, to create and configure files that enable deployment, and to create a non-administrator configuration and recovery profile.
- **User Configuration Utility:** The User Configuration Utility enables a client user to change the UVM passphrase, to enable Windows logon passwords to be recognized by UVM, to update key archives, and to register fingerprints. A user can also create backup copies of digital certificates created with the IBM embedded Security Subsystem.
- **User Verification Manager (UVM):** Client Security Software uses UVM to manage passphrases and other elements to authenticate system users. For example, a fingerprint reader can be used by UVM for logon authentication. Client Security Software enables the following features:
  - **UVM client policy protection:** Client Security Software enables a security administrator to set the client security policy, which dictates how a client user is authenticated on the system.

    If policy indicates that fingerprint is required for logon, and the user has no fingerprints registered, he will be given the option to register fingerprints as part of the logon. Also, if the Windows password is not registered, or incorrectly registered, with UVM, the user will have the opportunity to provide the correct Windows password as part of the logon.
  - **UVM system logon protection:** Client Security Software enables a security administrator to control computer access through a logon interface. UVM protection ensures that only users who are recognized by the security policy are able to access the operating system.

The relationship between passwords and keys

Passwords and keys work together, along with other optional authentication devices, to verify the identity of system users. Understanding the relationship between passwords and keys is vital to understand how IBM Client Security Software works.

The administrator password

The administrator password is used to authenticate an administrator to the IBM Embedded Security Subsystem. This password, which must be eight characters long, is maintained and authenticated in the secure hardware confines of the embedded security subsystem. Once authenticated, the administrator can perform the following actions:

- Enroll users
- Launch the policy interface
- Change the administrator password

The administrator password can be set in the following ways:

- Through the IBM Client Security Setup Wizard
- Through the Administrator Utility
- Using scripts
- Through the BIOS interface (ThinkCentre computers only)

It is important to have a strategy for creating and maintaining the administrator password. The administrator password can be changed if it is compromised or forgotten.

For those familiar with Trusted Computing Group (TCG) concepts and terminology, the administrator password is the same as the owner authorization value. Since the administrator password is associated with the IBM Embedded Security Subsystem it is sometimes also referred to as the *hardware password*.

The hardware public and private keys

The basic premise of the IBM Embedded Security Subsystem is that it provides a strong *root* of trust on a client system. This root is used to secure other applications and functions. Part of establishing a root of trust is to create a hardware public key and a hardware private key. A public key and private key, together referred to as a *key pair*, are mathematically related in such a way that:

- Any data encrypted with the public key can only be decrypted with corresponding private key.
- Any data encrypted with the private key can only be decrypted with corresponding public key.

The hardware private key is created, stored and used in the secure, hardware confines of the security subsystem. The hardware public key is made available for various purposes (hence the name public key), but it is never exposed outside of the secure, hardware confines of the security subsystem. The hardware public and private keys are a critical part of the IBM key-swapping hierarchy described in a following section.

Hardware public and private keys are created in the following ways:

- Through the IBM Client Security Setup Wizard
- Through the Administrator Utility
- Using scripts

For those familiar with Trusted Computing Group (TCG) concepts and terminology, the hardware public and private keys are known as the *storage root key* (SRK).

The administrator public and private keys

The administrator public and private keys are an integral part of the IBM key-swapping hierarchy. They also allow for user-specific data to be backed up and restored in the event of system board or hard drive failure.

Administrator public and private keys can either be unique for all systems or they can be common across all systems or groups of systems. It is important to note that these administrator keys must be managed, so having a strategy for using unique keys versus known keys is important.

Administrator public and private keys can be created in one of the following ways:

- Through the IBM Client Security Setup Wizard

- Through the Administrator Utility
- Using scripts

ESS archive

The administrator public and private keys allow user-specific data to be backed up and restored in the event of a system board or hard drive failure.

User public and private keys

The IBM Embedded Security Subsystem creates user public and private keys to protect user-specific data. These key pairs are created when a user is enrolled into IBM Client Security Software. These keys are created and managed transparently by the User Verification Manager (UVM) component of IBM Client Security Software. The keys are managed based upon which Windows user is logged into the operating system.

The IBM key-swapping hierarchy

An essential element of the IBM Embedded Security Subsystem architecture is the IBM key-swapping hierarchy. The base (or root) of the IBM key-swapping hierarchy are the hardware public and private keys. The hardware public and private keys, called the *hardware key pair*, are created by IBM Client Security Software and are statistically unique on each client.

The next “level” of keys up the hierarchy (above the root) is the administrator public and private keys, or the *administrator key pair*. The administrator key pair can be unique on each machine, or it can be the same on all clients or a subset of clients. How you manage this key pair depends upon how you want to manage your network. The administrator private key is unique in that it resides on the client system (protected by the hardware public key) in an administrator-defined location.

IBM Client Security Software enrolls Windows users into the Embedded Security Subsystem environment. When a user is enrolled, user public and private keys (the *user key pair*) are created and a new key ″level″ is created. The user private key is encrypted with the administrator public key. The administrator private key is encrypted with the hardware public key. Therefore, to utilize the user private key, the administrator private key (which is encrypted with the hardware public key) must be loaded into the security subsystem. Once in the chip, the hardware private key decrypts the administrator private key. The administrator private key is now ready for use inside the security subsystem so that data that is encrypted with the corresponding administrator public key can be swapped into the security subsystem, decrypted and utilized. The current Windows user’s private key (encrypted with the administrator public key) is passed into the security subsystem. Any data needed by an application that leverages the embedded security subsystem would also be passed into the chip, decrypted and leveraged within the secure environment of the security subsystem. An example of this is a private key used to authenticate to a wireless network.

Whenever a key is needed, it is swapped into the security subsystem. The encrypted private keys are swapped into the security subsystem, and can then be used in the protected environment of the chip. The private keys are never exposed or used outside of this hardware environment. This provides for nearly an unlimited quantity of data to be protected through the IBM Embedded Security Chip.

The private keys are encrypted because they must be heavily protected and because there is limited storage space available in the IBM Embedded Security Subsystem. Only a couple of keys can be stored in the security subsystem at any given time. The hardware public and private keys are the only keys that remain stored in the security subsystem from boot to boot. In order to allow for multiple keys and multiple users, CSS utilizes the IBM key-swapping hierarchy. Whenever a key is needed, it is swapped into the IBM Embedded Security Subsystem. The related, encrypted private keys are swapped into the security subsystem, and can then be used in the protected environment of the chip. The private keys are never exposed or used outside of this hardware environment.

The administrator private key is encrypted with the hardware public key. The hardware private key, which is only available in the security subsystem, is used to decrypt the administrator private key. Once the administrator private key is decrypted in the security subsystem, a user's private key (encrypted with the administrator public key) can be passed into the security subsystem and decrypted with the administrator private key. Multiple users' private keys can be encrypted with the administrator public key. This allows for virtually an unlimited number of users on a system with the IBM ESS; however, best practices suggest that limiting enrollment to 25 users per computer ensures optimal performance.

The IBM ESS utilizes a key-swapping hierarchy where the hardware public and private keys in the security subsystem are used to secure other data stored outside the chip. The hardware private key is generated in the security subsystem and never leaves this secure environment. The hardware public key is available outside of the security subsystem and is used to encrypt or secure other pieces of data such as a private key. Once this data is encrypted with the hardware public key it can only be decrypted by the hardware private key. Since the hardware private key is only available in the secure environment of the security subsystem, the encrypted data can only be decrypted and used in this same secure environment. It is important to note that each computer will have a unique hardware public and private key. The random number capability of the IBM Embedded Security Subsystem ensures that each hardware key pair is statistically unique.

CSS public key infrastructure (PKI) features

Client Security Software provides all of the components required to create a public key infrastructure (PKI) in your business, such as:

- **Administrator control over client security policy.** Authenticating end users at the client level is an important security policy concern. Client Security Software provides the interface that is required to manage the security policy of an IBM client. This interface is part of the authenticating software User Verification Manager (UVM), which is the main component of Client Security Software.
- **Encryption key management for public key cryptography.** Administrators create encryption keys for the computer hardware and the client users with Client Security Software. When encryption keys are created, they are bound to the IBM embedded Security Chip through a key hierarchy, where a base level hardware key is used to encrypt the keys above it, including the user keys that are associated with each client user. Encrypting and storing keys on the IBM embedded Security Chip adds an essential extra layer of client security, because the keys are securely bound to the computer hardware.
- **Digital certificate creation and storage that is protected by the IBM embedded Security Chip.** When you apply for a digital certificate that can be used for digitally signing or encrypting an e-mail message, Client Security Software enables you to choose the IBM embedded Security Subsystem as the

cryptographic service provider for applications that use the Microsoft CryptoAPI. These applications include Internet Explorer and Microsoft Outlook Express. This ensures that the private key of the digital certificate is encrypted with the user's public key on the IBM embedded Security Subsystem. Also, Netscape users can choose the IBM embedded Security Subsystem as the private key generator for digital certificates used for security. Applications that use the Public-Key Cryptography Standard (PKCS) #11, such as Netscape Messenger, can take advantage of the protection provided by the IBM embedded Security Subsystem.

- **The ability to transfer digital certificates to the IBM embedded Security Subsystem.** The IBM Client Security Software Certificate Transfer Tool enables you to move certificates that have been created with the default Microsoft CSP to the IBM embedded Security Subsystem CSP. This greatly increases the protection afforded to the private keys associated with the certificates because they will now be securely stored on the IBM embedded Security Subsystem, instead of on vulnerable software.

  Note: Digital certificates protected by the IBM embedded Security Subsystem CSP cannot be exported to another CSP.
- **A key archive and recovery solution.** An important PKI function is creating a key archive from which keys can be restored if the original keys are lost or damaged. IBM Client Security Software provides an interface that enables you to establish an archive for keys and digital certificates created with the IBM embedded Security Subsystem and to restore these keys and certificates if necessary.
- **File and folder encryption.** File and folder encryption enables a client user to encrypt or decrypt files or folders. This provides an increased level of data security on top of the CSS system-security measures.
- **Fingerprint authentication.** IBM Client Security Software supports the Targus PC card fingerprint reader and the Targus USB fingerprint reader for authentication. Client Security Software must be installed before the Targus fingerprint device drivers are installed for correct operation.
- **Smart card authentication.** IBM Client Security Software supports certain smart cards as an authentication device. Client Security Software enables smart cards to be used as a token of authentication for a single user at a time. Each smart card is bound to a system unless credential roaming is being used. Requiring a smart card makes your system more secure because this card must be provided along with a password, which can be compromised.
- **Credential roaming.** Credential roaming enables an authorized network user to use any computer on the network as though it was his own workstation. After a user is authorized to use UVM on any Client Security Software-registered client, he can then import his personal data to any other registered client in the credential roaming network. His personal data is then updated automatically and maintained in the CSS archive and on any computer to which it was imported. Updates to this personal data, such as new certificates or passphrase changes, are immediately available on all other computers connected to the roaming network.
- **FIPS 140-1 certification.** Client Security Software supports FIPS 140-1 certified cryptographic libraries. FIPS-certified RSA BSAFE libraries are used on TCG-compliant systems.
- **Passphrase expiration.** Client Security Software establishes a user-specific passphrase and a passphrase expiration policy when each user is added to UVM.

Chapter 2. Encrypting and decrypting files and folders

Encryption technology enables users to protect sensitive data contained on their computers. Encrypting a file ensures that no one can access the information in the encrypted file without fulfilling the specified security requirements. Encrypting files can also protect sensitive data in files sent over the Internet or across a network.

IBM Client Security Software enables users to encrypt and decrypt sensitive files and folders in the following ways:

- **Individual file ″right-click″ encryption using the Client Security Software application.**

  This feature is a part of the base IBM Client Security Software download.
- **Transparent, on-the-fly, file and folder encryption using the IBM File and Folder Encryption utility.**

  Note: The IBM File and Folder Encryption (FFE) utility must be downloaded for this feature to be enabled. IBM Client Security Software must be installed *before* you install the IBM File and Folder Encryption utility.

Right-click encryption

The basic right-click encryption function of Client Security Software enables users to protect sensitive files and folders using the right-click button of their mouse. No additional software needs to be downloaded to utilize this function. Files encrypted with this function will have the following characteristics:

- You must manually decrypt an encrypted file every time you want to use it, and, when finished, manually encrypt it to protect it again. UVM policy must be evoked every time you encrypt or decrypt the file. These requirements provide strong, manual control of the encryption and decryption of the selected files, but this stringent protection is less convenient to users who do not want to provide a password, fingerprint, or smart card every time that they use an encrypted file.
- Files can be sent to a remote location in their encrypted state; however, they can only be decrypted on the computer that was used to encrypt them because the keys used to encrypt the files are unique to the IBM embedded Security Subsystem on that computer.

Files can be encrypted and decrypted manually through the right-click menu. When files are encrypted in this manner, the encryption operation appends a `.$enc$` extension to the files. These encrypted files can then be securely stored on remote servers. They will remain encrypted and unavailable to applications for use until the right-click function is used again to decrypt them.

The contents of entire folders can also be encrypted with right-click encryption. When folders are encrypted in this manner, all the files contained within the selected folder are encrypted. The encryption operation appends a `.$enc$` extension to all files in the selected folder. These encrypted files can then be securely stored on remote servers. They will remain encrypted and unavailable to applications for use until the right-click function is used again to decrypt them.

Transparent on-the-fly encryption (FFE encryption)

While the basic function of right-click encryption enables the end user to explicitly protect individual files and folders, the process can be cumbersome since manual intervention is required each time a user wants to encrypt or decrypt a file. A more convenient, transparent way of encrypting and decrypting files is available through the File and Folder Encryption (FFE) utility, which can be downloaded from the Client Security Web site. Users who want to take advantage of FFE should download this utility from the Client Security Web site and install it after installing Client Security Software.

With File and Folder Encryption, users identify one or more folders to be designated as secure repositories for their critical data. After FFE is installed, users can right-click on a folder and use the `protect folder` option. When the user selects the protect folder option, he designates this folder to participate in FFE. All of the files contained in an FFE-protected folder or any of its subfolders are automatically encrypted when not in use.

The transparent, on-the-fly encryption feature of Client Security Software is enabled by downloading the IBM File and Folder Encryption (FFE) utility, which is available on the IBM Client Security Web site. FFE provides a more convenient, transparent form of encryption than the basic ″right-click″ encryption feature of CSS. FFE-encrypted folders will have the following characteristics:

- UVM policy only needs to be evoked at startup. This provides a more convenient form of encryption and decryption of the selected files because you do *not* need to provide a password, fingerprint, or smart card every time that you want to use an encrypted file.
- When an application opens a file that is encrypted using the File and Folder Encryption utility, the file is automatically decrypted. When a file that is encrypted using the File and Folder Encryption utility is saved, it is automatically encrypted.
- Files that are encrypted with the File and Folder Encryption (FFE) utility can be sent to a remote location; however, they will be sent in a decrypted state.

The Check Disk utility might run when restarting the operating system after protecting or unprotecting folders. Wait for the system to be checked before using your computer.

A UVM-enrolled user that has downloaded and installed the FFE utility can select a folder to protect or unprotect using the right-click interface. Note that the user can still right-click encrypt individual files manually on a file-by-file basis. However, after FFE is installed, all folder encryption is accomplished on-the-fly. When files are protected in this manner, no extension is appended to the file name. When an application accesses a file in an encrypted folder, the file will be decrypted into memory and will be re-encrypted before it is saved on the hard disk.

Any Windows operation that accesses a file in an FFE-protected folder will be given access to the data in a decrypted form. This feature makes encryption more convenient because a file does not have to be decrypted every time it is used, or re-encrypted every time a program is finished with it.

FFE folder-encryption status

The File and Folder Encryption utility enables users to protect sensitive files and folders using the right-click button of their mouse. How the software protects a file and folder differs depending upon how the file or folder is initially encrypted.

A folder can be in any one of the following states:

- **An Unprotected Folder**

  Neither this folder, its subfolders, nor any of its parents has been designated as protected. The user is given the option to protect this folder.

- **A Protected Folder**

  A protected folder can be in one of three states:

  - **Protected by the current user**

    The current user has designated this folder as protected. All files are encrypted, including files in all subfolders. The user is given the option to unprotect the folder.

  - **A subfolder of a folder protected by the current user**

    The current user has designated one of this folder's parents as protected. All files are encrypted. The current user has no right-click options.

  - **Protected by a different user**

    A different user has designated this folder as protected. All files are encrypted, including files in all subfolders, and are unavailable to the current user. The current user has no right-click options.

- **A Parent of a Protected Folder**

  A parent of a protected folder can be in one of three states:

  - **It can contain one or more subfolders protected by the current user**

    The current user has designated one or more subfolders as protected. All files in the protected subfolders are encrypted. The user is given the option to protect the parent folder. All subfolders in the parent folder must be unprotected before the parent folder can be protected.

  - **It can contain one or more subfolders protected by one or more different users**

    A different user or users have designated one or more subfolders as protected. All files in the protected subfolders are encrypted, and are unavailable to the current user. The current user has no right-click options.

  - **It can contain subfolders protected by the current user and one or more different users**

    Both the current user and one or more different users have designated subfolders as protected. The current user has no right-click options.

- **A Critical Folder**

  A critical folder is a folder in a critical path and, therefore, cannot be protected. There are two critical paths: the Windows path and the Client Security path.

Each state is handled differently by the right-click protect folder option.

File and Folder Encryption utility tips

The following information might be useful when performing certain FFE utility functions.

Deleting protected files and folders

To ensure that no sensitive files or folders are left unprotected in the Recycle Bin, you must use the Shift+Del key combination to delete protected folders and files. The Shift+Del key sequence performs an unconditional delete operation and does not attempt to put deleted files in the Recycle Bin.

Before upgrading from a previous version of the IBM FFE utility

Before you upgrade from version 2.0 or earlier of the IBM FFE utility, download and use the Access Control List (ACL) Repair Tool from the IBM Security Web site. This repair utility should be used *before* uninstalling any version of FFE prior to 2.0. Otherwise, the uninstallation process might fail and leave affected files inaccessible.

Before uninstalling the IBM FFE utility

Before you uninstall the IBM FFE utility, use the IBM FFE utility to unprotect any files or folders that are currently protected.

File and Folder Encryption (FFE) utility limitations

The IBM FFE utility has the following limitations:

Drive-letter protection

The IBM FFE utility can be used to encrypt files and folders on the C drive only. This utility does not support encryption on any other hard-disk partition or physical drive.

Limitations when moving protected files and folders

The IBM FFE utility does not support the following actions:

- Moving files and folders within protected folders
- Moving files or folders between protected and unprotected folders

If you attempt to perform either of these unsupported Move operations, an ″Access Denied″ message will be displayed by the operating system. This message is normal. It simply provides notification that this Move operation is not supported. As an alternative to using a Move operation, do the following:

1. Copy the protected files or folders to the new location.
2. Delete the original files or folders by using the Shift+Del key combination.

Limitations when running applications

The IBM FFE utility does not support running applications from a protected folder. For example, if you have an executable named PROGRAM.EXE, you cannot run that application from a protected folder.

Path name length limitations

As you attempt to protect a folder using the IBM FFE utility or attempt to copy or move a file or folder from an unprotected folder to a protected folder, you might receive a ″One or more path names are too long″ message from the operating system. If you receive this message, you have one or more files or folders that have

a path that exceeds the maximum allowable character length. To correct the problem, either rearrange the folder structure to shorten its depth or shorten some folder or file names.

Problems protecting a folder

If you attempt to protect a folder and receive a message stating, "The folder cannot be protected. One or more files may be in use," check the following:

- Verify that none of the files contained in the folder are currently in use.
- If Windows Explorer is displaying one or more subfolders of a folder that you are attempting to protect, make sure that the folder you are attempting to protect is highlighted and active, not any of the subfolders.

Chapter 3. CSS Credential Roaming

The credential roaming feature of IBM Client Security Software enables a UVM user's credentials to be used on all ESS-enabled computers within a network. This network, called a roaming network, enhances users' flexibility and increases application availability by enabling users to easily work from any computer in the network.

CSS Credential Roaming network requirements

A CSS Credential Roaming network is made up of the following necessary components:

- Roaming server
- Roaming clients
- Shared, mapped network drive to store UVM user archives

Note: The roaming server and authorized roaming clients are simply ESS-enabled computers with established administrator passwords that have IBM Client Security Software 5.1 or higher installed.

Setting up a roaming server

To configure a CSS Credential Roaming network, you must designate one computer as the roaming *server* (referred to as system A). The other computers, once registered by the roaming server, are authorized CSS-registered *clients*. (The first registered client is referred to as system B.)

There is nothing special about the computer that you designate the roaming server. You can use any computer that will be a part of the roaming network. The roaming server is simply the computer designated to establish which computers are ″trusted″ by the roaming network. After a computer is registered with the roaming server, it is trusted by all computers in the network.

Configuring a roaming network is a two step process:

1. Configure system A (server) by establishing the keys, archive, and roaming users.
2. Register system B and all other computers as roaming clients in the CSS Credential Roaming network.

The roaming server defines the CSS Credential Roaming network and initiates registration of roaming clients, but the focal point of a CSS Credential Roaming network is the mapped, network drive where user archives are stored. This archive is where all updates to user credentials are stored. The archive should *not* be located on the roaming server or on any of the roaming clients. After initializing the CSS clients, the roaming server acts like any other CSS-registered client.

Configuring a roaming server

To configure a roaming server, complete the following procedure:

1. On the designated computer, start the Administrator Console, and then click **Configure Credential Roaming**. Or, if the computer is already configured for roaming, select **Reconfigure this system as a CSS Roaming Server** and click **Next**.
2. Create the `c:\roaming` folder on the computer designated as the roaming server.
3. Start the Administrator Console and click **Configure Credential Roaming**.
4. Select **Configure this system as a CSS Roaming Server** and click **Next**.
5. Click **Configure**.
6. Select **Create new archive keys** and type the new key folder in the Archive key folder field, where the archive key folder is stored in `c:\roaming` folder.
7. Choose to use an existing key pair or to create a new key pair, and then click **Next**.
8. Enter the archive folder, and then click **Next**.

   Note: The archive folder and key folder must be accessible to the other computers that are registered for roaming (roaming clients). The `c:\roaming` directory must be a mapped network drive.

   If the archive currently has files in it, the next wizard page prompts you on how to handle the files.
9. Click **Finish**.

Registering clients on the roaming server

To register a roaming client on the roaming server, complete the following procedure:

1. Immediately after completing roaming server configuration, the Credential Roaming Network Configuration screen is displayed. Select **Enable client registration**, and then click **Next**.
2. Enter the name of the user on system B with administrator rights who will complete the client registration.
3. Enter and confirm an 8-character password to be used by that user. (Do not confuse this process with authorizing a user to use UVM, which happens later.)
4. If you want to register the client using the User Configuration Utility, you need to create an administrator configuration file for that user. This process generates a file that is unique to this user. Store this file in a location accessible to the user and to system B.

   Note: This file does not need to be generated when registering a client using the Administrator Utility.
5. Enter the administrator password for system B and click **Next**.
6. If you created an administrator configuration file, save the file in a location accessible to the user and to system B.

After completing the previous procedures, the roaming server is configured. Registration must be complete on each roaming client before the roaming network is ready for use.

Completing the roaming-client registration process

After the list of trusted systems have been registered on the roaming server, you must complete one of the following procedure on the client systems. The roaming server must be running and connected to the archive before you can complete the roaming-client registration process.

Registering a roaming client using the Administrator Utility

To register a roaming client using the Administrator Utility, complete the following procedure:

1. Click **Key Configuration**.
2. Click **No** if you are asked if you want to restore keys from the archive.
3. Select Register this system with a CSS Roaming Server, and then click **Next**.
4. Enter the archive location created by system A, type the system-registration password designated for this user on system A, and then click **Next**.

   It takes about a minute to complete the registration.

Registering a roaming client using the User Configuration Utility

To register a roaming client using the User Configuration Utility, complete the following procedure:

1. From the User Configuration tab, click **Register with a CSS Roaming Server**.
2. Select the administrator configuration file generated on system A, type the system-registration password designated for this user on system A, and then click **Next**.
3. Enter the archive location created by system A, and then click **Next**.

   It takes about a minute to complete the registration.

Registering a roaming client using mass deployment (silently)

To register a roaming client silently using mass deployment, complete the following procedure:

1. Create the `csec.ini` file. See the *Client Security Software Installation Guide* for details about how to create a CSS .ini file.
2. In the `csssetup` section of the file, add `"enableroaming=1"`. This indicates that the computer should be registered as a roaming client.
3. In the same section, add the entry `"username=OPTION"`. There are three possible options for this value:
   - **Option 1: The string `"[promptcurrent]"` - brackets included.** This designation should be used if a .dat file for the currently logged on user has been generated on the roaming server and the current user knows the system-registration password. This option causes a pop-up window to prompt the user to enter the system-registration password (`sysregpwd`) before deployment.
   - **Option 2: The string `"[current]"` - brackets included.** This designation should be used if a .dat file for the currently logged on user has been generated on the server. The `sysregpwd` is handled as described in the next step.
   - **Option 3: An actual user name such as `"joseph"`.** If such a designated user name is used, `"joseph.dat"` must have been previously generated by the roaming server. The `sysregpwd` for this case is also handled as described in the next step.
4. If options two or three above are used, another entry `"sysregpwd=SYSREGPW"` must be supplied. This is the eight-digit system-registration password associated either with the current user (if option two is implemented) or the designated user (if option three is implemented).

5. To complete the client registration, connect the computer to the archive set up by the roaming server. This archive is designated in the `csec.ini` file. The key folder which was set on the CSS Credential Roaming server is also designated in the `csec.ini` file.
6. Encrypt the `csec.ini` file using the Administrator Console.

Examples of the csec.ini file

The examples below show a sample `csec.ini` file, and how it changes depending upon which credential roaming option is selected. These options are as follows:

- **No roaming values.** This base file is not enabled for credential roaming.
- **Roaming option 1.** This file is enabled for roaming using option 1 for client registration. The current user must present the system-registration password before deployment.
- **Roaming option 2.** This file is enabled for roaming using option 2 for client registration. The current user must present the userID and the system-registration password designated in the .ini file.
- **Roaming option 3.** This file is enabled for roaming using option 3 for client registration. The user is designated in the .ini file. The system-registration password for the designated user must be presented in the .ini file.

Examples of four separate CSEC.INI file are as follows:

[CSSSetup]	**Option 1** [CSSSetup]	**Option 2** [CSSSetup]	Option 3 [CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\\computer name\jgk, where computer stored the key pair on the roaming server	kpl=c:\\computer name\jgk, where computer stored the key pair on the roaming server	kpl=c:\\computer name\jgk, where computer stored the key pair on the roaming server
kal=c:\jgk\archive	kal=c:\\computer name\archive, where computer stored the achive on the roaming server	kal=c:\\computer name\archive, where computer stored the achive on the roaming server	kal=c:\\computer name\archive, where computer stored the achive on the roaming server
pub= c:\jk\admin.key	pub= c:\jk\admin.key	pub= c:\jk\admin.key	pub= c:\jk\admin.key
pri= c:\jk\private1.key	pri= c:\jk\private1.key	pri= c:\jk\private1.key	pri= c:\jk\private1.key
wiz=0	wiz=0	wiz=0	wiz=0
clean=0	**enableroaming=1** **username=** **[promptcurrent]** clean=0	**enableroaming=1** **username=** **[current]** **sysregpwd=12345678** clean=0	**enableroaming=1** **username=** **joseph** **sysregpwd=12345678** clean=0
[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]
enrollall=0	enrollall=0	enrollall=0	enrollall=0
enrollusers=1	enrollusers=1	enrollusers=1	enrollusers=1
user1=joseph	user1=joseph	user1=joseph	user1=joseph
user1uvmpw= q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r
user1winpw=	user1winpw=	user1winpw=	user1winpw=

user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays= 184	user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184	user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184	user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184
[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0

Managing a roaming network

The network administrator of a roaming network must authorize users and manage user and client access to the network. This might include importing a user profile, synchronizing user data, or adding and removing users and clients is quick and easy on a CSS roaming network. It might also entail restoring the roaming network, changing the administrator key pair, or changing the archive location.

Authorizing users

After completing the previous procedures, the CSS Credential Roaming network is configured and the roaming clients are registered for roaming. Users can now be authorized using the Administrator Utility.

Synchronizing user data

Each user's data is stored in the archive location. A copy of that data is also stored locally on every computer to which he has roamed. When changes are made, such as obtaining a certificate or changing a passphrase, the local data is updated. If the computer is connected to the archive, the user's data is also updated. When the user logs onto another computer, updates are automatically downloaded to that computer, provided that it is also connected to the archive.

Connection to the archive is not always guaranteed, however, so sometimes a user's data can be inconsistent between computers and the archive. If a user's data is changed on a computer that is not connected to the archive, the changes are not reflected in the archive and, consequently, not on other computers either. Once the computer is connected to the archive, the changes are updated in the archive and any data inconsistencies are subsequently resolved on other connected computers as well. However, if changes are made on another computer that is connected to the archive before the first computer that contained changes gets connected to the archive, a non-correctable data inconsistency issue arises. The data in the archive contains changes that are not present on the first computer, while that computer contains changes that are not in the archive. If this occurs, the user is notified of the two different configurations and is prompted to choose which configuration to preserve, the local one or the archived one. The configuration changes that are not chosen are lost. It is important, therefore, to make sure that any changes made to a user's configuration are updated to the archive before making changes on any other computer.

Recovering a lost passphrase in a roaming environment

When a passphrase is lost or forgotten, the administrator can reset the user passphrase on the roaming server or any registered client. This change will be updated on all systems in the network *except* systems that the user has imported to that have secure UVM logon protection enabled. In these cases, the passphrase update will *not* be reflected on the computer. In order to gain access to the computer, the user will need a password override file and will need to complete the password override process.

Importing a user profile

A user profile can be imported to a new computer on the roaming network using the Administrator Utility, the User Configuration Utility, or the UVM GINA. If you want to import a user who does not have a user account on the new computer, you must create a Windows user account through the Windows Control Panel.

Note: In order to import a user to a roaming network, the user must be authorized on another computer in the roaming network.

Importing a user profile using the User Configuration Utility

To import a user profile to a new computer on the roaming network using the User Configuration Utility, log onto the system with the user you want to import, and click **Start > Programs > Access IBM > IBM Client Security Software > Modify Your Security Settings** and then click **Import existing configuration from archive** on the User Configuration tab.

Importing a user profile using the Administrator Utility

To import a user profile to a new computer on the roaming network using the Administrator Utility, select the user and then click **Authorize**. Click **Yes** when asked if you want to import the user from the archive.

Importing a user profile using the UVM GINA

A user profile can be imported to a new computer on the roaming network using the UVM GINA. This process is begun from the UVM-logon screen. If a user is not yet authorized to use UVM on a given system in the network, a message box is displayed asking if the user wants to be imported from the archive.

Notes:

1. If you want to import a user that does not have a user account on the new computer, you must create a Windows user account using the Windows Control Panel before continuing.
2. To access the archive on the roaming server, the directory must be a mapped network drive.

To import a user profile to a new computer on the roaming network using the UVM GINA on a computer running Windows 2000, complete the following procedure:

1. At logon, enter the user name and UVM passphrase of the user you would like to import. A message is displayed asking if you want to import the user profile from the archive.
2. Click **Yes** at the prompt to import user, and then **OK**.
3. If the archive location is on a network drive, click **Yes** at the prompt indicating a network share must be provided.
4. Enter your Windows password at the standard Windows logon screen. A prompt for the archive path is displayed.

5. Enter the archive network path.
6. Enter username and password for the network path.
7. Click **OK**. If the operation completed properly, a message displays indicating that the profile was successfully imported.

To import a user profile to a new computer on the roaming network using the UVM GINA on a computer running Windows XP, complete the following procedure:

1. At logon, enter the user name and UVM passphrase of the user you would like to import. A message is displayed asking if you want to import the user profile from the archive.
2. Click **Yes** at the prompt to import user, and then **OK**.
3. If the archive location is on a network drive, click **Yes** at the prompt indicating a network share must be provided.
4. At the standard Windows map network drive prompt, enter the archive network path.
5. Click **Finish**.
6. Enter the username and password for the network path and click **OK**. If the operation completed properly, a message displays indicating that the profile was successfully imported.

Note: In order to import a user to a roaming network, the user must be authorized on another computer in the roaming network.

After importing the user profile, authentication with UVM is based on that computer security policy. The security requirements for that computer must be successfully provided before the user can log on.

Removing and reinstating users in a roaming network

To remove a user from a roaming network, the network administrator must complete the following Administrator Console procedure:

1. Start the Administrator Console utility and enter the administrator password.
2. Click **Configure Credential Roaming**.
3. Select **Remove Users from UVM and the Credential Roaming Network** and click **Next**. Repeat as necessary.
4. Select the user to be removed and click **Remove**.

   Note: Once a user is removed from the network, all credentials belonging to that user are permanently lost.

Removed users may not be authorized to use UVM and the roaming network until reinstated by the network administrator.

To reinstate a user in a roaming network, the network administrator must complete the following Administrator Console procedure:

1. Start the Console Utility and enter the administrator password.
2. Click **Configure Credential Roaming**.
3. Select **Reinstate removed users** and click **Next**.
4. Select the user to be reinstated and click **Reinstate**. Repeat as necessary.

   Once the user is reinstated, he may be re-authorized to user UVM. Reinstating a user does not automatically authorize him to use UVM.

Removing and reinstating registered clients in a roaming network

To remove a registered client from a roaming network, the network administrator must complete the following Administrator Console procedure:

1. Start the Console Utility and enter the administrator password.
2. Click **Configure Credential Roaming**.
3. Select **Remove Registered Clients from the Credential Roaming Network** and click **Next**.
4. Select the system to be removed and click **Remove**. Repeat as necessary.

   Note: Once a client is removed from the network, all machine based credentials belonging to that system are permanently lost.

Removed clients may not be registered with the network roaming server until reinstated by the network administrator.

To reinstate a registered client to a roaming network, the network administrator must complete the following Administrator Console procedure:

1. Start the Console Utility and enter the administrator password.
2. Click **Configure Credential Roaming**.
3. Select **Reinstate removed clients** and click **Next**.
4. Select the client to be reinstated and click **Reinstate**. Repeat as necessary.

   Once the client is reinstated, it may be re-registered with the roaming server. Reinstating a client does not automatically re-register it.

Note: Any users whose credentials were present on the system at the time the client was removed, might need to import their credentials again.

Restricting access to registered clients in a roaming network

There might be times when a network administrator will want to allow some users access to a particular registered client while restricting access to other users.

To manage user access rights, the network administrator must complete the following Administrator Console procedure:

1. Start the Console Utility and enter the administrator password.
2. Click **Configure Credential Roaming**.
3. Select **Manage user access to Registered Clients** and click **Next**.
4. Select the registered client to manage in the **Select a system in the CSS Roaming Network** box. Users with and without access are listed in the two list boxes.
5. Do one of the following:
   - To restrict access to a user, select the user from the **Users with access** list and click **Restrict**. Repeat as necessary.
   - To grant access to a restricted user, select the user from the **Users with no access** list and click **Allow**. Repeat as necessary.

The access-management functions of the roaming network necessitate that a new folder be created in the archive. The new folder, named Protected, must be writable by the network administrator and must be read-only to other users. If users have write access to this folder, they can manually reinstate themselves or their systems.

Restoring a roaming network

In the event of a software or hardware failure, the roaming network might need to be restored. If the roaming server is corrupted or the data used by CSS is corrupted on a registered client, restore the data using the Administrator Utility in the same manner as a non-roaming environment. If the IBM embedded Security subsystem on a registered client fails or is cleared, the client must be re-registered with the roaming server. No other action is necessary.

Changing the administrator key pair

It is not recommended that you change the administrator key pair in a roaming network because it will require each client to be re-registered with the roaming server.

To change the administrator key pair in a roaming network, the following steps must be completed for the change to be reflected on all computers in the network.

1. On the roaming server, change the administrative key pair using the Administrator Utility.
2. Re-register all the clients in the network.
3. Preserve existing files whenever prompted.

Changing the archive folder

Changing the archive folder in a roaming environment differs slightly from a non-roaming environment because each computer in the network accesses the same archive location.

To change the archive folder on a roaming network, complete the following procedure:

1. Copy the files from the old archive folder to the new using the following procedure:
   a. Start the Administrator Utility and enter the administrator password.
   b. Click **Key Configuration**.
   c. Select Change the archive location, and then click **Next**.
   d. Enter the new folder of the archive, and then click **Next**.
   e. Click **Yes** when prompted to copy all the files from the old folder to the new one.
2. Update all other computers on the network to use the new archive folder using the following procedure:
   a. Start the Administrator Utility and enter the administrator password.
   b. Click **Key Configuration**.
   c. Select Change the archive location, and then click **Next**.
   d. Enter the new folder of the archive, and then click **Next**.
   e. Click **No** when prompted to copy all the files from the old folder to the new one.

File and Folder Encryption (FFE)

File and Folder Encryption functionality is unaffected by a roaming environment. However, protected folders are managed on a computer-by-computer basis. Thus, if a folder is protected by user A on system A, a folder of the same name on system B, if it exists, is not protected unless the user actively protects it on system B.

IBM Password Manager

All passwords protected using the IBM Password Manager are available on all computers in the roaming network.

Roaming terms and definitions

The following terms are useful to understand when discussing the concepts and procedures involved in setting up a roaming network:

Roaming client registration
The process of registering a computer with the roaming server.

Roaming clients
All trusted computers in the roaming network.

Roaming server
The ESS computer used to initiate the roaming network.

Roaming client-registration password
The password used to register the computer with the roaming server.

Chapter 4. Instructions for the client user

This section provides information to help a client user perform the following tasks:

- Use UVM protection for the system logon
- Use the User Configuration Utility
- Use secure e-mail and Web browsing
- Configure UVM sound preferences

Using UVM protection for the system logon

This section contains information about using UVM logon protection for the system logon. Before you can use UVM protection, it must be enabled for the computer.

UVM protection enables you to control access to the operating system through a logon interface. UVM logon protection replaces the Windows logon application, so that when a user unlocks the computer, the UVM logon window opens instead of the Windows logon window. After UVM protection is enabled for the computer, the UVM logon interface will open when you start the computer.

When the computer is running, you can access the UVM logon interface by pressing **Ctrl + Alt + Delete** to shut down or lock the computer, or to open the Task Manager or log off the current user.

Unlocking the client

To unlock a Windows client that uses UVM protection, complete the following procedure:

1. Press **Ctrl + Alt + Delete** to access the UVM logon interface.
2. Type your user name and the domain you are logged onto, and then click **Unlock**.

   The UVM passphrase window opens.

   Note: Although UVM recognizes multiple domains, your user password must be the same for all domains.
3. Type your UVM passphrase, and then click **OK** to access the operating system.

Notes:

1. If the UVM passphrase does not match the user name and domain entered, the UVM logon window opens again.
2. Depending on the UVM policy authentication requirements for the client, further authentication processes might also be required.

The User Configuration Utility

The User Configuration Utility enables the client user to perform various security maintenance tasks that do not require administrator access.

User Configuration Utility features

The User Configuration Utility enables the client user to do the following:

- **Update passwords and archive.** This tab enables you to perform the following functions:
  - **Change the UVM passphrase.** To improve security, you can periodically change the UVM passphrase.
  - **Update Windows password.** When you change the Windows password for a UVM-authorized client user with the Windows User Manager program, you must also change the password by using the IBM Client Security Software User Configuration Utility. If an administrator uses the Administrator Utility to change the Windows logon password for a user, all user encryption keys previously created for that user will be deleted, and the associated digital certificates will become invalid.
  - **Reset the Lotus Notes password.** To improve security, Lotus Notes users can change their Lotus Notes password.
  - **Update the key archive.** If you create digital certificates and want to make copies of the private key stored on the IBM embedded Security Chip, or if you want to move the key archive to another location, update the key archive.
- **Configure UVM sound preferences.** The User Configuration Utility enables you to select a sound file to be played at authentication success and failure.
- **User configuration.** This tab enables you to perform the following functions:
-
  - **Reset user.** This function enables you to reset your security configuration. When you reset your security configuration, all previous keys, certificates, fingerprints, etc. are erased.
  - **Restore user security configuration from archive.** This function enables you to restore settings from the archive. This is useful if your files have become corrupted or if you want to return to a previous configuration.
  - **Register with a CSS Roaming Server.** This function enables you to register this system with a CSS Roaming Server. Once the system is registered, you will be able to import your current configuration to this system.

User Configuration Utility Windows XP limitations

Windows XP imposes access restrictions which limit the functions available to a client user under certain circumstances.

Windows XP Professional

In Windows XP Professional, client user restrictions might apply in the following situations:

- Client Security Software is installed on a partition that is later converted to an NTFS format
- The Windows folder is on a partition that is later converted to an NTFS format
- The archive folder is on a partition that is later converted to an NTFS format

In the above situations, Windows XP Professional Limited Users might not be able to perform the following User Configuration Utility tasks:

- Change their UVM passphrases
- Update the Windows password registered with UVM
- Update the key archive

These limitations are cleared after an administrator starts and exits the Administrator Utility.

Windows XP Home

Windows XP Home Limited Users will not be able to use the User Configuration Utility in any of the following situations:

- Client Security Software is installed on an NTFS formatted partition
- The Windows folder is on an NTFS formatted partition
- The archive folder is on an NTFS formatted partition

Using the User Configuration Utility

To use the User Configuration Utility, complete the following procedure:

1. Click **Start > Programs > Access IBM > IBM Client Security Software > Modify Your Security Settings**.

   The IBM Client Security Software User Configuration Utility main screen is displayed.
2. Select one of the following tabs:
   - **Update Passwords and Archive.** This tab enables you to change your UVM passphrase, update your Windows password in UVM, reset your Lotus Notes password in UVM, and update your encryption archive.
   - **Configure UVM Sounds.** This tab enables you to select a sound file to be played at authentication success and failure.
   - **User Configuration.** This tab enables a user to restore his user configuration from archive, reset his security configuration, or register with the roaming server (if the computer can be used as a roaming client).
3. Click **OK** to exit.

Using secure e-mail and Web browsing

If you send unsecured transactions over the Internet, they are subject to being intercepted and read. You can prohibit unauthorized access to your Internet transactions by getting a digital certificate and using it to digitally sign and encrypt your e-mail messages or to secure your Web browser.

A digital certificate (also called a digital ID or security certificate) is an electronic credential issued and digitally signed by a certificate authority. When a digital certificate is issued to you, the certificate authority is validating your identity as the owner of the certificate. A certificate authority is a trusted provider of digital certificates and can be a third-party issuer such as VeriSign, or the certificate authority can be set up as a server within your company. The digital certificate contains your identity, such as your name and e-mail address, expiration dates of the certificate, a copy of your public key, and the identity of the certificate authority and its digital signature.

Using Client Security Software with Microsoft Applications

The instructions provided in this section are specific to the use of Client Security Software as it generally relates to obtaining and using digital certificates with applications that support the Microsoft CryptoAPI, such as Outlook Express.

For details on how to create the security settings and use e-mail applications such as Outlook Express and Outlook, see the documentation provided with those applications.

Obtaining a digital certificate for Microsoft applications

When you use a certificate authority to create a digital certificate to be used with Microsoft applications, you will be prompted to choose a cryptographic service provider (CSP) for the certificate.

To use the cryptographic capabilities of the IBM embedded Security Chip for your Microsoft applications, make sure you select **IBM embedded Security Subsystem CSP** as your cryptographic service provider when you obtain your digital certificate. This ensures that the private key of the digital certificate is stored on the IBM Security Chip.

Also, if available, select strong (or high) encryption for extra security. Because the IBM embedded Security Chip is capable of up to 1024-bit encryption of the private key of the digital certificate, select this option if it is available within the certificate authority interface; 1024-bit encryption is also referred to as strong encryption.

After you select **IBM embedded Security Subsystem CSP** as the CSP, you might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements for obtaining a digital certificate. The authentication requirements are defined in the UVM policy for the computer.

Transferring certificates from the Microsoft CSP

IBM CSS Certificate Transfer Wizard enables you to transfer certificates that have been created with the default Microsoft CSP to the IBM embedded Security System CSP. Transferring your certificates greatly increases the protection afforded to the private keys associated with the certificates because they will be securely stored through the IBM embedded Security Subsystem, instead of through vulnerable software.

There are two types of security certificates that can be transferred:

- **User Certificates:** The purpose of a user certificate is to authorize a given user. It is a common practice to obtain a user certificate from a Certificate Authority (CA), such as cssdesk. A Certificate Authority is a trusted entity that stores, issues, and publishes certificates. You might need a user certificate to sign emails, encrypt emails, or to log on to a specific server.
- **Machine Certificates:** The purpose a machine certificate is to uniquely identify a specific computer. When a machine certificate is used, the authentication is based on the computer used, not on who is using it.

The CSS Certificate Transfer Wizard application only transfers Microsoft certificates that are marked as exportable, and is limited to certificates that are no more than 1024 bits in key size.

If a user needs to transfer a machine certificate but does not have administrator rights for the system, an administrator can send an administrator configuration file that enables a user transfer a certificate without having to provide the administrator password. Use the Administrator Console utility, located in the `c:\\program files\ibm\security` folder, to create an administrator configuration file.

To use the CSS Certificate Transfer Wizard, complete the following procedure:

1. Click **Start > Access IBM > IBM Client Security Software > CSS Certificate Transfer Wizard**.

   The IBM CSS Certificate Transfer Wizard welcome screen is displayed.

2. Click **Next** to begin.
3. Select the types of certificates to transfer and click **Next**. The CSS Certificate Transfer Wizard can only transfer certificates in the Microsoft certificate store that are marked as exportable.
4. Select the certificates to transfer by clicking on the certificate name displayed in the Issued to area of the interface and then click **Next**. A message indicates that the certificate transferred successfully.

   Note: Transferring a machine certificate will require the administrator password or an administrator configuration file.
5. Click **OK** to return to the CSS Certificate Transfer Wizard.

After certificates are transferred, they are associated with the IBM embedded Security Subsystem CSP, and the private keys are protected by the IBM embedded Security Subsystem. Any operations using these private keys, such as creating digital signatures or decrypting e-mail, will be done from within the protected environment of the IBM embedded Security Subsystem.

Updating the key archive for Microsoft applications

After you create a digital certificate, back up the certificate by updating the key archive. You update the key archive using the Administrator Utility.

Using the digital certificate for Microsoft applications

Use the security settings in your Microsoft applications to view and use digital certificates. See the documentation provided by Microsoft for more information.

After you create the digital certificate and use it to sign an e-mail message, UVM will prompt you for authentication requirements the first time you digitally sign an e-mail message. You might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements for using the digital certificate. The authentication requirements are defined in the UVM policy for the computer.

Configuring UVM sound preferences

The User Configuration Utility enables you to configure sound preferences using the provided interface. To change the default sound preferences, complete the following procedure:

1. Click **Start > Programs > Access IBM > IBM Client Security Software > Modify Your Security Settings**.

   The IBM Client Security Software user Configuration Utility screen is displayed.
2. Select the **Configure UVM Sounds** tab.
3. In the UVM Authentication Sounds area, type the file path to the sound file that you would like to associate with a successful authentication in the Authentication success field, or click **Browse** to select the file.
4. In the UVM Authentication Sounds area, type the file path to the sound file that you would like to associate with an unsuccessful authentication in the Authentication failure field, or click **Browse** to select the file.
5. Click **OK** to complete the process.

Chapter 5. Troubleshooting

The following section presents information that is helpful for preventing, or identifying and correcting problems that might arise as you use Client Security Software.

Administrator functions

This section contains information that an administrator might find helpful when setting up and using Client Security Software.

IBM Client Security Software can only be used with IBM computers that contain the IBM embedded Security Subsystem. This software consists of applications and components that enable IBM clients to secure their sensitive information through secure hardware rather than through vulnerable software.

Authorizing users

Before client user information can be protected, IBM Client Security Software **must** be installed on the client and users **must** be authorized to use the software. An easy-to-use Setup Wizard guides you through the entire installation process.

Important: At least one client user **must** be authorized to use UVM during setup. If no user is authorized to use UVM when initially setting up Client Security Software, your security settings will **not** be applied and your information will **not** be protected.

If you completed the Setup Wizard without authorizing any users, shut down and restart your computer; then run the Client Security Setup Wizard from the Windows Start menu and authorize a Windows user to use UVM. This will enable IBM Client Security Software to apply your security settings and protect your sensitive information.

Deleting users

When you delete a user, the user name is deleted from the list of users in the Administrator Utility.

Setting a BIOS administrator password (ThinkCentre)

Security settings available in the Configuration/Setup Utility enable administrators to do the following:

- Enable or disable the IBM embedded Security Subsystem
- Clear the IBM embedded Security Subsystem

Attention:

- When the IBM embedded Security Subsystem is cleared, all encryption keys and certificates stored on the subsystem are lost.

Because your security settings are accessible through the Configuration/Setup Utility of the computer, set an administrator password to deter unauthorized users from changing these settings.

To set a BIOS administrator password:

1. Shut down and restart the computer.
2. When the Configuration/Setup Utility prompt appears on the screen, press **F1**.
   The main menu of the Configuration/Setup Utility opens.
3. Select **System Security**.
4. Select **Administrator Password**.
5. Type your password and press the down arrow on your keyboard.
6. Type your password again and press the down arrow.
7. Select **Change Administrator password** and press Enter; then press Enter again.
8. Press **Esc** to exit and save the settings.

After you set a BIOS administrator password, a prompt appears each time you try to access the Configuration/Setup Utility.

Important: Keep a record of your BIOS administrator password in a secure place. If you lose or forget the BIOS administrator password, you cannot access the Configuration/Setup Utility, and you cannot change or delete the BIOS administrator password without removing the computer cover and moving a jumper on the system board. See the hardware documentation that came with your computer for more information.

Setting a supervisor password (ThinkPad)

Security settings available in the IBM BIOS Setup Utility enable administrators to perform the following tasks:

- Enable or disable the IBM embedded Security Subsystem
- Clear the IBM embedded Security Subsystem

Attention:

- It is necessary to temporarily disable the supervisor password on some ThinkPad models before installing or upgrading Client Security Software.

After setting up Client Security Software, set a supervisor password to deter unauthorized users from changing these settings.

To set a supervisor password, complete one of the following procedures:

Example 1

1. Shut down and restart the computer.
2. When the Setup Utility prompt appears on the screen, press F1.
   The main menu of the Setup Utility opens.
3. Select **Password**.
4. Select **Supervisor Password**.
5. Type your password and press Enter.
6. Type your password again and press Enter.
7. Click **Continue**.
8. Press F10 to save and exit.

Example 2

1. Shut down and restart the computer.

2. When the ″To interrupt normal startup, press the blue Access IBM button″ message is displayed, press the blue Access IBM button.

   The Access IBM predesktop area opens.
3. Double-click **Start setup utility**.
4. Select **Security** using the directional keys to navigate down the menu.
5. Select **Password**.
6. Select **Supervisor Password**.
7. Type your password and press Enter.
8. Type your password again and press Enter.
9. Click **Continue**.
10. Press F10 to save and exit.

After you set a supervisor password, a prompt appears each time you attempt to access the BIOS Setup Utility.

Important: Keep a record of your supervisor password in a secure place. If you lose or forget the supervisor password, you cannot access the IBM BIOS Setup Utility, and you cannot change or delete the password. See the hardware documentation that came with your computer for more information.

Protecting the administrator password

The administrator password protects access to the Administrator Utility. Guard the administrator password to prohibit unauthorized users from changing settings in the Administrator Utility.

Clearing the IBM embedded Security Subsystem (ThinkCentre)

If you want to erase all user encryption keys from the IBM embedded Security Subsystem and clear the administrator password for the subsystem, you must clear the chip. Read the information below before clearing the IBM embedded Security Subsystem.

Attention:

- When the IBM embedded Security Subsystem is cleared, all encryption keys and certificates stored on the subsystem are lost.

To clear the IBM embedded Security Subsystem, complete the following procedure:

1. Shut down and restart the computer.
2. When the Setup Utility prompt appears on the screen, press F1.

   The main menu of the Setup Utility opens.
3. Select **Security**.
4. Select **IBM TCPA Security Feature** and press Enter.
5. Select **Yes**.
6. Press Enter to confirm you choice.
7. Press F10 to save your changes and exit the Setup Utility.
8. Select **Yes** and press Enter. The computer will restart.

Clearing the IBM embedded Security Subsystem (ThinkPad)

If you want to erase all user encryption keys from the IBM embedded Security Subsystem and clear the administrator password, you must clear the subsystem. Read the information below before clearing the IBM embedded Security Subsystem.

Attention:

- When the IBM embedded Security Subsystem is cleared, all encryption keys and certificates stored on the subsystem are lost.

To clear the IBM embedded Security Subsystem, complete the following procedure:

1. Shut down and restart the computer.
2. When the Setup Utility prompt appears on the screen, press F1.
   The main menu of the Setup Utility opens.
3. Select **Security**.
4. Select **IBM Security Chip** and press Enter.
5. Press Enter and select **Disabled**.
6. Press Enter to confirm you choice.
7. Press Enter to continue.
8. Press F10 to save your changes and exit the Setup Utility.
9. Select **Yes** and press Enter. The computer will restart.

Known issues or limitations with CSS Version 5.3

The following information might be helpful when using the features of Client Security Software Version 5.3.

Roaming limitations

Using a CSS roaming server

The CSS administrator password prompt will appear whenever anyone attempts to log on to the CSS roaming server. However, the computer can be used normally without entering this password.

Using the IBM Security Password Manager in a roaming environment

Passwords stored on one system using IBM Client Security Password Manager can be used on other systems within the roaming environment. New entries are automatically retrieved from the archive when the user logs onto another system (if the archive is available) in the roaming network. Therefore, if a user is already logged onto one system, he must log off and log on again before any new entries will be available on the roaming network.

Internet Explorer certificate and roaming refresh delays

Internet Explorer certificates are refreshed in the archive every 20 seconds. When a new Internet Explorer certificate is generated by a roaming user, the user must wait at least 20 seconds before importing, restoring, or changing his CSS configuration on another system. Attempting any of these actions before the 20 second refresh interval will cause the certificate to be lost. Also, if the user was not connected to the archive when the certificate was generated, the user should wait 20 seconds after connecting to the archive to be sure the certificate is updated in the archive.

Lotus Notes password and credential roaming

If Lotus Notes support is enabled, users' Lotus Notes password will be stored by UVM. Users will not need to enter their Notes password to log on to Lotus Notes. They will be asked for their UVM passphrase, fingerprint, smart card, etc. (depending on the security policy settings) to gain access to Lotus Notes.

If a user changes his Notes password from within Lotus Notes, the Lotus Notes ID file is updated with the new password and UVM's copy of the new Notes password is also updated. In a roaming environment, the user's UVM credentials will be available on other systems on the roaming network that the user can access. It is possible that UVM's copy of the Notes password might not match the Notes password in the ID file on other systems in the roaming network if the Notes ID file with the updated password is not also available on the other system. If this occurs, the user will not be able to access Lotus Notes.

If a user's Notes ID file with updated password is not also available on another system, the updated Notes ID file should be copied to the other systems in the roaming network so that the password in the ID file will match the copy stored by UVM. Alternately, users can run Modify Your Security Settings from the Start Menu, and change the Notes password back to the old value. The Notes password can then be updated again via Lotus Notes.

Credential availability at logon in a roaming environment

When an archive is located on a network share, the latest sets of user credentials are downloaded from the archive as soon as the user has access to the archive. At logon, users do not yet have access to network shares, so the latest credentials might not be downloaded until after system logon is complete. For example, if the UVM passphrase was changed on another system in the roaming network, or new fingerprints were registered on another system, those updates will not be available until the logon process is complete. If updated user credentials are not available, users should try the previous passphrase or other registered fingers to log on to the system. After log on is complete, the user's updated credentials will be available and the new passphrase and fingerprints will be registered with UVM.

Restoring keys

After performing a key restore operation, you must restart the computer before you can continue using Client Security Software.

Local and domain user names

If domain and local user names are the same, you should use the same Windows password for both accounts. IBM User Verification Manager only stores one Windows password per ID, so users should use the same password for local and domain logon. If not, they will be prompted to update the IBM UVM Windows password when they switch between local and domain logins when IBM UVM secure Windows logon replacement is enabled.

CSS does not provide the ability to enroll separate domain and local users with the same account name. If you attempt to enroll local and domain users with the same ID, the following message is displayed: The selected user ID has already been configured. CSS does not allow separate enrolling of common domain and local user ID's on one system so that the common user ID will have access to the same set of credentials, like certificates, stored fingerprints, etc.

Re-installing Targus fingerprint software

If the Targus fingerprint software is removed and re-installed, the needed registry entries for enabling fingerprint support in Client Security Software must be added manually for fingerprint support to be enabled. Download the registry file that contains the needed entries (atplugin.reg) and double-click it to have the registry entries merged into the registry. Click Yes, when prompted, to confirm this operation. The system must be rebooted for Client Security Software to recognize the changes and enable fingerprint support.

Note: You must have administrator privileges on the system in order to add these registry entries.

BIOS supervisor passphrase

IBM Client Security Software 5.3 and earlier does not support the BIOS supervisor passphrase feature available on some ThinkPad systems. If you enable use of the BIOS Supervisor Passphrase, any enabling and disabling of the security subsystem must be done from BIOS Setup.

Using Netscape 7.x

Netscape 7.x behaves differently from Netscape 4.x. The passphrase prompt does not appear as soon as Netscape is started. Rather, the PKCS#11 module is only loaded when needed, so that the passphrase prompt only appears when performing an operation that requires the PKCS#11 module.

Using a diskette for archiving

If you specify a diskette as your archive location when configuring the security software, long delays will be experienced as the configuration process writes data to the diskette. Some other medium, such as a network share or a USB key, might be a superior archive location.

Smart card limitations

Registering smart cards

Smart cards must be registered with UVM before a user can successfully authenticate using the card. If one card is assigned to multiple users, only the last user to register the card will be able to use the card. Consequently, smart cards should be registered for one user account only.

Authenticating smart cards

If a smart card is required for authentication, UVM will display a dialog requesting the smart card. When the smart card is inserted in the reader, a dialog requesting the smart card PIN will be displayed. If the user enters an incorrect PIN, UVM will request the smart card again. The smart card must be removed and re-inserted before the PIN can be re-entered. Users must continue to remove and re-insert the smart card until the correct PIN for the card is entered.

The plus (+) character is displayed on folders after encryption

After encrypting files or folders, Windows Explorer might display an extraneous plus (+) character before the folder icon. This extra character will disappear when the Explorer window is refreshed.

Windows XP limited user limitations

Windows XP limited users cannot update their UVM passphrase, Windows password, or update their key archive using the User Configuration Utility.

Other limitations

This section contains information about other known issues and limitations related to Client Security Software.

Using Client Security Software with Windows operating systems

All Windows operating systems have the following known limitation: If a client user that is enrolled in UVM changes his Windows user name, all Client Security functionality is lost. The user will have to re-enroll the new user name in UVM and request all new credentials.

Windows XP operating systems have the following known limitation: Users enrolled in UVM that previously had their Windows user name changed will not be recognized by UVM. UVM will point to the former user name while Windows will only recognize the new user name. This limitation occurs even if the Windows user name was changed prior to installing Client Security Software.

Using Client Security Software with Netscape applications

Netscape opens after an authorization failure: If the UVM passphrase window opens, you must type the UVM passphrase, and then click **OK** before you can continue. If you type an incorrect UVM passphrase (or provide an incorrect fingerprint for a fingerprint scan), an error message is displayed. If you click **OK**, Netscape will open, but you will not be able to use the digital certificate generated by the IBM embedded Security Subsystem. You must exit and re-enter Netscape, and type the correct UVM passphrase before you can use the IBM embedded Security Subsystem certificate.

Algorithms do not display: All hashing algorithms supported by the IBM embedded Security Subsystem PKCS#11 module are not selected if the module is viewed in Netscape. The following algorithms are supported by the IBM embedded Security Subsystem PKCS#11 module, but are not identified as being supported when viewed in Netscape:

- SHA-1
- MD5

IBM embedded Security Subsystem certificate and encryption algorithms

The following information is provided to help identify issues about the encryption algorithms that can be used with the IBM embedded Security Subsystem certificate. See Microsoft or Netscape for current information about the encryption algorithms used with their e-mail applications.

When sending e-mail from one Outlook Express (128-bit) client to another Outlook Express (128-bit) client: If you use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0 to send encrypted e-mail to other clients using Outlook Express (128-bit), e-mail messages encrypted with the IBM embedded Security Subsystem certificate can only use the 3DES algorithm.

When sending e-mail between an Outlook Express (128-bit) client and a Netscape client: An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm.

Some algorithms might not be available for selection in the Outlook Express (128-bit) client: Depending on how your version of Outlook Express (128-bit) was configured or updated, some RC2 algorithms and other algorithms might not be available for use with the IBM embedded Security Subsystem certificate. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.

Using UVM protection for a Lotus Notes User ID

UVM protection does not operate if you switch User IDs within a Notes session: You can set up UVM protection only for the current user ID of a Notes session. To switch from a User ID that has UVM protection enabled to another User ID, complete the following procedure:

1. Exit Notes.
2. Disable UVM protection for the current User ID.
3. Enter Notes and switch User IDs. See your Lotus Notes documentation for information about switching User IDs.

   If you want to set up UVM protection for the User ID that you have switched to, proceed to step 4.
4. Enter the Lotus Notes Configuration tool provided by Client Security Software and set up UVM protection.

User Configuration Utility limitations

Windows XP imposes access restrictions which limit the functions available to a client user under certain circumstances.

Windows XP Professional

In Windows XP Professional, client user restrictions might apply in the following situations:

- Client Security Software is installed on a partition that is later converted to an NTFS format
- The Windows folder is on a partition that is later converted to an NTFS format
- The archive folder is on a partition that is later converted to an NTFS format

In the above situations, Windows XP Professional Limited Users might not be able to perform the following User Configuration Utility tasks:

- Change their UVM passphrases
- Update the Windows password registered with UVM
- Update the key archive

Windows XP Home

Windows XP Home Limited Users will not be able to use the User Configuration Utility in any of the following situations:

- Client Security Software is installed on an NTFS formatted partition
- The Windows folder is on an NTFS formatted partition
- The archive folder is on an NTFS formatted partition

Tivoli Access Manager limitations

The **Deny all access to selected object** check box is not disabled when Tivoli Access Manager control is selected. In the UVM-policy editor, if you select **Access Manager controls selected object** to enable Tivoli Access Manager to control an authentication object, the **Deny all access to selected object** check box is not disabled. Although the **Deny all access to selected object** check box remains active, it cannot be selected to override Tivoli Access Manager control.

Error messages

Error messages related to Client Security Software are generated in the event log: Client Security Software uses a device driver that might generate error messages in the event log. The errors associated with these messages do not affect the normal operation of your computer.

UVM invokes error messages that are generated by the associated program if access is denied for an authentication object: If UVM policy is set to deny access for an authentication object, for example e-mail decryption, the message stating that access has been denied will vary depending on what software is being used. For example, an error message from Outlook Express that states access is denied to an authentication object will differ from a Netscape error message that states that access was denied.

Troubleshooting charts

The following section contains troubleshooting charts that might be helpful if you experience problems with Client Security Software.

Installation troubleshooting information

The following troubleshooting information might be helpful if you experience problems when installing Client Security Software.

Problem Symptom	Possible Solution
An error message is displayed during software installation	**Action**
A message is displayed when you install the software that asks if you want to remove the selected application and all of its components.	Click **OK** to exit the window. Begin the installation process again to install the new version of Client Security Software.
A message is displayed during installation stating that you must upgrade or remove the program.	Do one of the following: • If a version prior to Client Security Software 5.0 is installed, select **Remove** to remove it. Then, restart the computer and clear the security subsystem using the IBM BIOS Setup Utility. • Otherwise, select **Upgrade** and continue the installation.
Installation access is denied due to an unknown administrator password	**Action**
When installing the software on an IBM client with an enabled IBM embedded Security Subsystem, the administrator password for the IBM embedded Security Subsystem is unknown.	Clear the security subsystem to continue with the installation.

Problem Symptom	Possible Solution
An error message is displayed when attempting certain Client Security administrator functions	**Action**
An error message is displayed after trying to perform a Client Security administrator function.	The ThinkPad supervisor password or ThinkCentre BIOS administrator password must be disabled to generate the hardware key pair on a Crypto 1 (non-TCG) system. The CSS installation process cannot enable the IBM embedded Security Subsystem until the appropriate password is disabled.

Administrator Utility troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using the Administrator Utility.

Problem Symptom	Possible Solution
The Next button is unavailable after entering and confirming your UVM passphrase in the Administrator Utility	**Action**
When you add users to UVM, the **Next** button might not be available after you enter and confirm your UVM passphrase in the Administrator Utility.	Click the **Information** item on the Windows Task Bar and continue the procedure.
An error message displays when you change the administrator public key	**Action**
When you clear the embedded Security Subsystem and then restore the key archive, an error message might display if you change the administrator public key.	Add the users to UVM and request new certificates, if applicable.
An error message displays when you attempt to recover a UVM passphrase	**Action**
When you change the administrator public key and then attempt to recover a UVM passphrase for a user, an error message might display.	Do one of the following: • If the UVM passphrase for the user is not needed, no action is required. • If the UVM passphrase for the user is needed, you must add the user to UVM, and request new certificates, if applicable.
An error message displays when you try to save the UVM-policy file	**Action**
When you attempt to save a UVM-policy file (globalpolicy.gvm) by clicking **Apply** or **Save**, an error message is displayed.	Exit the error message, edit the UVM-policy file again to make your changes, and then save the file.
An error message displays when you try to open the UVM-policy editor	**Action**
When the current user (logged on to the operating system) has not been added to UVM, the UVM-policy editor will not open.	Add the user to UVM and open the UVM-policy editor.
An error message displays when you are using the Administrator Utility	**Action**

Problem Symptom	Possible Solution
When you are using the Administrator Utility, the following error message might display: A buffer I/O error occurred while trying to access the IBM embedded Security Subsystem. This might be corrected by a reboot.	Exit the error message and restart your computer.
A disable chip message is displayed when changing the administrator password	**Action**
When you attempt to change the administrator password, and you press Enter or Tab > Enter after you type the confirmation password, the **Disable Chip** button is enabled and a disable chip confirmation message is displayed.	Do the following: 1. Exit from the disable chip confirmation window. 2. To change the administrator password, type the new password, type the confirmation password, and then click **Change**. Do not press Enter or Tab > Enter after you type the confirmation password.

User Configuration Utility troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using the User Configuration Utility.

Problem Symptom	Possible Solution
Limited Users are unable to perform certain User Configuration Utility functions in Windows XP Professional	**Action**
Windows XP Professional Limited Users might not be able to perform the following User Configuration Utility tasks: • Change their UVM passphrases • Update the Windows password registered with UVM • Update the key archive	This is a known limitation with Windows XP Professional. There is no solution to this problem.
Limited Users are unable to use the User Configuration Utility in Windows XP Home	**Action**
Windows XP Home Limited Users will not be able to use the User Configuration Utility in any of the following situations: • Client Security Software is installed on an NTFS formatted partition • The Windows folder is on an NTFS formatted partition • The archive folder is on an NTFS formatted partition	This is a known limitation with Windows XP Home. There is no solution to this problem.

ThinkPad-specific troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using Client Security Software on ThinkPad computers.

Problem Symptom	Possible Solution
An error message is displayed when attempting certain Client Security administrator functions	**Action**
An error message is displayed after trying to perform a Client Security administrator function.	The ThinkPad supervisor password must be disabled to generate the hardware key pair on a Crypto 1 (non-TCG) system. The CSS installation process cannot enable the IBM embedded Security Subsystem until the supervisor password is disabled. To disable the supervisor password, complete the following procedure: 1. Press F1 to access the IBM BIOS Setup Utility. 2. Enter the current supervisor password. 3. Enter a blank new supervisor password, and confirm a blank password. 4. Press Enter. 5. Press F10 to save and exit.
Different UVM-aware fingerprint sensor does not work properly	**Action**
The IBM ThinkPad computer does not support the interchanging of multiple UVM-aware fingerprint sensors.	Do not switch fingerprint sensor models. Use the same model when working remotely as when working from a docking station.

Microsoft troubleshooting information

The following troubleshooting charts contain information that might be helpful if you experience problems using Client Security Software with Microsoft applications or operating systems.

Problem Symptom	Possible Solution
Screen saver only displays on the local screen	**Action**
When using the Windows Extended Desktop function, the Client Security Software screen saver will only be displayed on the local screen even though access to your system and its keyboard will be protected.	If any sensitive information is being displayed, minimize the windows on your extended desktop before you invoke the Client Security screen saver.
Client Security does not work properly for a user enrolled in UVM	**Action**
The enrolled client user might have changed his Windows user name. If that occurs, all Client Security functionality is lost.	Re-enroll the new user name in UVM and request all new credentials.
Note: In Windows XP, users enrolled in UVM that previously had their Windows user name changed will not be recognized by UVM. This limitation occurs even if the Windows user name was changed prior to installing Client Security Software.	
Problems reading encrypted e-mail using Outlook Express	**Action**

Problem Symptom	Possible Solution
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient.	Verify the following: 1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses. 2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.
Problems using a certificate from an address that has multiple certificates associated with it	**Action**
Outlook Express can list multiple certificates associated with a single e-mail address and some of those certificates can become invalid. A certificate can become invalid if the private key associated with the certificate no longer exists on the IBM embedded Security Subsystem of the sender's computer where the certificate was generated.	Ask the recipient to resend his digital certificate; then select that certificate in the address book for Outlook Express.
Failure message when trying to digitally sign an e-mail message	**Action**
If the composer of an e-mail message tries to digitally sign an e-mail message when the composer does not yet have a certificate associated with his or her e-mail account, an error message displays.	Use the security settings in Outlook Express to specify a certificate to be associated with the user account. See the documentation provided for Outlook Express for more information.
Outlook Express (128 bit) only encrypts e-mail messages with the 3DES algorithm	**Action**
When sending encrypted e-mail between clients that use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0, only the 3DES algorithm can be used.	See Microsoft for current information on the encryption algorithms used with Outlook Express.
Outlook Express clients return e-mail messages with a different algorithm	**Action**
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
Error message when using a certificate in Outlook Express after a hard disk drive failure	**Action**
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, do one of the following: • obtain new certificates • register the certificate authority again in Outlook Express

Problem Symptom	Possible Solution
Outlook Express does not update the encryption strength associated with a certificate	**Action**
When a sender selects the encryption strength in Netscape and sends a signed e-mail message to a client using Outlook Express with Internet Explorer 4.0 (128-bit), the encryption strength of the returned e-mail might not match.	Delete the associated certificate from the address book in Outlook Express. Open the signed e-mail again and add the certificate to the address book in Outlook Express.
An error decryption message displays in Outlook Express	**Action**
You can open a message in Outlook Express by double-clicking it. In some instances, when you double-click an encrypted message too quickly, a decryption error message appears.	Close the message, and open the encrypted e-mail message again.
Also, a decryption error message might display in the preview pane when you select an encrypted message.	If an error message appears in the preview pane, no action is required.
An error message displays when you click the Send button twice on encrypted e-mails	**Action**
When using Outlook Express, if you click the send button twice to send an encrypted e-mail message, an error message displays stating that the message could not be sent.	Close the error message, and then click the **Send** button once.
An error message displays when you requesting a certificate	**Action**
When using Internet Explorer, you might receive an error message if you request a certificate that uses the IBM embedded Security Subsystem CSP.	Request the digital certificate again.

Netscape application troubleshooting information

The following troubleshooting charts contain information that might be helpful if you experience problems using Client Security Software with Netscape applications.

Problem Symptom	Possible Solution
Problems reading encrypted e-mail	**Action**
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient.	Verify the following: 1. That the encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses. 2. That the encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.
Failure message when trying to digitally sign an e-mail message	**Action**

Problem Symptom	Possible Solution
When the IBM embedded Security Subsystem certificate has not been selected in Netscape Messenger, and the writer of an e-mail message tries to sign the message with the certificate, an error message displays.	Use the security settings in Netscape Messenger to select the certificate. When Netscape Messenger is open, click the security icon on the toolbar. The Security Info window opens. Click **Messenger** in the left panel and then select the **IBM embedded Security Chip certificate**. See the documentation provided by Netscape for more information.
An e-mail message is returned to the client with a different algorithm	**Action**
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
Unable to use a digital certificate generated by the IBM embedded Security Subsystem	**Action**
The digital certificate generated by the IBM embedded Security Subsystem is not available for use.	Verify that the correct UVM passphrase was typed when Netscape was opened. If you type the incorrect UVM passphrase, an error message displays stating an authentication failure. If you click **OK**, Netscape opens, but you will not be able to use the certificate generated by the IBM embedded Security Subsystem. You must exit and re-open Netscape, and then type the correct UVM passphrase.
New digital certificates from the same sender are not replaced within Netscape	**Action**
When a digitally signed e-mail is received more than once by the same sender, the first digital certificate associated with the e-mail is not overwritten.	If you receive multiple e-mail certificates, only one certificate is the default certificate. Use the security features in Netscape to delete the first certificate, and then re-open the second certificate or ask the sender to send another signed e-mail.
Cannot export the IBM embedded Security Subsystem certificate	**Action**
The IBM embedded Security Subsystem certificate cannot be exported in Netscape. The export feature in Netscape can be used to back up certificates.	Go to the Administrator Utility or User Configuration Utility to update the key archive. When you update the key archive, copies of all the certificates associated with the IBM embedded Security Subsystem are created.
Error message when trying to use a restored certificate after a hard disk drive failure	**Action**

Problem Symptom	Possible Solution
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, obtain a new certificate.
Netscape agent opens and causes Netscape to fail	**Action**
Netscape agent opens and closes Netscape.	Turn off the Netscape agent.
Netscape delays if you try to open it	**Action**
If you add the IBM embedded Security Subsystem PKCS#11 module and then open Netscape, a short delay will occur before Netscape opens.	No action is required. This is for informational purposes only.

Digital certificate troubleshooting information

The following troubleshooting information might be helpful if you experience problems obtaining a digital certificate.

Problem Symptom	Possible Solution
UVM passphrase window or fingerprint authentication window displays multiple times during a digital certificate request	**Action**
The UVM security policy dictates that a user provide the UVM passphrase or fingerprint authentication before a digital certificate can be acquired. If the user tries to acquire a certificate, the authentication window that asks for the UVM passphrase or fingerprint scan displays more than once.	Type your UVM passphrase or scan your fingerprint each time the authentication window opens.
A VBScript or JavaScript error message displays	**Action**
When you request a digital certificate, an error message related to VBScript or JavaScript might display.	Restart the computer, and obtain the certificate again.

Tivoli Access Manager troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using Tivoli Access Manager with Client Security Software.

Problem Symptom	Possible Solution
Local policy settings do not correspond to those on the server	**Action**
Tivoli Access Manager allows certain bit configurations that are not supported by UVM. Consequently, local policy requirements can override settings made by an administrator when configuring the PD server.	This is a known limitation.
Tivoli Access Manager setup settings are not accessible	**Action**

Problem Symptom	Possible Solution
Tivoli Access Manager setup and local cache setup settings are not accessible on the Policy Setup page in the Administrator Utility.	Install the Tivoli Access Manager runtime Environment. If the Runtime Environment is not installed on the IBM client, the Tivoli Access Manager settings on the Policy Setup page will not be available.
A user's control is valid for both the user and the group	**Action**
When configuring the Tivoli Access Manager server, if you define a user to a group, the user's control is valid for both the user and the group if **Traverse bit** is on.	No action is required.

Lotus Notes troubleshooting information

The following troubleshooting information might be helpful if you experience problems with using Lotus Notes with Client Security Software.

Problem Symptom	Possible Solution
After enabling UVM protection for Lotus Notes, Notes is not able to finish its setup	**Action**
Lotus Notes is not able to finish setup after UVM protection is enabled using the Administrator Utility.	This is a known limitation. Lotus Notes must be configured and running before Lotus Notes support is enabled in the Administrator Utility.
An error message displays when you try to change the Notes password	**Action**
Changing the Notes password when using Client Security Software might display in an error message.	Retry the password change. If this does not work, restart the client.
An error message displays after you randomly-generate a password	**Action**
An error message might display when you do the following: • Use the Lotus Notes Configuration tool to set UVM protection for a Notes ID • Open Notes and use the function provided by Notes to change the password for Notes ID file • Close Notes immediately after you change the password	Click **OK** to close the error message. No other action is required. Contrary to the error message, the password has changed. The new password is a randomly-generated password created by Client Security Software. The Notes ID file is now encrypted with the randomly-generated password, and the user does not need a new User ID file. If the end user changes the password again, UVM will generate a new random password for the Notes ID.

Encryption troubleshooting information

The following troubleshooting information might be helpful if you experience problems when encrypting files using Client Security Software 3.0 or later.

Problem Symptom	Possible Solution
Previously encrypted files will not decrypt	**Action**

Problem Symptom	Possible Solution
Files encrypted with previous versions of Client Security Software do not decrypt after upgrading to Client Security Software 3.0 or later.	This is a known limitation. You must decrypt all files that were encrypted using prior versions of Client Security Software *before* installing Client Security Software 3.0 or later. Client Security Software 3.0 cannot decrypt files that were encrypted using prior versions of Client Security Software because of changes in its file encryption implementation.

UVM-aware device troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using UVM-aware devices.

Problem Symptom	Possible Solution
A UVM-aware device stops working properly	**Action**
A UVM-aware security device, such as smart card, smart card reader, or finger print reader, is not working properly.	Confirm whether the device is configured correctly by the system. After a device is configured, you might need to reboot the system to start the service correctly. For device trouble-shooting information, see the device documentation or contact the device vendor.
A UVM-aware device stops working properly	**Action**
When you disconnect a UVM-aware device from a Universal Serial Bus (USB) port, and then reconnect the device to the USB port, the device might not work properly.	Restart the computer after the device has been reconnected to the USB port.

Appendix A. Password and passphrase information

This appendix contains password and passphrase information.

Password and passphrase rules

When dealing with a secure system, there are many different passwords and passphrases. Different passwords have different rules. This section contains information about the administrator password and the UVM passphrase.

Administrator password rules

The rules that govern the administrator password can not be changed by a security administrator.

The following rules pertain to the administrator password:

Length
The password must be exactly eight characters long.

Characters
The password must contain alphanumeric characters only. A combination of letters and numbers is allowed. No exceptional characters, like space, !, ?, %, are allowed.

Properties
Set the administrator password to enable the IBM Embedded Security Chip in the computer. This password must be typed each time you access the Administrator Utility and Administrator Console.

Incorrect attempts
If you incorrectly type the password ten times, the computer locks up for 1 hour and 17 minutes. If after this time period has passed, you type the password incorrectly ten more times, the computer locks up for 2 hours and 34 minutes. The time the computer is disabled doubles each time you incorrectly type the password ten times.

UVM passphrase rules

IBM Client Security Software enables security administrators to set rules that govern a user's UVM passphrase. To improve security, the UVM passphrase is longer and can be more unique than a traditional password. UVM passphrase policy is controlled by the Administrator Utility.

The UVM Passphrase Policy interface in the Administrator Utility enables security administrators to control passphrase criteria through a simple interface. The UVM Passphrase Policy interface enables the administrator to establish the following passphrase rules:

Note: The default setting for each passphrase criterion is provided in parenthesis below.

- establish whether to set a minimum number of alphanumeric characters allowed (yes, 6)

  For example, when set to ″6″ characters allowed,1234567xxx is an invalid password.

- establish whether to set a minimum number of digit characters allowed (yes, 1)

  For example, when set to ″1″, `thisismypassword` is an invalid password.
- establish whether to set the minimum number of spaces allowed (no minimum)

  For example, when set to ″2″, `i am not here` is an invalid password.
- establish whether to enable the passphrase to begin with a digit (no)

  For example, by default, `1password` is an invalid password.
- establish whether to enable the passphrase to end with a digit (no)

  For example, by default, `password8` is an invalid password.
- establish whether to allow the passphrase from containing a user ID (no)

  For example, by default, `UserName` is an invalid password, where `UserName` is a User ID.
- establish whether to ensure that the new passphrase is different from the last x passphrases, where x is an editable field (yes, 3)

  For example, by default, `mypassword` is an invalid password if any of your last three passwords was `mypassword`.
- establish whether the passphrase can contain more than three identical consecutive characters in any position from the previous password (no)

  For example, by default, `paswor` is an invalid password if your previous password was `pass` or `word`.

The UVM Passphrase Policy interface in the Administrator Utility also enables security administrators to control passphrase expiration. The UVM Passphrase Policy interface enables the administrator to choose between the following passphrase expiration rules:

- establish whether to have the passphrase expire after a set number of days (yes, 184)

  For example, by default the passphrase will expire in 184 days. The new passphrase must adhere to the established passphrase policy.
- establish whether the passphrase will expire (yes)

  When this option is selected, the passphrase will never expire.

The passphrase policy is checked in the Administrator Utility when the user is enrolled, and is also checked when the user changes the passphrase from the Client Utility. The two user settings related to the previous password will be reset and any passphrase history will be removed.

The following general rules pertain to the UVM passphrase:

Length
: The passphrase can be up to 256 characters long.

Characters
: The passphrase can contain any combination of characters that the keyboard produces, including spaces and non-alphanumeric characters.

Properties
: The UVM passphrase is different from a password that you might use to log on to an operating system. The UVM passphrase can be used in conjunction with other authenticating devices, such as a UVM-aware fingerprint sensor.

Incorrect attempts
: If you incorrectly type the UVM passphrase multiple times during a

session, the computer will exercise a series of anti-hammering delays. These delays are specified in the following section.

Fail counts on TCG-systems using the National TPM

The following table shows the anti-hammering delay settings for a National TPM TCG-compliant system:

Attempts	Delay on next failure
7-13	4 seconds each
14-20	8 seconds each
21-27	16 seconds each
28-34	32 seconds each
35-41	64 seconds each (1.07 minutes each)
42-48	128 seconds each (2.13 minutes each)
49-55	256 seconds each (4.27 minutes each)
56-62	512 seconds each (8.53 minutes each)
63-69	1,024 seconds each (17.07 minutes each)
70-76	2,048 seconds each (34.13 minutes each)
77-83	68.26 minutes each (1.14 hours each)
84-90	136.52 minutes each (2.28 hours each)
91-97	273.04 minutes each (4.55 hours each)
98-104	546.08 minutes each (9.1 hours each)
105-111	1,092.16 minutes each (18.2 hours each)
112-118	2,184.32 minutes each (36.4 hours each)

National TPM TCG-compliant systems do not distinguish between user passphrases and the administrator password. Any authentication using the IBM Embedded Security Chip adheres to the same policy. There is no maximum timeout. Each failed attempt triggers the delay indicated above. The anti-hammering delays do not end at the 118th attempt; rather, they continue in the manner illustrated above indefinitely.

Fail counts on TCG-systems using the Atmel TPM

The following table shows the anti-hammering delay settings for an Atmel TPM TCG-compliant system:

Attempts	Delay on next failure
15	1.1 minutes
31	2.2 minutes
47	4.4 minutes
63	8.8 minutes
79	17.6 minutes
95	35.2 minutes
111	1.2 hours
127	2.3 hours

Attempts	Delay on next failure
143	4.7 hours

Atmel TPM TCG-compliant systems do not distinguish between user passphrases and the administrator password. Any authentication using the IBM Embedded Security Chip adheres to the same policy. The maximum timeout is 4.7 hours. Atmel TPM TCG-compliant systems will not delay for longer than 4.7 hours.

Fail counts on non TCG-compliant systems

Systems that are not TCG-compliant systems distinguish between the administrator password and user passphrases. On systems that are not TCG-compliant, the administrator password has a 77-minute delay after 10 failed attempts; user passwords have only a one-minute delay after 32 failed attempts, and then the lockout time doubles after every 32 failed attempts.

Resetting a passphrase

If a user forgets his passphrase, the administrator can enable the user to reset his passphrase.

Resetting a passphrase remotely

To reset a password remotely, complete the following procedure:

- **Administrators**

  A remote administrator must do the following:

  1. Create and communicate a new one-time password to the user.
  2. Send a data file to the user.

     The data file can be sent to the user by e-mail, it can be copied to a removable media such as a diskette, or it can be written directly to the user's archive file (assuming the user can get access to this system). This encrypted file is used to match against the new one-time password.

- **Users**

  The user must do the following:

  1. Log on to the computer.
  2. When prompted for a passphrase, check the "I forgot my passphrase" check box.
  3. Enter the one-time password communicated by the remote administrator, and provide the location of the file sent by the administrator.

     After UVM verifies that the information in the file matches the provided password, the user is granted access. The user is then immediately prompted to change the passphrase.

This is the recommended manner to reset a lost passphrase.

Resetting a passphrase manually

If the administrator can go to the system of the user that forgot his passphrase, the administrator can log on to the user's system as the administrator, provide the

administrator private key to the Administrator Utility, and manually change the user's passphrase. An administrator does not have to know a user's old passphrase to change the passphrase.

Appendix B. Notices and Trademarks

This appendix gives legal notice for IBM products as well as trademark information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Licensees of this program who wish to have information about it for the purpose of enabling: (1) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks

IBM and SecureWay are trademarks of the IBM Corporation in the United States, other countries, or both.

Tivoli is a trademark of Tivoli Systems Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Printed in USA