IBM® Client Security Solutions

Client Security Software Version 1.2 Installation Guide

June 2000

Before using this information and the product it supports, be sure to read "Appendix A - U.S. export regulations for Client Security Software," on page 29 and "Appendix C - Notices and Trademarks," on page 35.

Table of Contents

About this Guide

The guide contains information to help you install Client Security Software on networked IBM computers that have the IBM embedded Security Chip. Throughout this document, these computers are referred to as *IBM clients*.

Instructions for enabling the IBM embedded Security Chip and setting the hardware password for the security chip are included.

The guide is organized as follows:

"Chapter 1 - Introducing IBM Client Security Software," contains an overview of the software components that are included.

"Chapter 2 – Getting started," contains computer hardware and software prerequisites as well as instructions for downloading the software.

"Chapter 3 - Installing the software," contains instructions for installing Client Security Software.

"Chapter 4 - Using the unattended installation option," contains instructions for installing the software with the unattended option.

"Chapter 5 - Uninstalling Client Security Software," contains instructions for uninstalling the software from the IBM client.

"Chapter 6 - Installing new software on an IBM client that has a previous version installed," contains instructions for installing new software when a previous version of the software is already installed.

"Chapter 7 - Troubleshooting," contains information that can help you if you experience problems while installing the software.

"Appendix A - U.S. export regulations for Client Security Software," contains information about U.S. export regulations about the software.

"Appendix B - Rules for the hardware password ," contains a description of the rules for the hardware password.

"Appendix C - Notices and Trademarks," contains legal notices and trademark information.

How to use this guide

This guide is intended for use by network or systems administrators who set up personal-computing security for IBM clients. Knowledge of security concepts, such as public key infrastructure (PKI) and key and digital certificate management within a networked environment is required.

Compare to the Administrator's and Client User's Guide

As an administrator, use this guide to enable the IBM embedded Security Chip and install Client Security Software on IBM clients.

After you install the software, use the instructions in the *Administrator's Guide* to set up and maintain the security policy for each client. Important troubleshooting information is also provided in the *Administrator's Guide*.

The *Client Security User's Guide* is a companion to *Administrator's Guide* and contains information that a client user will find helpful when performing tasks

with Client Security Software, such as using UVM logon protection and the screen saver, creating a digital certificate, and using the Client Utility.

All guides are available for download from the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html

Conventions used in this guide

IBM client is a term used to describe networked IBM computers that have the IBM embedded Security Chip.

Also, this guide uses several typeface conventions:

- *Bold* - Commands, keywords, authorization roles, and other information that you must use literally appear in *bold*.

- *Italics* - Variables and values that you must provide appear in *italic*s. Words and phrases that are emphasized also appear in *italic*s.

- `Monospace` - Code examples, output, and system messages appear in `monospace`.

Chapter 1 - Introducing IBM Client Security Software

Client Security Software consists of software applications and components that enable IBM clients to use client security across a local network, an enterprise, or the Internet. Client Security Software provides many of the components required to create a public key infrastructure (PKI) in your business, including:

- *Encryption key management for public key cryptography[1]*. Client Security Software is designed for IBM computers that use the IBM embedded Security Chip to encrypt and store encryption keys. You create the 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 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 Chip 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 stored on the IBM embedded Security Chip. Also, for Netscape users, you can choose the IBM embedded Security Chip as the generator of the private key for digital certificates used for security. Applications such as Netscape Messenger that use Public-Key Cryptography Standard (PKCS) #11 can take advantage of the protection provided by the IBM embedded Security Chip.

  Note: For information on the specific applications that Client Security Software supports, see "Before you install the software," on page 9.

- *Administrator control over client security policy*. A concern of security policy at the client level is authenticating the end user. Client Security Software provides the interface and underlying software required to manage the security policy of the IBM client. This interface is part of the authenticating software User Verification Manager (UVM), the main component of Client Security Software.

- *A key archive and recovery solution*. An important function in a PKI is creating a key archive from which keys can be restored in the event that the original keys are lost or damaged. Client Security Software provides the interface that enables you to set up an archive for the keys and digital certificates (that you create with the IBM embedded Security Chip) and to restore the keys and certificates if necessary.

---

[1] Public key cryptography uses encryption keys that are issued in pairs. One is the public key; the other is the private key. Both keys are required to encrypt and decrypt information and are also used to identify and authenticate client users.

What software is installed?

When you install and set up Client Security Software, the following software components are installed:

- *Administrator Utility:* The Administrator Utility is the administrator interface you use to create encryption keys with the IBM embedded Security Chip in your computer. In addition, the Administrator utility enables you to add users to the security policy provided by Client Security Software.

- *User Verification Manager:* User Verification Manager (UVM) is software that enables you to set the security policy for the computer, which dictates how a client user is authenticated on the system. Client Security Software uses the UVM passphrase and other authentication elements to authenticate users to the system. For example, you can use a fingerprint reader for authentication.

- *UVM protection for the system logon:* UVM protection for the system logon lets you control access to the computer through a logon interface. UVM protection ensures that only those users who are recognized by the security policy of the computer are able to access the operating system.

- *Client Security screen saver:* The Client Security screen saver enables you to control access to the computer through a screen saver interface.

- *Client Utility:* The Client Utility enables a client user to change the UVM passphrase. For Windows NT users, the Client Utility enables a user to change the Windows NT logon password so that it is recognized by UVM. Also, the user can update the key archive with the Client Utility. A user can create backup copies of the digital certificates created with the IBM embedded Security Chip by updating the key archive.

- *Support for the Microsoft CryptoAPI:* Support for Microsoft CryptoAPI is built into Client Security Software. Defined by Microsoft, CryptoAPI is used as the default cryptographic service for Microsoft operating systems and applications. With built-in CryptoAPI support, Client Security Software enables you to use the cryptographic operations of the IBM embedded Security Chip when you create digital certificates for Microsoft applications.

- *Support for PKCS#11:* Defined by RSA Data Security Inc., PKCS#11 is used as the cryptographic standard for Netscape and other products. After you install the IBM embedded Security Chip PKCS#11 module, you can use the IBM embedded Security Chip when you generate a digital certificate for Netscape applications and other applications that use PKCS#11.

- *Support for Lotus Notes®:* Notes users can set up UVM protection for their Notes User ID.

What is new in this release

The new features in Client Security Software version 1.2 are:

- UVM protection for your Lotus Notes User ID

- Compatibility with UVM-aware fingerprint sensors

- UVM policy

- Support for use with Policy Director[2]

Additional information

You can obtain additional information and security product updates, when available, from the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/index.html

---

[2] Support for Policy Director can be set up on Windows NT clients only.

Chapter 2 – Getting started

This chapter contains information about the software that is compatible for use with Client Security Software. Also, information about downloading the software is provided.

Before you install the software

Before you download and install the software, make sure that your computer hardware, software, and operating system are compatible with Client Security Software.

For the most recent information on hardware and software requirements, go to the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html

Supported hardware

Only IBM personal computers and workstations that have the IBM embedded Security Chip support Client Security Software. If you try to download and install the software onto a computer that does not have an IBM embedded Security Chip, the software will not install or run properly.

UVM-aware products

Products that are UVM aware can use security features provided by Client Security Software. Examples of such products are:

- UVM-aware fingerprint sensors. You must install Client Security Software before you install a UVM-aware sensor.   To use a UVM-aware sensor that is already installed on an IBM client, you must uninstall the UVM-aware sensor, install Client Security Software, and then reinstall the UVM-aware sensor.

- IBM Tivoli® SecureWay® Policy Director. You must install some Policy Director components before you install Client Security Software. For details, see *Using Client Security with Policy Director*.

- Lotus Notes version 4.5 or later. You can install Lotus Notes before or after you install Client Security Software.

Supported operating systems

Client Security Software is supported only on the following operating systems:

- Windows NT® 4.0 Workstation, with Service Pack 5 or later

- Windows® 98

- Windows 95, with OEM Service Release 2.5 or later3

Supported Web browsers

Client Security Software supports the following Web browsers for requesting digital certificates:

---

[3] Windows 95 support for Client Security Software is not available for IBM PC 300PL (6584 and 6594) and IntelliStation M Pro (6868).

- Internet Explorer 4.01 with Service Pack 1a or Internet Explorer 5.0 or later

- Netscape 4.51 or 4.61 or later

Important information about Web browser encryption strengths: During the installation process, immediately after the software is installed, a window opens that notifies you if support for strong-encryption Web browsers or standard-encryption Web browsers was installed on your computer. Note the following:

- If support for strong encryption is installed, use the 128-bit version of your Web browser.

- If the software installed supports up to 56-bit encryption, strong encryption was not installed, and a 40-bit Web browser must be used.

To check the encryption strength of your Web browser, see the help system provided with the browser.

Supported e-mail applications

Client Security Software supports the following applications for sending and receiving encrypted e-mail messages:

- E-mail applications that use the Microsoft CryptoAPI for cryptographic operations, such as Outlook Express and Outlook

- E-mail applications that use Public Key Cryptographic Standard #11 (PKCS#11) for cryptographic operations, such as Netscape Messenger

Download the software

Client Security Software is available as a free download from the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html

Registration form

When you download the software, you must complete a registration form and questionnaire, and agree to the license. Follow the instructions that are provided at the Web site when downloading the software.

All the setup files for Client Security Software are included within one self-extracting file named CSEC12.EXE.

Export regulations

Client Security Software Version 1.2 contains encryption code that can be downloaded within North America and internationally. If you live in a country where downloading encryption software from a Web site in the United States is prohibited, you cannot download Client Security Software Version 1.2. For more information on the export regulations governing Client Security Software, see "Appendix A - U.S. export regulations for Client Security Software," on page 29.

Chapter 3 - Installing the software

This chapter contains instructions for running the installation program and configuring Client Security Software on IBM clients. All files required for the installation are provided within CSEC12.EXE, the file that you download from the IBM Web site.

The installation program was designed to help you do the following:

- Install Client Security Software on the IBM client

- Enable the security subsystem of the IBM client, which includes setting a hardware password to enable the IBM embedded Security Chip and generating the hardware encryption keys and key archive

Important information for Windows NT: If you are installing the software on a Windows NT client, you must log on with a user ID that has administrator user rights before you can install Client Security Software.

Using admin keys

The admin keys are your *administrator keys* that enable you to generate the hardware encryption keys for an IBM client. The admin keys are actually a key pair that includes the admin public key and the admin private key.

Because you must use the Administrator Utility to create the admin keys, you must install the software on an initial IBM client and then use the Administrator Utility to create the admin keys. Instructions for installing and configuring the software on the first IBM client are provided below.

After you create the admin keys, you can use the installation program to quickly install and configure the software on other IBM clients without having to use the Administrator Utility. See "Installation on other IBM clients when the admin public key is available" on page 18 for more information.

Note: If you intend to use a UVM policy that can be used on remote clients, you must the same admin public key when you install the software on those clients. For more information on UVM policy, see the *Client Security Software Administrator's Guide*.

Installation on the first IBM client

Use the following steps to install and configure the software on the first IBM client.

1. Install the software on the first IBM client.

2. Use the Administrator Utility to enable the IBM embedded Security Chip and to set a hardware password.

3. Create an admin key pair.

4. Generate the hardware encryption keys and set up the key archive.

Install the software on the first IBM client

Because you must shut down and restart the computer to complete the installation, close all other Windows programs before starting the installation procedure.

To install Client Security Software on the first IBM client:

1. From the Windows desktop, click *Start → Run*.
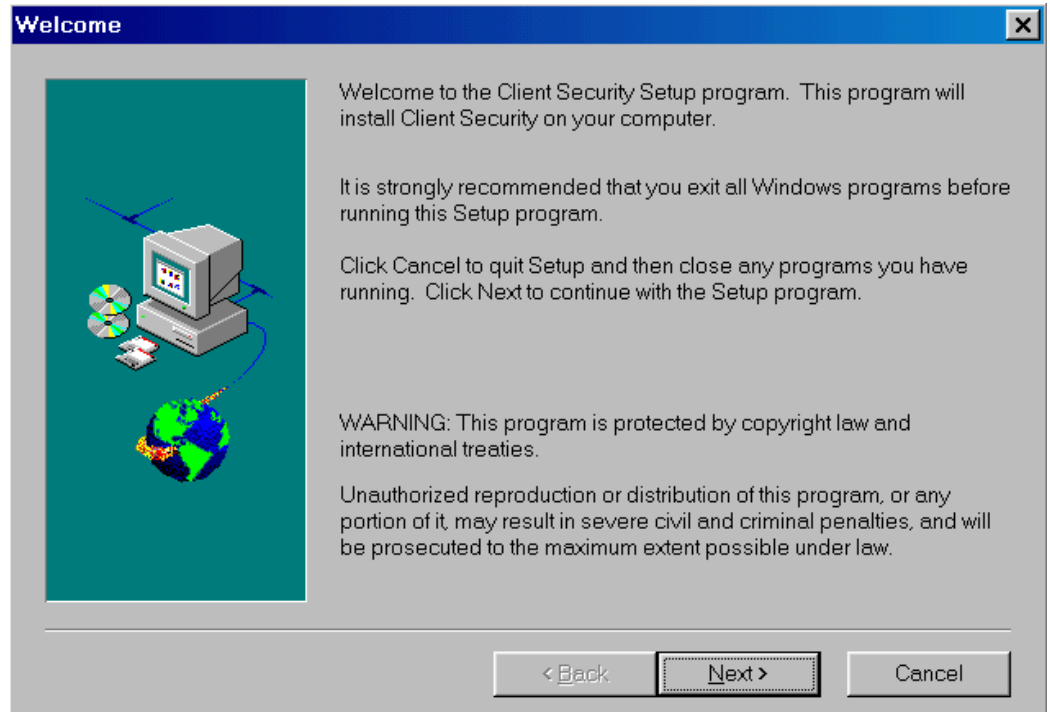
2. In the *Run* field, type:

   d:*directory*\csec12.exe

   where *d:* and *directory* are the drive letter and the directory where the file is located.

   Running this file unzips all the installation files for the software. When prompted, type the path to the folder where you want the files to be copied and click *OK*. SETUP.EXE, the file that runs the installation program, is one of the files that will be stored in the folder you specify.

3. Run SETUP.EXE.

   The installation program opens the Welcome window, which reminds you to exit from all Windows programs before you begin to install Client Security and notifies you of the copyright laws associated with Client Security Software.

4. Click *Next*.

   The installation program opens the Select Language window. Select the language you want to use during installation.

5. Click *Next*.
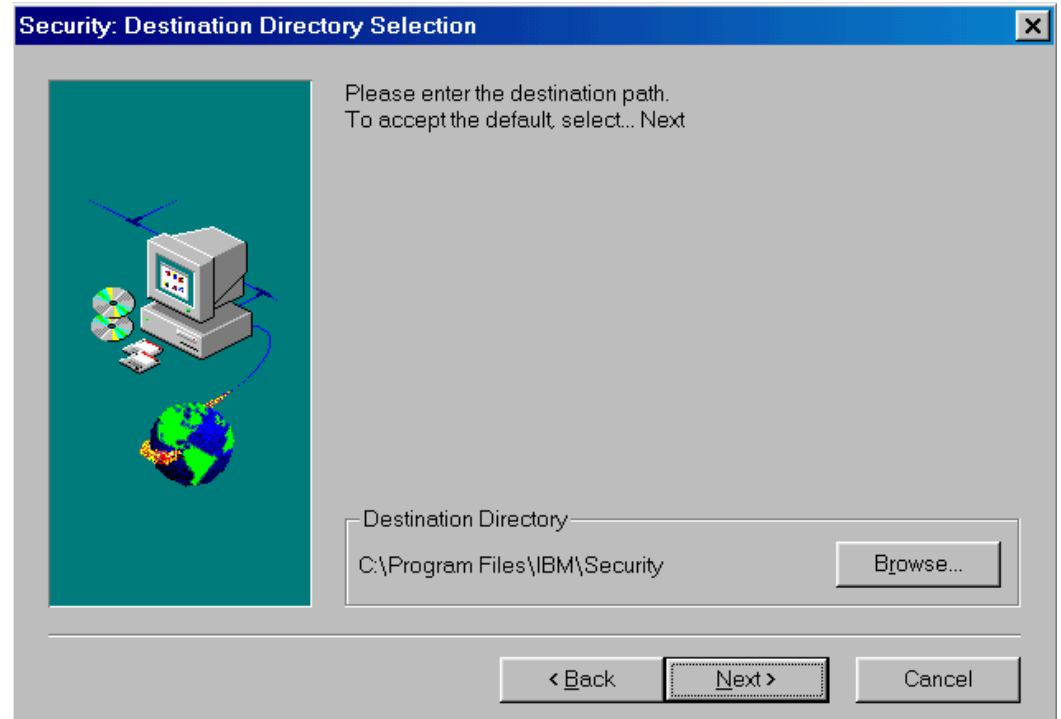
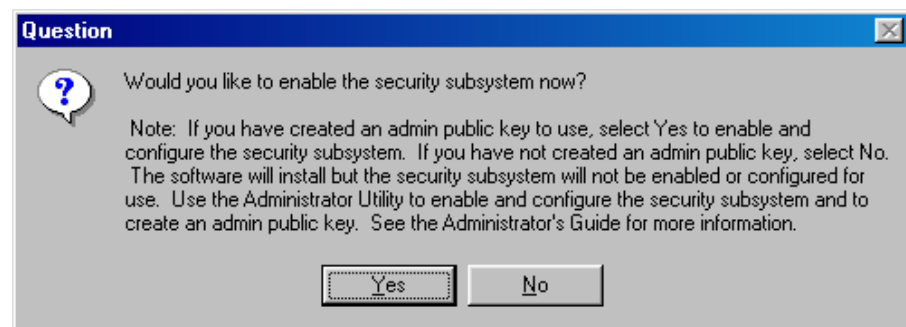The installation program opens the License Agreement window.

6. Click *I Agree* to proceed.

   Note: You must agree to the terms of the License Agreement to install Client Security Software. If you click *I Disagree*, the installation program will close without installing Client Security Software.

   After you click *I Agree*, the Destination Directory Selection window opens.

Security: Destination Directory Selection

Please enter the destination path.
To accept the default, select... Next

Destination Directory
C:\Program Files\IBM\Security   Browse...

< Back   Next >   Cancel

7. Click *Next* to accept the default directory, C:\Program Files\IBM\Security, or click *Browse* to choose a different directory, and then click *Next*.

8. A window opens that asks if you want to enable the security subsystem for the IBM client. You can enable the security subsystem with the installation program only if you know the location of the admin public key. Because you have not yet created the admin key pair, click *No*.

Question

Would you like to enable the security subsystem now?

Note: If you have created an admin public key to use, select Yes to enable and configure the security subsystem. If you have not created an admin public key, select No. The software will install but the security subsystem will not be enabled or configured for use. Use the Administrator Utility to enable and configure the security subsystem and to create an admin public key. See the Administrator's Guide for more information.

Yes   No

9. A window opens that notifies you that you must run the Administrator Utility to enable the security subsystem.

> Click *OK* and the installation program installs Client Security Software on the IBM client.

10. A window opens that notifies you of the Web browser encryption strength that must be used with Client Security Software.

   Click *OK* to continue.

11. The Setup Complete window opens. You must restart the computer before Client Security Software will run properly.

   Select *Yes, I want to restart my computer now* to restart the computer, or click *No, I will restart my computer later*; then click *Finish*.
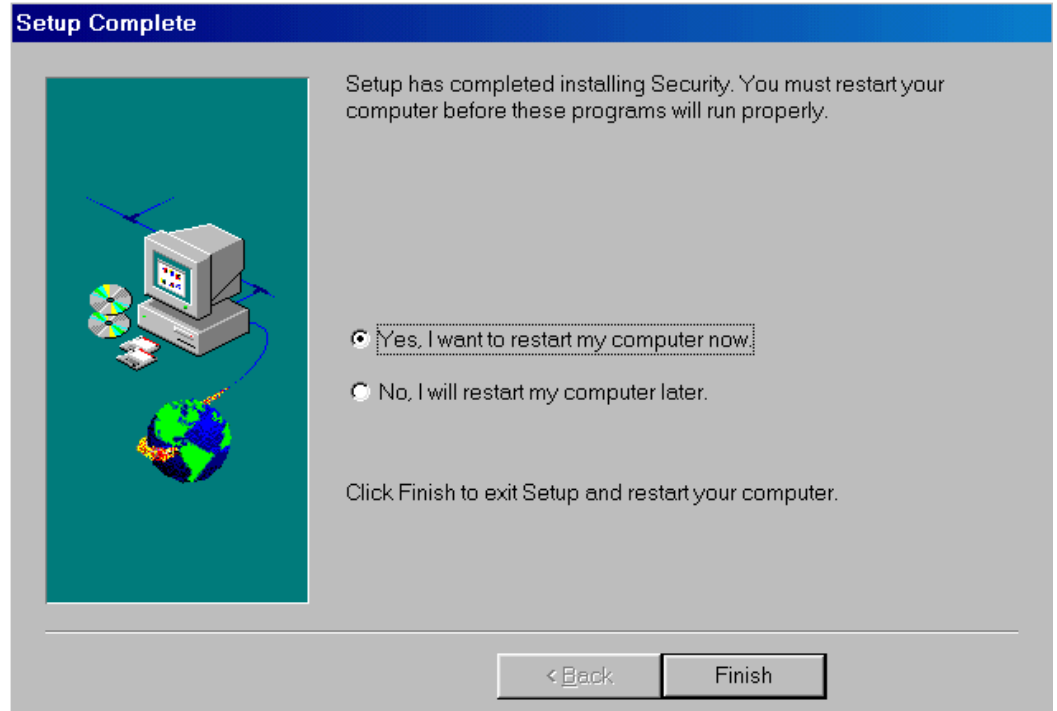
12. After the computer restarts, go the next section to enable the IBM embedded Security Chip and to set a hardware password.

Use the Administrator Utility to enable the IBM embedded Security Chip and to set a hardware password

> After the software is installed on the client, use the Administrator Utility to enable the IBM embedded Security Chip and to set the hardware password.
>
> *Note:* For Windows NT users, you must have administrator user rights assigned to your user ID to open and use the Administrator Utility.
>
> From the Windows desktop, do the following:

1. Click *Start → Programs → Client Security Software Utilities → Administrator Utility*.

   The following window opens and asks you to enable the IBM embedded Security Chip for the IBM client.

2. Click *Yes*.

3. You must restart the computer before the IBM embedded Security Chip will become enabled. A window opens that asks you to restart the computer. Click *OK*.

4. After the computer restarts, from the Windows desktop, click *Start →
   Programs → Client Security Software Utilities → Administrator Utility*.

   Because access to the Administrator Utility is protected by the hardware password, the following window opens that asks you to type the hardware password.

5. Type a new hardware password, and then type it again in the *Confirm* field. Click *OK*. The Administrator Utility window opens.

   For information on the rules for the hardware password, see "Appendix B - Rules for the hardware password ," on page 34.

6. Go to the next section to create an admin key pair.

Create an admin key pair

You use the admin key pair to generate the hardware encryption keys for each client. In a network environment, you can create one instance of an admin key pair and store the admin public key on a shared directory or diskette so that it is accessible to the other clients on which you want to install Client Security Software.

Note: If you want to save the admin key pair to a shared directory, you must map a drive letter to the shared network resource where that directory exists. Before you can save the admin key pair to a shared directory, use the instructions found in your Windows operating system documentation to map a drive letter to a shared network resource.

To create an admin key pair:

1. Click the *Administrator Keys* tab.

2. In the *Key storage directory (path)* field, type the path (not the file names) where the admin key pair files will be stored. If you choose to store the admin key pair files on a diskette, insert a formatted diskette into the diskette drive.

   Tip: If diskette drives are available on the IBM clients, use a diskette to store the admin public key so that it is accessible to you when you install and set up the software on other IBM clients.

3. Do one of the following:

   - If you do not want to separate the admin private key into multiple files, select the number 1 from the drop-down list in the *Split count* field.

   - If you want to separate the admin private key into multiple files, select a number from 2 to 5 from the drop-down list in the *Split count* field.

   A note about splitting the admin private key: When you create the admin keys, the admin public key file (ADMIN.KEY) and one admin private key file (Private1.key) are always created. To enhance security when the admin private key is required, the admin private key can be split into two, three, four, or five files. The files are named Private2.key, Private3.key, Private4.key, and Private5.key, and they are stored in the same directory when they are created. If the admin private key is split, you can distribute the different files to other administrators (or other trusted parties), which forces all administrators to be present when the admin private key is required, for example to perform a key restoration. It is important that the admin private key files are stored in a safe place.

4. Click *Create*. A window opens that notifies you that the operation was successful. Click *OK*.

5. Go to the next section to generate the hardware encryption keys and to set up the key archive.

Generate the hardware encryption keys and set up the key archive

The hardware encryption keys are the base keys that are created and stored on the IBM embedded Security Chip. You must generate the hardware keys before you can use the IBM embedded Security Chip for cryptographic operations, such as creating a digital certificate that can be used for digital signatures or encryption.

To create the hardware keys and setup the key archive:

1. Click the *Key Setup and Archive* tab.

2. In the *Hardware key setup* area, type the path and file name of the admin public key or click *Browse* to search for the file. The following example shows that ADMIN.KEY is stored on a diskette. If you stored ADMIN.KEY on a diskette, insert the diskette into the diskette drive.
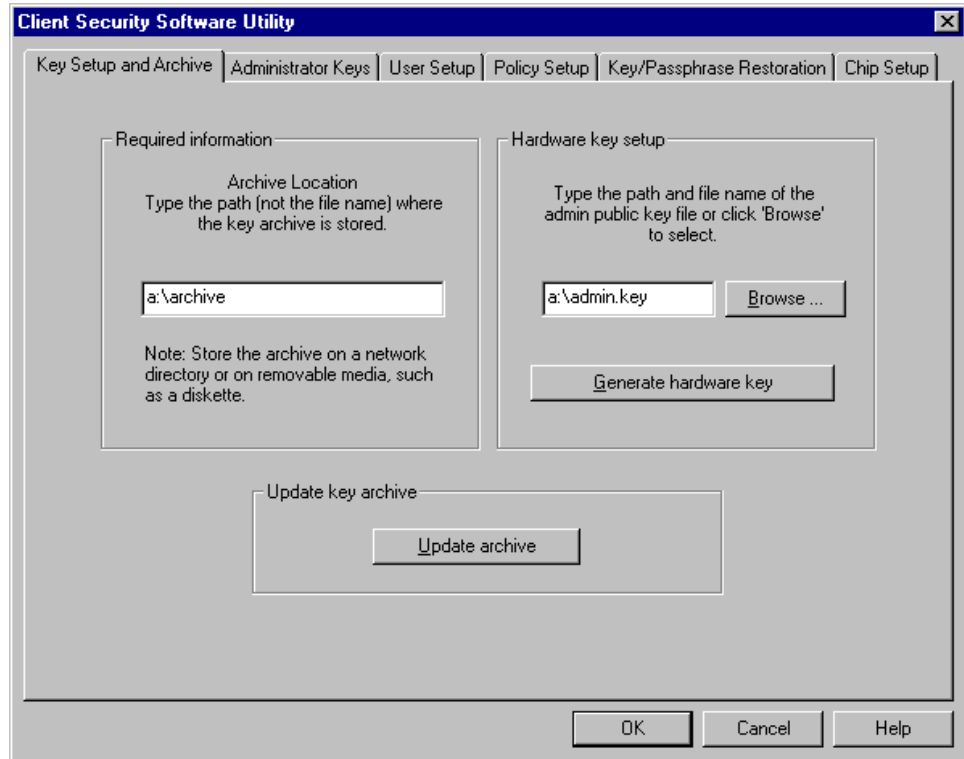
3. In the *Required information* area, type the path (not the file name) where the key archive will be stored. Store the archive on a diskette or shared directory. The previous example shows that the archive will be stored on a diskette in the ARCHIVE directory.

    Notes:

    ▪   If you want to save the archive to a shared directory, you must first map a drive letter to the shared network resource where that directory exists. For information on mapping a drive letter to a shared network resource, see your Windows operating system documentation.

    ▪   Because a hard disk drive failure can damage files, do not store the key archive on a local drive.

4. Click *Generate hardware key*. A window opens that notifies you that the operation was successful. Click *OK*.

    The hardware keys are generated for the client and copies of the keys are stored in the archive.

    Notes:

17

- When you create a key archive for a client, a subdirectory is automatically created that is named the same as the computer name. For example, if the computer name is CLIENT1, all archived keys for that computer would be stored in the subdirectory named CLIENT1. If you had typed in the path shown in the previous example, the archived files would be stored in A:\ARCHIVE\CLIENT1.

- If hardware keys exist for an IBM client and you choose to generate hardware keys again for that client, any existing user keys and digital certificates associated with the IBM embedded Security Chip will become invalid.

This completes the installation and setup of Client Security Software on the first IBM client.

Next, do one of the following:

- See the *Client Security Software Administrator's Guide* for instructions on how to set up the UVM security policy for the IBM client. You must set up UVM security policy before you can use the IBM embedded Security Chip for creating digital certificates or before you can use client authentication on the computer.

- Go to the next section and use the installation program to install the software, set a hardware password to enable the IBM embedded Security Chip, and generate the hardware encryption keys and key archive for other IBM clients.

Installation on other IBM clients when the admin public key is available

If you have installed the software on the first IBM client and created an admin key pair, you can install the software and enable the security subsystem on other IBM clients by using the installation program.

Notes:

- For Windows NT users, you must log on with a user ID that has administrator user rights before you can install Client Security Software.

- Because you must shut down and restart the computer to complete the installation, close all other Windows programs before starting the installation procedure.

- During the installation, you will be asked to choose the location of the admin public key and the key archive. If you want to use an admin public key that resides on a shared directory or save the key archive to a shared directory, you must first map a drive letter to the shared network resources for those directories before you can use the installation program. For information on mapping a drive letter to a shared network resource, see your Windows operating system documentation.

- The following instructions describe an attended installation, an installation where you physically reside at the computer during installation. For information on performing an unattended installation, see "Chapter 4 - Using the unattended installation option" on page 23.

To install and set up the software on other IBM clients:

1. Go to the next IBM client, and from the Windows desktop, click **Start → Run**.
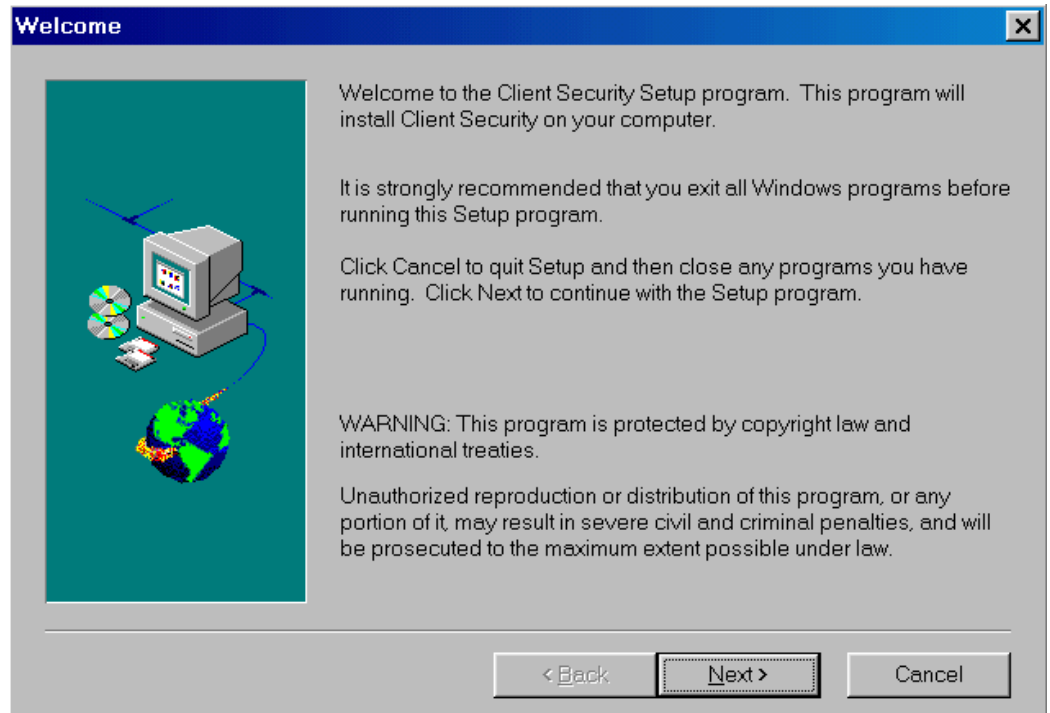
2. In the **Run** field, type:

   d:*directory*\csec12.exe

   where *d:* and *directory* are the drive letter and the directory where the file is located.

   Running this file unzips all the installation files for the software. When prompted, type the path to the folder where you want the files to be copied and click **OK**. SETUP.EXE, the file that runs the installation program, is one of the files that will be stored in the folder you specify.

3. Run SETUP.EXE.

   The installation program opens the Welcome window, which reminds you to exit from all Windows programs before you begin to install Client Security and notifies you of the copyright laws associated with Client Security Software.

4. Click **Next**.

   The installation program opens the Select Language window. Select the language you want to use during installation.

5. Click **Next**.

   The installation program opens the License Agreement window.
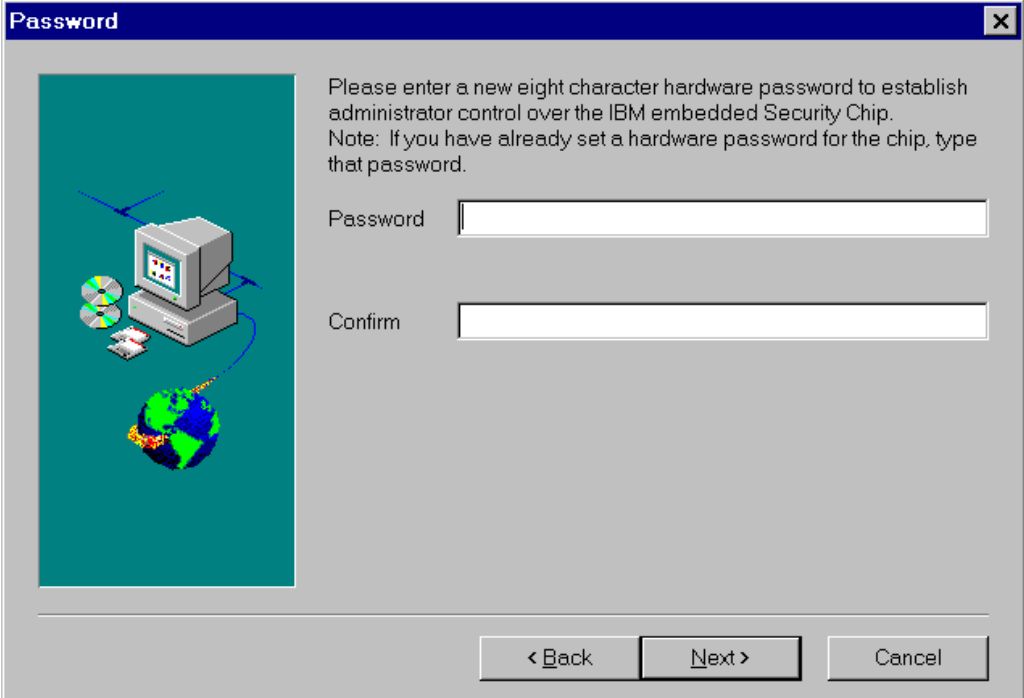
6. Click **I Agree** to proceed.

   Note: You must agree to the terms of the License Agreement to install Client Security Software. If you click **I Disagree**, the installation program will close without installing Client Security Software.

After you click *I Agree*, the Destination Directory Selection window opens.

7. Click *Next* to accept the default directory, C:\Program Files\IBM\Security, or click *Browse* to choose a different directory, and then click *Next*.

8. A window opens that asks if you want to enable the security subsystem for the IBM client. Click *Yes*.

The Password window opens.

9. In the *Password* field, type a hardware password. Next, in the *Confirm* field, type the password again to confirm it. Click *Next* to proceed to the next window.

For information on the rules for the hardware password, see "Appendix B - Rules for the hardware password ," on page 34.

10. If you stored the ADMIN.KEY file in the same directory as SETUP.EXE, the installation program automatically detects the admin public key file, and you do not need to provide the file name. Skip to step 11.

If the Choose Destination Location window opens, type the path to ADMIN.KEY or click *Browse* to search for the directory, and then click *Next*.
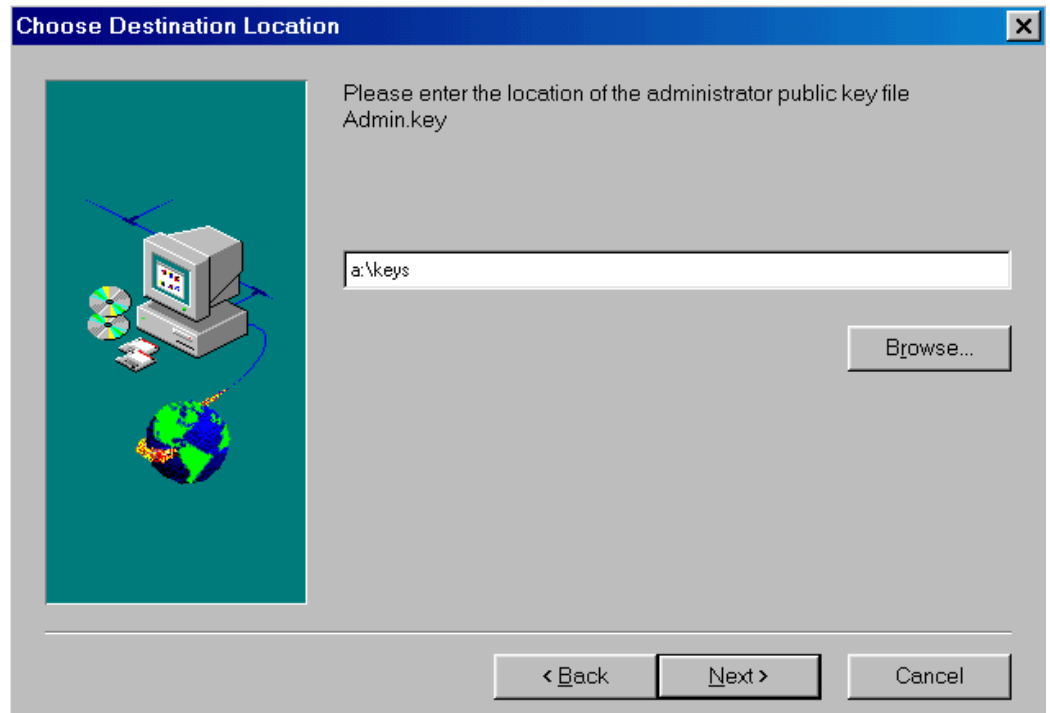
11. The Enter Information window opens and asks you where you would like to archive the key files. Type the path and directory to the key archive, and then click *Next* to install Client Security Software on the IBM client.

    Note: If you want to save the key archive to a shared directory, you must first map a drive letter to the shared network resource where that directory exists. For information on mapping a drive letter to a shared network resource, see your Windows operating system documentation.
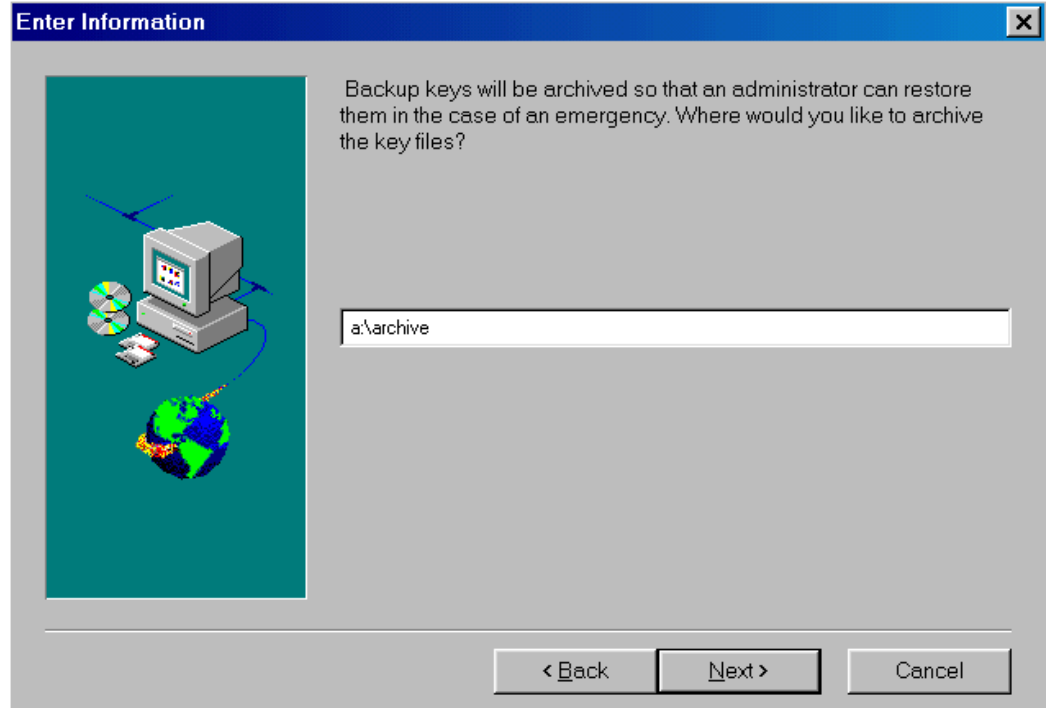
12. After the software is installed, a window opens that notifies you of the Web browser encryption strength that must be used with Client Security Software.

    Click *OK* to continue.

13. The Setup Complete window opens and asks you to restart the computer. Select *Yes, I want to restart my computer now* to restart the computer, or click *No, I will restart my computer later*.

    Note: You must restart the computer before Client Security Software will run properly. Also, if you used a diskette during the installation, remove it from the diskette drive before the computer restarts.

14. Click *Finish*.

Next, do one of the following:

• See the *Client Security Software Administrator's Guide* for instructions on how to set up UVM security policy for the IBM client. You must set up UVM security policy before you can use the IBM embedded Security Chip for creating digital certificates or before you can use client authentication on the computer.

• Repeat the steps in this section to install and set up the software on other IBM clients by exclusively using the installation program.

Chapter 4 - Using the unattended installation option

You can use the unattended installation option to install Client Security Software without having to be present at the computer.

Notes:

- For Windows NT users, you must log on with a user ID that has administrator user rights before you can install Client Security Software.

- To perform an unattended installation, you must have an admin public key (ADMIN.KEY). You create the admin key pair during the installation of Client Security Software on the first IBM client. If the ADMIN.KEY file you use is stored on a diskette, copy it to the hard disk of the IBM client or to a shared network directory so that it is available for the unattended installation.

To use the unattended installation option:

1. Run CSEC12.EXE on the IBM client to unzip the setup files. When prompted, enter the path to the folder where you want the files to be copied. Note that SETUP.EXE and SETUP.ISS are stored in the folder you specify.

2. Open the SETUP.ISS file in a text editor such as Notepad. The SETUP.ISS file is shown below.

```
[InstallShield Silent]
Version=v3.00.000
File=Response File

[Application]
Name=Client Security Software
Version=1.2 Beta
Company=IBM

[DlgOrder]
Dlg0=Welcome-0
Count=7
Dlg1=AskDestPath-0
Dlg2=AskYesNo-0
Dlg3=SdShowUserAndPassword-0
Dlg4=AskText-0
Dlg5=AskPath-0
Dlg6=SdFinishReboot-0

[Welcome-0]
Result=1

[AskDestPath-0]
szPath=C:\Program Files\IBM\Security
Result=1

[AskYesNo-0]
Result=1

[SdShowUserAndPassword-0]
svPassword=password
Result=1

[AsKeyPath-0]
szKF=C:\Program Files\IBM\Security
Result=1

[AskArchivePath-0]
szAP=C:\Program Files\IBM\Security
Result=1

[SdFinishReboot-0]
Result=1
BootOption=1
```

3. If desired, edit the SETUP.ISS file as shown below in bold and save the file. All bold entries are examples only. You can run the unattended installation without changing any values in SETUP.ISS, but make sure that the path to the ADMIN.KEY file is correct.

```
[InstallShield Silent]
Version=v3.00.000
File=Response File

[Application]
Name=Client Security Software
Version=1.2
Company=IBM

[DlgOrder]
Dlg0=Welcome-0
Count=7
Dlg1=AskDestPath-0
Dlg2=AskYesNo-0
Dlg3=SdShowUserAndPassword-0
Dlg4=AskKeyPath-0
Dlg5=AskArchivePath-0
Dlg6=SdFinishReboot-0

[Welcome-0]
Result=1

[AskDestPath-0]
szPath=C:\MySecurity
Result=1

[AskYesNo-0]
Result=1

[SdShowUserAndPassword-0]
svPassword=12345678
Result=1

[AskKeyPath-0]
szKF=C:\MyKeyFile
Result=1

[AskArchivePath-0]
szAP=K:\MyArchive
Result=1

[SdFinishReboot-0]
Result=1
BootOption=1
```

Notes:

- szPath=C:\MySecurity designates where Client Security Software will be installed.

- svPassword=12345678 assigns the hardware password for the IBM embedded Security Chip as "12345678." You can assign any hardware password you want, as long as it adheres to the rules for the hardware password. For information on the rules for the hardware password, see "Appendix B - Rules for the hardware password ," on page 34.

- szKF=C:\MyKeyFile designates the path to the ADMIN.KEY file. For the unattended installation to run properly, ADMIN.KEY must be in the specified path on the client hard disk or on a shared network directory. If the ADMIN.KEY file you use is stored on a diskette, copy it to the client hard disk or to a shared network directory so that it is available for the unattended installation.

- szAP=K:\MyArchive designates the path where the keys are archived. For the unattended installation to run properly, do not store the key archive on a diskette. If you want to store the key archive on a diskette, store the key archive on the client hard disk or a shared network directory during the unattended installation, and then copy it to a diskette after the installation is complete.[4]

4. From the Windows desktop, click **Start → Run**.

5. Type the path to SETUP.EXE, and add [space]-s to the path (for example, C:\Security\setup.exe -s). All files will be installed in the path specified for szPath, and the computer will restart.

---

[4] Hard disk failures can damage files; store key archive files on hard disks on a temporary basis only. Also, if you want to save the key archive to a shared directory, you must map a drive letter to the shared network resource where that directory exists before you can use the uninstallation program. For information on mapping a drive letter to a shared network resource, see your Windows operating system documentation.

Chapter 5 - Uninstalling Client Security Software

Because you must shut down and restart the computer to uninstall the software, close all other Windows programs before starting.

Attention: For Windows NT users, log on with a user ID that has administrator user rights before you uninstall Client Security Software. Do not attempt to uninstall the software while logged on with a user ID that does not have administrator user rights; if you do, you might not be able to log on to the operating system.

To uninstall Client Security Software:

1. Close all other Windows programs.

2. Click *Start → Settings → Control Panel*.

3. Click the *Add/Remove Programs* icon.

4. In the list of software that can be automatically removed, select *IBM Client Security*.

5. Click *Add/Remove....*

   Note: On clients running Windows NT Workstation, the next window (Uninstall) opens behind the Add/Remove Programs Properties window. Click the Uninstall window to make it the active window.

6. Click *Yes* to uninstall the software.

7. Do one of the following:

   - If you installed the IBM embedded Security Chip PKCS#11 module for Netscape, go to step 8.

   - If you did not install the IBM embedded Security Chip PKCS#11 module for Netscape, go to step 9.

8. The following window opens that asks you to start the process to disable the IBM embedded Security Chip PKCS#11 module. Click *Yes* to proceed.

   A series of windows will open. Click *OK* for each window until the IBM embedded Security Chip PKCS#11 module is removed.

9. A window opens that asks if you want to delete shared .DLL files that were installed with Client Security Software. Click *Yes* to uninstall these files, or

click *No* to leave the files installed. Leaving these files installed has no affect on the normal operation of your computer.

10. Click *OK* after the software is removed. You must restart the computer after uninstalling Client Security Software.

When you uninstall Client Security Software, you remove only the software components that were installed. Any encryption keys that you created remain stored on the IBM embedded Security Chip. Also, the key archive is not affected when Client Security Software is uninstalled.

Chapter 6 - Installing new software on an IBM client that has a previous version installed

If you want to install a new version of Client Security Software on an IBM client that has a previous version of Client Security Software installed, you must do the following:

1. Uninstall the previous software. For more information, see "Chapter 5 - Uninstalling Client Security Software" on page 27.

2. Install the new software. For more information, see "Chapter 3 - Installing the software" on page 11.

    Note: If you want to use the same hardware password that was set for the IBM embedded Security Chip, you do not have to clear the IBM embedded Security Chip. If the hardware password is unknown, you can clear the IBM embedded Security Chip to reset the password and clear all user encryption keys from the chip. See "Clearing the IBM embedded Security Chip" for more information.

3. Create new user encryption keys, set up user authentication, and obtain and use a new digital certificate for e-mail use. For details, see the *Client Security Software Administrator's Guide*.

Clearing the IBM embedded Security Chip

If you want to erase all user encryption keys from the IBM embedded Security Chip and clear the hardware password for the chip, you must clear the chip. Read the information in the Attention box below before clearing the IBM embedded Security Chip.

Attention

*   If a user clears the IBM embedded Security Chip, all encryption keys and certificates stored on the chip will be lost and the contents of the hard disk could become unusable.

*   Do not clear or disable the IBM embedded Security Chip if UVM logon protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software. To clear UVM logon protection, open the Administrator Utility, click the *Key Setup and Archive* tab, and clear the *UVM protection* check box. You must shut down and restart the computer before UVM logon protection is disabled.

To clear the IBM embedded Security Chip:

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 *IBM Embedded Security Chip*.

5. Select *Clear IBM Security Chip*.

6. Select *Yes* for Clear IBM Security Chip.

7. Press Esc to continue.

8. Press Esc to exit and save the settings.

Chapter 7 - Troubleshooting

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

Installing Client Security Software

During the installation process, a previously installed version of Client Security Software is detected.	Action
You attempt to install the software and a window opens that notifies you that a previous version of Client Security Software is already installed.	Click *OK* to exit from the window and the installation process. Do the following: 1. Uninstall the software. See "Chapter 5 - Uninstalling Client Security Software" for instructions. 2. Reinstall the software. See "Chapter 3 - Installing the software" for instructions. *Note:* If you plan to use the same hardware password to secure the IBM embedded Security Chip, you do not have to clear the chip and reset the password.

A hardware password has been set for the IBM embedded Security Chip, and that password is unknown.	Action
You attempt to install the software on an IBM client that already has an enabled IBM embedded Security Chip. The hardware password for the IBM embedded Security Chip is unknown.	You must clear the chip to continue with the installation. For more information, see "Clearing the IBM embedded Security Chip" on page 29.

After you install the software, the computer restarts, and an error message displays that states: "Hardware password check failed.".	*Action*
If the security subsystem is enabled when you install the software, you are still required to type a hardware password in the installation program. You must type the correct hardware password. If you type an incorrect password in the installation program, Client Security Software will install, but an error message will appear after you restart the computer.	No action is required. The software was installed and the security subsystem is still enabled with a previous hardware password. To enter the Administrator Utility, you must type the correct hardware password.

Note: You can receive this error message if you uninstall Client Security Software (with the security subsystem enabled), and then re-install Client Security Software and type the wrong hardware password |

Installing UVM-aware fingerprint sensor

During installation of the DigitalPersona U.are.UPro, the system will restart without providing you with the opportunity to finish the installation.	*Action*
During installation of the DigitalPersona U.are.UPro fingerprint sensor, a window opens and asks that you do the following:

1. Attach the fingerprint sensor

2. Wait for the red light to illuminate on the sensor

3. Click *OK*

The system will restart without providing an opportunity for you to click OK. | No action is required. This tip is for informational purposes only.   The fingerprint sensor will install correctly. |

32

Appendix A - U.S. export regulations for Client Security Software

The IBM Client Security Software package has been reviewed by the IBM Export Regulation Office (ERO), and as required by U.S. government export regulations, IBM has submitted appropriate documentation and obtained retail classification approval for up to 256 bit encryption support from the U.S. Department of Commerce for international distribution except in those countries embargoed by the U.S. Government. Regulations in the U.S.A. and other countries are subject to change by the respective country government.

If you are not able to download the Client Security Software package, please contact your local IBM sales office to check with your IBM Country Export Regulation Coordinator (ERC).

Appendix B - Rules for the hardware password

This appendix contains rules for the hardware password.

The following table describes the rules for the hardware 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.
Properties	You set the hardware password to enable the IBM embedded Security Chip in the computer. The hardware password must also be typed each time you access the Administrator Utility.
Incorrect attempts	If you incorrectly type the password 10 times, the computer locks up for 1 hour and 17 minutes. If after this time period has passed, you type the password incorrectly 10 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 10 times.

Appendix C - 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 is a trademark of IBM Corporation in the U.S., other countries, or both.

Lotus Notes is a registered trademark of Lotus Development Corporation.

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

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

Other company, product, and service names mentioned in this document may be trademarks or servicemarks of others.