User Manual for Macintosh

SafeMail

Highware, Inc.
151 rue Jourdan
1060 Brussels, Belgium
Voice: +32 2 537 68 10
Fax: +32 2 537 51 55

info@highware.com
http://www.highware.com
ftp://ftp.highware.com

SafeMail®

This manual and the software described in it are copyrighted with all rights reserved. Under the copy laws, this manual or the software may not be copied in whole or in part, without written consent of Highware, except as set forth in the License Agreement found on the envelope containing the software floppies.

The software contained on the enclosed disk is the property of Highware. It can be used either by the original purchaser or by any other person possessing the software (hereafter know as "the User") in accordance with the terms of the licensing agreement executed with the original purchaser at the time of the acquisition of SafeMail (hereafter known as the "Licensing Agreement"). The User must have studied the Licensing Agreement and signed and returned a Registration Card (thereby agreeing to be bound by the terms and conditions foreseen by the Licensing Agreement).

As stated more fully in the Licensing Agreement, all copying, duplication, sale or distribution of this software (including, and without limitation, all or part of the software contained in this package) is hereby expressly forbidden.

THE DEVELOPERS AND DISTRIBUTORS OF SAFEMAIL AND SafeMail MAKE NO EXPRESS OR IMPLIED WARRANTIES WITH RESPECT TO THE PRODUCT AND SPECIFICALLY DISCLAIM WITHOUT LIMITATION (1) ANY WARRANTIES OF MERCHANTIBILITY OR FITNESS FOR ANY PARTICULAR PURPOSE AND (2) ANY LIABILITY FOR ANY DAMAGES - INCLUDING LOST PROFITS, LOST SAVINGS, LOSS OF USE, INTERRUPTION OF BUSINESS, OR OTHER INCIDENTAL, SPECIAL, COMPENSATORY, INDIRECT, EXEMPLARY, OR CONSEQUENTIAL DAMAGES - ARISING OUT THE USE OF THE PRODUCT, EVEN IF THE COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SafeMail is a registered trademark of Highware, Inc.
Macintosh, Mac and the Mac OS logo are trademarks of Apple Computer, Inc., used under license.
All other trademarks or registered trademarks are the property of their respective owners.

10/99

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION

Thank you for choosing SafeMail! We hope this software will satisfy all your security requirements in sending e-mails and protecting your data.

The terminology used when describing security systems may seem somewhat “obscure” to you if you are not familiar with encryption technology. Therefore, we will try to use simple wording throughout this manual. Our objective is to bring you an easy-to-use software for a technology that is very secure but has had a very complex interface for years. At the end of this manual and on our web site we refer to books and web sites that explain in-depth the different technologies used in SafeMail.

Advanced users familiar with public key cryptography may go directly to the next chapter.

OVERVIEW

It is about privacy.

SafeMail® allows you to communicate and exchange information securely with other people. The information (mail, files, etc.) can be sent over the Internet or through any kind of electronic channel or media.
With SafeMail, you will be able to *protect* (encrypt) and/or digitally ***Sign*** (authenticate) any data, such as an e-mail or a computer file.

In brief, SafeMail is a high security cryptographic software with an easy-to-use interface, based on a technology known as public key encryption and compatible with a standard known as OpenPGP.
SafeMail is integrated into the System and is available in all applications you want it to be. This makes SafeMail much more easy to use than many other encryption software.

Introduction

The need for security has always existed but since the advent and evergrowing popularity of the Internet, this need is extended to a much wider group of people. Sending a mail through the Internet is much less secure than sending a letter with the Post Office or even by fax. The content of your mail normally transits in clear text from server to server and anyone could read and modify its content. You don't have to be paranoid to acknowledge the risk is there and is real. It is probably not so important for a personal message to your brother or girlfriend but when exchanging information with a confidential character, the implications can be quite different if someone intercepts the message…

Encryption is about your rights to privacy.

Encryption and Digital Signature

Encryption is used to protect information and to keep it confidential. A document which has been encrypted must first be decrypted in order to be accessed and view its contents in a readable form. Encryption software has existed for many years and the most common way of encryption is to protect a document with a password (we also refer to such kind of encryption as "conventional encryption" or "simple key encryption"). To decrypt the document you use the same password. It is easy to use but not the most secure system. Why? Because most of the time, and contrary to the advise of all encryption software manuals, most passwords used are easy to guess, for example, a pet's name, birthday dates, etc. Moreover, in case of file transferts, the sender has to communicate the password of the encrypted document to the recipient.
SafeMail uses an encryption method called Public Key Encryption which does not require any password to be transmitted to the recipient.

A **digital signature** is applied to an electronic document to authenticate it much like your handwritten signature on a paper document. By using SafeMail, in addition to be able to ***authenticate*** a document - proving that YOU have signed the document - your recipient will also be able to verify the ***integrity*** of the document, that is he will be able to check that nobody modified the document once you have signed it.

Because of its strong security and multiple functions, Public Key Cryptography such as the one supported by SafeMail is likely to replace conventional or password encryption software in many domains.

How does Public Key Encryption work?

To communicate securely with other users, each user will have to create two complementary keys - also called a key pair - which consist of a **private key** and a **public key**.
Your private key is confidential and only you have access to it.
Your public key is automatically generated from your private key. As its name implies, it is “public” and can be freely exchanged with other users. To facilitate this key distribution, there are several “Key Servers” on the Internet. Their purpose is to be a repository of public keys. They contain hundreds of thousands - soon millions... - of public keys belonging to people from all over the world. Once you have created your own key pair, SafeMail will assist you in publishing your public key on one of these key servers. The key servers are regularly synchronized.

Sending and receiving encrypted messages

To send someone a private mail, SafeMail will use that person’s public key to encrypt the information, which only he can decrypt by using the corresponding private key.

Conversely, when someone wants to send you a private mail, he will use your **public key** to encrypt the mail, which only you can decrypt by using your **private key**.

Sending and Receiving Signed messages

To **sign** an e-mail or a file you send to others, SafeMail will use your **private key** to authenticate them. The recipients can then use your public key to determine if it is really you who sent the e-mail or the file and whether it has been altered during its transfer.

Conversely, when someone sends you an e-mail or a file with his digital signature, SafeMail will use his public key to check the signature and to verify that no one has tampered with the contents.

SECURING FILES ON YOUR COMPUTER

You can also use SafeMail to secure files that are on your computer and are not intended to be sent to someone else. You can encrypt them with your public key and you will be the only one able to decrypt them. You can also sign sensitive files to periodically check that they have not been altered.
A file can be encrypted, it can be signed or it can be encrypted **and** signed.

ENCRYPTING FOR MANY RECIPIENTS

To encrypt a message or a file for a group of people, you use the public keys of all the recipients at once. Every owner of a private key which corresponds to one of the public keys you have used will be able to decrypt the document.

MANAGING KEYS

Besides your own Private and public keys, you are bound to accumulate many public keys from your colleagues, friends, and other people with whom you want to share private information. For easy management, all keys are stored in Keyrings.
You may have as many keyrings as you want. The SafeMail Keyring Manager application will enable you to manage them easily.

CERTIFICATION AND TRUST

When you obtain someone's public key, you have to check to make sure that the key really belongs to the purported owner. We will explain how to verify this later on.
Once you are certain that the public key is valid, you can apply a **Certificate** to that key. It indicates that you feel, you "certify", the key is safe to use and it belongs to its purported owner.
Many people can apply certificates to the same public key. The trust you have in these people is very important to determine the quality of the key ,unless you have verified the key yourself. In addition to your own Certificates, you can grant a person's key a **level of trust** indicating how much confidence you have in that person's key to certify someone else's public key.

COMPRESSION

Two tools in one: In addition to the security feature of SafeMail, every encrypted file is compressed using the Zip standard. It implies that it will take less time to send a file and that the encrypted files will occupy less space on your hard disk.

COMPATIBILITY

SafeMail is compatible with the OpenPGP message format, an IETF proposed standard in public-key encryption software. It means that the people to whom you send encrypted or signed files will be able to receive your messages whether they use PGP software or SafeMail. Alternatively, you will be able to verify signatures or decrypt data sent by people using PGP under any operating system, be it Mac OS, Windows or UNIX.

Additional information on public key encryption and other useful terms are explained in the Glossary section at the end of the manual.

CHAPTER 2 - GETTING STARTED

This chapter contains:

- General information about this manual.
- Customer Support information.
- System Requirements for installing SafeMail.
- **Installing SafeMail**: Read this section if you install SafeMail for the first time.
- **Upgrading to SafeMail**: Read this section if you upgrade to SafeMail from a version previous to Version 2 or from another software.
- **What will be installed on your Macintosh** and where.

Before going any further, please complete and return your Registration Card. If you purchased the software through the Internet, you are automatically registered with us. Store your license number in a safe place. You will require it during installation and whenever you contact our customer support.

ABOUT THIS MANUAL

This manual guides you through the process of installing, configuring and using SafeMail. Many of the techniques you use in SafeMail, such as using the mouse or working with windows, are standard ways of working with a Macintosh. If you are unfamiliar with these techniques or the vocabulary used to describe certain features, you should refer to your Macintosh Owner's Guide for further information.

This manual is organized as both a tutorial and a reference guide:

Chapter 1 is an introduction to securing mail and files with SafeMail. If you are not familiar with public keys, read this section.

Chapter 2 is about installing/upgrading SafeMail. It explains what will be installed on your Macintosh and gives a short description of the different components of SafeMail.

Chapter 3 describes how to create your private and public keys.

Chapter 4 describes how to distribute your public key and how to obtain public keys from other people.

Chapter 5 describes how to send and receive secure e-mail and files. It explains how to encrypt or sign files on your computer.

Chapter 6 describes how to manage keys and keyrings on your computer.

Chapter 7 describes how to configure SafeMail. It explains all menu items and features available within the SafeMail Keyring Manager application.

Chapter 8 explains how to set the general options for the SafeMail menu, available in the Control Panel.

Chapter 9 explains how to use the SafeMail for Eudora plug-in.

Chapter 10 explains how to use the SafeMail Contextual menu.

Appendix A lists all icons available in SafeMail.

A **Glossary** at the end of the manual briefly explains the terms and principles used in SafeMail and gives you more detailed information about public key encryption terminology.

Customer Support

You may contact us if you have any queries about SafeMail. You will find the address of the distributor for your country in the Customer Support file on the SafeMail program CD or on our web site. For quick answers to frequently asked questions, we refer to our web site at http://www.highware.com. When you call for support, please make sure you have returned your Registration Card (if you purchased the software through the Internet, you are automatically registered with us) and have the following items handy:

- This manual and your SafeMail license number.
- Your current SafeMail version number.

You can find the SafeMail version number by choosing About SafeMail… from the SafeMail Menu or in the SafeMail Keyring Manager.

- The type of Macintosh you are using and your System version number. You can find this information under the Apple menu by choosing About This Macintosh… while in the Finder.

System Requirements

SafeMail requires a PowerPC Macintosh running System 7.6 or later. See the Read Me file on the SafeMail folder for up-to-date details on System requirements and compatibility.

Installing SafeMail

Double-click the SafeMail Installation file or select it and choose Open in the File menu. Choose the disk on which you want to install SafeMail then click Install.

When you are finished installing, click the Restart button. As soon as startup has completed, the SafeMail menu will be available in the menu bar and a folder called “SafeMail Folder” is now created on your hard disk. Double-click the folder’s icon, then double-click the Read Me icon to view late-breaking information about SafeMail.

The first time you will launch SafeMail, the registration window appears. Enter your name, organization and the serial number you received with the program.

Upgrading to SafeMail

Upgrading from SafeMail 2.0 or higher: The installer will upgrade all necessary files and throw the old files into the Trash.

Upgrading from FileCrypt 1.0: Make a backup copy of your current keyring. Remove or delete the FileCrypt 1.0 extension file (inside the Extensions folder in the System Folder). You may also delete the FileCrypt

Preferences file inside the Preferences folder. Restart the computer and proceed with the installation as described above.

Upgrading from other PGP software: Make a backup copy of your current keyring. Consult the manual of the PGP software on how to remove it then restart the computer and proceed with the installation as described above.

Once the installation has been completed, you will have to indicate to SafeMail the location of your current keyring. The Keyrings folder can be anywhere on your disk but we suggest you store it inside the SafeMail Folder. Select Settings from the Edit menu and define the location of your private and public keyrings' files in the Keyring panel.

What will be installed on your Macintosh?

1. The folder SafeMail Folder is created on the hard disk root. It contains:

- The **SafeMail Keyring Manager** application, which allows you to create your private key and manage your keyrings. You can also use this application to encrypt and sign documents.
- The Keyrings folder, containing a sample keyring.
- The Eudora Plug-in folder, containing the **SafeMail for Eudora** plug-in. To use the plug-in, store it into the Eudora Stuff folder inside the Eudora Folder. The plug-in will be active the next time you start Eudora.
- The Sherlock Plug-in folder, containing the Sherlock plug-in PublicKeyServer.src. This plug-in allows you to search other people's keys using the Finder Find command. To use it, move this file to the Internet Search Sites folder inside your System Folder.
- The Contextual Menu folder, containing the SafeMail Contextual Menu plug-in called SafeMail CM. To use this plug-in, move it to the Contextual Menu Items folder inside your System Folder and restart the computer. You may then sign or secure a file by clicking on its icon while holding down the Control key.

2. The **SafeMail Menu** file is created in the Control Panels folder. The control panel allows Finder and applications' integration of SafeMail features. It will allow you to easily encrypt and/or sign documents in any application and offers several shortcuts to access all main features of SafeMail.
3. The folder "**OpenLib Folder**" is created inside the Extensions folder in the System Folder. It contains several files or libraries required for all components of SafeMail to operate.

Note: *All SafeMail components can be used independently. You can use the Keyring Manager even if the Control Panel is not installed and vice versa. However, they all require the OpenLib folder to be present on the disk to operate. The OpenLib folder contains code that is shared by all SafeMail components (and possibly also by other software installed on the computer).*

SafeMail Pro

Users who need more features can upgrade to SafeMail Pro. Check our web site for upgrade information and pricing.
SafeMail Pro contains all SafeMail features, plus some interesting extras.

For example, SafeMail Pro can open multiple keyrings at the same time, allowing simultaneous management of different keyrings and amongst others, drag & drop of keys from one keyring to another. Also, you can set up a list of as many keyservers as you like, which will all be checked when looking for another person's key. You can personalize the comments which appear in the messages you send: Define a separate message for when you export keys, when you encrypt and when you sign a message. SafeMail Pro also contains an advanced method for key creation, including a fast way to create multiple key pairs.

Files can be encrypted and signed in the Finder simply by adding a suffix to the filename. Decryption and signature verification happens automatically when removing the suffix. Finally, SafeMail Pro allows the creation of Cryptlets. A Cryptlet is a small application you create that contains one or more public keys. Any file or folder dropped onto this Cryptlet will be encrypted with the keys embedded in the Cryptlet. No dialog appears, it is just a drag & drop action.

Chapter 3 - Creating a Key Pair

This chapter describes:

- How to create a private and a public key or a key pair.
- How to protect your private key
- What is a key fingerprint and a key ID

Key concepts

You generate a key pair consisting of a private key and a public key. Only you have access to your private key but in order to communicate with other users you need a copy of their public key and they need a copy of yours.

You use your private key to sign messages or files and to decrypt messages and files you receive.

Conversely, you use the public keys of others to send them encrypted messages and to verify their digital signatures.

Keys are always stored in keyrings.
A keyring is thus a group of keys: they can be private or public and can be of different types such as, for example, RSA keys or DSS keys.

Creating a key pair

The first thing you must do is create your private key. We call this operation also “creating a key pair” because each time a Private key is created, its related public key is also created. A key pair consists of a private key that only you possess - as its name implies - and a public key that you freely distribute to people with whom you correspond.

Usually, you will create a new key only once. You may have to create a new key in the future if you loose your key or if its security has been jeopardized.

Note: *If you have already generated your keys with a previous version of SafeMail or with another software, your have probably already distributed your public key and there is no need for you to create a new key pair. Open the*

***Settings** dialog to indicate SafeMail the location of your existing keyrings.*

To create a new key pair, you must first open or create a new keyring.

Launch the SafeMail Keyring Manager application. The keyring window will appears. If not, select **Open Keyring** from the File menu.
If you have just installed the software, the keyring is named **Default Keyring.pub** and is located in the Keyrings folder. You will notice that the keyring already contains some public keys.

***Note:** if SafeMail cannot find a keyring (for example if you moved the Keyring folder at a different location) a dialog will appear allowing you to locate the keyring or to create a new one.*

Choose **New Key Pair…** from the Keyring menu.

There are several steps involved to create a new key.
Read the text which appears on the screen and click the **Next** button.

1. Key Name or Identifier

The first step is to define a name for your key. The name is an identifier and is usually your real name but it can also be a company name or some other type of information identifying you.

Enter an e-mail address (e.g. john.smith@internet.com). The e-mail address is optional but we suggest you enter: It will allow better integration with e-mail software and other Internet applications.

In order to better identify you, SafeMail allows you to create more identifiers for your key, for example, a second e-mail address, another nickname etc. We will come back on this later in the manual (page 49).

2. Choose theType of Key

You may choose different types of keys depending on your needs. All OpenPGP compatible software use the RSA algorithm except for the PGP freeware which only uses the Diffie-Hellman/DSS algorithms.If you communicate with many users and you do not know if their security software understands both algorithms, you may have to create two key pairs, one with each algorithm type.

If you really don’t know, we suggest you choose the DSS key type.
Key Size: Larger keys are more secure but slower to perform the decryption and encryption process. For most uses, 1024 bits will do. If you plan to use RSA and you want to be compatible with older versions of the PGP software, you should not choose a key size larger than 2048 bits.
The time required to generate a new key depends on the speed of your computer but generally should not take more than a few minutes for standard key sizes, that is less than 2048.

3. Key Expiration

A key can expire after a defined number of days. Once the limit is reached:

- The public key can no longer be used by someone to encrypt mail for you but it can still be used to verify a document that has been signed by you.
- The private key can still be used to decrypt mail that was sent to you before your public key expired but it can no longer be used to sign new mail.

It is generally recommended that you generate a key which does ***not expire*** because once you have distributed your public key worldwide, you will probably want to continue using the same key.

Note that the key expiration cannot be changed later.

4. Add an URL and some Information

These fields are optional. They will appear when a user chooses Get Info on your key. If you enter the URL (Internet address) of a web page (for example, a document that refers to you or that describes the owner or the policy under which the key was issued), the user will be able to click on this URL and a browser will automatically launch a connection to the specified web page.

You can add the same kind of information for each Certificate you will make in the future on your key, on another person’s key or on a key's identifier.

Note: *The information is embedded into the key certificate at certification time and cannot be changed afterwards. You can modify the information under one condition only: If you did not yet send your key to a key server or to another*

user. In this case, you can replace the certificate by another one: Open the SafeMail Keyring Manager application and select your key's certificate. Delete it by pressing the Delete key (or choose Delete in the Edit menu).
Choose ***Certify****, type the new information anc click* ***Certify*** *to create the new certificate.*

Click the Next button to continue.

5. Choose a Passphrase

The passphrase or password protects your private key. We strongly recommend your passphrase to be at least 8 characters long and also to include non-alphabetic characters.

Note: *The word passphrase incites you not to use a single short word. In practice, many people do not want to type a complete phrase each time they sign or decrypt a message but this is at the risk of compromising your security. A strong passphrase includes upper and lowercase letters, numbers, punctuation, and spaces. The longer your passphrase is, the more secure it is.*

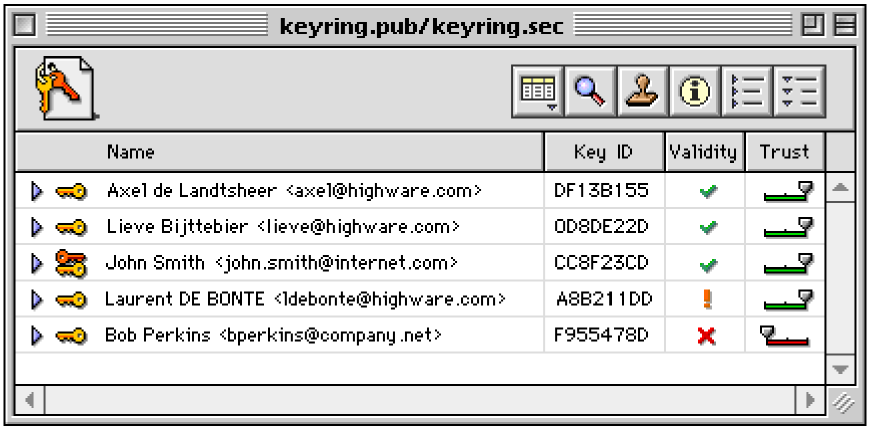
It is very important that you remember this passphrase! It will be required each time you use your private key, i.e. to sign a document or to decrypt a message. You may change your passphrase at any time in the future.

⚠ There is NO POSSIBILITY to recover a “lost” password or passphrase!

Enter your passphrase twice for confirmation then click the **Create Keys** button.

6. Key Generation

The key generation process begins and it may take a few seconds to a few minutes to generate the new key pair. Once generated, your new key will appear in the keyring window.

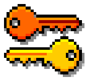


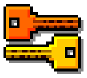
keyring.pub/keyring.sec

Name	Key ID	Validity	Trust
Axel de Landtsheer <axel@highware.com>	DF13B155	✓	
Lieve Bijttebier <lieve@highware.com>	0D8DE22D	✓	
John Smith <john.smith@internet.com>	CC8F23CD	✓	
Laurent DE BONTE <ldebonte@highware.com>	A8B211DD	!	
Bob Perkins <bperkins@company.net>	F955478D	✗	

Your new Key Pair →

In a keyring, a private key is always shown as a key pair because there is always a public key associated with a private key. The other public keys are shown as single keys since you do not possess their private keys.

Icon of an RSA type key pair: or 

Icon of a DSS type key pair: or 

The red key represents the private key. The yellow key is the public key.

Protecting your private key

The private key will remain on your computer and should be kept confidential. SafeMail will use your private key whenever you want to sign a message or decrypt a document. The passphrase will be required each time your private key is solicited. **Keep this passphrase confidential**.

You should also take the following precautions:

1. Be careful where you store your private key (stored in the private keyring). A password or passphrase "only known by yourself" is required to use your private key but it is always possible that someone discovers the password: Somebody could look over your shoulder when you type in your password or could use keystroke recording software to try and recover your password... If someone is able to retrace your passphrase and to obtain a copy of your private key, he can then forge your digital signature and read your confidential mail.
   As a rule, keep your key on your own computer only and make sure you don't back it up on a central server where other people may have access to it. You can also change the name of your private keyring to a name less obvious than "My private key". Private keyrings can be anywhere you want on your hard disk or on another media or even on a floppy disk.

   Note: *To keep a keyring on a floppy disk: Copy the keyring on the floppy disk then make an alias of it. Place this alias on your hard disk (for example in the folder Keyrings) and select this alias in SafeMail Settings as your default keyring. The floppy containing your keyring will be automatically requested each time you want to sign or decrypt a message.*

2. **Make a backup copy of your key pair and store it in a safe place**.
   You can always recreate your public keyring by importing keys from a key server or by requesting a new copy of a person's key. However, if you loose your original private key, for example after a disk failure, you will not be able to decrypt files that have been encrypted by others with your public key. Private keys and public keys are saved in two separate keyring files (name.sec and name.pub) even if they appear in the same window. Copy the two files on another disk or on any other media.

If your key gets compromised, for example if it is lost or stolen, see "Key Revocation" on page 50.

Your Key Name, Fingerprint and Key ID

Every key is identified by a Name, a Key ID and its “Fingerprint”.

The **Name** of the key is usually the name of the owner of the key together with his/her e-mail address.

The **Key ID** of a key is an identification number that allows you to distinguish the key from another key which has, for example, the same name. Here is an example of a Key ID: 58AD0F35.

The **Fingerprint** of a key is a unique number computed using a hash algorithm, e.g. 9E94 4513 3983 5F70 7BE7 D8ED C4BE 5AA6.

Several keys named “John Smith” may exist but their fingerprints will differ. The Fingerprint helps you to verify the authenticity of a key.

Unless you really trust the people who applied the certificates on a public key, the best way to verify the authenticity of a key is to ***compare its fingerprint*** (not the Key ID): Call the purported owner of the key you want to verify. Ask him to read you the fingerprint of his private key. It has to correspond with the fingerprint of his public key. Once you are certain of its authenticity, you may decide to certify his public key.

Your Key’s Certificate

Once you have created your key, you will notice that your key already has a certificate. When you create a new private key, its public key is automatically created and a certificate is applied to it because SafeMail knows for sure to whom this new public key belongs.

CHAPTER 4 - EXCHANGING PUBLIC KEYS

This chapter describes:

- How to distribute your public key
- How to obtain other people's keys

DISTRIBUTING YOUR PUBLIC KEY

You should give your public key to everyone you know. They will use it to send you encrypted data and to verify your signature.

There are different ways to distribute your public key:
- Make your key available on a public key server
- Include it in an e-mail
- Make your key available on your web site
- Export your key and send it as a file

SENDING YOUR KEY TO A PUBLIC KEY SERVER

This is the best method. By posting your Key on a public key server, your key will be accessible to everyone on the Internet. There are a number of key servers worldwide and they are all periodically synchronized. The service is free. The advantage of using this method is that:

- People will be able to send you secured mail without having to request a copy of your public key first.
- You don't have to keep a large number of public keys of people with whom you rarely correspond.

To send your key to a public key server:

1. Connect to the Internet.
2. Open your keyring and **select** your public key. Although its icon represents a key pair, **only** your public key will be sent.
3. Choose **Send** from the **Server** menu. SafeMail will automatically establish a connection to a public key server and send a copy of the key.

If you modify your key, for example by adding another identifier, a new e-mail address or if you get new certificates, repeat the above procedure to update the information regarding your public key on the public key server. The key server will merge the modifications with the previous copy information on your key.

Note: *We suggest you wait until you are familiar with SafeMail and the concept of public key Encryption before sending a key to a key server. This is just in case you change your mind and would like to modify the type of key or its name. Once your key is on a public key server, it cannot be removed. Each time you submit a key to a key server, the server will perform a merge of the new data concerning your key with the existing data on your key, if any. You can add information to your key such as an additional identifier or certificates but you should keep in mind that the old data will not be removed. These restrictions may change in the future as key servers evolve.*

SafeMail establishes a transparent connection to a public key server. You can also connect to the key server with a web browser such as Netscape or Internet Explorer by entering the address: http://www.key server.net. This site contains links to many other key servers available on the Internet.

INCLUDING YOUR PUBLIC KEY IN AN E-MAIL

A public key can easily be transformed into a block of text, so it is very easy to include it in an electronic message.

Open your keyring, select the key then choose Copy from the Edit menu. The key has been copied into the Clipboard. Go to your e-mail software and place the cursor where you want the key to be pasted. Choose Paste from the Edit menu. Do not forget to sign the message so the key can be easily verified by your recipient.

Note: *You may also option-click on a public key icon in your keyring to open a popup menu and select Copy key.*

MAKE YOUR KEY AVAILABLE ON YOUR WEB SITE

Follow the same method as described for e-mail but paste your key on a web page and establish a link to your key on your home page. You may also add the URL to your e-mail signature.

OBTAINING PUBLIC KEYS FROM OTHER PEOPLE

You need to obtain public keys from other people if you want to send them encrypted messages or to verify their signatures.

There are different ways to obtain public keys:
- Search on a public key server.
- Receive the key with an e-mail or text file, from a web site, etc.
- Import a file.

OBTAINING A KEY FROM A PUBLIC KEY SERVER

You can either let SafeMail access the Public Server for you or you can use a browser. We suggest you let SafeMail do the work for you.

1. Connect to the Internet.
2. Select **Find Keys**... from the Edit menu of the Keyring Manager application. A dialog will appear. Choose the key server on which you would like to perform your search by clicking the popup button on the upper right side of the window.

   Note: *If you have just installed the software, a key server is already selected by default. If none is present, see "Settings" on page 57.*
3. Type the name of the person's key you are looking for or his e-mail address and click the **Find** button. SafeMail will establish a connection to the key server and the result of your query will be displayed in a new window after a few seconds.
4. Select the key(s) you are looking for and choose Import to add the key to your keyring.
   If you do not find someone's public key it may be because this person did not post his key on the key server yet. Contact him and ask him to send you his key.

Note: *To connect to a key server with a browser, open a new window in your browser and enter the key server address. There are many key servers on the Internet. Try http://www.publickeyserver.net or http://pgp.ai.mit.edu.*

Getting the Key from an e-mail or a text file

Since a public key can easily be transformed into a block of text, it is very simple to copy it from an electronic mail or a text file.

SafeMail allows you to import keys directly by selecting the text corresponding to the keys in a message. This feature is very handy to import a key sent via an e-mail message or to import a key from a key server. You can recognize keys included in a message by the following header and footer:-

```
----BEGIN PGP PUBLIC KEY BLOCK----------
```

and

```
-----END PGP PUBLIC KEY BLOCK-----
```

To import a key, simply place your cursor somewhere in the text that contains the key and choose **Decrypt/Verify** from the SafeMail menu. SafeMail will find the key and will ask you if you want to import the key in your default keyring. Click **Yes** and the key will be automatically added to your Keyring.

Note: *If the message or the text file contains several encrypted parts, you may want to select only the part of the text which contains the key. Select from the beginning of the header to the end of the footer (see above) and choose Decrypt/ Verify in the SafeMail menu. In this case, SafeMail will only decrypt your selection.*

Import from a File

If the file is:

A text file: Select the file and choose Decrypt/Verify in the SafeMail menu. You may also drop the file onto the Decrypt/Verify button of the Keyring Manager toolbar.

A keyring file: Open the Keyring Manager, select **Import...** in the File menu.

When adding a public key to your keyring, you have to check that the key really belongs to the purported owner. Verify its authenticity, assign the trust you have in the owner of the key. You may also want to certify it. See the chapter “Keys & Keyrings Management” for more information on certificates and how to verify a key’s authenticity.

If you attempt to use a public key that is not valid, SafeMail will issue a warning.

⚠ Never grant a certificate to a public key if you did not verify its authenticity first.

CHAPTER 5 - EXCHANGING SECURE MAIL & FILES

This chapter describes:

- How to send and receive secure e-mail.
- How to secure parts of a text file.
- How to secure files on your computer.

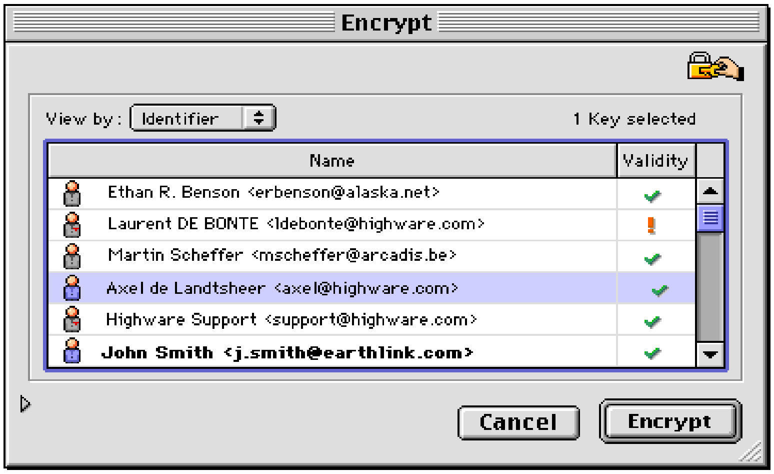
SECURING E-MAIL OR TEXT

There are several ways to secure e-mails. You may encrypt the text of the e-mail itself or you may send an e-mail with an attached file that is encrypted. All encrypted files are automatically Zip-compressed which implies that the file transfer takes less time.

ENCRYPTING E-MAIL OR TEXT

Compose your e-mail as usual.

1. Choose Encrypt... from the SafeMail menu. A dialog will appear listing all public keys contained in your default keyring.
Note that private keys are used to sign and decrypt messages only. They do not appear in this list.



View by: Identifier

1 Key selected

Name	Validity
Ethan R. Benson <erbenson@alaska.net>	✓
Laurent DE BONTE <ldebonte@highware.com>	!
Martin Scheffer <mscheffer@arcadis.be>	✓
Axel de Landtsheer <axel@highware.com>	✓
Highware Support <support@highware.com>	✓
John Smith <j.smith@earthlink.com>	✓

The validity icons indicate the level of confidence SafeMail has deducted from information based on the key certificates and on the level of trust you have assigned to those people that have certified the keys. See “The Validity of a Key” on page 48 for details.

Note: *Option-click on a list item will open a popup window with information about that item.*

2. Select one or more public keys and click Encrypt.
If you want to send the message to several people, you will also have to select their respective public keys. Use the Shift key to select adjacent keys or the Command key to select non-adjacent keys.

Shortcut: If you want to encrypt the message for one recipient, choose Encrypt... in the SafeMail menu, type the first letters of the recipient's name and press Return.

Once the encryption is finished, the message will be replaced by the encrypted text, preceded by the header:

```
----BEGIN PGP MESSAGE----------
```

and followed by the footer:

```
-----END PGP MESSAGE-----
```

Note: *If you checked the “Encrypt to self” option in the SafeMail settings - this option is selected by default when you first install the software - your public key will be automatically added to the selected keys. This means you will always be able to decrypt the messages you send. If “Encrypt to self” is checked and you did not select the default public key, an alert will warn you that you will not be able to decrypt the message once you've encrypted it. Click* ***OK*** *if you agree or* ***Cancel*** *if you want to add your public key.*

To encrypt only a part of the message, select the part you want to encrypt. To encrypt the entire message, either select the entire message or make sure the cursor is located in the message body and that no part of the message is selected.

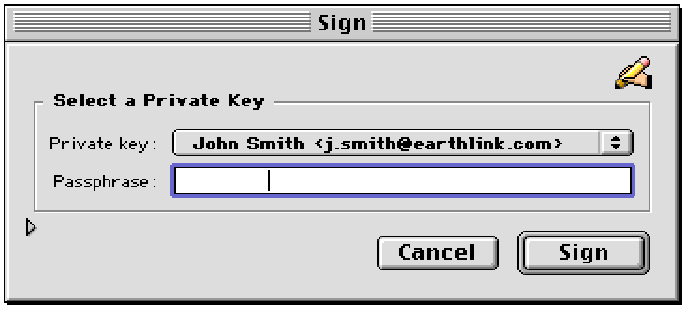
☞ TIP: It can be very useful to encrypt and/or sign only a selected portion of a message. For example, you may want to send a message to more than one person in which some paragraphs are not destined to all recipients. Select and encrypt the paragraphs with the respective keys and sign the entire text. All recipients will be able to verify your signature but the encrypted paragraphs will be available only to the recipients to whom they were destined.

When clicking the left triangle, more options become available. They are described on page 39.

Signing e-mail or Text

Compose your e-mail as usual then:

1. Choose Sign... from the SafeMail menu. A dialog will appear with a popup listing all private keys contained in your default keyring.
   In most cases, only one private key - yours - is listed. If there is more than one, the default private key will be selected.



Private key : John Smith <j.smith@earthlink.com>

Passphrase :

2. Enter your passphrase and click Sign.

Once the signing process is finished, the message will be preceded by the header:

```
-----BEGIN PGP SIGNED MESSAGE-----
```

The text that has been signed is placed here.
At the end of the signed text is the signature itself:

```
-----BEGIN PGP SIGNATURE-----

signature

-----END PGP SIGNATURE-----
```

Note: *When choosing Sign... in the SafeMail menu, SafeMail will locate the insertion point and select the text. In an e-mail, be sure to place the cursor in the message part before choosing* ***Sign...*** *from the menu. If you have selected part of the text, only that selection will be signed by SafeMail.*

When clicking the left triangle, more options become available. They are described on page 39.

Encrypting and Signing Simultaneously

If you want to encrypt as well as sign a text at the same time, choose Encrypt & Sign... from the SafeMail menu.

Decrypting or Verifying a Signature in an E-mail or a Text

An e-mail or a paragraph that has been secured always begins with one of the following headers:

```
-----BEGIN PGP SIGNED MESSAGE-----
```

if the text is signed, or

```
-----BEGIN PGP MESSAGE-----
```

if the text is encrypted

A secure text always ends with one of the following footers:

```
-----END PGP MESSAGE-----
```

or

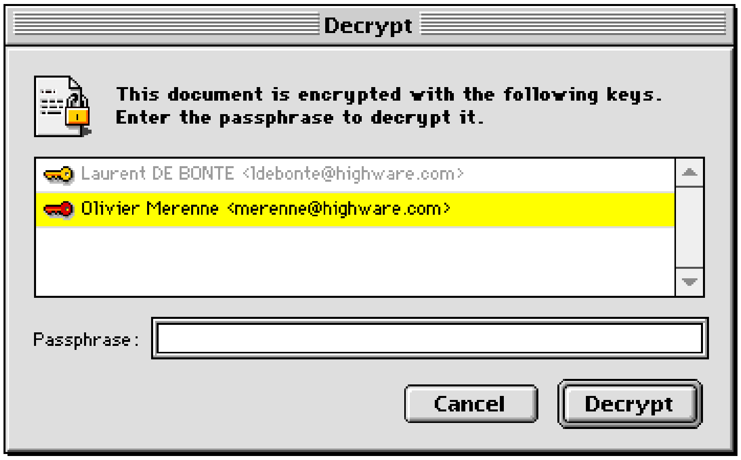
```
-----END PGP SIGNATURE-----
```

Place the cursor somewhere in the text and select Decrypt/Verify... in the SafeMail menu. SafeMail will search all secured parts, i.e. all headers followed by their corresponding footers.

If there are several secured parts in the same document, SafeMail can process them all at once. If you prefer to decrypt or verify only one part, select the part and choose Decrypt/Verify in the SafeMail menu. SafeMail will only process the selection.

A secured text can have different parts encrypted for different users and the whole encrypted message can be signed.

- If the text is encrypted, SafeMail will request the passphrase of your private key to decrypt it.



This document is encrypted with the following keys.
Enter the passphrase to decrypt it.

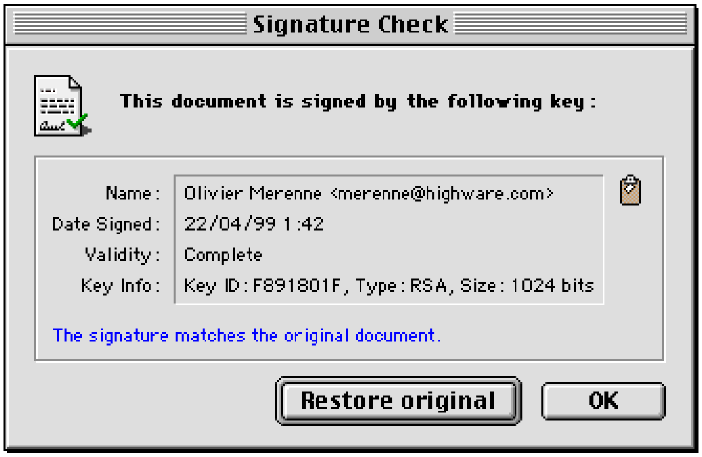
Laurent DE BONTE <ldebonte@highware.com>

Olivier Merenne <merenne@highware.com>

Passphrase:

Note: *If the text was also encrypted using other keys, they are also listed in the above dialog but they are grayed out since you do not have the related private keys. They will inform you to whom the secure text was addressed since you can view all recipients who are able to decrypt it.*

- If the text is signed, SafeMail will check the document and verify the signature. The result will appear in the following window:



This document is signed by the following key :

Name : Olivier Merenne <merenne@highware.com>
Date Signed : 22/04/99 1 :42
Validity : Complete
Key Info : Key ID : F891801F, Type : RSA, Size : 1024 bits

The signature matches the original document.

- If you click the OK button, it means that you have read the results and no further action is required. The text will remain signed for future checking.

- If you click the **Restore original** button, SafeMail will restore the original message before it was signed. This can be useful if you want to obtain a hard copy of the SafeMail report or to read the message if the text was scrambled and thus not readable (when signing a text, you have the option to “scramble” it (see page 39). It is not as secure as encryption but enough to be illegible).

Here is an example of a signed text that has been verified and restored:

```
1.   ***  Begin Signed Section  ***
2.   ~~~  Good signature.  3. The Signer’s Key is valid
4.   ~~~  Signed by: John Smith <jsmith@earthlink.com>,  Key ID: F764806F.
5.   ~~~  Signed on 17/5/98 at 19:13.  6.  Verified on 17/5/98 at 19:14
7.   Dear Mr. Perkins,

     Further to your call, I am pleased to confirm you that the contract was
     signed yesterday at 11am. A 3% commission will be transferred into your
     bankaccount as agreed.

     Sincerely,

     John Smith

8.   ***  End Signed Section  ***
```

1. Header: Indicates beginning of the signed text.
2. Indicates if the signature is valid for the document, that is, the document has not been altered during its transfer.
3. Indicates whether the signer’s key is valid or not.
4. Indicates the signer’s name and its key ID.
5. Indicates date of signature.
6. Indicates date and hour of verification.
7. Original text in clear.
8. Footer: Indicates end of signed text.

SECURING E-MAIL WITH THE EUDORA PLUG-IN

The SafeMail for Eudora plug-in allows you to better integrate the SafeMail features with the Eudora™ software from Qualcomm.

Please see “Chapter 9 - SafeMail for Eudora” on page 70 for more information on how to use this software.

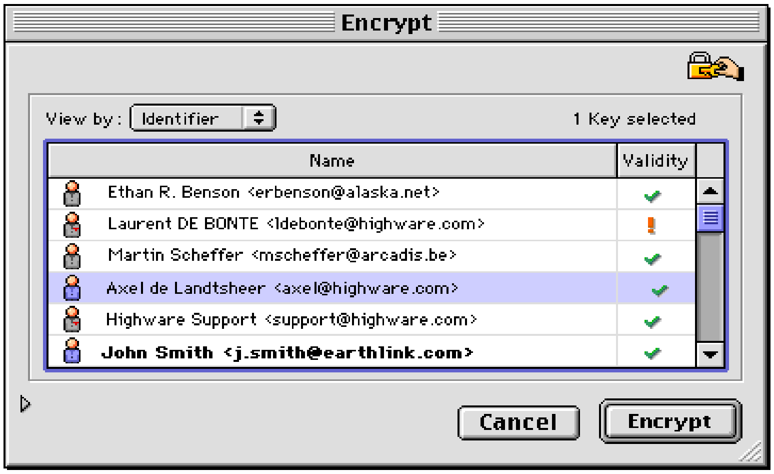
Securing Files on your Computer

Files can be secured either to send them attached with an e-mail or to hide their contents should other people access your computer. All encrypted files are automatically Zip-compressed meaning that once secured, they will take less space on your computer.

Encrypting Files

Select one or several files or a folder and choose Encrypt... in the SafeMail menu. A dialog appears with a list of all public keys contained in your default keyring. Private keys are used to sign and decrypt messages only and will not appear in the list.

Note: *When selecting a folder instead of a file, SafeMail will encrypt all individual files located in the folder and well as in its sub-folders. The folder hierarchy will remain as is.*



View by : Identifier

1 Key selected

Name	Validity
Ethan R. Benson <erbenson@alaska.net>	✓
Laurent DE BONTE <ldebonte@highware.com>	!
Martin Scheffer <mscheffer@arcadis.be>	✓
Axel de Landtsheer <axel@highware.com>	✓
Highware Support <support@highware.com>	✓
John Smith <j.smith@earthlink.com>	✓

Select one or more public keys and click the Encrypt button.
If you secure a file which will be used on your computer, you will probably only select your own public key. If the files are intended to be used by other people, select the relevant public keys of the recipients. Use the Shift key to select adjacent keys in the list or the Command key to select non-adjacent keys.

Shortcut: To encrypt the message for one recipient, choose Encrypt... and type the first letters of the recipient's name, then press the Return key.

Note: *Option-click on a list item will open a popup window.*

When the encryption process is finished, the icons of the files which have been encrypted will be replaced with the following icon:

Once encrypted, the original document is wiped and cannot be restored, not even by using a recovery utility such as Norton Utilities. If you prefer to keep the original documents, uncheck the “Delete and wipe original” option in the SafeMail settings.

Note: *The option “Encrypt to self” in the SafeMail settings is set by default when first installing the software. This implies that your public key will be automatically added to the selected keys. Consequently, you will always be able to decrypt the files you encrypted. If you unchecked “Encrypt to self”* ***and*** *you do not select your public key when encrypting a file, an alert will warn you that you will not be able to decrypt the message once you've encrypted it. Click the* ***OK*** *button if that is what you want, or the* ***Cancel*** *button if you want to add your public key.*

The validity icons next to the Key Name indicate the level of confidence SafeMail has deducted based on the information from the key certificates and the level of trust you assigned to the people who certified the keys. See “The Validity of a Key” on page 48 for details.

When clicking the triangle on the left, more options become available. They are described on page 39.

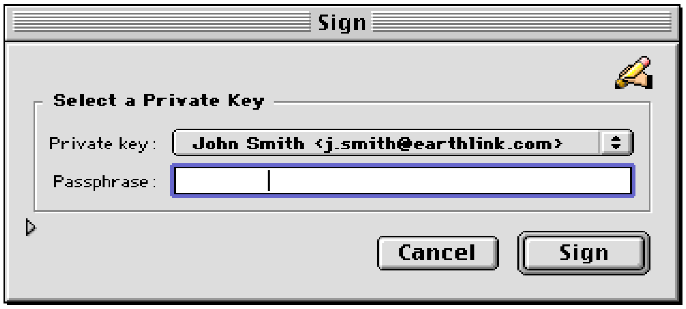
SIGNING FILES

There are two ways of signing files in the Finder. You have the signature of the embedded file in the file itself or you create a separate signature. A separate signature does not modify the original file.

Signature enclosed in the file

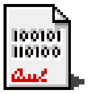
1. Select one or several files or a folder and choose Sign… from the SafeMail menu. When selecting a folder instead of a file, SafeMail will sign all individual files located in that folder as well as in its sub-folders. The folder hierarchy will remain as is.

A dialog appears with a popup listing all private keys contained in your default keyring.
In most cases, only one private key - yours - is listed. If there is more than one, the default private key is selected.



Private key : John Smith <j.smith@earthlink.com>

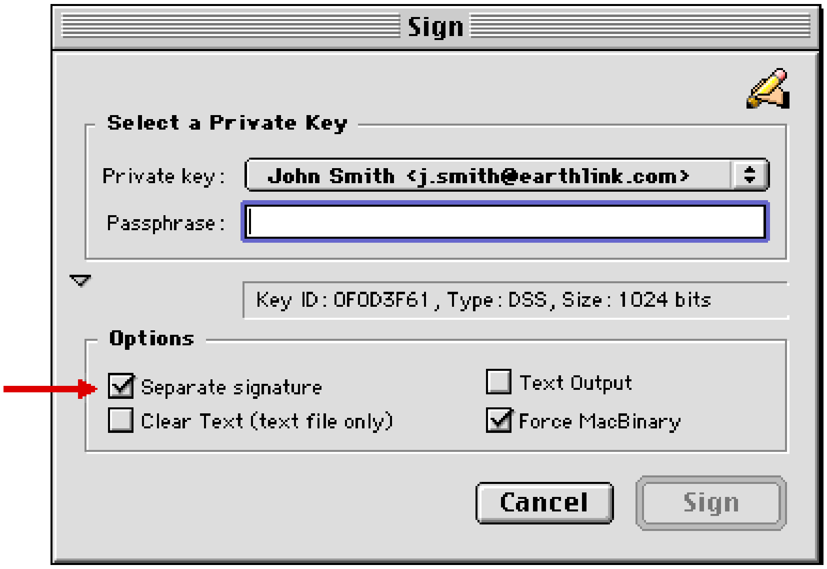
2. Enter your passphrase and click Sign.
Once the signing process is finished, the icons of the files that have been signed are replaced with the following icon:



Separate Signature

1. Select a file or a folder and choose **Sign…** from the SafeMail menu. A dialog will appear with a popup listing all private keys contained in your default keyring. Click the small triangle located on the left.

In the new extended window, check the option Separate signature.



Select a Private Key

Private key: John Smith <j.smith@earthlink.com>

Passphrase:

Key ID: 0F0D3F61, Type: DSS, Size: 1024 bits

Options

☑ Separate signature □ Text Output

□ Clear Text (text file only) ☑ Force MacBinary

2. Enter your passphrase and click Sign.
   Once the signing process is finished, a new file will have been created next to the original file. It will have the following icon:

The file contains the signature of the original document which remains untouched. You can use this signature file to check the integrity of the document whenever you want.

Note: *If you've selected a folder instead of a file, SafeMail will create a signature file next to each original file contained in that folder and in its sub-folders. This feature allows you to authenticate the contents of an entire disk or a main directory in one step.*

The other options available when clicking the left triangle are described on page 39.

ENCRYPTING AND SIGNING SIMULTANEOUSLY

If you want to encrypt **and** sign a message or a text at the same time, choose Encrypt & Sign... from the SafeMail menu.

A file that has been encrypted and signed has the following icon:

ENCRYPTION AND SIGNATURE OPTIONS

The following options appear when you extend the encryption or signature windows by clicking the small triangle at the left side.

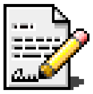
Keep text in clear: This option is available in the extended signature window and works only on text, not on files, except if the file is a TEXT file. This option is checked by default.
- When checked, the resultant signed text will appear in clear on screen followed by its signature. This can be handy so that someone without SafeMail or a PGP compatible software will still be able to read the text.
- If you uncheck this option, the resultant signed text will be illegible on screen - it will be “scrambled” - and followed by its signature. Note that the “scrambled” text has not been encrypted. It is just a convenient way to make the text illegible until someone has verified its signature.

Macintosh format (MacBinary): This option allows you to change the default setting. See page 59 for further information on MacBinary.

Text Output: By selecting this option, the content of the encrypted file will be converted into a text message such as when you choose **Encrypt...** in the SafeMail menu while in a word processor or an e-mail program.
The content of the encrypted file will begin with the header BEGIN PGP MESSAGE and will end with the footer END PGP MESSAGE. You can then open the encrypted file in any text editing application, select its content and paste it, for example, in your e-mail program. This feature is not very often used since most modern e-mail programs support sending files as attachments. It could be useful, however, for certain advanced users in a particular situation.

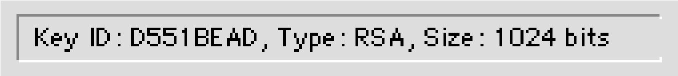
If you select this option, the secured file icon is almost the same as that of a regular encrypted file except for one detail: The "OIOIO" (representing binary data) that you see in the center of the icon is replaced with lines suggesting that there is a text inside:

or



Note that if you did not select the MacBinary nor the Text Output option, you may loose information such as type and creator of the document.

In addition, the following information appears when you extend the signature windows by clicking the small triangle at the left.



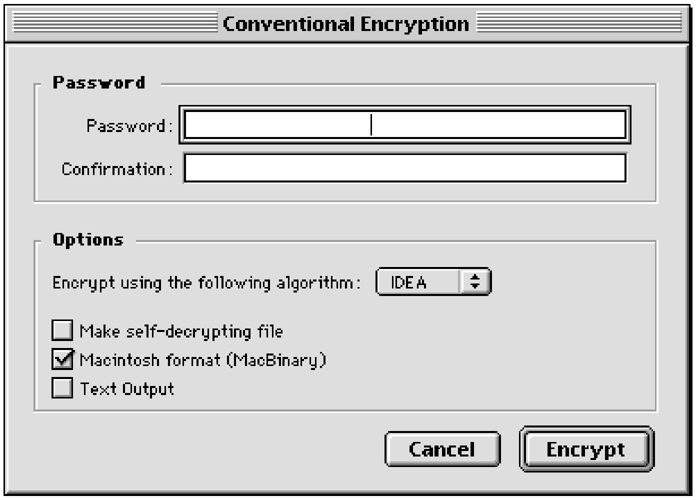
Key ID : D551BEAD, Type : RSA, Size : 1024 bits

This string gives you more technical information about the type of key you have selected. Itcan be helpfull if you have two private keys (for example, one DSS key andone RSA key) with the same name.

CONVENTIONAL ENCRYPTION

Conventional encryption - also known as Single Key Cryptography - is based on a single key (a password or a passphrase) rather than on a public key (Public Key Cryptography). The file is encrypted using a password which has to be transmitted to the users who have to decrypt the file.

Select one or more files or a folder and choose Conventional Encryption in the SafeMail menu or in the SafeMail application.



Conventional Encryption

Password

Password:

Confirmation:

Options

Encrypt using the following algorithm: IDEA

□ Make self-decrypting file

☑ Macintosh format (MacBinary)

□ Text Output

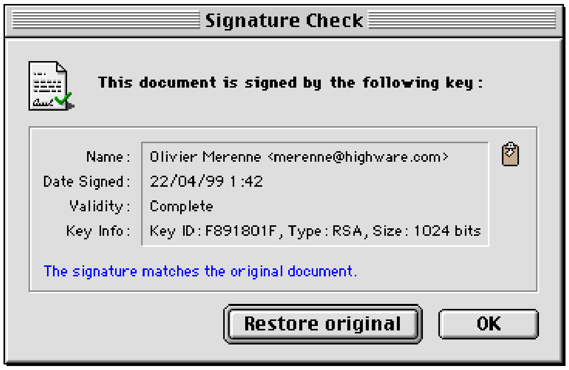
Encrypt using the following algorithm: Select the encryption algorithm of your choice in the popup menu. They are all considered to be equally secure at the time of the publication of this manual. Check also the Read me file which comes with the SafeMail application to see whether there is new relevant information on this topic.

Make self-decrypting file: Check this option to make the file a self-decrypting file. This is useful to transmit encrypted files to people who do not have SafeMail.
During the encryption process, the file will be transformed into a small application. When double-clicking the file, its password will be requested and the file will be automatically decrypted.

Decrypting Files or Verifying Signatures

To decrypt or verify the signature of a file, select the file and choose Decrypt/Verify... from the SafeMail menu. Alternatively, you can also double-click the file and the SafeMail application will be launched. When selecting a folder instead of a file, SafeMail will try to decrypt/verify all individual files contained in that folder and in its sub-folders.

- If the file was encrypted, a dialog will appear and SafeMail will request the passphrase of your private key to decrypt it. If the file was encrypted with a password only, you will have to enter the same password.
- If the file was signed, SafeMail will check the document and verify its signature. The result of the verification will appear in a window:



This document is signed by the following key :

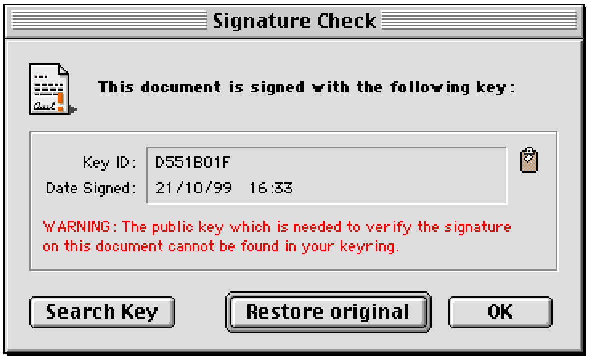
Name : Olivier Merenne <merenne@highware.com>
Date Signed : 22/04/99 1:42
Validity : Complete
Key Info : Key ID : F891801F, Type : RSA, Size : 1024 bits

The signature matches the original document.

SafeMail Report

- Click the OK button to inform SafeMail that you have read the results and no further action is required. The text will remain signed for future checking. If the document is important, we suggest you keep a signed copy of the document.
- Click the Restore original button to inform SafeMail that it has to restore the original message as it was before it was signed. This can be useful to get a hard copy of the SafeMail report or to read the message if the text was scrambled (when signing a text, you have the option to “scramble” the text (see page 39). It is not as secure as encryption but is sufficient to make the text illegible).

If you do not have the related public key to verify the signature, the following window will appear with a new **Search Key** button.



This document is signed with the following key:

Key ID: D551B01F
Date Signed: 21/10/99 16:33

WARNING: The public key which is needed to verify the signature on this document cannot be found in your keyring.

Clicking on **Search Key** will open a connection to your default key server to request the missing key. If the key if found, the key will be imported in your keyring then SafeMail will immediately perform a new verification. Everything is done automatically but your computer must be connected to the Internet (or a local network able to reach the key server).

- If the file is a separate signature file, SafeMail will ask you to locate the original file and verify it.

After the verification is done, click the OK button to inform SafeMail that you have read the results. As long as you keep the separate signed file, you will be able to check the document's integrity.

- If the file is encrypted and signed, SafeMail will decrypt the file and verify its signature in the same sequence.

CHAPTER 6 - KEYS & KEYRING MANAGEMENT

This chapter describes:

- How to authenticate a key
- How to certify a public key
- How to revoke a key
- How to update a key from a key server
- How to use your keyring
- How to generate a key pair with more settings

MANAGING KEYS

A key is a digital identification of a person.

There are several ways to verify the authenticity of a key. When using public key encryption software, verifying the authenticity of a key is the most important part. SafeMail will, of course, assist you in this task but it is important to note that the reliability of the system will depend on your own judgement to decide whether or not a key is authentic.

Intercepting mail over the Internet is pretty easy. In addition, most e-mail messages transit in clear from one computer to another and those computers are rarely located in inaccessible bunkers… Keep also in mind that the e-mail address of a sender - usually shown in a message header next to the word "From:" - can easely be forged and is not a trusted information.

Here is an example of a risk often quoted in security books (the "intruder-in-the-middle" attack) and that you may encounter if you do not verify the authenticity of a key: You send a message to Paul by using his public key. You did not check this public key and in reality you use a key which is named Paul but which was in fact created by John. John intercepts your e-mail, decrypts it and reads its content. He then re-encrypts your message but this time he uses Paul’s genuine public key. He sends the message to Paul as if nothing has happened. Paul receives the e-mail and cannot possibly know that someone read his encrypted message with his public key… John could even have a computer do this task for him.

The above example shows the danger is real and we cannot enough stress the importance of verifying the authenticity of a key before using it.

Legitimate Copies of a Public key

There are several ways to check the authenticity of a key, that is, verify if the key really belongs to its purported owner.

Unless you physically received a key, for example, by means of a floppy disk, or unless you really trust the person who applied his/her Certificate on a public key, the best way to verify the authenticity of a key is to ***compare its fingerprint***. Call the purported owner of the key you want to verify. Ask him to read the fingerprint of his private key: It has to match that of his public key.
After this verification, you may decide to certify his public key yourself.

Note: *Sending a key fingerprint via e-mail is not the best way to verify the key because e-mail can be intercepted and modified. To compare a fingerprint, always use a different channel than the one that was used to send the key itself. Some people have their key fingerprints printed on their business cards. However, we think a voice telephone conversation is one of the most secure solutions.*

Certificates

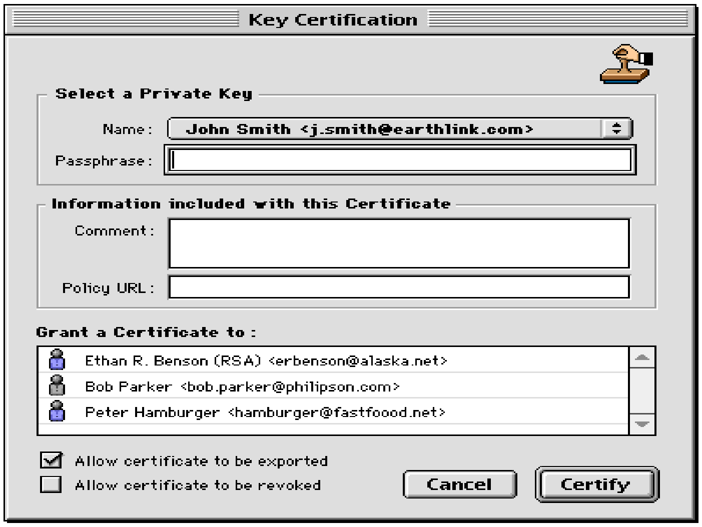
Once you are absolutely sure that you have a legitimate copy of a user's public key, you can choose to certify the key.

Note: When you create a new key pair yourself, the key is automatically certified because SafeMail knows for sure to whom this new key belongs. It also prevents anyone else from modifying your key.

Applying your certificate on someone's public key means that you confirm you are convinced the key belongs to its purported owner.

1. Select one or more keys in your keyring, then click the Key Certification button or choose Certify Key... in the Keyring menu.

The following dialog appears:



Key Certification

Select a Private Key

Name : John Smith <j.smith@earthlink.com>

Passphrase :

Information included with this Certificate

Comment :

Policy URL :

Grant a Certificate to :

Ethan R. Benson (RSA) <erbenson@alaska.net>
Bob Parker <bob.parker@philipson.com>
Peter Hamburger <hamburger@fastfoood.net>

☑ Allow certificate to be exported
□ Allow certificate to be revoked

2. Verify whether the key listed in the window is the one you want to certify and choose the private key that will be used to make the Certificate.

3. Enter the passphrase and click Certify.
When the certification process is done an icon (large) or (small) associated with your name, is included in the public key you just certified. You can check it by selecting the user name and clicking the Expand button or by clicking the small triangle on the left of the user's name.

Allow certificate to be exported:
By default a certificate is not exportable. It means that when you export the key from your keyring the certificate will not be exported. To make your certificate exportable, check the option "Allow certificate to be exported" in the Key Certification window (see above).

Allow certificate to be revoked:
By default a certificate is revocable. If you do not want your certificate to be revoked - either by yourself or by a mandated revoker - uncheck this option.

Note: *Before posting a key which also includes your exportable certificate on a key server, we recommend to check with the owner of the key. Firstly because your name will be permanently associated with the key and secondly, he may not want to have hundreds of certificates included with his public key...*

To attest the authenticity of your public key, send your key to people you trust. Ask them to apply a certificate and to return the key. You can then repost your key - including its certificates - on a public key server. When someone downloads or obtains a copy of your public key, he can rely on the certificates of your key to check its authenticity.

Never certify a public key if you have not verified its authenticity. See Legitimate Copies of a public key above.

GRANTING TRUST LEVEL

You can assign a level of trust to the owner of a public key.
Click and hold down the mouse on the trust icon of the key (located under the column named **Trust**). A popup menu will appear. You have three choices: **Never trust**, **Marginally trust** and **Always trust**.

They indicate how well you trust the owner of a key to certify someone else's key. If you ever receive a key that was certified by someone whom you designated as trustworthy, the key will be considered as valid even if you did not check its validity yourself.

By granting a level of trust to a key owner, you define him as an introducer to other people's public keys. Note that trust levels only work on valid keys.

Again, the best way to verify the authenticity of a key is to check it yourself. If this is not possible, you will have to rely on your introducers' judgements.

The Validity of a Key

The validity of a key is calculated by SafeMail. It is the level of confidence indicating whether the public key really belongs to its purported owner:

✓ - A green check mark means the key is valid.
! - An orange exclamation point means that the key is probably valid but that the validity is not complete.
✗ - A red cross means the key is not valid according to SafeMail.

The validity of a key is based on the certificates associated with the key and the level of trust you have in the people who gave the certificates.

A key that was certified by you is valid since you are supposed to have verified its authenticity before applying your certificate.

If a key was not certified by you, its validity will depend on the level of trust you granted to the users who applied their certificates.
If a key does not have a certificate or if there is no level of trust associated with a certificate, the key will not be considered as valid.

You may, of course, use a non-valid key but SafeMail will warn you of the danger of using such a key.

Key Name and Identifiers (or Users)

A key can have multiple identifiers.

The first identifier or user listed when you open a key is always the primary one and is the same as the Key Name. We refer to it as the primary identifier or primary user.
We refer to the others as secondary identifiers or secondary users.

When you create a key, the name you give to the key is the primary identifier. You may create additional identifiers (secondary identifiers) at any time and you may permute one of these to become the primary identifier. The permuted secondary identifier will then also become the new Key Name. This can be useful, for example, if you use a new e-mail address.

In many PGP compatible software, the word “User” is used because in the majority of cases, a key belongs to a person. However, if it is a corporate key it can also be the name of a company. We think the word “Identifier” is perhaps more appropriate because you can type other information than just a user name and an e-mail address. Also, you can have multiple identifiers: The main identifier (the Key Name), for example, is a user name and an e-mail address and the secondary identifiers contain nicknames, other e-mail addresses or other information identifying you. Another example would be a key shared by several people such as a corporate key or a family key.

Create Secondary Identifiers

To add a new secondary identifier, select the key pair and choose New Identifier... in the Keyring menu. Enter your information and click the Add Identifier button.

The new identifier is added to the list of identifiers associated with the key. To view it, select the key and click the **Expand** button.

Set a New Primary Identifier (changing the Key Name)

Select a secondary identifier and choose Set Primary... in the Keyring menu. Enter your passphrase and click the **OK** button.

Key Disabled

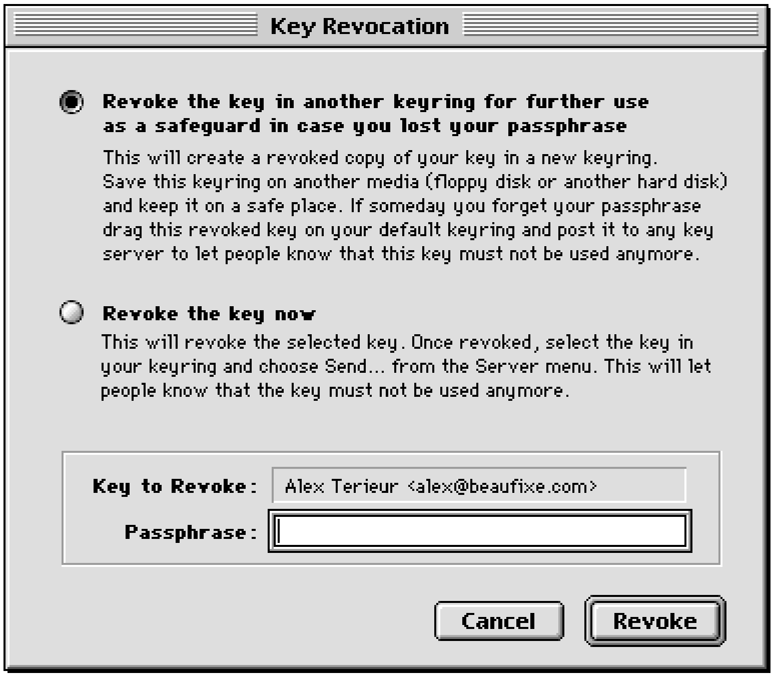
A disabled key will not be listed in the SafeMail encrypt and sign dialogs. However, SafeMail will still be able to use the key to verify a message or a document signed with this key.

To disable a key, select the key and choose **Get Info** in the File menu or double-click the key. Uncheck the Enabled option.
To re-enable the key, check the option again.

KEY REVOCATION

You may have to revoke your key if it gets compromized, for example, if the private key is lost or stolen or if you forget your passphrase.

1. To revoke a key, select a key pair and choose Revoke... from the Keyring menu. Choose Revoke the key now and click the **OK** button. Enter the key's passphrase and click Revoke. The revoked key will now be crossed with a line indicating that the key is no longer valid.



● **Revoke the key in another keyring for further use as a safeguard in case you lost your passphrase**

This will create a revoked copy of your key in a new keyring. Save this keyring on another media (floppy disk or another hard disk) and keep it on a safe place. If someday you forget your passphrase drag this revoked key on your default keyring and post it to any key server to let people know that this key must not be used anymore.

○ **Revoke the key now**

This will revoke the selected key. Once revoked, select the key in your keyring and choose Send... from the Server menu. This will let people know that the key must not be used anymore.

Key to Revoke: Alex Terieur <alex@beaufixe.com>

Passphrase:

2. After the key has been revoked, post it on a key server by selecting the key again and choosing **Send...** from the Server menu. This is important to inform other people that they should no longer use your old key.

You may be unable to revoke your key if you forget your passphrase. For thisreason, you have the possibility to immediately create a revoked copy of your key that you should store in another keyring. Select your private key or key pair and choose **Revoke...** from the Keyring menu. Choose Revoke a copy of this key in a new keyring and click the **OK** button. This will create a revoked copy of your key in a new keyring. Save the keyring on another disk and keep it in a safe place. If, some day, you forget your passphrase, you should drag the revoked key onto your default keyring and post it to a key server to inform people that the key should no longer be used. Be careful where you store the key. If someone gets hold of it, he/she could revoke your key without your permission.

Certificate Revocation

A certificate revocation is usually done on a certificate you have made on a user’s public key. Revoking a certificate means that you no longer trust that the key or its identifier belongs to its purported owner or that you think that the key’s security has been compromized. You can only revoke those certificates which you previously issued.

To revoke a certificate, select a certificate and choose Revoke... in the Keyring menu.

Important: *You should be sure of yourself before revoking a certificate on other people’ s keys: Revoking your key only concerns yourself whereas revoking a certificate on someone else’s key may arise suspicion about this person’s public key. Revoke your certificate only if you really think that the key may have been compromized.*

Note: *Do not revoke a certificate if, by doing so, you merely have the intention to remove your certificate from a public key. A certificate cannot be removed from the key server. Even if you delete the certificate from your local keyring and repost the key on the key servers, the certificate will remain on the server since a key server does not delete data, but only adds new information. Again, this may change when key servers evolve.*

Viewing Key Information

A key can be represented by different icons depending on the kind of the key (RSA, DSS, etc.) and the status of the key (expired, time limited, revoked, disabled, etc.)

To obtain information on a key, double-click the Key Name or select the key and click on the Get Info icon.

You can also obtain instant information on a key in a Keyring window or in any key list, for example in dialogs when encrypting or signing:

• Clicking on a Key Name (the line itself, not the icon) while holding down the Option key on your keyboard will display an information popup window about the key and its identifiers (users).
• Clicking on a user name while holding down the Option key on your keyboard will display an information popup window about the key and the certificates associated with the user.

FINDING UNKNOWN CERTIFIER

When you obtain a new public key and list its certificates, you will probably see that some of them display “Unknown Certifier” next to the Certificate icon. This means that you do not have the public key of this certifier in your keyring.

Select one or more certificates named Unknown Certifier and choose Find Unknown Certifier in the Edit menu. SafeMail will then initiate a search on the default key server and will download and add the associated public keys to your keyring.

UPDATING KEYS FROM A KEY SERVER

As seen in previous chapters, you may obtain a key from a key server by choosing **Find Keys...** in the Edit menu or you may post a key to a key server by selecting the key and choosing **Send...** from the Server menu.

From time to time, you may also want to update a public key already in your keyring. This can be useful to look for new identifiers/users and certificates associated with the key and thus obtaining the latest public version of this key.

Select a key and choose Update from the Server menu.
SafeMail will then initiate a search on the default key server and will update the public key on your keyring with new data, if any, from the copy of the selected key on the key server.

MANAGING YOUR KEYRING

A keyring is a group of keys. These keys can be private or public and can be of different types such as, for example, RSA keys or DSS keys.

SafeMail allows you to open one keyring at a time. See "The Keyring Panel" in the next chapter on how to designate the default keyring.

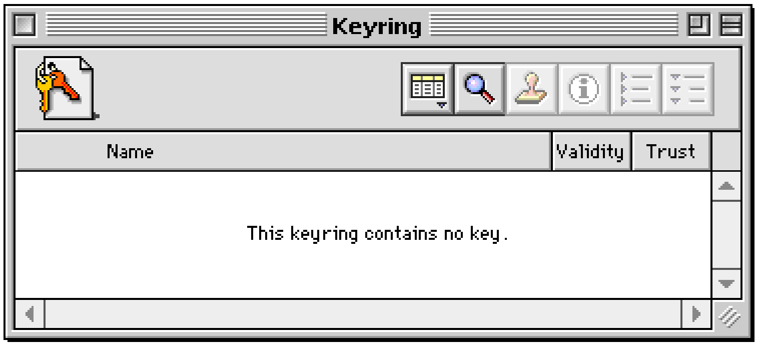
Note: *If you need to open more than one keyring at a time, you have to upgrade to SafeMail Pro.*

Although a keyring is displayed on screen in one window, a keyring always consists of two files: A public keyring file and a private keyring file which are associated. When you open a public keyring file, the related private keyring will also be opened.
Private keys are stored in small files. Even if you have more than 1000 public keys, you will probably never have more than a few private keys.

OPEN OR CREATE A KEYRING

To open your keyring, choose Open... in the File menu. If Safemail does not find a default keyring, a dialog will appear with the following options:
Create a New Keyring
Choose this option if you just installed the software and do not have a keyring yet. A new empty keyring will be created.
Locate an existing Keyring
Choose this option if you already have a keyring from another OpenPGP compatible software or a previous version of SafeMail or FileCrypt.
Scan All Disks
This option will scan your disks to locate existing keyring files. The first keyring found will be opened.
Cancel
No action will be performed.

If you choose New Keyring, a new empty keyring will be displayed on the screen:



This keyring contains no key.

To add keys to the keyring, you can either drag and drop keys from the Finder or select Find Keys... in the Edit menu to get keys from a key server.

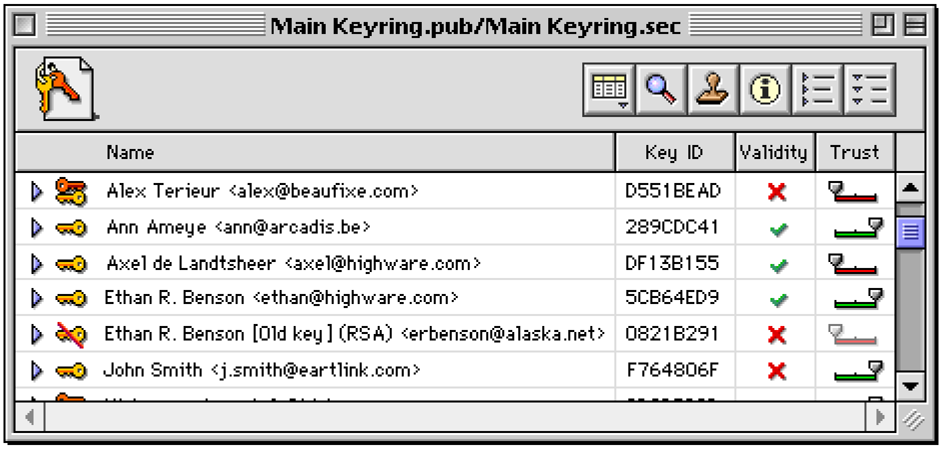
Choose Save in the File menu. A dialog window will appear: Enter a name for your keyring and click Save.

Note: *Another method to create a new keyring is to select one or more keys in an existing keyring then drag them onto your Desktop or onto a folder window. A dialog will appear: Select the radio button* ***Keyring*** *and a new keyring containing your selection will be created.*

Each time you create or modify a keyring, SafeMail will create next to this keyring another keyring with the same name but with the suffix ".bak". This ".bak" file is a backup file made by SafeMail in case the original file gets corrupted, for example by disk failure.

The Keyring Window

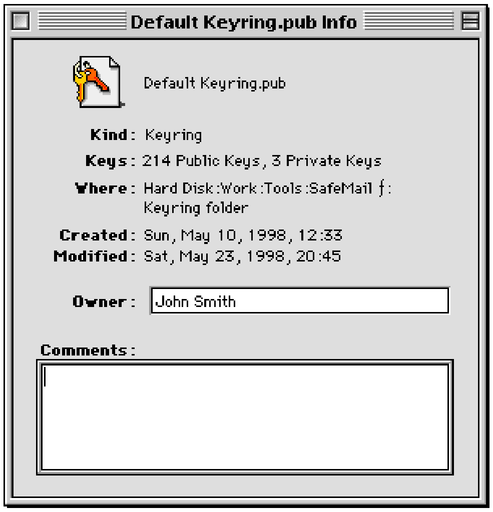
Below is an example of a Keyring window:



Main Keyring.pub/Main Keyring.sec

Name	Key ID	Validity	Trust
Alex Terieur <alex@beaufixe.com>	D551BEAD	✗	
Ann Ameye <ann@arcadis.be>	289CDC41	✓	
Axel de Landtsheer <axel@highware.com>	DF13B155	✓	
Ethan R. Benson <ethan@highware.com>	5CB64ED9	✓	
Ethan R. Benson [Old key] (RSA) <erbenson@alaska.net>	0821B291	✗	
John Smith <j.smith@eartlink.com>	F764806F	✗	

Click on the icon to obtain information on the current keyring.



Default Keyring.pub Info

Default Keyring.pub

Kind: Keyring
Keys: 214 Public Keys, 3 Private Keys
Where: Hard Disk:Work:Tools:SafeMail ƒ: Keyring folder
Created: Sun, May 10, 1998, 12:33
Modified: Sat, May 23, 1998, 20:45

Owner: John Smith

Comments:

The owner and comments field are optional: You can type in information that can be useful when exchanging keyrings with other SafeMail users.

To copy a key in the clipboard, select a key and choose Copy from the Edit menu. You may then paste the key in any text document.

You may also option-click on a public key icon to open a popup menu allowing you to select Copy key or Copy Fingerprint.

The Column button: Click on it to display a list of all available columns. You can hide or show a column by selecting it in the list.
Almost all columns can be moved by placing the cursor on the column title. The cursor will then change into a hand. Click and drag the hand to the left or to the right. They can also be resized by placing the cursor between two columns.

The Get Info button: Select an item and click on it to obtain further information on that particular item.

The Expand button: Select one or more keys and click this button to expand the key(s) and view all its identifiers/users and their certificates. Press the Option key while clicking the button to expand all the selected keys with their identifiers and certificates at once.

The Collapse button: It does the reverse of the **Expand** button: Press the Option key while clicking the button will collapse all your keys and identifiers at once.

The Find button: Has the same function as choosing **Find...** in the Edit menu. It displays a dialog that will let you search for a key in one of your keyrings or on a key server on the network.

The Certify button: Select a key and click this button to certify one or more keys.

The Stop button: This button will only appear when necessary, for example to stop a verification process that you initiated. Click this button to stop the process.

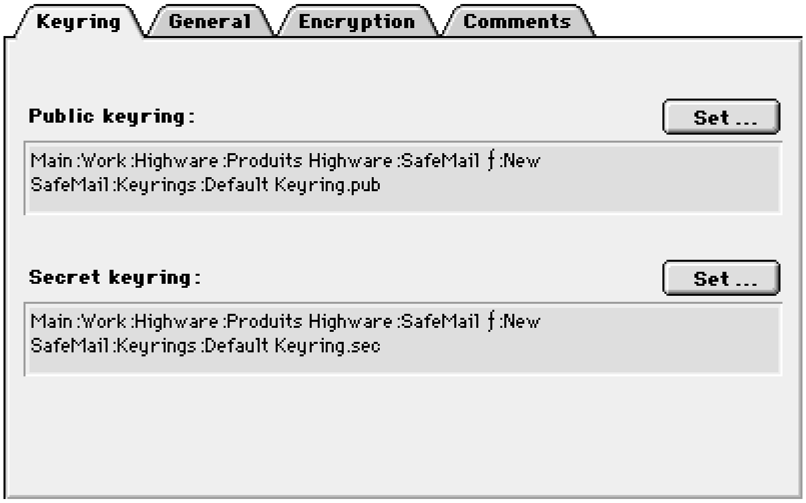
CHAPTER 7- SAFEMAIL KEYRING MANAGER

This chapter describes how to use and configure SafeMail Keyring Manager. It explains how to set the general options of the software.

SETTINGS

Choose **Settings...** in the Edit menu to open the Settings panel. This is where you define several default values and other preferences. The Settings window can also be opened by choosing **Settings...** in the SafeMail menu.

1. The Keyring Panel



Public keyring:

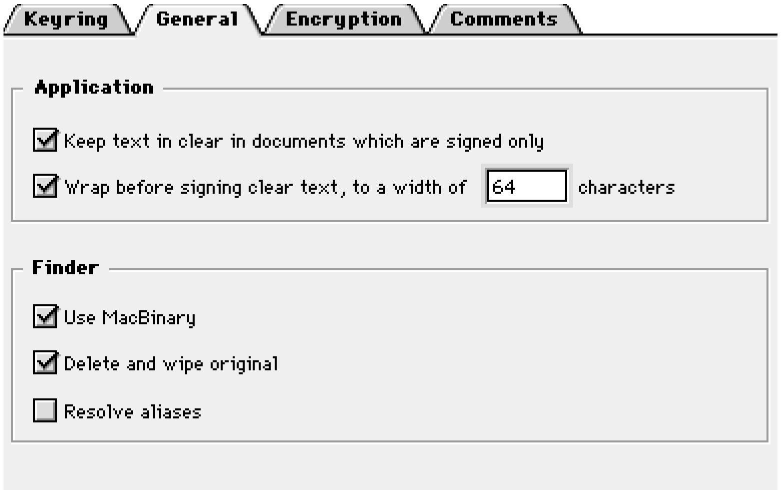
Main :Work :Highware :Produits Highware :SafeMail ƒ :New SafeMail :Keyrings :Default Keyring.pub

Secret keyring:

Main :Work :Highware :Produits Highware :SafeMail ƒ :New SafeMail :Keyrings :Default Keyring.sec

The Keyring Panel is where you indicate your default keyrings. You may indicate two different paths if your private keyring is at a different location than your public keyring.

2. The General Panel



Application

☑ Keep text in clear in documents which are signed only

☑ Wrap before signing clear text, to a width of 64 characters

Finder

☑ Use MacBinary

☑ Delete and wipe original

□ Resolve aliases

The General panel has two types of options:

- Options available when you are encrypting or signing in an Application such as a word processor, an e-mail software or a text editor.
- Options related to actions usually executed in the Finder.

Application

- Keep text in clear in documents which are signed only: When checking this option, the text of your signed message will be kept “as is” and SafeMail will only add a header and a footer to indicate that the message has been signed. If you uncheck this option, SafeMail will “scramble” the text of the message and the latter will become illegible. It is important to note that the latter is not an encryption process and does not offer strong security. It will merely keep the message “private” to prying eyes over your shoulder.

  In most cases, you can leave this option checked. If you want to secure your signed message, you should also encrypt them.
  This value is checked by default. You can change the status of this feature at any time in the bottom part of the Signing window. Click the small triangle to view all options available.

- Wrap before signing clear text, to a width of n characters: You normally do not have to change this setting which is essentially for e-mail software. When sending a message, most e-mail applications wrap lines or add carriage return characters after each line. This can modify the message **after** you have signed it. Consequently, when the signed message is verified, it will appear as having been altered during the transmission. To avoid this situation, have this option checked. Before signing a message, SafeMail will limit the line length of your message to the number of characters defined in this option. In most applications, the default setting of 64 characters will do.

Finder

- Use MacBinary: MacBinary is the standard conversion method used to transfer files over the network between Macintosh computers or to/from Windows computers. MacBinary is in fact a format and both the sending and the receiving programs should understand this format. If you send an encrypted file in a MacBinary format to a Windows users who uses a receiving software that does not understand MacBinary, the user will not be able to decrypt the file. In most cases, you will be able to use MacBinary since more and more software understand and convert MacBinary files.

  In general, **you use** MacBinary:
  - When sending to another user of SafeMail on any platform
  - When sending to a user of PGP 5.5 or above on any platform

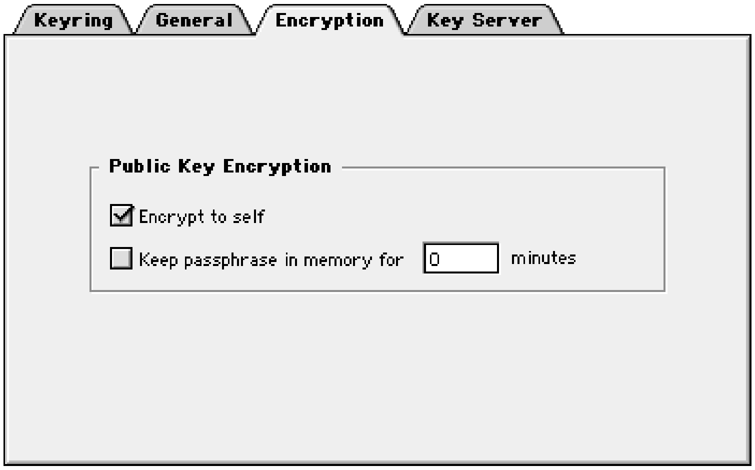
  In general, **you do not use** MacBinary when sending a file that you know is cross-platform such as Word, Excel, MicroSoft Office, compressed files such as Stuffit, Zip, Compactor, Arc, graphic files such as GIF and JPEG, etc.

  This value is set by default. You can change the status of this feature at any time in the bottom part of the Encrypt or Sign window. Click the small triangle to view all options available.

- Delete and Wipe original: If this option is checked, SafeMail will delete and wipe (overwriting 7 times) the original file after its encryption or signature. Uncheck this option if you want to keep the original document on your disk.

- Resolve aliases: If this option is checked and SafeMail encounters an alias during an encryption or a signature process, SafeMail will process the original file instead of the alias. We must advise you to be very careful when using this option. For example, if you encrypt a folder that contains the alias of a server, all files residing on that server will be encrypted…

3. The Encryption Panel



Public Key Encryption

☑ Encrypt to self

□ Keep passphrase in memory for 0 minutes

The Encryption panel has the following options:

- Encrypt to self: When this box is checked, your own public key is added to the list of keys you select when encrypting a message. It implies you will always be able to decrypt the messages you encrypt. For SafeMail, your public key is the default public key located in the default keyring.

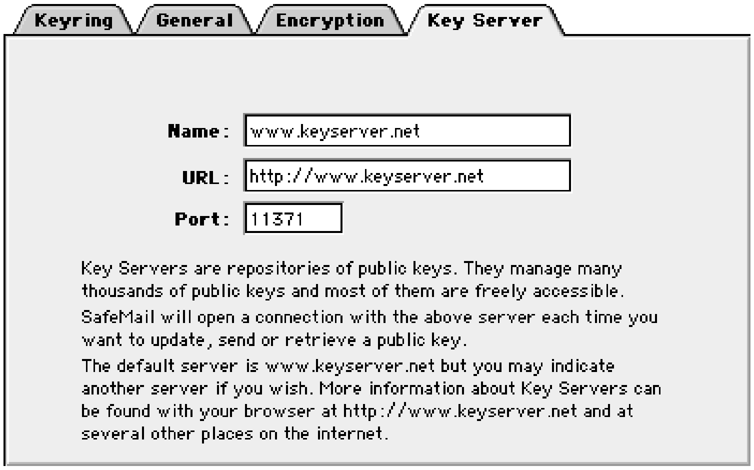
  If you uncheck this option and you encrypt a message without including your own public key, an alert will warn you that you will not be able to decrypt the message once it is encrypted. You can then choose to encrypt the message anyway, or add your key before you encrypt the message.

- Keep Passphrase in memory for n minutes: When this option is checked, your passphrase will be stored in your computer memory for the time defined in this option after the first successful use of your passphrase.

  This can be useful if you receive a lot of encrypted mail and do not want to re-enter your passphrase for each message. In most situations, the defined time should not be longer than a few minutes though. In any event, you must never leave your computer unattended as long as the elapsed time is not over. If not, anyone having access to your computer will be able to read all your secured files.

Important:
If you have to leave your computer suddenly and the defined time in the above option is not elapsed, open the ***Settings*** *and uncheck then check again the Keep Passphrase option. This operation will initialize the counter and the countdown will be cancelled. You may also install an access control software such as DiskGuard or FileGuard to prevent anyone from using your computer during your absence.*

4. The Key Server Panel



Name: www.keyserver.net

URL: http://www.keyserver.net

Port: 11371

Key Servers are repositories of public keys. They manage many thousands of public keys and most of them are freely accessible.

SafeMail will open a connection with the above server each time you want to update, send or retrieve a public key.

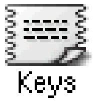
The default server is www.keyserver.net but you may indicate another server if you wish. More information about Key Servers can be found with your browser at http://www.keyserver.net and at several other places on the internet.

In this panel you can specify the key server address that will be reached went you post or get a key from the server.
Name: Enter the name of the key server.
URL: Enter the exact Internet address of the key server in URL format such as http://www.keyserver.net. If you have a key server located on your network, follow the instructions as given by your Network Administrator.
Port: Most key servers use port 11371. If you do not know the port number, leave this field empty or ask the key server administrator.

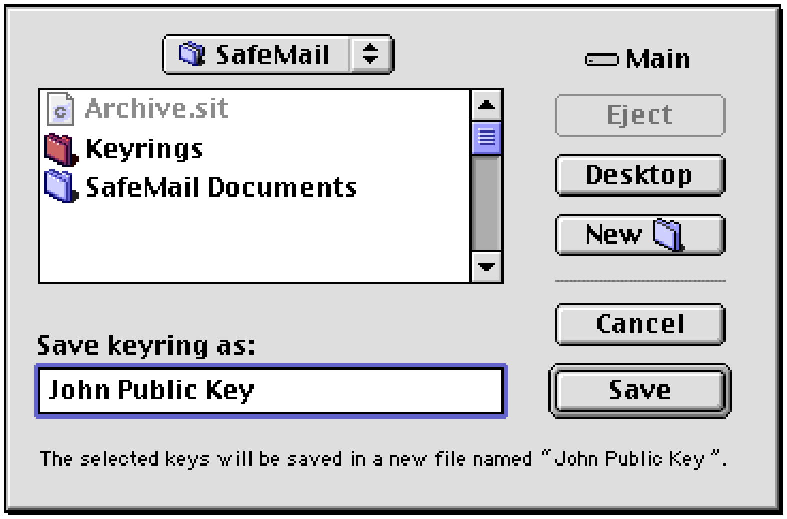
Exporting Keys and Keyrings

There are two ways to export keys in SafeMail:

- Select one or more keys in your keyring then drag & drop them onto your Desktop. This will create a Clipping file containing your key(s). It can then be dropped on any application that is drag & drop aware.



- You may also select the keys and choose **Export...** from the File menu. Enter a name, click Save and a text file will be created containing your keys. Since a key is basically composed of a block of text, it is quite easy to copy it and include it in an electronic message.



Save keyring as: John Public Key

The selected keys will be saved in a new file named "John Public Key".

Keyring Manager Menus

File

Open keyring

Open your default keyring.

Close

Close the current window.

Save

Save changes in the current Keyring.

Get Info...

Select an item in a SafeMail window and choose **Get Info** to obtain more information about the item.

Import...

Choose this item to import keys from a Keyring made by another software such as the PGP software from Network Associates.

Export...

Select one or more keys and choose **Export…** to export the keys. You may also just drag the keys from a Keyring to the Finder.

Edit

Find Keys...

To search for a specific key, choose **Find Keys...** SafeMail will search on a local Keyring or on a key server on the network.

Find Unknown Certifiers...

Select a certificate with an unknown certifier and choose this feature. SafeMail will find and download the public keys belonging to the user who made the certificate.

Set as Default

Lets you set the selected item as the default item.

Settings

Opens the Settings panels to configure SafeMail.

Keyring

Verify Certificates...

Will perform a check on the current Keyring and verify all certificates. The results will be shown in a new window.
(See “Managing your Keyring”, page 53)

New key pair...

Generation of a new key pair: A private key and its related public key.
(See “Creating a key pair”, page 16)

Certify...

Select a public key and choose this menu item to apply a Certificate.
(See “Certificates”, page 45)

Revoke...

Select a key pair or a certificate and choose **Revoke...** to revoke a key or a certificate. Once revoked, post it on a key server to inform people that it has been revoked. (See “Key Revocation”, page 50)

Add Secondary Identifier/User...

Lets you create another identifier or user for the selected Key. You will need the related private key to perform this operation.
(See “Create Secondary Identifiers”, page 49)

Set as Primary Identifier/User

If a Key has several identifiers, you may choose to permute a secondary identifier with the primary identifier and thus changing the Key Name.
(See “Set a New Primary Identifier (changing the Key Name)”, page 49)

Change Passphrase

Select a key pair and choose this menu item to change the passphrase of a private key.

Server

Update Selection...

SafeMail will establish a connection to the key server and download new data, if any, to update the selected Key(s) in your keyring.

Send Selection...

SafeMail will establish a connection to the key server and send a copy of the selected Key(s).

Tools

Sign..., Encrypt..., Decrypt/Verify...

Same as described in “Securing Files on your Computer” on page 35.

Encrypt Conventionally...

Choose this menu item to encrypt a file using a password instead of public key cryptography. (See “Conventional Encryption”, page 41)

Wipe...

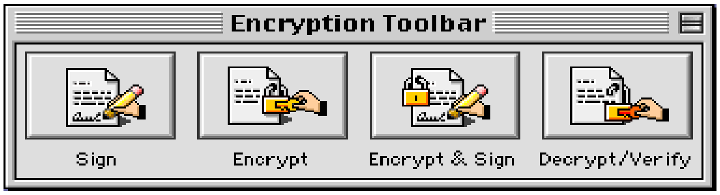
Choose Wipe then select a document to “Wipe” it. This will permanently erase the document. When you delete a file by moving it to the Trash, the file is in fact not really deleted. It is merely deleted from the System directory structure. It will be considered as “empty space” by the System and will be genuinely deleted once another file is written over. A trashed file can usually be recovered by specialized software.

By using the Wipe feature, even a recovery tool will not be able to restore the document as it will be erased and overwritten 7 times.

Windows

Show/Hide Toolbar

This item will show or hide the Toolbar.



The Toolbar is convenient if you did not install the SafeMail menu or if you prefer to work from the Keyring Manager application. Simply drag and drop documents or folders from the Finder onto one of the Toolbar’s icons.

You can also click directly on one of the Toolbar’s icons: It is the equivalent of using the Tools menu item with the same name.

See “Securing Files on your Computer” on page 35 for more detailed information on encrypting/decrypting and signing/verifying documents.

View by Small Icon and View by Icon

These menu items let you change the size of the icons in many of the application windows and lists.

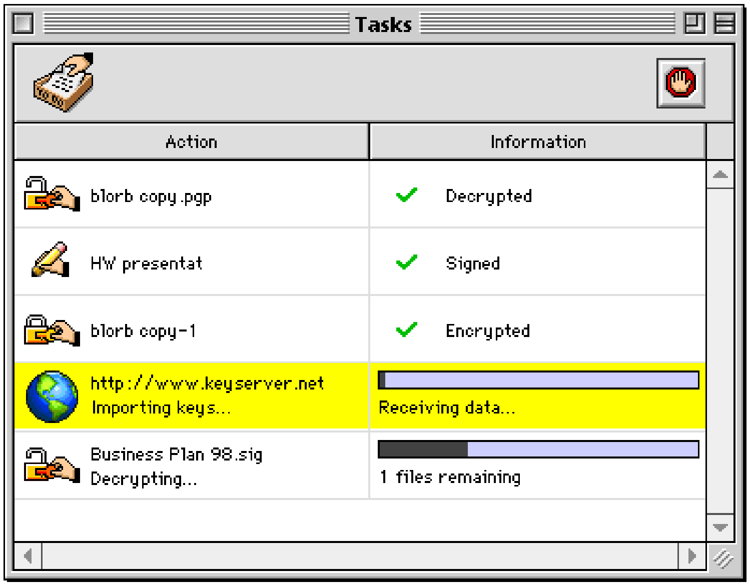
Today's Log

This item will open the log window for the current day. Log files are saved in the SafeMail Preference folder in the Prederences folder of your System Folder. To view the log of a previous day, you may double-click a log file.

Tasks

This item will open the Task Window if you previously closed it. The Task Window will automatically appear each time you perform an operation requiring a process. Since SafeMail is a multi-process application, you can follow the completion of each independent process. You can, for example, encrypt a large folder, then launch a request on a key server and simultaneously verify a signed document.

To cancel a process, select the process and click the **Stop** button.



Action	Information
blorb copy.pgp	✓ Decrypted
HW presentat	✓ Signed
blorb copy-1	✓ Encrypted
http://www.keyserver.net Importing keys...	Receiving data...
Business Plan 98.sig Decrypting...	1 files remaining

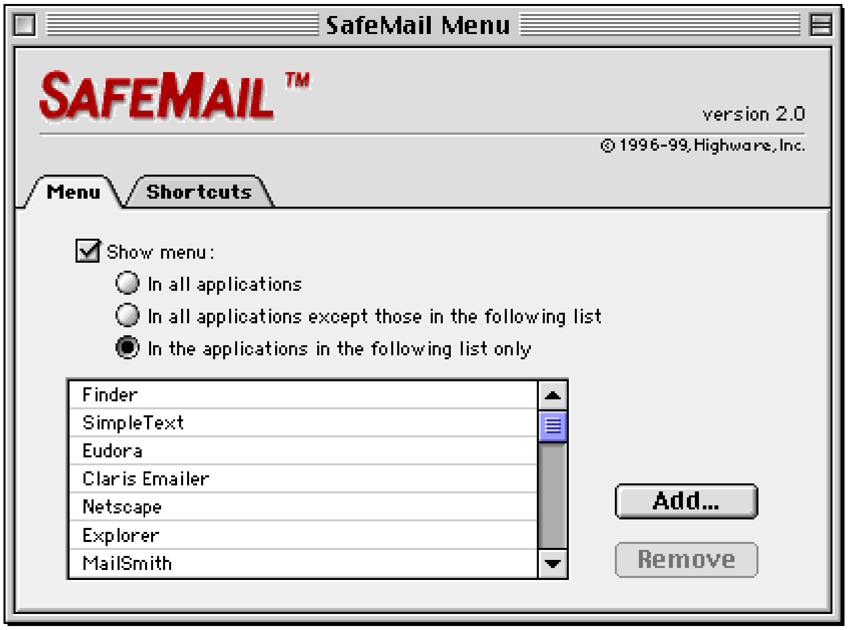
CHAPTER 8 - SAFEMAIL CONTROL PANEL

This chapter describes how to use and configure the SafeMail Control Panel. It also explains how to use the SafeMail menu.

The settings and options shown in the SafeMail Control Panel will only work if the Control Panel was loaded at startup. If you disabled the Control Panel with software such as the Apple Extension Manager or Conflict Catcher™, those options will not be operational and the menu will not be present.

Open the Control Panel folder and double-click the SafeMail Menu file.

THE MENU PANEL



☑ Show menu:

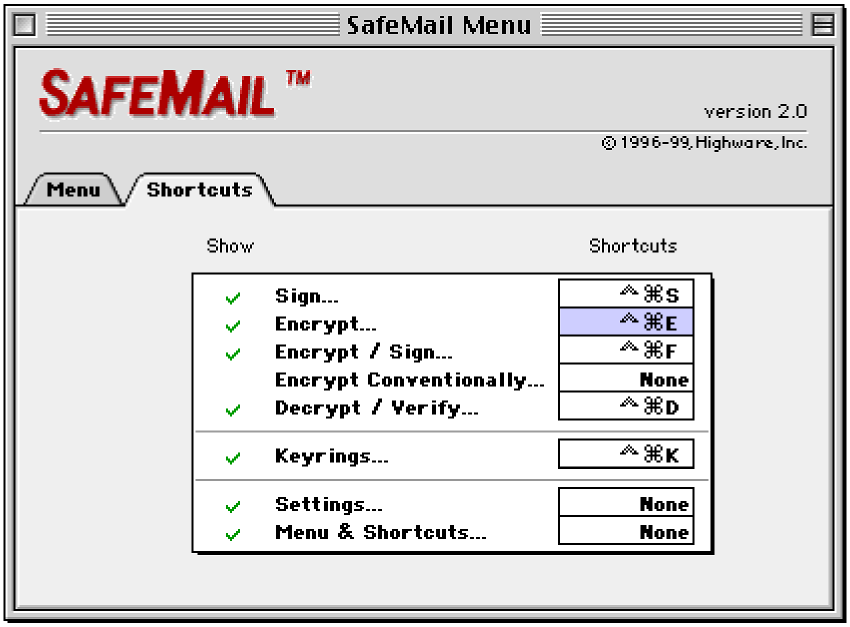
○ In all applications
○ In all applications except those in the following list
● In the applications in the following list only

Finder
SimpleText
Eudora
Claris Emailer
Netscape
Explorer
MailSmith

The control panel lists all applications in which the SafeMail menu will be available. It implies that the menu will only be active in the applications in which you will require it. By default, the list contains the most frequently used applications in which SafeMail proves to be useful.

Adding an application: To add an application to the list, click the **Add** button. A dialog appears. Locate and select the application you want to add to the list, then click the **OK** button.
Removing an application: To remove an application from the list, select it in the list and click the **Remove** button. SafeMail will no longer be available in that application.
Show Menu: Check this option to make the menu active in the list of applications.

The Shortcuts Panel



Show		Shortcuts
✓	Sign...	^⌘S
✓	Encrypt...	^⌘E
✓	Encrypt / Sign...	^⌘F
	Encrypt Conventionally...	None
✓	Decrypt / Verify...	^⌘D
✓	Keyrings...	^⌘K
✓	Settings...	None
✓	Menu & Shortcuts...	None

Show: A checkmark indicates that the item will be shown in the menu. Click on the left of a menu item to have it either shown or hidden in the SafeMail menu.

Shortcuts: You can assign a keyboard shortcut to each menu item. Click in the shortcut box next to the item for which you want to create a shortcut. Enter a new shortcut or modify the existing one. Be careful not to enter a keyboard shortcut that conflicts with another application. If this is the case, try another one. To remove a shortcut, press the Delete key.

CHAPTER 9 - SAFEMAIL FOR EUDORA

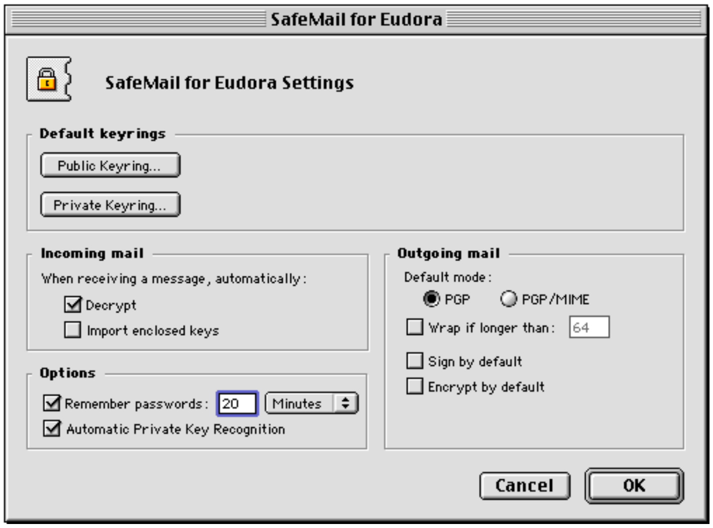
This chapter describes how to use and configure the SafeMail for Eudora plug-in. The software will allow you to automatically encrypt outgoing mails and decrypt incoming mails. Once the plug-in is installed, securing, signing and decrypting e-mails will become virtually transparent.

INSTALLATION

The SafeMail for Eudora plug-in only works with Eudora 3.0 and higher. Place the **SafeMail for Eudora** file in the Eudora Stuff folder inside the Eudora application folder and launch Eudora. You will notice the presence of SafeMail for Eudora by two new icons in the toolbar of every new Message window. The first time you launch Eudora after installing the SafeMail for Eudora plug-in, an alert will appear to suggest that you verify the settings and indicate the location of your keyrings.

SETTINGS

You need to set up the SafeMail for Eudora plug-in before you can start using it. To open the SafeMail for Eudora settings, choose SafeMail plug-in from the Plug-in Settings... submenu in the Special menu of Eudora.



Incoming mail

When receiving a message, automatically:

☑ Decrypt

□ Import enclosed keys

Options

☑ Remember passwords: 20 Minutes

☑ Automatic Private Key Recognition

Outgoing mail

Default mode: ● PGP ○ PGP/MIME

□ Wrap if longer than: 64

□ Sign by default

□ Encrypt by default

Default Keyrings

Indicate to SafeMail for Eudora the location of both your public and private keyrings.

Incoming Mail

Decrypt: Check this box to automatically process all incoming mail. Signatures on signed mail will be verified and encrypted mail will be decrypted after you have entered the correct passphrase.

If you prefer not to use this automatic feature, SafeMail will not intervene and you can decrypt or verify each message at a later stage.

Import enclosed keys: Some messages may include one or more public keys. If this box is checked, SafeMail will automatically import all public keys it finds into your default keyring.

Outgoing Mail

Default Mode: Upon sending secured e-mails you can choose between two methods namely OpenPGP or PGP/MIME. The OpenPGP method is the most common one, its advantage being that almost every security software compatible with the OpenPGP or PGP format will be able to decrypt it. The PGP/MIME method should only be used if you are sure that your recipient uses a software that will be able to understand this format. If this is not the case, your recipient may have some difficulties reading your message (depending on the recipient’s e-mail software).

The advantage of the PGP/MIME format is that your message will be sent as is, that is including all styles applied in your original message like bold, italic, etc. If you decide to use the regular OpenPGP format, all style attributes will be removed before the encryption is done and only pure text will be transmitted. In general, the PGP/MIME format is used only with e-mail software. The normal OpenPGP format is more compatible with other PGP compatible software and can be used in any application.

Sign by default: By checking this option, the **Sign** button in the message toolbar is on by default (📝). You can override this option for any message by clicking the **Sign** button in the message toolbar to turn signing off (📝).

Encrypt by default: By checking this option, the **Encrypt** button in the message toolbar is on by default (🔒). You can override this option for any message by clicking the **Encrypt** button in the message toolbar to turn encryption off (🔒).

Passphrase

Remember passphrase for: Enter the amount of time you want SafeMail to remember the passphrases you enter. This can be helpful if you receive several encrypted messages and you do not want to enter the key's passphrase for each mail. Each time the passphrase is used, SafeMail will memorize it for the period of time you previously specified. Once the period has elapsed, the passphrase is cleared from the SafeMail memory. The next time you want to decrypt or sign a mail, you will have to enter the passphrase again.

⚠ ***Note:*** *Upon deciding on the length of time SafeMail has to memorize your passphrase, you should keep into account that if you leave your computer unattended, anyone having access to your computer can send signed messages or read your secured e-mails as they will be automatically decrypted by SafeMail.*

Automatic Private Key Recognition

Check this option and SafeMail will be more "transparent": If the sender's e-mail address corresponds to a private key name no key selection dialog will appear . You will only be requested to enter the password of the private key; if you set the password cache (see above), no dialog will intervene and your message will be automatically signed.
If you want to select the private key yourself, uncheck this option.

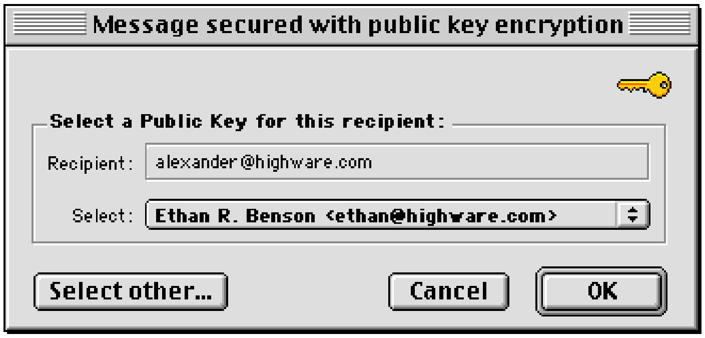
Encrypting an e-mail Message

- Compose your mail as usual.
- Click the Encrypt button (🔒) in the message toolbar.
- Send your message.

When Eudora sends the message, SafeMail will search your public keyring for the public keys which match the recipients' e-mail addresses.

- If SafeMail finds a public key for each recipient, the message will be automatically encrypted and no further action will be required from your part.

- If SafeMail does not find a public key for each recipient, it will present you with a dialog for each recipient for which no matching key was found. The dialog contains a pop-up menu which lists all the public keys in your public keyring which closely match the recipient's e-mail address (same domain name, similarity in the name, etc.)


Message secured with public key encryption
Select a Public Key for this recipient:
Select other...
Cancel
OK

Recipient: alexander@highware.com

Select: Ethan R. Benson <ethan@highware.com>

If the pop-up menu contains the key which corresponds to the recipient, choose the key in the pop-up menu and click **OK**.
If the key you are looking for is not listed in the pop-up menu, click on **Select Other...** This will open a dialog which lists all keys in your public keyring.

- If SafeMail does not find any public key that matches any recipient's e-mail address, a keyring window that lists all keys available in your default public keyring will appear. Select one or more keys and click OK.

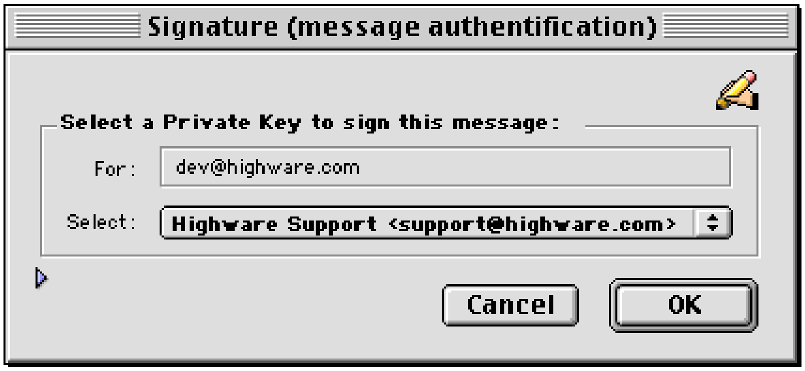
Signing an E-mail Message

- Compose your mail as usual.
- Click the Sign button (✎) in the message toolbar.
- Send your message.

When Eudora sends the message, SafeMail will search the default private keyring for the private key that matches the sender's e-mail address.

- If SafeMail finds the private key, a dialog will appear inviting you to enter the private key's passphrase.

- If SafeMail does not find the private key, it will show a dialog containing a pop-up menu with all the private keys in your default private keyring. Select the private key you want to use to sign the message and click OK or click Cancel to cancel the operation.


Signature (message authentification)
Select a Private Key to sign this message :
Cancel
OK

For : dev@highware.com

Select : Highware Support <support@highware.com>

Encrypting and Signing Simultaneously

If you want to encrypt as well as sign a text, click both the Sign (✎) and the Encrypt (🔒) buttons in the message toolbar.

Encrypting or Signing part of a message

If you do not want the entire message to be encrypted or signed, do not click the icons located in the toolbar. Instead, select the text to be signed or encrypted and choose **Sign** or **Encrypt** in the Message Plug-Ins submenu of the Eudora Edit menu.

Note: *If the SafeMail Menu control panel is installed you can also choose* ***Sign...*** *or* ***Encrypt...*** *in the SafeMail menu. If part of the message is selected, only that part will be signed or encrypted. If no text is selected, the complete message will be signed or encrypted.*

Defining a specific key for a Recipient

For each recipient listed in the Eudora Address Book, you can assign a public key which SafeMail can use. If the information exists, SafeMail will automatically use that key and will not try to find a key that matches the recipient’s e-mail address. Besides a Key ID, you can also add "PGP" for standard OpenPGP and "PGPM" for PGP/MIME.

Example of a Eudora Address Book entry:

John Smith <jsmith@earthlink.com>

can be modified by adding a Key ID and/or an encryption method:

John Smith#F764806F <jsmith@earthlink.com>

John Smith#F764806F#PGP <jsmith@earthlink.com>

John Smith#F764806F#PGPM <jsmith@earthlink.com>

John Smith#PGP <jsmith@earthlink.com>

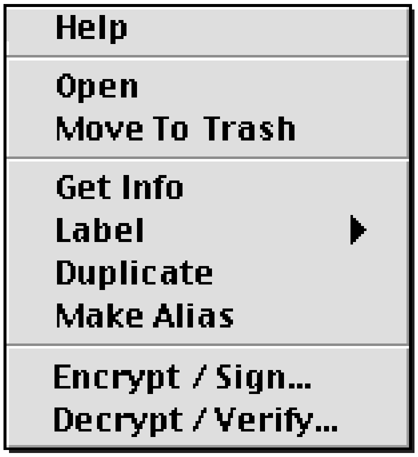
The presence of the pound key information will supersede all other preferences and settings you previously defined.

Chapter 10- SafeMail Contextual Menu

SafeMail Contextual Menu is a contextual menu for Mac OS 8.5 or later.

To install SafeMail CM drop it on your System Folder's icon or move it manually into the Contextual Menu Items folder inside your System Folder, then restart the computer.

After restarting your Macintosh, SafeMail CM will be available in the menu that pops up whenever you Control-Click on a file. Choose an option from the popup menu.



SafeMail CM software will work only if the control panel SafeMail Menu has been installed. However, if you prefer to use only the contextual menu and not have the SafeMail menu to appear in the menu bar, you may uncheck the Show Menu option (see page 69).

SafeMail CM works in the Finder (to secure or verify files) and in any application to secure or verify text parts. Select the text to be encrypted, press the Control key and choose a menu item.

GLOSSARY

This chapter briefly explains the terms and principles used in SafeMail.

You will find explanations on the following:

- Authentication
- Certificates
- Conventional Encryption
- Key
- Key Management
- Keyring
- Message Signature
- Passphrase
- Public key
- Public-key Encryption
- Private key
- Signature

For more detailed information we refer to the book “Protect Your Privacy” by William Stallings, published by Prentice Hall PTR and to the information on PGP available on the Internet. Parts of this chapter are based on “Protect Your Privacy”.

ENCRYPTION

Encryption is the transformation of data into a format that can be safely transmitted, without fear of anyone intercepting and reading the message. Once encrypted, data must be decrypted to be read.

CONVENTIONAL ENCRYPTION

A useful analogy to conventional encryption is a strongbox with a single lock and two copies of the key (Figure 1). Say Bob wants to send a secure message to Alice and suppose that Bob and Alice each have one of the two keys. Bob places the message in the strongbox and locks it with his copy of the key. The strongbox is then transported to Alice. Anyone can be trusted to do the transporting, since the box is locked. When Alice gets the box, she unlocks it, using her copy of the key. Now let us look at conventional encryption. Again, Bob wants to send a message to Alice in such a way that no one else except Alice can read the message (Figure 2). The original message is referred to as plain text. To thwart potential eavesdroppers, Bob scrambles the message using an encryption algorithm, producing cipher text. Anyone reading the cipher text would see an apparently random string of nonsense. For this scheme to work, the key must be kept private, known only to Bob and Alice, and so we shall call this a private key. Once the cipher text is produced, Bob transmits the message to Alice. Alice can then transform the cipher text back to the original plain text by using a reverse version of the same algorithm with the same key that Bob used.

There are two requirements for communication by conventional encryption:

- We need a strong encryption algorithm.
- Alice and Bob must have obtained copies of the private key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Figure 1

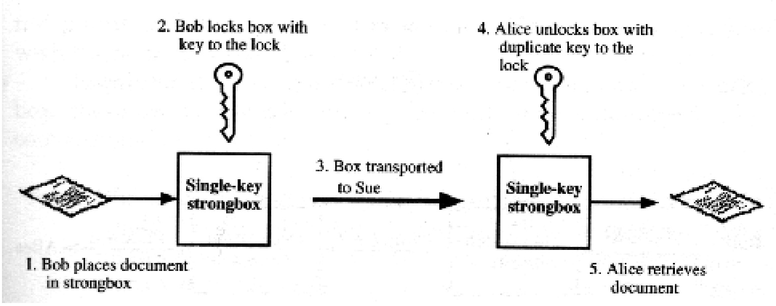
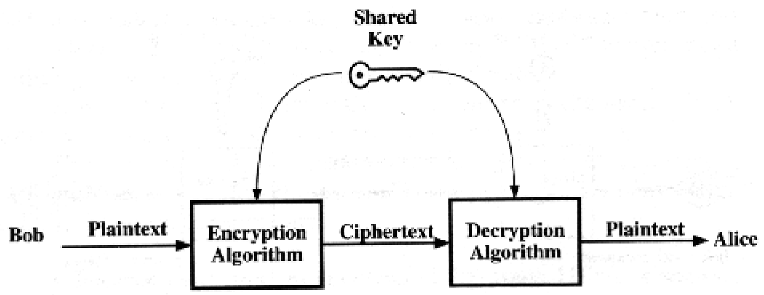

2. Bob locks box with key to the lock
4. Alice unlocks box with duplicate key to the lock
Single-key strongbox
3. Box transported to Sue
Single-key strongbox
1. Bob places document in strongbox
5. Alice retrieves document

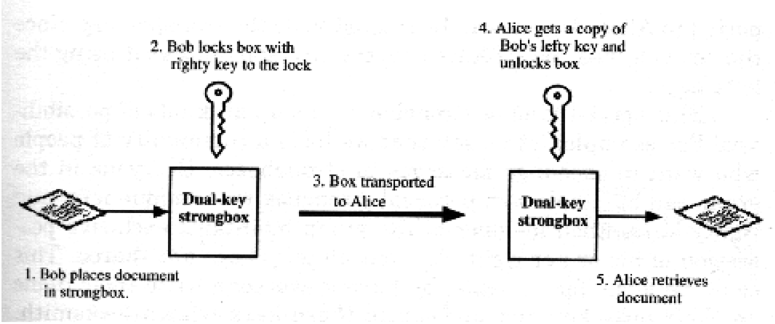
Figure 2



Public Key Encryption

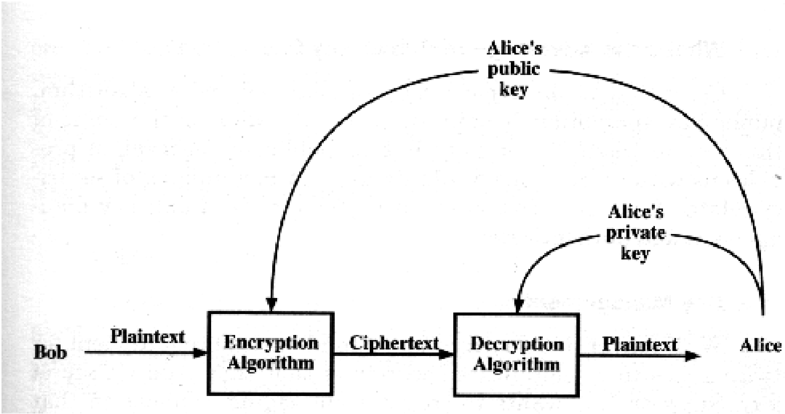
Public-key cryptography involves the use of two separate keys, in contrast to conventional encryption, which uses only one key. A useful analogy to public-key encryption is a strongbox with a special kind of lock that accommodates two types of keys (Figure 3). One key, a lefty key, turns the locking mechanism to the left and the other key, a righty key, turns it to the right. When the mechanism is unlocked, it is in a center position. If it is turned to either the left or the right, it is locked and the box cannot be opened. So an unlocked box can be locked with either a lefty key or a righty key; however, if the box is locked with a lefty key, the only way to unlock it is with a righty key and, similarly, if it is locked with a righty key, the only way to unlock it is with a lefty key.

Figure 3


2. Bob locks box with righty key to the lock
4. Alice gets a copy of Bob's lefty key and unlocks box
Dual-key strongbox
3. Box transported to Alice
Dual-key strongbox
1. Bob places document in strongbox.
5. Alice retrieves document

Now, say that Bob wants to send a secure message to Alice and suppose that he has the righty key for a strongbox and Alice has the matching lefty key. Bob places the message in the strongbox and locks it with the righty key. The strongbox is then transported to Alice. Anyone can be trusted to do the transporting, since the box is locked. When Alice gets the box, she unlocks it using the lefty key. This special kind of strongbox opens up all kinds of possibilities. For example, let us say that we have a community of people who want to exchange messages in strongboxes. Everyone in the group can buy their own personal strongbox with unique lefty and righty keys. Each member of the group maintains exclusive possession of his or her righty key but all lefty keys are shared. This could be done, for example, by having everyone write their name on their lefty key and depositing these keys with a locksmith. When anyone wants someone else's lefty key, they can go to the locksmith, who will duplicate the requested key. Consider the following scenario (figure 4): Bob wants to send a message to Alice and make sure that no one but Alice can read it. Here's how: Bob gets a duplicate of Alice's lefty key and of her strongbox, puts the message in the box, and locks the box. Since only Alice has the righty key for this box, only she can open the box. Another scenario: Bob wants to send a message to Alice and, although it isn't important that the message is kept private, he wants Alice to be certain that the message is indeed from him. In this case Bob uses his own strongbox and locks it with his righty key. When Alice receives the box she finds that she can open it with Bob's lefty key, thus proving that the box must have been locked by Bob. Now let us look at public key encryption. A general-purpose public-key cryptographic algorithm relies on one key for encryption and a different but related key for decrypting. Furthermore, these algorithms have the following important characteristics:

Figure 4



- It is computationally infeasible to determine the decrypting key given only knowledge of the cryptographic algorithm and the encryption key.
- Either of the two related keys can be used for encryption, with the other used for decryption.

The essential steps are the following:

- Each user generates a pair of keys to be used for the encryption and decryption of messages.
- Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private.
- If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice's public key.
- When Alice receives the message, she decrypts it, using her private key. No other recipient can decrypt the message because only Alice knows her private key.

With this approach, all participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a user protects his or her private key, incoming communication is secure. At any time, a user can change the private key and publish the companion public key to replace the old public key.

As an example of public-key encryption, Bob encrypts a plain text message with Alice's public key, producing ciphertext. The ciphertext depends on the encryption algorithm and also on the key. When Alice receives the ciphertext, she can decrypt it using her private key. Public-key encryption provides us with tremendous flexibility to perform a number of security-related functions. Two areas in particular stand out: Key management and authentication.

KEY

A key is the code which is used to encrypt or decrypt a text. In conventional encryption, the same key is used to encrypt or decrypt. In public-key encryption, different keys are used to encrypt and to decrypt.

PRIVATE KEY

Private keys are used to create digital signature or to decrypt electronic data. It is not possible to encrypt messages using a private key. Because you use the private key to decrypt messages people send to you and to authenticate the messages you send, this key is for your personal use only, and must never be disclosed to the public.

PASSPHRASE

A passphrase is a word or phrase, or even just random characters, which allows you to use your private key. Your passphrase should be more than one word, and never ever something which a person who knows about you could guess, i.e., your name, your middle name, your pet's name, your kid's name, your birthday, your anniversary, your girl/boyfriend's name, your spouse's name, your address, your favorite band, etc. It should contain irregular capitalization, e.g. tHe, $mith. It should also be easy to type quickly, without errors, and without your needing to see it on the screen. It is also recommended to change your passphrase regularly.

Public key

In public-key encryption, public keys are used to encrypt messages only. A public key is always associated with a private key and messages encrypted with a public key can only be decrypted with the associated private key. Your public key is used by everybody who want to send you encrypted messages and can be distributed to the world at large, through any channel, secure or insecure.

Keyring

A keyring is a document which holds a collection of keys

Private keyring

A private keyring is a document which contains private keys only.

Public keyring

A public key ring is a document which contains public keys only.

Key Management

With conventional encryption, a fundamental requirement for two parties to communicate securely is that they share a private key. Suppose Bob wants to create a messaging application that will enable him to exchange e-mail securely with anyone who has access to the Internet or to some other network that the two of them share (e.g., an on-line service such as Compuserve). Suppose Bob wants to do this using only conventional encryption. With conventional encryption, Bob and his correspondent, say, Alice, must come up with a way to share of a unique private key that no one else knows. How are they going to do that? If Alice is in the next room from Bob, Bob could generate a key and write it down on a piece of paper or store it on a diskette and hand it to Alice. But if Alice is on the other side of the continent or the world, what can Bob do? Well, he could encrypt this key using conventional encryption and e-mail it to Alice, but this means that Bob and Alice must share a private key in order to encrypt this new private key. Furthermore, Bob and everyone else who uses this new e-mail package faces the same problem with every potential correspondent: Each pair of correspondents must share a unique private key.

How to distribute private keys securely is the most difficult problem for conventional encryption. This problem is wiped away with public-key encryption by the simple fact that the private key is never distributed. If Bob wants to correspond with Alice and other people, he generates a single pair of keys, one private and one public. He keeps the private key secure and broadcasts the public key to all and sundry. If Alice does the same, then Bob has Alice's public key, Alice has Bob's public key, and they can now communicate securely. It is only fair to point out, however, that we have replaced one problem with another. Bob's private key is secure since he need never reveal it. However, Alice must be sure that the public key with Bob's name written all over it is in fact Bob's public key. Someone else could have broadcast a public key and said it was Bob's.

AUTHENTICATION

Suppose that Bob and Alice share a private key for conventional encryption and that Alice receives an encrypted message that is allegedly from Bob. Alice decrypts the message and recovers intelligible plaintext. Conclusion: This is a genuine message from Bob, since Bob is the only person other than Alice who knows the shared private key. One weak spot in this arrangement is that Bob can send Alice a message and later deny it. What would be the point? Well, suppose Bob is an investor and Alice a broker. On Monday Bob sends Alice a message with instructions to buy a thousand shares of Speculative Unlimited. On Tuesday the stock drops 10 points on bad news. On Wednesday Bob gets a written confirmation of the Monday trade and promptly denies that he ever gave such instructions. Can Alice prove otherwise? No, because Alice could have easily generated the buy order, encrypted it with the key she shares with Bob, and then decrypted her own message! Public-key encryption solves this problem. This time, let us say Bob sends a message to Alice encrypted with his private key. Alice decrypts the message, using Bob's public key, but also retains the encrypted version. If Bob later denies he sent the message, all

Alice has to do is present a judge or other arbitrator with the ciphertext, the plaintext, and Bob's public key. The arbitrator can confirm that the ciphertext translates into the plaintext in question with Bob's public key, and that the ciphertext must therefore have been created by Bob with his private key.

INDEX