IBM® Client Security Solutions

Client Security User's Guide
Version 1.3.1

August 2000

Before using this information and the product it supports, be sure to read "Appendix B - Notices and Trademarks," on page 28.

First Edition (August 2000)

Table of Contents

About this Guide

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

The guide is organized as follows:

"Chapter 1 - Overview of IBM Client Security Software," contains an overview of the components provided by Client Security Software.

"Chapter 2 - Using UVM protection for the system logon," contains instructions for using UVM protection with the system logon. Instructions for users of Windows NT Workstation 4.0, Windows 98 and Windows 95 are provided.

"Chapter 3 - Setting up the Client Security screen saver," contains instructions on how to set up the Client Security screen saver.

"Chapter 4 - Using the Client Utility," contains information and instructions on how to change your UVM passphrase. Also, for Windows NT users, instructions for changing the Windows NT password is provided.

"Chapter 5 - Using secure e-mail and Web browsing," contains information about using Microsoft and Netscape applications with the cryptographic capabilities provided by Client Security Software.

"Chapter 6 - Troubleshooting," contains troubleshooting information associated with Client Security Software.

"Appendix A - Rules for the UVM passphrase," contains a description of the rules for the UVM passphrase.

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

How to use this guide

This guide is intended for Client Security end users (or client users). Client Security 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.

The information provided in this guide is also provided in the *Client Security Software Administrator's Guide*. The *Client Security Software Administrator's Guide* is intended for a security administrator who installs and sets up Client Security Software on IBM clients. For information about installing and setting up Client Security Software, contact your administrator.

Conventions used in this guide

This guide uses several typeface conventions that have the following meaning:

- **Bold -** Commands, keywords, file names, 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 - Overview of 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:

- **User encryption key management with the IBM embedded Security Chip**. Encrypting and storing your user keys on the IBM embedded Security Chip adds an extra layer of client security, because the keys are securely bound to the computer hardware. A security administrator generates the hardware and user encryption keys for you.
- **Digital certificate creation and storage that is protected by the IBM hardware**. If you apply for a digital certificate that can be used for an e-mail application, Client Security Software enables you to choose the IBM embedded Security Chip as the cryptographic service provider associated with the certificate.
- **Access to the security policy of your computer:** A security administrator sets up the security policy for your computer and provides you with your User Verification Manager (UVM) passphrase. You use the UVM passphrase to authenticate yourself as a trusted user of the security policy for the computer.
- **A key archive and recovery solution**. Two important functions in a PKI are creating a key archive and then restoring keys from that archive when necessary. If the encryption keys for your computer are lost, the security administrator can restore them from a key archive.

What software is installed?

When Client Security Software is installed and set up on your computer, the following software components are installed:

- **Client Utility:** The Client Utility enables you to change your UVM passphrase. Also, for Windows NT users, if you change your Windows NT password in the User Manager program, use the Client Utility to update the Windows NT password so that it is recognized by the security policy set for your computer. Finally, you can use the Client Utility to update the key archive after you use the IBM embedded Security Chip to generate a digital certificate.
- **User Verification Manager (UVM):** UVM is software that enables an administrator to set the security policy for the computer. As a client user of that security policy, you can use your UVM passphrase for authentication when you use UVM protection for the system logon, the Client Security screen saver, and when you create digital certificates with the IBM embedded Security Chip as the cryptographic service provider.
- **UVM protection for the system logon:** The security administrator sets up UVM protection for the system logon. UVM protection ensures that only those users who are recognized by the security policy of the computer are able to access the operating system. You use your UVM passphrase when you attempt to log on to the computer.

- **Client Security screen saver:** The Client Security screen saver enables you to control access to the computer through a screen saver interface. You use your UVM passphrase to bypass the screen saver and gain access to the computer.
- **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.
- **Administrator Utility:** The Administrator Utility is the administrator interface to the client security features. Access to the Administrator Utility is protected by a password that the administrator creates.

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

Chapter 2 - Using UVM protection for the system logon

This chapter contains information about using UVM protection for the system logon. Before you can use UVM protection, it must be enabled for the computer. For information on enabling UVM protection for the system logon, contact your security administrator.

UVM protection enables you to control access to the operating system through a logon interface. The logon procedure can differ depending on which operating system is used, Windows NT Workstation 4.0 or Windows 98 and Windows 95.

Windows NT users

For Windows NT, the UVM logon interface replaces the Windows NT logon application, so that, if you try to unlock the computer, the UVM logon interface opens instead of the Windows NT logon window.

Access the UVM logon interface

To access the UVM logon interface, press **Ctrl + Alt + Delete**. You can perform the following tasks:

- click **Shut down** to shut down the computer
- click **Lock Workstation** to lock the computer (see below for information on unlocking the computer)
- click **Task Manager** to open Task Manager
- click **Logoff** to log off the current user

Unlock a Windows NT client

To unlock a client that runs Windows NT and uses UVM protection:

1. Press **Ctrl + Alt + Delete** to access the UVM logon interface.
2. Type your user name and the domain where you are logged on, 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.
   - If the UVM passphrase does not match the user name and domain entered, the UVM logon window opens again.
   - If you type the correct UVM passphrase for the user name and domain entered, the logon is successful.

   Note: Depending on what authentication requirements have been set in the security policy for the computer, you might have to type your UVM passphrase and scan your fingerprints to unlock your computer. Contact your security administrator for more information.

Windows 98 and Windows 95 users

For Windows 98 and Windows 95, UVM protection supports the use of the operating system logon window. UVM protection forces a Client Security screen saver session to be immediately launched upon logon.

To unlock a computer that uses Windows 98 or Windows 95 and UVM protection:

1. When the operating system logon window opens, type your user name and password information, and click **OK**.
2. Depending on what authentication requirements have been set in the security policy for the computer, you might have to type your UVM passphrase (associated with the user name in the operating system logon) and scan your fingerprints to unlock your computer. Contact your security administrator for more information.

   If you fulfill the authentication requirements set for the computer, the computer unlocks.

   If you do not fulfill the authentication requirements, the Client Security screen saver displays without unlocking the computer.[1]

[1] The Client Security screen saver may or may not be the selected screen saver for your computer. For Windows 98 and Windows 95, UVM logon protection uses the Client Security screen saver to secure the logon.

Chapter 3 - Setting up the Client Security screen saver

This section contains information about setting up the Client Security screen saver. The Client Security screen saver is one of the software components that is automatically installed by Client Security Software. Before you can use the Client Security screen saver, at least one user must exist on the security policy of your computer. Contact your security administrator for information about adding new users to the security policy for your computer.

The Client Security screen saver is a series of moving images that display after your computer is idle for a specified period of time. Setting up the Client Security screen saver is a way to control access to the computer through a screen saver application.

To set up the Client Security screen saver:

1. Click **Start → Settings → Control Panel**.
2. Click the **Display** icon.
3. Click the **Screen Saver** tab.
4. In the **Screen Saver** drop-down menu, select **Client Security**. To change the speed of the screen saver, click **Settings** and select the desired speed.
5. Click **OK**.

If the Client Security is activated, press any key or move the mouse to unlock the computer. Depending on what authentication requirements have been set in the security policy for the computer, you might have to type your UVM passphrase and scan your fingerprints to unlock your computer. Contact your security administrator for more information.

Note: If the IBM embedded Security Chip is disabled or all users are removed from the security policy for your computer, the Client Security screen saver is unavailable for use. See the security administrator for more information.

Chapter 4 - Using the Client Utility

The Client Utility enables you to change the following:

- **UVM passphrase**. Your UVM passphrase authenticates you as a trusted user to the security policy of the computer. To improve security, you can periodically change your UVM passphrase. Also, the UVM can be longer and more unique than traditional passwords.
- **Windows NT logon settings**.[2] If you change your Windows NT password with the User Manager program, you must also change the password by using the Client Utility.

  Note: Only change Windows logon information in User Manager for the user currently logged on.
- **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.
- **Register user fingerprints**. If you want to use a fingerprint reader (or scanner) for authentication, you can register your fingerprints with UVM.

  Notes

  - You can use your fingerprints for authentication only if a UVM policy has been set up for your computer. Contact your security administrator for more information.
  - Before you can register fingerprints with UVM, a fingerprint scanner must be attached to the IBM client system. For instructions on how to attach and use the fingerprint scanner, refer to the documentation provided by the hardware vendor.

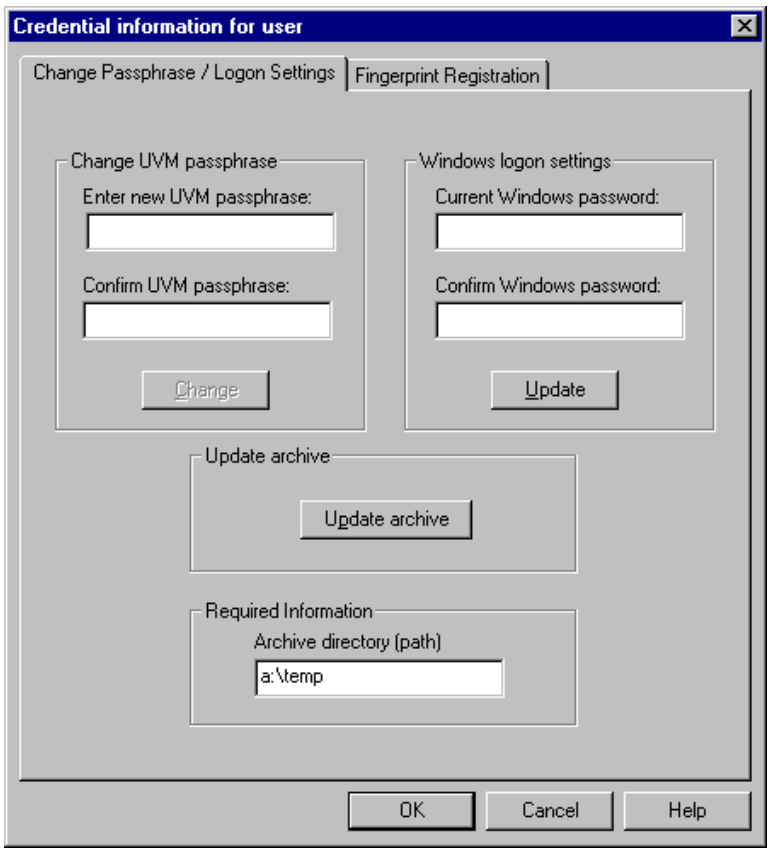
Change your UVM passphrase

To change your UVM passphrase:

1. Click **Start → Programs → Client Security Software Utilities→ Client Utility**.
2. Type your UVM passphrase and click **OK**.

   The following window opens.

[2] Changing the Windows logon password is applicable for users of Windows NT only.



3. In the **Required information** area, type the path to the key archive that was set up for you. Contact your security administrator for the location of the key archive.
4. In the **Change current passphrase** area, type a new passphrase in the **New passphrase** field. Next, type the passphrase again in the **Confirm new passphrase** field, and then click **Change**. For information on the rules for the UVM passphrase, see "Appendix A - Rules for the UVM passphrase," on page 27.
5. Click **OK** to exit.

Change your Windows NT logon settings

To change your Windows NT logon settings:

1. Click **Start → Programs → Client Security Software Utilities→ Client Utility**.
2. Type your UVM passphrase and click **OK**.
3. In the **Required information** area, type the path to the key archive that was set up for you. Contact your security administrator for the location of the key archive.
4. In the **Current Windows password** field, type a new Windows NT password. Next, type the new password again in the **Confirm Windows**

password field, and then click **Update**. For rules on the Windows NT logon password, see the operating system documentation.

5. Click **OK** to exit.

Update the key archive

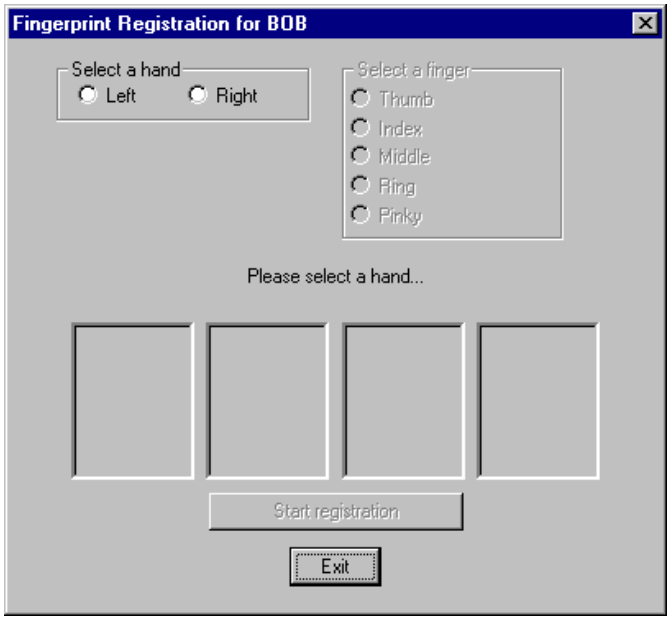
To update the key archive:

1. Click **Start → Programs → Client Security Software Utilities→ Client Utility**.
2. Type your UVM passphrase and click **OK**.
3. In the **Required information** area, type the path to the key archive that was set up for you. Contact your security administrator for the location of the key archive.
4. Click **Update archive**, and then click **OK** on the window that opens to notify you that the operation was successful.
5. Click **OK** to exit.

Register your fingerprints

To register your fingerprints:

1. Click **Start → Programs → Client Security Software Utilities→ Client Utility**.
2. Type your UVM passphrase and click **OK**. The Client Utility opens.
3. Click the **Fingerprint Registration** tab, and then click the **Click to launch fingerprint registration** button. The following window opens.

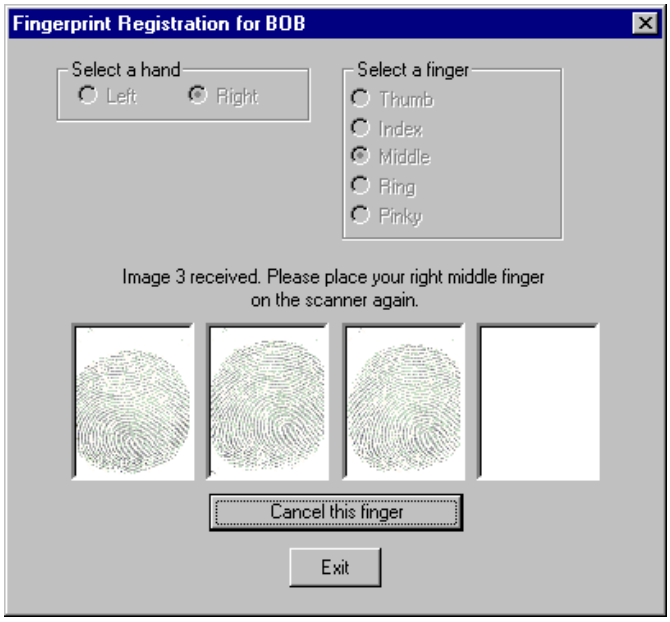


4. In the **Select a hand** area, click **Left** or **Right**.

5. In the **Select a finger** area, click to select the finger you will scan for prints, and click **Start registration**.
6. Place your finger on the fingerprint reader and follow the instructions on screen to scan four copies of your fingerprint. (The fingerprint registration program requires that four fingerprints be scanned.) When you have finished scanning your fingerprints, click **Exit**.

   You can click **Cancel this finger** at any time to cancel the scan of the finger you selected.

   The window below shows that three fingerprints have been registered.



Chapter 5 - Using secure e-mail and Web browsing

If you send unsecured transactions sent 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 (or 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.

Tips for 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.

Notes:

- To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see your security administrator.
- For information about known limitations when using Client Security Software with Microsoft applications and troubleshooting information, see "Known limitations," on page 19 and "Troubleshooting charts," on 20.

Obtain a digital certificate

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 Chip CSP** as your CSP when you obtain your digital certificate. This ensures that the private key of the digital certificate is stored on the IBM embedded 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.

The following graphic shows what the certificate authority interface might look like when you are prompted to select a CSP.

After you select **IBM embedded Security Chip CSP** as the CSP, the UVM component in Client Security Software will prompt you for your UVM passphrase or for fingerprint authentication. Contact your security administrator for more information on what authentication requirements have been set for the security policy of your computer.

Update the key archive

After you create a digital certificate, back up the certificate by updating the key archive. Use the Client Utility to update the key archive. See "Chapter 4 - Using the Client Utility," on page 11 for details.

Use the digital certificate

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. See your security administrator for more information.

Tips for using Client Security Software with Netscape 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 PKCS#11, specifically Netscape applications.

For details on how to use the security settings for Netscape applications, see the documentation provided by Netscape.

Notes:

- To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see your security administrator.
- For information about known limitations when using Client Security Software with Netscape applications and troubleshooting information, see "Known limitations," on page 19 and "Troubleshooting charts," on 20.

Install the IBM embedded Security Chip PKCS#11 module

Before you can use a digital certificate, you must install the IBM embedded Security Chip PKCS#11 module onto the computer. Because the installation of

the IBM embedded Security Chip PKCS#11 module requires a UVM passphrase, you must add at least one user to the security policy for the computer. Your security administrator adds users to the security policy for your computer.

To install the IBM embedded Security Chip PKCS#11 module, do one of the following:

1. Do one of the following:
   - If Netscape was installed on the computer before Client Security Software was installed, you can run the installation file from the Windows Start menu to add the IBM embedded Security Chip module. Click **Start → Programs → Client Security Software Utilities → Add IBM Embedded Security Chip Module**.
   - If Netscape was installed on the computer after Client Security Software was installed, open and run the installation file in Netscape. Open Netscape and click **File → Open page**. Locate the install file, IBMPKCSINSTALL.HTML, and open it in Netscape. (If Client Security Software was installed in the default directory, the file is located in C:\Program Files\IBM\Security. See your security administrator for details.) When you open the file in Netscape, the installation file runs.
2. The UVM passphrase window opens. Type the UVM passphrase and click **OK**.
3. The following window appears when you run the installation file. Click **OK.**

4. A window opens that notifies you that the module was installed. Click **OK**.

Using the PKCS#11 logon protection

If PKCS#11 logon protection is set up for the computer, you must meet the authentication requirements each time you log on to Netscape. You might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements. The authentication requirements are defined in the UVM policy for the computer. See your security administrator for more information.

Select IBM embedded Security Chip when generating a digital certificate

When you generate a digital certificate in Netscape, select the IBM embedded Security Chip as the generator of the private key associated with the certificate.

During digital certificate creation, you will see the following window. Make sure you select **IBM embedded Security Chip**.

For more information on generating a digital certificate and using it with Netscape, see the documentation provided by Netscape.

Update the key archive

After you create a digital certificate, back up the certificate by updating the key archive. Use the Client Utility to update the key archive. See "Chapter 4 - Using the Client Utility," on page 11 for details.

Use the digital certificate

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

After you have installed the IBM embedded Security Chip PKCS#11 module, UVM will prompt you for authentication requirements each time you use the digital certificate. You might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements. The authentication requirements are defined in the UVM policy for the computer.

Note: If you do not meet the authentication requirements set by the UVM, a window opens that displays an authentication failure message. For more information, see "Client Security Software and Netscape," on page 19.

Chapter 6 - Troubleshooting

This chapter provides known limitations and troubleshooting information that is helpful for identifying or solving problems.

Known limitations

This section provides information about known limitations related to Client Security Software.

Client Security Software and Netscape

Netscape opens after an authentication failure: If you type an incorrect UVM passphrase or provide the wrong fingerprints for a fingerprint scan, the following window opens.

Click **OK**, and Netscape opens. You will not be able to use the digital certificate generated by the IBM embedded Security Chip until you close and restart Netscape, and provide the correct UVM passphrase, fingerprints, or both.

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

- SHA-1
- MD5

IBM embedded Security Chip 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 Chip 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 Chip 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 Chip certificate. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.

Troubleshooting charts

Use the troubleshooting charts in this section to find solutions to problems that have definite symptoms.

Client Security Software and Microsoft applications

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

Problems reading encrypted e-mail using Outlook Express	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. 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. **Note:** To use 128-bit Web browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. See your security administrator for more information.

Problems using a certificate from an e-mail 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 Chip of the sender's computer where the certificate was generated.	Ask the recipient to re-send 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) encrypts e-mail messages with the 3DES algorithm only	**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.	To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. See your security administrator for more information. Also, 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 trying to use a certificate that has been restored 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 a new certificate ▪ re-register the certificate authority with Outlook Express

Outlook Express does not update the encryption strength associated with a certificate sent from Netscape Messenger.	**Action**
If 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. Re-open the signed e-mail and add the certificate to the address book in Outlook Express.

In Outlook Express, the error decryption message displays in the preview pane, or if a message is opened too quickly.	**Action**
A message in Outlook Express can be opened if you double-click on it. In some instances, if you double-click quickly on an encrypted e-mail message, an error decryption message appears. This error message will also appear in the preview pane of Outlook Express if an encrypted message is selected.	No action is required is the error message appears in the preview pane. If you attempted to open an e-mail message and the decryption error message appears, close the message, and then re-open the encrypted e-mail message.

An error message displays if you click the Send button twice when you are trying to send an encrypted e-mail message.	**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 this error message and click the Send button once.

Client Security Software and Netscape

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

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. 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. **Note:** To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. See your security administrator for more information.

Failure message when trying to digitally sign an e-mail message when using Netscape Messenger	**Action**
If the IBM embedded Security Chip certificate has not been selected in Netscape Messenger, and a composer 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 and 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 sent from Netscape Messenger to Outlook Express is returned to the Netscape 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 the digital certificate generated by the IBM embedded Security Chip	**Action**
The digital certificate generated by the IBM embedded Security Chip 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 Chip. 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**
If 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 Chip certificate	**Action**
The IBM embedded Security Chip certificate cannot be exported in Netscape. The export feature in Netscape can be used to back up certificates.	Go to the Client Utility to update the key archive. If you update the key archive, copies of all the certificates associated with the IBM embedded Security Chip are created.

Error message when trying to use a certificate that has been restored 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, obtain a new certificate. See your security administrator for more information on restoring keys.

Netscape agent opens and causes Netscape to fail	**Action**
Netscape agent opens and closes the Netscape application you are working in.	Turn off the Netscape agent.

Netscape delays if you try to open it	**Action**
If you install the PKCS#11 module, a short delay might occur each time you open Netscape.	No action is required. This tip is for informational purposes only.

Appendix A - Rules for the UVM passphrase

This appendix contains the rules for the UVM passphrase. To improve security, the UVM passphrase is longer and can be more unique than a traditional password.

The following table describes the rules for 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 nonalphanumeric characters.
Properties	The UVM passphrase is different from a password that you might use to log on to an operating system. The user passphrase can be used in conjunction with other authenticating devices, such as a fingerprint reader or a smart card.
Incorrect attempts	If you incorrectly type the UVM passphrase multiple times during a session, the computer will not lock up.

Appendix B - Notices and Trademarks

This appendix gives legal notice of IBM product availability, patents, and patents pending, 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.

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.