PGP Freeware
for MacOS

User’s Guide

Version 7.0

PGP*, Version 7.0.3

01-2001. Printed in the United States of America.

Network Associates, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

(972) 308-9960 main
http://www.nai.com

***** is sometimes used instead of the ® for registered trademarks to protect marks registered outside of the U.S.

LIMITED WARRANTY

Limited Warranty. Network Associates Inc. warrants that the Software Product will perform substantially in accordance with the accompanying written materials for a period of sixty (60) days from the date of original purchase. To the extent allowed by applicable law, implied warranties on the Software Product, if any, are limited to such sixty (60) day period. Some jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies. Network Associates Inc's and its suppliers' entire liability and your exclusive remedy shall be, at Network Associates Inc's option, either (a) return of the purchase price paid for the license, if any or (b) repair or replacement of the Software Product that does not meet Network Associates Inc's limited warranty and which is returned at your expense to Network Associates Inc. with a copy of your receipt. This limited warranty is void if failure of the Software Product has resulted from accident, abuse, or misapplication. Any repaired or replacement Software Product will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, neither these remedies nor any product support services offered by Network Associates Inc. are available without proof of purchase from an authorized international source and may not be available from Network Associates Inc. to the extent they subject to restrictions under U.S. export control laws and regulations.

NO OTHER WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT FOR THE LIMITED WARRANTIES SET FORTH HEREIN, THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" AND NETWORK ASSOCIATES, INC. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, CONFORMANCE WITH DESCRIPTION, TITLE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM JURISDICTION TO JURISDICTION.

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL NETWORK ASSOCIATES, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES OR LOST PROFITS WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF NETWORK ASSOCIATES, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, NETWORK ASSOCIATES, INC'S CUMULATIVE AND ENTIRE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE PURCHASE PRICE PAID FOR THIS LICENSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Table of Contents

Part I: Overview

Part II: Working with Keys

Part III: Securing Your Files and Communications

Part IV: Securing Your Network Communications with PGPnet

Part V: Appendices and Glossary

Part I: Overview

Preface

PGP is part of your organization’s security toolkit for protecting one of your most important assets: *information*. Corporations have traditionally put locks on their doors and file cabinets and require employees to show identification to prove that they are permitted access into various parts of the business site. PGP is a valuable tool to help you protect the security and integrity of your organization’s data and messages. For many companies, loss of confidentiality means loss of business.

This guide describes how to use PGP® Freeware for the Macintosh. PGP Freeware (also referred to in this document simply as PGP) has many new features, which are described in the *ReadMe.txt* file that accompanies the product.

NOTE: If you are new to cryptography and would like an overview of the terminology and concepts you will encounter while using PGP, see *An Introduction to Cryptography*, which is included with the product.

Organization of this Guide

This Guide is divided into the following parts and chapters:

Part I, “The Basics”

This section introduces you to the features of PGP and gives you a quick look at the PGP user interface. Part I includes the following chapters:

- Chapter 1, “PGP Basics,” provides an overview of the capabilities of PGP and how PGP fits into the larger security structure of an organization.
- Chapter 2, “A Quick Tour of PGP,” provides you with a brief introduction to accessing PGP utilities from your desktop.

Part II, “Working With Keys”

This section introduces the important concept of *keys*, which are fundamental to data encryption. Part II includes the following chapters:

- Chapter 3, “Making and Exchanging Keys,” explains the concept of a data encryption key and describes how you create, protect, exchange, and validate keys.
- Chapter 4, “Managing Keys,” provides you with more details of key maintenance, including managing your *keyring*, examining and changing *key properties*, creating *split keys*.

Part III “Securing Your Files and Communications”

This section explains how to use your data encryption keys to secure data that you send from or store on your computer. Part III includes the following chapters:

- Chapter 5, “Securing Email,” describes how to send encrypted email, and how to decrypt and verify email you receive.
- Chapter 6, “Securing Files,” describes how to use PGP to securely maintain files, either for email or for storage on your computer.

Part IV, “Securing Your Network Communications with PGPnet”

This section describes the features of PGPnet, a PGP tool that enables you to create Virtual Private Networks (VPNs) with trusted users not directly connected to your network. The chapters of Part IV also guide you through configuring the features of PGPnet to customize the security of your workstation. Part IV includes the following chapters:

- Chapter 7, “PGPnet Basics,” gives you an overview of Virtual Private Networks.

- Chapter 8, "A Quick Tour of PGPnet," introduces you to aspects of PGP's user interface that are related to PGPnet.
- Chapter 9, "Configuring PGPnet's VPN Feature," describes how to use PGPnet to set up and customize a Virtual Private Network (VPN).

Part V, "Appendices and Glossary"

This section includes information on how to further customize PGP on your computer, as well as troubleshooting tips should you encounter problems using PGP. A Glossary is included as a convenient reference spot where you will find definitions of terms related to network security. Part V includes the following appendices:

- Appendix A, "Setting Preferences," explains how to use the Preferences dialog box to create a version of PGP on your computer that best suits your needs.
- Appendix B, "Troubleshooting PGP," guides you in solving problems you may encounter when using PGP.
- Appendix C, "Troubleshooting PGPnet," guides you in solving problems you may encounter when using PGP's PGPnet feature.
- Appendix D, "Transferring Files Between the MacOS and Windows," explains how PGP translates files that are sent between two systems when one system operates using a Mac operating system (OS) and the other system operates using a Windows OS.
- Appendix E, "Biometric Word Lists," explains biometric word lists and how they are used by PGP.
- Glossary, page 203, provides you with definitions for many terms related to PGP and network security.

How to contact PGP Security and Network Associates

Customer service

Network Associates continues to market and support the product lines from each of the new independent business units. You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to the Network Associates Customer Service department at the following address:

Network Associates Customer Service
4099 McEwen, Suite 500
Dallas, Texas 75244
U.S.A.

The department's hours of operation are 8 A.M. to 8 P.M. Central time, Monday through Friday.

Other contact information for corporate-licensed customers:

Phone:	(972) 308-9960
E-Mail:	services_corporate_division@nai.com
World Wide Web:	http://support.nai.com

Other contact information for retail-licensed customers:

Phone:	(972) 308-9960
E-Mail:	cust_care@nai.com
World Wide Web:	http://www.pgp.com/

Technical support

Network Associates does not provide technical support for freeware products.

Network Associates training

For information about scheduling on-site training for any PGP Security or Network Associates product, call Network Associates Customer Service at: (972) 308-9960.

Comments and feedback

PGP Security appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please send any documentation comments to **tns_documentation@nai.com**.

Recommended readings

This section identifies Web sites, books, and periodicals about the history, technical aspects, and politics of cryptography, as well as trusted PGP download sites.

The history of cryptography

- *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., 1999, ISBN 0-385-49531-5.
- *The Codebreakers: The Story of Secret Writing*, David Kahn, Simon & Schuster Trade, 1996, ISBN 0-684-83130-9 (updated from the 1967 edition). This book is a history of codes and code breakers from the time of the Egyptians to the end of WWII. Kahn first wrote it in the sixties—this is the revised edition. This book won't teach you anything about how cryptography is done, but it has been the inspiration of the whole modern generation of cryptographers.

Technical aspects of cryptography

Web sites

- www.iacr.org—International Association for Cryptologic Research (IACR). The IACR holds cryptographic conferences and publishes journals.
- www.pgpi.org—An international PGP Web site, which is not maintained by PGP Security, Inc. or Network Associates, Inc., is an unofficial yet comprehensive resource for PGP.
- www.nist.gov/aes—The National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) Development Effort, perhaps the most interesting project going on in cryptography today.
- www.ietf.org/rfc/rfc2440.txt—The specification for the IETF OpenPGP standard.

Books and periodicals

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edition, Bruce Schneier, John Wiley & Sons, 1996; ISBN 0-471-12845-7. If you can only buy one book to get started in cryptography, this is the one to buy.
- *Handbook of Applied Cryptography*, Alfred Menezes, Paul van Oorschot and Scott Vanstone, CRC Press, 1996; ISBN 0-8493-8523-7. This is the technical book you should get after Schneier. There is a lot of heavy-duty math in this book, but it is nonetheless usable for those who do not understand the math.
- *Journal of Cryptology*, International Association for Cryptologic Research (IACR). See www.iacr.org.
- *Advances in Cryptology*, conference proceedings of the IACR CRYPTO conferences, published yearly by Springer-Verlag. See www.iacr.org.
- *Cryptography for the Internet*, Philip Zimmermann, Scientific American, October 1998 (introductory tutorial article).
- *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*, Bruce Schneier, et al, John Wiley & Sons, Inc., 1999; ISBN: 0471353817. Contains details about the Twofish cipher ranging from design criteria to cryptanalysis of the algorithm.

Politics of cryptography

Web sites

- www.epic.org—Electronic Privacy Information Center.
- www.crypto.org—Internet Privacy Coalition.
- www.eff.org—Electronic Frontier Foundation.
- www.privacy.org—The Privacy Page. Great information resource about privacy issues.
- www.cdt.org—Center for Democracy and Technology.
- www.pgp.com / phil—Phil Zimmermann's home page, his Senate testimony, and so on.

Books

- *Privacy on the Line: The Politics of Wiretapping and Encryption*, Whitfield Diffie and Susan Landau, The MIT Press, 1998, ISBN 0-262-04167-7. This book is a discussion of the history and policy surrounding cryptography and communications security. It is an excellent read, even for beginners and non-technical people. Includes information that even a lot of experts don't know.
- *Technology and Privacy: The New Landscape*, Philip Agre and Marc Rotenberg, The MIT Press, 1997;ISBN 0-262-01162-x.
- *Building in Big Brother, The Cryptographic Policy Debate*, edited by Lance Hoffman, Springer-Verlag, 1995; ISBN 0-387-94441-9.
- *The Official PGP User's Guide*, Philip Zimmermann, The MIT Press, 1995; ISBN 0-262-74017-6. How to use PGP, written in Phil's own words.
- *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. This book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography.

Network security

Books

- *Building Internet Firewalls*, Elizabeth D. Zwicky, D. Brent Chapman, Simon Cooper, and Deborah Russell (Editor), O'Reilly & Associates, Inc., 2000; ISBN: 1565928717. This book is a practical guide to designing, building, and maintaining firewalls.
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick, Steven M. Bellovin, Addison Wesley Longman, Inc., 1994; ISBN: 0201633574. This book is a practical guide to protecting networks from hacker attacks through the Internet.
- *Hacking Exposed: Network Security Secrets and Solutions*, Stuart McClure, Joel Scambray, and George Kurtz, The McGraw-Hill Companies, 1999; ISBN: 0072121270. The state of the art in breaking into computers and networks, as viewed from the vantage point of the attacker and the defender.

PGP Basics 1

This chapter provides you with an overview of how PGP Freeware fits into the larger security structure of your organization and how PGP Freeware strengthens that security structure. PGP's features are outlined, and you will get a quick look at the procedures you normally follow in the course of using PGP.

PGP as part of your security structure

Your company has various means by which it can protect information. It can physically lock doors to the building and specific rooms in the building, making those places accessible only to authorized personnel. It can require employees to use passwords to log on to the network. It can control the flow of information traffic between the corporate network and outside networks by setting up one computer as a firewall server that all information must pass through. These are all mechanisms by which a corporation can bolster the security of its information.

PGP Freeware adds to this security system by offering information protection for *individual* computers. The types of added security include:

1. data encryption, including email, stored files, and instant messaging
2. virtual private networking, for secure remote communications

Data encryption enables users to protect information that they send out—such as emails—as well as information that they store on their own computers. Files and messages are encrypted with a user's *key*, which works in conjunction with scrambling algorithms to produce data that can be decrypted only by its intended recipients.

Data encryption is also an important part of a Virtual Private Network (VPN): information is first encrypted and then sent in this secure form over the Internet—an otherwise very insecure medium—to a remote host. Virtual Private Networks are a feature of PGPnet, which is a PGP tool used for setting up VPNs.

You should now be familiar with an overall picture of what PGP does. The next section lists the features of PGP and gives references to specific chapters in this User's Guide for more detailed information.

PGP features

PGP offers several features and utilities to help you secure your email, files, disk, and network traffic with encryption and authentication.

Here is what you can do with PGP:

- **Encrypt/sign and decrypt/verify within any application.** With the PGP menus and email plug-ins, you can access PGP functions while in any application. To learn how to access PGP, see Chapter 2, “A Quick Tour of PGP.” To learn how to encrypt/sign and decrypt/verify, see “Part III: Securing Your Files and Communications.”
- **Create and manage keys.** Use PGPkeys to create, view, and maintain your own PGP key pair as well as any public keys of other users that you have added to your public keyring. To learn how to create a key pair, see Chapter 3, “Making and Exchanging Keys.” To learn about managing your keys, see Chapter 4, “Managing Keys.”
- **Create self-decrypting archives (SDAs).** You can create self-decrypting executable files that anyone can decrypt with the proper password. This feature is especially convenient for sending encrypted files to people who do not have PGP installed. For more information about SDAs, see Chapter 6, “Securing Files.”
- **Permanently erase files, folders, and free disk space.** You can use the PGPtools utility to thoroughly delete your sensitive files and folders without leaving fragments of their data behind. You can also use PGPtools to erase the free disk space on your hard drive that contains data from previously deleted files and programs. Both utilities ensure that your deleted data is unrecoverable. To learn about file, folder, and free space wiping, see “Permanently erasing files and free disk space” on page 109.
- **Secure network traffic.** You can use PGPnet, a *Virtual Private Network (VPN),* to communicate securely and economically with other PGPnet users over the internet. To learn more about PGPnet and its components, see “Part IV: Securing Your Network Communications with PGPnet.”

Basic steps for using PGP

1. **Install PGP on your computer.**

   Refer to the *PGP Installation Guide* or the *ReadMe* file that accompanies the product for complete installation instructions.

2. **Create a private and public key pair.**

   Before you can begin using PGP, you need to generate a key pair.

   You have the option of creating a new key pair during the PGP installation procedure, or you can do so at any time by opening the PGPkeys application.

   You need a key pair to:

   - encrypt information
   - decrypt information that has been encrypted to your key
   - sign information

   For more information about creating a private and public key pair, refer to "Making a key pair" on page 32.

3. **Exchange public keys with others.**

   After you have created a key pair, you can begin corresponding with other PGP users. You will need a copy of their public key and they will need yours. Your public key is just a block of text, so it's quite easy to trade keys with someone. You can include your public key in an email message, copy it to a file, or post it on a public or corporate key server where anyone can get a copy when he or she needs it.

   For more information about exchanging public keys, refer to "Exchanging public keys with others" on page 43.

4.Validate public keys.

Once you have a copy of someone's public key, you can add it to your public keyring. You should then check to make sure that the key has not been tampered with and that it really belongs to the purported owner. You do this by comparing the unique *fingerprint* on your copy of someone's public key to the fingerprint on that person's original key. When you are sure that you have a valid public key, you sign it to indicate that you feel the key is safe to use. In addition, you can grant the owner of the key a level of trust indicating how much confidence you have in that person to vouch for the authenticity of someone else's public key.

For more information about validating your keys, refer to "Verifying the authenticity of a key" on page 49.

5. **Start securing your email and files.**

   After you have generated your key pair and have exchanged public keys, you can begin encrypting, signing, decrypting and verifying your email messages and files.

   To perform a PGP task, you must select the file or email message that you want to secure and then choose your task (Encrypt, Sign, Decrypt, or Verify) from a PGP menu. PGP menus are available from most applications. To learn how to access a PGP menu, see Chapter 2, "A Quick Tour of PGP."

   For detailed instructions about securing email and files, refer to "Part III: Securing Your Files and Communications." For more information about securing your network communications, refer to "Part IV: Securing Your Network Communications with PGPnet."

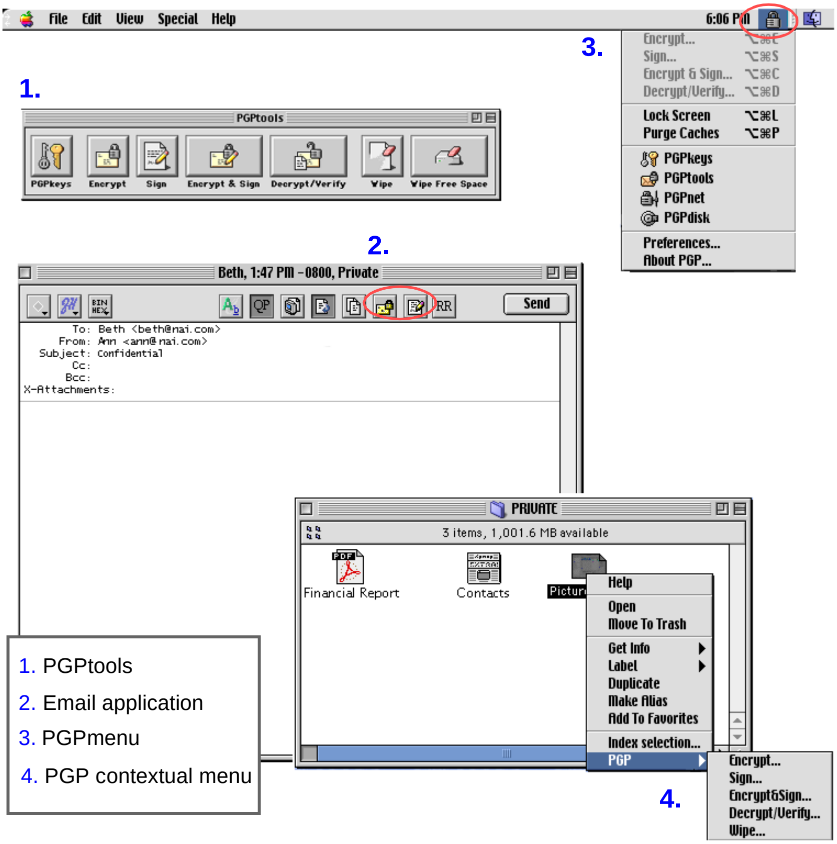
6. **Wipe files.**

   When you need to permanently delete a file, you can use the Wipe feature to ensure that the file is unrecoverable. The file is immediately overwritten so that it cannot be retrieved using disk recovery software.

   For more information about wiping files, refer to "Permanently erasing files and free disk space" on page 109.

A Quick Tour of PGP 2

The way in which you access PGP largely depends on your preference—what is easiest at the time. PGP works on the data generated by other applications. Therefore, the appropriate PGP functions are designed to be immediately available to you based on the task you are performing at any given moment.



To: Beth <beth@nai.com>
From: Ann <ann@nai.com>
Subject: Confidential
Cc:
Bcc:
X-Attachments:

Figure 2-1. Accessing PGP

PGPtools

If you are using an email application that is not supported by the plug-ins, or if you want to perform PGP functions from within other applications, you can encrypt and sign, decrypt and verify, or securely wipe messages and files directly from PGPtools. You can open PGPtools (as shown in Figure 2-1, #1) from your PGP folder or from PGPmenu which is located in the Finder (as shown in Figure 2-1, #3).

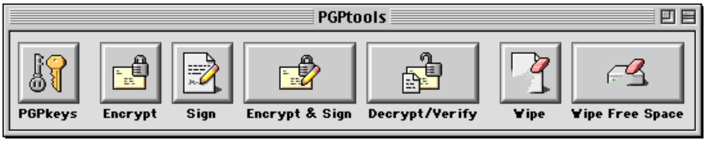


Figure 2-2. PGPtools

If you are working with text or files, you can encrypt, decrypt, sign, and verify by selecting the text or file and then dragging it onto the appropriate button in PGPtools.

If you are working with files, click on the appropriate button in PGPtools to choose a file or select the Clipboard data.

PGP within supported email applications

PGP “plugs in” to many popular email applications. With these plug-ins, you can perform most PGP operations with a simple click of a button while you are composing and reading your mail.

If you are using an email application that is not supported by the plug-ins, you can easily encrypt / decrypt messages using one of the other PGP utilities.

PGP has plug-ins for the following email applications:

- Qualcomm Eudora 3.0 - 4.0
- Claris Emailer 2.0
- Outlook Express 4.0 and greater

When a PGP plug-in is installed, **Encrypt** and **Sign** buttons appear in your application's toolbar (as shown in Figure 2-1, #2). You click the envelope and lock icon (🔏) to indicate that you want to encrypt your message, and the pen and paper icon (📝) to indicate that you want to sign your message. Some applications also have an icon of both a lock and quill, which lets you encrypt and sign at once. For more information about using PGP within email applications, see Chapter 5, "Securing Email."

PGPmenu

NOTE: You can access many of the main PGP functions by clicking the gray lock icon (🔒), which is located in the Finder, and then choosing the appropriate menu item. This feature gives you immediate access to the PGP functions regardless of which application you are using.

NOTE: PGPmenu offers direct support for Outlook Express 4.0 or greater and Claris Emailer.

While using email or other text-based applications to which you have added PGPmenu, you can encrypt and sign and decrypt and verify text by choosing **Preferences** from PGPmenu. While in the **Finder**, you can encrypt, sign, decrypt, verify, lock down your computer screen, and open other PGP applications as shown in Figure 2-3.

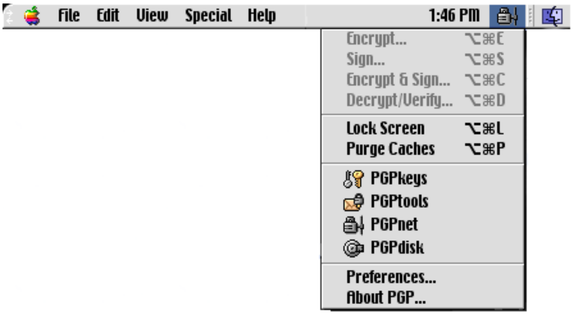


Figure 2-3. PGPmenu

NOTE: If you cannot find PGPmenu in one of your applications, you need to add the application to the **Menu** panel of the **Preferences** dialog box. For more information on setting preferences, see Appendix A, "Setting Preferences".

The PGP contextual menu, and other shortcuts

Although you will find that PGP is quite easy to use, a number of shortcuts are available to help you accomplish your encryption tasks even quicker. For example, you can perform most PGP functions on files or volumes on your disk using PGP contextual menu (for Mac OS 8 users), PGPmenu (for System 7 users), or by dragging the file or volume and dropping it onto one of the PGPtools icons. You can also drag a file containing a key into the PGPkeys window to add it to your keyring.

Getting Help

When you choose **Help** from PGPmenu or from the **Help** menu within PGPkeys, you access the PGP Help system, which provides a general overview and instructions for all of the procedures you are likely to perform.

Part II: Working with Keys

Making and Exchanging Keys 3

This chapter describes how to generate the public and private key pairs that you need to correspond with other PGP users. It also explains how to distribute your public key and obtain the public keys of others so that you can begin exchanging private and authenticated email.

“Key” concepts

PGP is based on a widely accepted and highly trusted *public key encryption* system, as shown in Figure 3-1, by which you and other PGP users generate a key pair consisting of a *private* key and a *public* key. As its name implies, only you have access to your private key, but in order to correspond with other PGP users you need a copy of their public key and they need a copy of yours. You use your private key to sign the email messages and file attachments you send to others and to decrypt the messages and files they send to you. Conversely, you use the public keys of others to send them encrypted email and to verify their digital signatures.

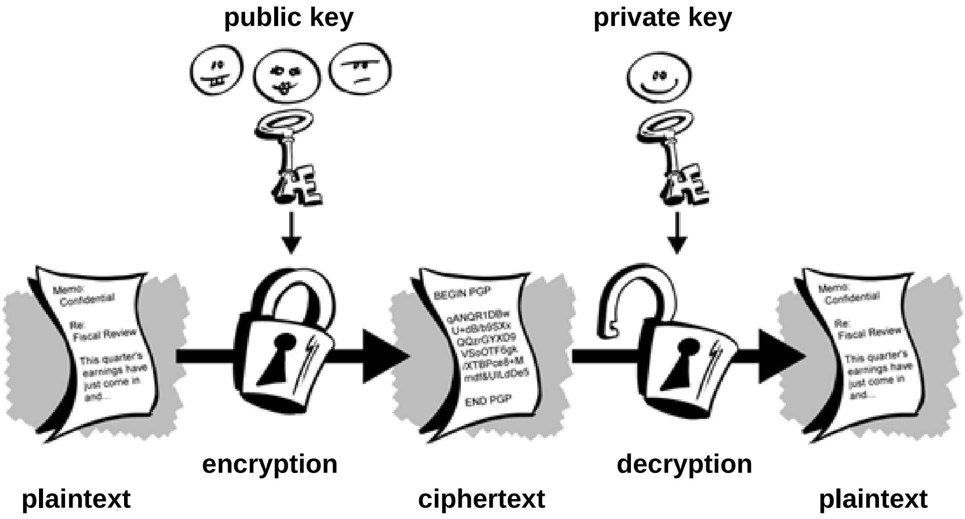


Figure 3-1. Public Key Cryptography diagram

Making a key pair

Unless you have already done so while using another version of PGP, the first thing you need to do before sending or receiving encrypted and signed email is create a new key pair. You generate a new key pair from PGPkeys using the PGP Key Generation Wizard, which guides you through the process. However, if you have not already created a new key pair, the PGP Key Generation Wizard leads you through the necessary steps.

NOTE: If you have an existing key pair, specify the location of your keys when you run the PGPkeys application. You can go to the **Files** panel of the **Preferences** dialog box and locate your keyring files at any time.

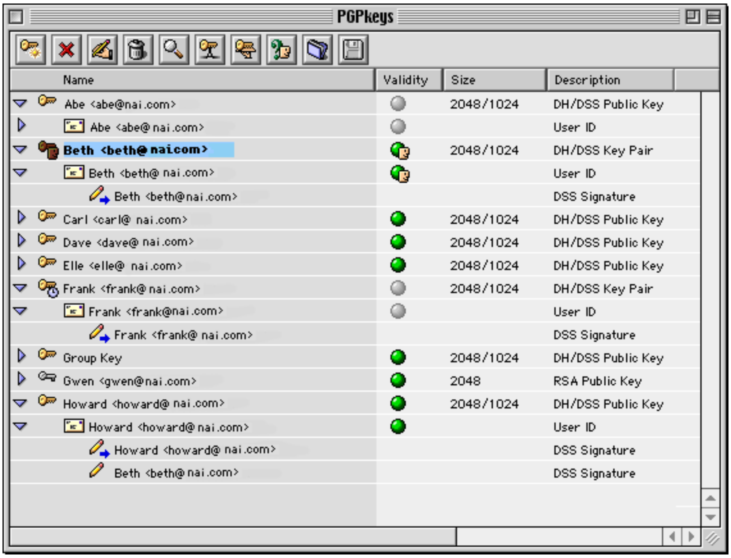
IMPORTANT: Although it’s fun, try not to create more than one key pair unless you need to. When another user wants to send you email, it might confuse them if you have more than one key pair. Also, you might not remember all of the passwords for each key pair.

To create a new key pair:

1. Open PGPkeys. You can open PGPkeys by:

   - Double-clicking the PGPkeys icon in the PGP folder.
   - Clicking the PGPmenu icon (🔒) in the Finder, then selecting **PGPkeys**

   The PGPkeys window (Figure 3-2 on page 33) displays the private and public key pairs you have created for yourself, as well as any public keys of other users that you have added to your public keyring. It is from this window that you will perform all future key management functions.



Name	Validity	Size	Description
Abe <abe@nai.com>	○	2048/1024	DH/DSS Public Key
Abe <abe@nai.com>	○		User ID
Beth <beth@naicom>	●	2048/1024	DH/DSS Key Pair
Beth <beth@nai.com>	●		User ID
Beth <beth@nai.com>			DSS Signature
Carl <carl@nai.com>	●	2048/1024	DH/DSS Public Key
Dave <dave@nai.com>	●	2048/1024	DH/DSS Public Key
Elle <elle@nai.com>	●	2048/1024	DH/DSS Public Key
Frank <frank@nai.com>	○	2048/1024	DH/DSS Key Pair
Frank <frank@nai.com>	○		User ID
Frank <frank@nai.com>			DSS Signature
Group Key	●	2048/1024	DH/DSS Public Key
Gwen <gwen@nai.com>	●	2048	RSA Public Key
Howard <howard@nai.com>	●	2048/1024	DH/DSS Public Key
Howard <howard@nai.com>	●		User ID
Howard <howard@nai.com>			DSS Signature
Beth <beth@nai.com>			DSS Signature

Figure 3-2. PGPkeys

2. Click 🔑 in the PGPkeys menu bar.

   The PGP Key Generation Wizard provides some introductory information on the first screen.

3. After you read this information, click **Next** to advance to the next panel.

   Click the **Expert** button if you want to create a custom key. You can choose the type of key to generate, specify a key size, and set an expiration date. If you want to create a custom key, continue with the instructions outlined in "To generate a custom key:" on page 35.

   The PGP Key Generation Wizard asks you to enter your name and email address.

4. Enter your name in the **Name** box and your email address in the **Email** box.

5. It is not absolutely necessary to enter your real name or even your email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, by using your correct email address, you and others can take advantage of the plug-in feature that automatically looks up the appropriate key on your current keyring when you address mail to a particular recipient. Click **Next** to continue.

   The PGP Key Generation Wizard asks you to enter a passphrase.

6. In the **Passphrase** dialog box, enter the string of characters or words you want to use to maintain exclusive access to your private key. To confirm your entry, press the TAB key to advance to the next line, then enter the same passphrase again.

   Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, clear the **Hide Typing** checkbox.

   NOTE: Your passphrase should contain multiple words and may include spaces, numbers, and punctuation characters. Choose something that you can remember easily but that others won't be able to guess. The passphrase is case sensitive, meaning that it distinguishes between uppercase and lowercase letters. The longer your passphrase, and the greater the variety of characters it contains, the more secure it is. Strong passphrases include upper and lowercase letters, numbers, punctuation, and spaces but are more likely to be forgotten. See "Creating a passphrase that you will remember" on page 38, for more information about choosing a passphrase.

   WARNING: Unless your administrator has implemented a PGP key reconstruction policy for your company, no one, including Network Associates, can salvage a key with a forgotten passphrase.

7. Click **Next** to begin the key generation process.

   The PGP Key Generation Wizard indicates that it is busy generating your key.

   If you have entered an inadequate passphrase, a warning message appears before the keys are generated and you have the choice of accepting the bad passphrase or entering a more secure one before continuing. For more information about passphrases, see "Creating a passphrase that you will remember" on page 38.

   Your mouse movements and keystrokes generate random information that is needed to create a unique key pair. If there is not enough random information upon which to build the key, the **PGP Random Data** dialog box appears. As instructed in the dialog box, move your mouse around and enter a series of random keystrokes until the progress bar is completely filled in.

NOTE: PGPkeys continually gathers random data from many sources on the system, including mouse positions, timings, and keystrokes. If the **Random Data** dialog box does not appear, it indicates that PGP has already collected all the random data that it needs to create the key pair.

After the key generation process begins, it may take a while to generate the keys.

When the key generation process is complete, the final panel appears.

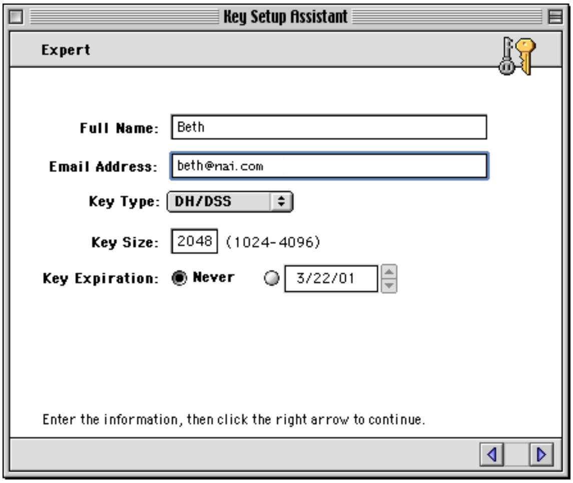
8. Click **Finish**. PGP automatically puts your private key on your private keyring and your public key on your public keyring.

Once you have created a key pair, you can use PGPkeys to create new key pairs and manage all of your other keys. For instance, this is where you examine the attributes associated with a particular key, specify how confident you are that the key actually belongs to the alleged owner, and indicate how well you trust the owner of the key to vouch for the authenticity of other users' keys. For a complete explanation of the key management functions you perform from the PGPkeys window, see Chapter 4.

To generate a custom key:

1. Follow steps 1 - 2 in "To create a new key pair:" on page 32.
2. At the **Key Generation Wizard Welcome** screen, click the **Expert** button to choose the key type, size, and / or an expiration date.

   The **Key Generation Wizard Expert** panel appears, as in Figure 3-3 on page 36.



Full Name: Beth

Email Address: beth@nai.com

Key Type: DH/DSS

Key Size: 2048 (1024-4096)

Key Expiration: ● Never ○ 3/22/01

Enter the information, then click the right arrow to continue.

Figure 3-3. Key Generation Wizard
(Expert Panel)

3. Select a key type from the **Key Type** box**.**

   Choose **Diffie-Hellman/DSS** if you want to take advantage of many PGP key features including Additional Decryption Key (ADK), designated revoker, multiple encryption subkeys, and photo ID.

   Choose **RSA** or **RSA Legacy** if you plan to correspond with people who are using RSA keys.

   The RSA key format provides support for PGP's Additional Decryption Key (ADK), designated revoker, multiple encryption subkeys and photo ID features. Previously these features were only available to users with Diffie-Hellman keys. PGP will continue to support users who have RSA keys in the older key format (now called the RSA Legacy key format).

   IMPORTANT: The RSA key type is only fully compatible with PGP versions 7.0 and above and other OpenPGP applications.

   Choose the RSA Legacy key format only if those you communicate with are using older versions of PGP; otherwise choose the new RSA key format. RSA Legacy keys do not support many of the newer PGP key features.

4. Click **Next**.

5. In the **Key Size** box, select a key size from 1024 to 4096 bits for Diffie-Hellman / DSS keys and 1024 to 2048 for RSA keys.

   NOTE: A large key size may take a long time to generate, depending on the speed of the computer you are using.

   The key size corresponds to the number of bits used to construct your digital key. The larger the key, the less chance that someone will be able to crack it, but the longer it takes to perform the decryption and encryption process. You need to strike a balance between the convenience of performing PGP functions quickly with a smaller key and the increased level of security provided by a larger key. Unless you are exchanging extremely sensitive information that is of enough interest that someone would be willing to mount an expensive and time-consuming cryptographic attack in order to read it, you are probably safe using a key composed of 1024 bits.

   NOTE: When creating a Diffie-Hellman / DSS key pair, the size of the DSS portion of the key is less than or equal to the size of the Diffie-Hellman portion of the key and is limited to a maximum size of 1024 bits.

6. Indicate when you want your keys to expire. You can either use the default selection, which is **Never**, or you can enter a specific date after which the keys will expire.

   Once you create a key pair and have distributed your public key to the world, you will probably continue to use the same keys from that point on. However, under certain conditions you may want to create a special key pair that you plan to use for only a limited period of time. In this case, when the public key expires, it can no longer be used by someone to encrypt mail to you but it can still be used to verify your digital signature. Similarly, when your private key expires, it can still be used to decrypt mail that was sent to you before your public key expired but can no longer be used to sign mail to others.

7. Follow Step 6 through Step 8 on page 34 to complete your key generation.

   A key pair representing your newly created keys appears in the PGPkeys window. At this point you can examine your keys by checking their properties and the attributes associated with the keys; you may also want to add other email addresses that belong to you. See “Changing your key pair” on page 39, for details about modifying the information in your key pair.

Creating a passphrase that you will remember

Encrypting a file and then finding yourself unable to decrypt it is a painful lesson in learning how to choose a passphrase you will remember. Most applications require a single word password between three and eight letters. For a couple of reasons we do not recommend that you use a single-word passphrase. A single word password is vulnerable to a dictionary attack, which consists of having a computer try all the words in the dictionary until it finds your password. To protect against this manner of attack, it is widely recommended that you create a word that includes a combination of upper and lowercase alphabetic letters, numbers, punctuation marks, and spaces. This results in a stronger password, but an obscure one that you are unlikely to remember easily.

Trying to thwart a dictionary attack by arbitrarily inserting a lot of funny non-alphabetic characters into your passphrase has the effect of making your passphrase too easy to forget and could lead to a disastrous loss of information because you can’t decrypt your own files. A multiple word passphrase is less vulnerable to a dictionary attack. However, unless the passphrase you choose is something that is easily committed to long-term memory, you are unlikely to remember it verbatim. Picking a phrase on the spur of the moment is likely to result in forgetting it entirely. Choose something that is already residing in your long-term memory. It should not be something that you have repeated to others recently, nor a famous quotation, because you want it to be hard for a sophisticated attacker to guess. If it’s already deeply embedded in your long-term memory, you probably won’t forget it.

Of course, if you are reckless enough to write your passphrase down and tape it to your monitor or to the inside of your desk drawer, it won't matter what you choose.

Changing your key pair

Once you create your key, you can add, remove, or change a number of items in your key pair at any time.

To:	See:
add a photographic ID	"Adding a photographic ID to your key" on page 68
add additional subkeys	"Creating new subkeys" on page 70
add a new user name and email address	"Adding a new user name or address to your key pair" on page 67
add or remove signatures	"Deleting a key or signature on your PGP keyring" on page 58
change your passphrase	"Changing your passphrase" on page 66
add designated revokers	"Appointing a designated revoker" on page 74.
add an X.509 certificate	"Adding an X.509 certificate to your PGP key" on page 76.
split a key into multiple shares	"Splitting and rejoining keys" on page 80

Backing up your keys

Once you have generated a key pair, it is wise to put a copy of it in a safe place in case something happens to the original. PGP prompts you to save a backup copy when you close the PGPkeys application after creating a new key pair.

Your private and public keys are stored in separate keyring files. You can copy them to another location on your hard drive or to a floppy disk. By default, the private keyring (PGP Private Keys) and the public keyring (PGP Public Keys) are stored along with the other program files in your "PGP" folder; you can save your backups in any location you like.

You can configure PGP to back up your keyrings automatically after you close PGP. Your keyring backup preferences can be set in the **Advanced** panel of the **Preferences** dialog box. See "Setting advanced preferences" on page 166 for more information.

Protecting your keys

Besides making backup copies of your keys, you should be especially careful about where you store your private key. Even though your private key is protected by a passphrase that only you should know, it is possible that someone could discover your passphrase and then use your private key to decipher your email or forge your digital signature. For instance, somebody could look over your shoulder and watch the keystrokes you enter or intercept them on the network or even over the Internet.

To prevent anyone who might happen to intercept your passphrase from using your private key, store your private key only on your own computer. If your computer is attached to a network, make sure that your files are not automatically included in a system-wide backup where others might gain access to your private key. Given the ease with which computers are accessible over networks, if you are working with extremely sensitive information, you may want to keep your private key on a floppy disk, which you can insert like an old-fashioned key whenever you want to read or sign private information.

As another security precaution, consider assigning a different name to your private keyring file and then storing it somewhere other than in the default location. Use the **Files** panel of the **Preferences** dialog box to specify a name and location for your private and public keyring files. For more information, see “Setting file preferences” on page 155.

What if I forget my passphrase or lose my key?

If you lose your key or forget your passphrase and do not have a backed up copy from which to restore your key, you will never again be able to decrypt any information encrypted to your key. You can, however, reconstruct your key if you implemented a PGP key restoration policy, where your key is encrypted and stored on a PGP key reconstruction server.

What is PGP key reconstruction?

A PGP key reconstruction server can be set up to act as sort of a safety-net for you if you lose your private key or passphrase. The reconstruction server stores your key in such a way that only you can access it.

If you incorporated key reconstruction as part of your security policy, you will be prompted to enter additional “secret” information when you create your PGP key pair or when you choose **Send to... Key Reconstruction Server** from the **Server** menu in PGPkeys.

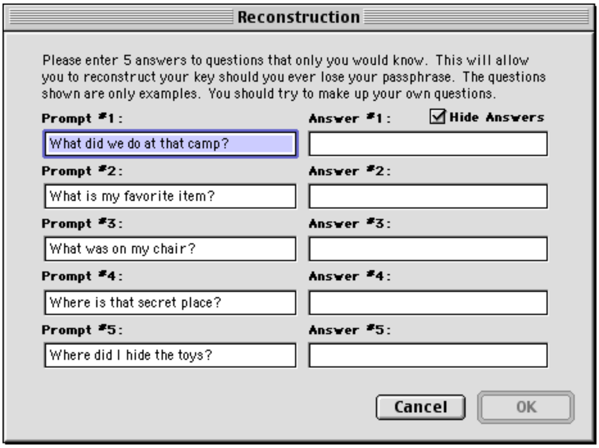
Once your key is on the server, you can restore it at anytime by selecting **Reconstruct Key** from the **Keys** menu in PGPkeys. To learn how to reconstruct your key, see “Reconstructing your key” on page 89.

To send your key to a key reconstruction server:

1. If the **Key Reconstruction** dialog box opened automatically as you created a key pair, continue with Step 3; otherwise, open PGPkeys and select your key pair.

2. Open the **Server/Send To** menu and choose **Copy** from the **Edit** menu.

   The **Key Reconstruction** dialog box appears, as shown in Figure 3-4.



Please enter 5 answers to questions that only you would know. This will allow you to reconstruct your key should you ever lose your passphrase. The questions shown are only examples. You should try to make up your own questions.

☑ Hide Answers

Prompt #1: What did we do at that camp?
Answer #1:

Prompt #2: What is my favorite item?
Answer #2:

Prompt #3: What was on my chair?
Answer #3:

Prompt #4: Where is that secret place?
Answer #4:

Prompt #5: Where did I hide the toys?
Answer #5:

Figure 3-4. Key Reconstruction dialog box

3. In the **Key Reconstruction** dialog box, as shown in Figure 3-4, enter five questions that only you can answer in the **Prompt** boxes (the default questions are examples only). Choose obscure personal questions with answers that you are not likely to forget. Your questions can be up to 95 characters in length.

   An example of a good question might be, “Who took me to the beach?” or “Why did Fred leave?”

   An example of a bad question would be, “What is my mother’s maiden name?” or “Where did I go to high school?”

   NOTE: If you prefer, you can also leave the questions blank and simply provide 5 answers.

4. In the **Answer** boxes, enter the answers to the corresponding questions. Your answers are case sensitive and can be up to 255 characters in length.

   Use the **Hide Answers** checkbox to view or hide your answers.

5. Click **OK** to continue.

   If the **PGP Enter Passphrase for Key** dialog box appears, enter the passphrase for your key, then click **OK**.

   If the **Server User ID and Password** dialog box appears, enter your user ID and password to log on to the server. If you do not know your user ID or password, consult your administrator.

6. Click **OK**.

   Your private key is then split into five pieces, using Blakely-Shamir key splitting. Three of the five pieces are needed to reconstruct the key. Each piece is then encrypted with the *hash*, the uniquely identifying number, of one answer. If you know any 3 answers, you can successfully reconstruct the whole key. To learn how to reconstruct your key, see “Reconstructing your key” on page 89.

Exchanging public keys with others

After you create your keys, you need to exchange keys with those whom you intend to correspond. You make your public key available to others so that they can send you encrypted information and verify your digital signature; to encrypt, you'll need copies of others' keys. Your public key is basically composed of a block of text, so it is quite easy to make it available through a public key server, include it in an email message, or export or copy it to a file. The recipient can then use whatever method is most convenient to add your public key to his or her public keyring.

Distributing your public key

You can distribute your public key in three ways:

- Make your public key available through a public key server
- Include your public key in an email message
- Export your public key or copy it to a text file

Placing your public key on a key server

The best method for making your public key available is to place it on a public key server, which is a large database of keys, where anyone can access it. That way, people can send you encrypted email without having to explicitly request a copy of your key. It also relieves you and others from having to maintain a large number of public keys that you rarely use. There are a number of key servers worldwide, including those offered by Network Associates, Inc., where you can make your key available for anyone to access.

When you're working with a public key server, such as keyserver.pgp.com, keep these things in mind before you send your key.

– Is this the key you intend to use? Others attempting to communicate with you might encrypt important information to that key. For this reason, we strongly recommend that you only put keys on a key server that you intend for others to use.

– Will you remember your passphrase for this key so you can retrieve data encrypted to it or, if you don't want to use the key, so you can revoke it?

– Once it's up there, it's up there. Some public servers have a policy against deleting keys. Others have replication features that replicate keys between key servers, so that even if you are able to delete your key on one server, it will probably reappear later.

To send your public key to a key server:

1. Connect to the Internet.
2. Open PGPkeys.
3. Select the public key to copy to the key server.
4. Open the **Server** menu, then select the key server on which you want to add your key from the **Send To** submenu. (The key server at Network Associates is http://keyserver.pgp.com.) PGP lets you know that the keys are successfully copied to the server.

Once you place a copy of your public key on a key server, it's available to people who want to send you encrypted data or to verify your digital signature. Even if you don't explicitly point people to your public key, they can get a copy by searching the key server for your name or email address. Many people include the Web address for their public key at the end of their email messages. In most cases the recipient can just double-click the address to access a copy of your key on the server. Some people even put their PGP fingerprint on their business cards for easier verification.

Including your public key in an email message

Another convenient method of delivering your public key to someone is to include it with an email message. When you send someone your public key, be sure to sign the email. That way, the recipient can verify your signature and be sure that no one has tampered with the information along the way. Of course, if your key has not yet been signed by any trusted introducers, recipients of your signature can only truly be sure the signature is from you by verifying the fingerprint on your key.

To include your public key in an email message:

1. Open PGPkeys.
2. Select your key pair and then choose **Copy** from the **Edit** menu.
3. Open the editor you use to compose your email messages, place the cursor in the desired area, and then choose **Paste** from the **Edit** menu. In some email applications, you can simply drag your key from PGPkeys into the text of your email message to transfer the key information.

Exporting your public key to a file

Another method of distributing your public key is to copy it to a file and then make this file available to the person with whom you want to communicate.

To export your public key to a file:

There are three ways to export or save your public key to a file:

- Select the icon representing your key pair from PGPkeys, then choose **Export** from the **Keys** menu. Enter the name of the file to which you want to save the key.
- Drag the icon representing your key pair from PGPkeys to the folder where you want to save the key.
- Select the icon representing your key pair in PGPkeys, choose **Copy** from the **Edit** menu, then choose **Paste** to insert the key information into a text document.

NOTE: If you are sending your key to colleagues who are using PCs, enter a name of up to eight initial characters and three additional characters for the file type extension (for example, MyKey.txt).

Obtaining the public keys of others

Just as you need to distribute your public key to those who want to send you encrypted mail or to verify your digital signature, you need to obtain the public keys of others so you can send them encrypted mail or verify their digital signatures.

There are three ways to obtain someone’s public key:

- Get the key from a public key server
- Add the public key to your keyring directly from an email message
- Import the public key from an exported file

Public keys are just blocks of text, so they are easy to add to your keyring by importing them from a file or by copying them from an email message and then pasting them into your public keyring.

Getting public keys from a key server

If the person to whom you want to send encrypted mail is an experienced PGP user, it is likely that a copy of his or her public key is on a key server. This makes it very convenient for you to get a copy of the most up-to-date key whenever you want to send him or her mail and also relieves you from having to store a lot of keys on your public keyring.

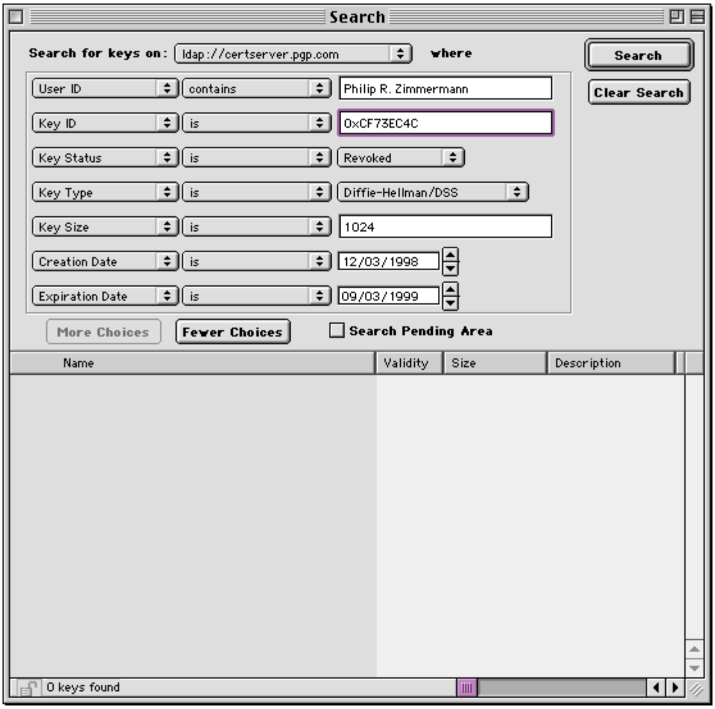
If you are in a corporate setting, then your administrator may direct you to use a corporate key server that holds all of your organization's frequently used keys. In this case, your PGP software is probably already configured to access the appropriate server.

There are a number of public key servers, such as the one maintained by Network Associates, Inc., where you can locate the keys of most PGP users. If the recipient has not pointed you to the Web address where his or her public key is stored, you can access any key server and do a search for the user's name or email address. This is because all key servers are regularly updated to include the keys stored on all the other servers.

To get someone's public key from a key server:

1. Open PGPkeys.
2. Choose **Search** from the **Server** menu or click the **Search** button (🔍) in PGPkeys.

   The **PGPkeys Search** window appears as in Figure 3-5.



Search for keys on: ldap://certserver.pgp.com where

User ID contains Philip R. Zimmermann

Key ID is 0xCF73EC4C

Key Status is Revoked

Key Type is Diffie-Hellman/DSS

Key Size is 1024

Creation Date is 12/03/1998

Expiration Date is 09/03/1999

□ Search Pending Area

0 keys found

Figure 3-5. PGPkeys Search window
(*More Choices view*)

3. Choose the server you wish to search from the **Search for Keys On** menu.
4. Specify your search criteria.

   You can search for keys on a key server by specifying values for multiple key characteristics.

   The inverse of most of these operations is also available. For example, you may search using “User ID is not Charles” as your criteria.
5. Enter the value you want to search for.
6. Click **More Choices** to add additional criteria to your search; for example, Key IDs with the name Susan created on or before March 5, 1998.

7. To begin the search, click **Search**.

   A progress bar appears displaying the status of the search.

   NOTE: To cancel a search in progress, click **Cancel**.

   The results of the search appear in the window.

8. To import the keys, drag them to the PGPkeys main window.

9. Click **Clear Search** to clear your search criteria.

Getting public keys from email messages

A convenient way to get a copy of someone's public key is to have that person include it in an email message. When a public key is sent through email, it appears as a block of text in the body of the message.

To add a public key from an email message:

– If you have an email application that is supported by the PGP plug-ins, then click in your email application to extract the sender's public key from the email and add it to your public keyring.

– If you are using an email application that is not supported by the plug-ins, you can add the public key to the keyring by copying the block of text that represents the public key and pasting it into PGPkeys.

Importing keys

You can import PGP public keys to your PGP public keyring.

Another method for obtaining someone's public key is to have that person save it to a file from which you can import it or copy and paste it into your public keyring.

To import a public key:

There are three methods of extracting someone's public key and adding it to your public keyring:

- Choose **Import from the Keys** menu and then navigate to the file where the public key is stored
- Drag the file containing the public key onto the main PGPkeys window
- Open the text document where the public key is stored, select the block of text representing the key, and then choose **Copy** from the **Edit** menu. Go to PGPkeys and choose **Paste** from the **Edit** menu to copy the key. The key then shows up as an icon in PGPkeys

Verifying the authenticity of a key

When you exchange keys with someone, it is sometimes hard to tell if the key really belongs to that person. PGP software provides a number of safeguards that allow you to check a key's authenticity and to certify that the key belongs to a particular owner (that is, to *validate* it). The PGP program also warns you if you attempt to use a key that is not valid and also by default warns you when you are about to use a marginally valid key.

Why verify the authenticity of a key?

One of the major vulnerabilities of public key encryption systems is the ability of sophisticated eavesdroppers to mount a "man-in-the-middle" attack by replacing someone's public key with one of their own. In this way they can intercept any encrypted email intended for that person, decrypt it using their own key, then encrypt it again with the person's real key and send it on to them as if nothing had ever happened. In fact, this could all be done automatically through a sophisticated computer program that stands in the middle and deciphers all of your correspondence.

Based on this scenario, you and those with whom you exchange email need a way to determine whether you do indeed have legitimate copies of each others' keys. The best way to be completely sure that a public key actually belongs to a particular person is to have the owner copy it to a floppy disk and then physically hand it to you. However, you are seldom close enough to personally hand a disk to someone; you generally exchange public keys via email or get them from a public key server.

Verify with a digital fingerprint

You can determine if a key really belongs to a particular person by checking its digital fingerprint, a unique series of numbers or words generated when the key is created. By comparing the fingerprint on your copy of someone's public key to the fingerprint on their original key, you can be absolutely sure that you do in fact have a valid copy of their key. To learn how to verify with a digital fingerprint, see "Verifying someone's public key" on page 61.

Validating a public key

Validity and trust are two tricky, yet vital concepts in PGP. *An Introduction to Cryptography* discusses them in detail. In short, once you are absolutely convinced that you have a legitimate copy of someone's public key, you can then sign that person's key. By signing someone's public key with your private key, you are certifying that you are sure the key belongs to the alleged user. For instance, when you create a new key, it is automatically certified with your own digital signature. By default, signatures you make on other keys are not exportable, which means they apply only to the key when it is on your local keyring. For detailed instructions on signing a key, see "Signing someone's public key" on page 63.

Working with trusted introducers

PGP users often have other trusted users sign their public keys to further attest to their authenticity. For instance, you might send a trusted colleague a copy of your public key with a request that he or she certify and return it so you can include the signature when you post your key on a public key server. Using PGP, when users get a copy of your public key, they don't have to check the key's authenticity themselves, but can instead rely on how well they trust the person(s) who signed your key. PGP provides the means for establishing this level of validity for each of the public keys you add to your public keyring and shows the level of trust and validity associated with each key. This means that when you get a key from someone whose key is signed by a trusted introducer, you can be fairly sure that the key belongs to the purported user. For details on how to sign keys and validate users, see "Signing someone's public key" on page 63.

In a corporate setting, your corporate Security Officer can act as a trusted introducer, and you may then trust any keys signed by the corporate key to be valid keys. If you work for a large company with several locations, you may have regional introducers, and your Security Officer may be a meta-introducer, or a trusted introducer of trusted introducers.

What is a trusted introducer?

PGP uses the concept of a trusted introducer, someone you trust to provide you with keys that are valid. This concept may be familiar to you from Victorian novels, in which people gave letters of introduction to one another. For example, if your uncle knew someone in a faraway city with whom you might want to do business, he might write a letter of introduction to his acquaintance. With PGP, users can sign one another's keys to validate them. You sign someone's key to indicate that you are sure that his or her key is valid, which means that it truly is his or her key. There are several ways to do this. When a trusted introducer signs another person's key, you trust that the keys they sign are valid, and you do not feel that you must verify their keys before using them.

What is a meta-introducer?

PGP also supports the concept of a meta-introducer—a trusted introducer of trusted introducers. If you work in a very large company, you might have a regional Security Officer, a trusted introducer, who would sign users' keys. You could trust that these keys were valid because the regional Security Officer had performed the actions to ensure validity. The organization may also have a head Security Officer who works with the local Security Officers, so that a person in a West Coast office could trust a person in an East Coast office. This is because both their keys had been signed by their respective regional Security Officers, who in turn had their keys signed by the head Security Officer, who is a meta-introducer. This allows the establishment of a trust hierarchy in the organization.

Managing Keys 4

This chapter explains how to examine and manage the keys stored on your keyrings.

Managing your PGP keyrings

The keys you create, as well as those you collect from others, are stored on keyrings, which are essentially files stored on your hard drive or on a floppy disk. Normally your private keys are stored in a file named PGP Private Keys and your public keys are stored in another file named PGP Public Keys. These files are usually located in your PGP folder and can be viewed and edited from the PGPkeys window (Figure 4-1).

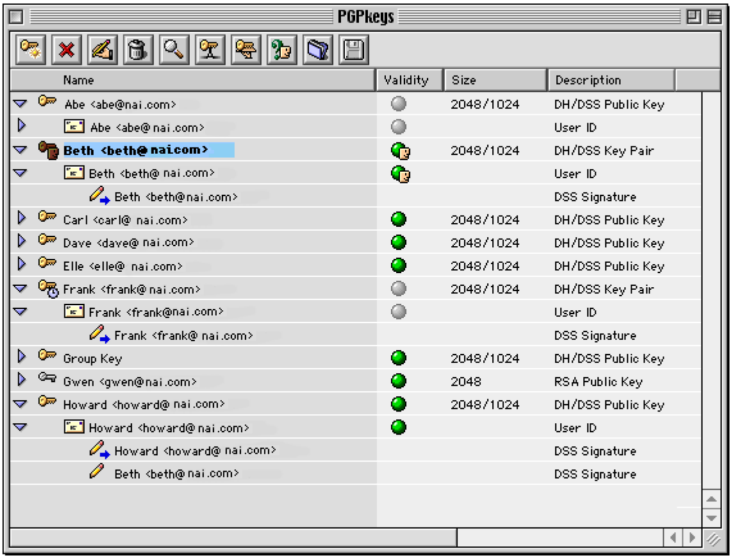
NOTE: As a result of your private key being encrypted automatically and your passphrase being uncompromised, there is no danger in leaving your keyrings on your computer. However, if you are not comfortable storing your keys in the default location, you can choose a different filename or location. For details, see "Setting PGP preferences" on page 151.

Occasionally, you may want to examine or change the attributes associated with your keys. For instance, when you obtain someone's public key, you might want to identify its type (either RSA or Diffie-Hellman / DSS), check its fingerprint, or determine its validity based on any digital signatures included with the key. You may also want to sign someone's public key to indicate that you believe it is valid, assign a level of trust to the key's owner, or change a passphrase for your private key. You may even want to search a key server for someone's key. You perform all of these key-management functions from PGPkeys.

The PGPkeys window

The PGPkeys window, as shown in Figure 4-1, displays the keys you have created for yourself, as well as any public keys you have added to your public keyring. It is from this window that you perform all your key management functions.

To open the PGPkeys window, choose PGPkeys from PGPmenu or double-click the keys icon ( ) in the PGP program folder.



Name	Validity	Size	Description
Abe <abe@nai.com>	○	2048/1024	DH/DSS Public Key
Abe <abe@ nai.com>	○		User ID
Beth <beth@ nai.com>	●	2048/1024	DH/DSS Key Pair
Beth <beth@ nai.com>	●		User ID
Beth <beth@nai.com>			DSS Signature
Carl <carl@ nai.com>	●	2048/1024	DH/DSS Public Key
Dave <dave@ nai.com>	●	2048/1024	DH/DSS Public Key
Elle <elle@ nai.com>	●	2048/1024	DH/DSS Public Key
Frank <frank@ nai.com>	○	2048/1024	DH/DSS Key Pair
Frank <frank@nai.com>	○		User ID
Frank <frank@ nai.com>			DSS Signature
Group Key	●	2048/1024	DH/DSS Public Key
Gwen <gwen@nai.com>	●	2048	RSA Public Key
Howard <howard@ nai.com>	●	2048/1024	DH/DSS Public Key
Howard <howard@ nai.com>	●		User ID
Howard <howard@ nai.com>			DSS Signature
Beth <beth@ nai.com>			DSS Signature

Figure 4-1. PGPkeys window

PGPkeys attribute definitions

Some of the attributes associated with keys can be displayed in the main PGPkeys window. You can choose which attributes you want to make visible by selecting them from the View menu. For each selected item in the View menu, PGPkeys displays a column in the main window. If you want to change the order of these columns, click and drag the header of the column you want to move. For a list of PGPkeys attribute definitions, see Table 4-1 on page 55.

Table 4-1. PGPkeys attribute overview

Attribute	Description
Name	Shows an iconic representation of the key along with the user name, email address, photograph of the owner, and the names of the key's signers. A gold key and user represents your Diffie-Hellman/DSS key pair, which consists of your private key and your public key. A gray key and user represents an RSA key pair, which consists of your private key and your public key. A single gold key represents a Diffie-Hellman/DSS public key. A single gray key represents an RSA public key. When a key or key pair is dimmed, the keys are temporarily unavailable for encrypting and signing. You can disable a key from the PGPkeys window, which prevents seldom-used keys from cluttering up the Key Selection dialog box. A key with a red X indicates that the key has been revoked. Users revoke their keys when they are no longer valid or have been compromised in some way. A single key with a clock icon represents a public key or key pair that has expired. Additional icons can be listed with a key indicating that a signature, certificate, or photographic user ID accompanies the key. A pencil or fountain pen indicates the signatures of the PGP users who have vouched for the authenticity of the key. -A signature with a red X through it indicates a revoked signature. -A signature with a dimmed pencil icon indicates a bad or invalid signature. -A signature with a blue arrow next to it indicates that it is exportable. A certificate represents an X.509 certificate, a recognized electronic document used to prove identity and public key ownership over a communication network. A clock indicates an expired X.509 certificate. A red X indicates a revoked X.509 certificate. This icon indicates that a photographic user ID accompanies the public key.

Attribute	Description
Validity	Indicates the level of confidence that the key actually belongs to the alleged owner. The validity is based on who has signed the key and how well you trust the signer(s) to vouch for the authenticity of a key. The public keys you sign yourself have the highest level of validity, based on the assumption that you only sign someone’s key if you are totally convinced that it is valid. The validity of any other keys, which you have not personally signed, depends on the level of trust you have granted to any other users who have signed the key. If there are no signatures associated with the key, then it is not considered valid, and a message indicating this fact appears whenever you encrypt to the key. Validity is indicated by either circle or bar icons, depending upon your **Advanced Preferences** “Display marginal validity level” setting (see “Setting advanced preferences” later in this chapter). If not enabled, then validity appears as: ⚪ a gray circle for invalid keys and marginally valid keys if the **Advanced Preferences** “Treat marginally valid keys as invalid” is set 🟢 a green circle for valid keys that you do not own 🟢👤 a green circle and a user for valid keys that you own In a corporate environment, your security officer may sign users’ keys with the Corporate Signing Key. Keys signed with the Corporate Signing Key are usually assumed to be completely valid. See Chapter 2, “A Quick Tour of PGP,” for more information.
Size	Shows the number of bits used to construct the key. Generally, the larger the key, the less chance that it will ever be compromised. However, larger keys require slightly more time to encrypt and decrypt data than do smaller keys. When you create a Diffie-Hellman/DSS key, there is one number for the Diffie-Hellman portion and another number for the DSS portion. The DSS portion is used for signing, and the Diffie-Hellman portion for encryption.
Description	Describes the type of information displayed in the **Name** column: key type, type of ID, or signature type.
Additional Decryption Key	Shows whether the key has an associated Additional Decryption Key.
Key ID	A unique identifying number associated with each key. This identification number is useful for distinguishing between two keys that share the same user name and email address.

Attribute	Description
Trust	Indicates the level of trust you have granted to the owner of the key to serve as an introducer for the public keys of others. This trust comes into play when you are unable to verify the validity of someone's public key for yourself and instead rely on the judgment of other users who have signed the key. When you create a new key pair, these keys are considered implicitly trustworthy, as shown by the striping in the trust and validity bars, or by a green dot and user icon. □ An empty bar indicates an invalid key or an untrusted user. ◧ A half-filled bar indicates a marginally valid key or marginally trusted user. ▨ A striped bar indicates a valid key that you own and is implicitly trusted, regardless of the signatures on the key. ■ A full bar indicates a completely valid key or a completely trusted user. When a public key on your keyring is signed by another user, the level of authenticity for that key is based on the trust you have granted to the signer. Use the **Key Properties** dialog box to assign the signer a level of trust—Trusted, Marginal, or Untrusted.
Expiration	Shows the date when the key will expire. Most keys are set to Never; however, there may be instances when the owner of a key wants it to be used for only a fixed period of time. A single key with a clock icon represents a public key or key pair that has expired.
Creation	Shows the date when the key was originally created. You can sometimes make an assumption about the validity of a key based on how long it has been in circulation. If the key has been in use for a while, it is less likely that someone will try to replace it because there are many other copies in circulation. Never rely on creation dates as the sole indicator of validity.

Specifying a default key pair on your PGP keyring

When encrypting messages or files, PGP gives you the option to additionally encrypt to a key pair that you specify as your default key pair. When you sign a message or someone's public key, PGP will use this key pair by default. Your default key pair is displayed in bold type to distinguish it from your other keys. If you have more than one key pair, you may want to specifically designate one pair as your default pair.

To specify your default key pair:

1. Open PGPkeys and highlight the key pair you want to designate as your default key.
2. Choose **Set Default** from the **Keys** menu.

   The selected key pair is displayed in bold type, indicating that it is now designated as your default key pair.

Importing and exporting keys on your PGP keyring

Although you often distribute your public key and obtain the public keys of others by cutting and pasting the raw text from a public or corporate key server, you can also exchange keys by importing and exporting them as separate text files. For instance, someone could hand you a disk containing their public key, or you might want to make your public key available over an FTP server. Refer to "Exchanging public keys with others" on page 43 for details about importing and exporting public keys.

Deleting a key or signature on your PGP keyring

At some point you may want to remove a key or a signature from your PGP keyring. When you delete a key or signature from a key, it is removed and not recoverable. Signatures and user IDs can be re-added to a key, and an imported public key can be re-imported to your keyring. However, a private key that exists only on that keyring cannot be recreated, and all messages encrypted to its public key copies can no longer be decrypted.

NOTE: If you want to delete a signature or user ID associated with your public key on a key server, see "Updating your key on a key server" on page 87 for instructions.

To delete a key or signature from your PGP keyring:

1. Open PGPkeys and select the key or signature you want to delete.
2. Choose **Clear** from the **Edit** menu or click 🗑 in the PGPkeys menu bar.

   The **Confirmation** dialog box appears.
3. Click the **OK** button.

Disabling and enabling keys on your PGP keyring

Sometimes you may want to temporarily disable a key. The ability to disable keys is useful when you want to retain a public key for future use, but you don’t want it cluttering up your recipient list every time you send mail.

To disable a key:

1. Open PGPkeys and select the key you want to disable.
2. Select **Disable** in the **Keys** menu.

   The key is dimmed and is temporarily unavailable for use.

To enable a key:

1. Open PGPkeys and select the key you want to enable.
2. Select **Enable** in the **Keys** menu.

   The key becomes visible and can be used as before.

Examining and setting key properties

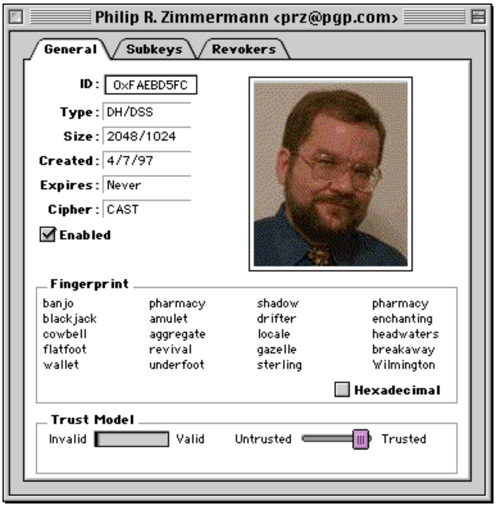
In addition to the general attributes shown in the **PGPkeys** window, you can also examine and change other key and subkey properties.

The **Key Properties** window includes the **General**, **Subkeys**, **Revokers**, and **ADK** tabbed pages, each of which gives you necessary information about a person’s public key, or the ability to create, configure, edit, or delete attributes in your own public key. The following sections describe each element in more detail.

For details on the:	See:
General tab	“General key properties” on page 60
Subkeys tab	“Subkeys properties” on page 70
Revokers tab	“Designated revoker properties” on page 73
ADK tab	“Additional Decryption Key properties” on page 75

General key properties

From the **General** tabbed page, you can verify someone’s public key using their key fingerprint, grant trust to a key, and change the passphrase on your own key as well as view other key attributes. To access the **General Key Properties** panel (Figure 4-2 on page 61) for a particular key, select the desired key and then choose **Properties** from the **Keys** menu.



Philip R. Zimmermann <prz@pgp.com>

ID : 0xFAEBD5FC
Type : DH/DSS
Size : 2048/1024
Created : 4/7/97
Expires : Never
Cipher : CAST
☑ Enabled

Fingerprint

banjo	pharmacy	shadow	pharmacy
blackjack	amulet	drifter	enchanting
cowbell	aggregate	locale	headwaters
flatfoot	revival	gazelle	breakaway
wallet	underfoot	sterling	Wilmington

□ Hexadecimal

Trust Model
Invalid Valid Untrusted Trusted

Figure 4-2. Key Property dialog box (General panel)

Verifying someone’s public key

In the past it was difficult to know for certain whether a key belonged to a particular individual unless that person physically handed the key to you on a floppy disk. Exchanging keys in this manner is not usually practical, especially for users who are located many miles apart.

There are several ways to check a key’s fingerprint, but the safest is to call the person and have them read the fingerprint to you over the phone. Unless the person is the target of an attack, it is highly unlikely that someone would be able to intercept this random call and imitate the person you expect to hear on the other end. You can also compare the fingerprint on your copy of someone’s public key to the fingerprint on their original key on a public server.

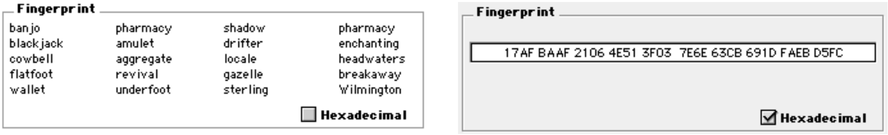
The fingerprint can be viewed in two ways: in a unique list of words or in its hexadecimal format.

To check a public key with its digital fingerprint:

1. Open PGPkeys and select the public key in which you want to verify.
2. Choose **Properties** from the **Keys** menu or click to open the **Properties** dialog box.

   The **Properties** dialog box opens, as shown in Figure 4-2.
3. Use the series of words or characters displayed in the **Fingerprint** text box to compare with the original fingerprint.

   By default, a word list is displayed in the **Fingerprint** text box (example shown in Figure 4-3). However, you can select the **Hexadecimal** check box to view the fingerprint in 20 hexadecimal characters (example also shown in Figure 4-3).



```
Fingerprint
banjo       pharmacy    shadow      pharmacy
blackjack   amulet      drifter     enchanting
cowbell     aggregate   locale      headwaters
flatfoot    revival     gazelle     breakaway
wallet      underfoot   sterling    Wilmington
                                 □ Hexadecimal
```

Word list view

```
Fingerprint
17AF BAAF 2106 4E51 3F03  7E6E 63CB 691D FAEB D5FC
                                 ☑ Hexadecimal
```

Hexadecimal view

Figure 4-3. Fingerprint text box

The word list in the fingerprint text box is made up of special authentication words that PGP uses and are carefully selected to be phonetically distinct and easy to understand without phonetic ambiguity.

The word list serves a similar purpose as the military alphabet, which allows pilots to convey information distinctly over a noisy radio channel. If you'd like to know more about the word hash technique and view the word list, see Appendix E, "Biometric Word Lists."

Signing someone's public key

When you create a key pair, the keys are automatically signed by themselves. Similarly, once you are sure that a key belongs to the proper individual, you can sign that person's public key, indicating that you are sure it is a valid key. When you sign someone's public key, a signature icon along with your user name is shown attached to that key.

To sign someone's public key:

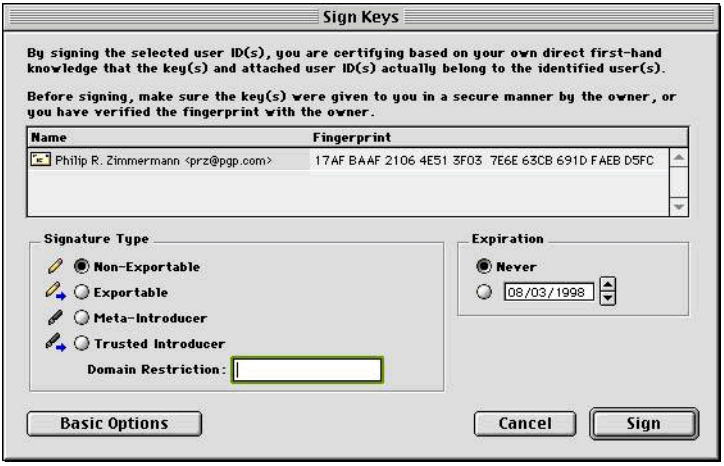
1. Open PGPkeys and select the public key which you want to sign.
2. Choose **Sign** from the **Keys** menu or click to open the **Sign Keys** dialog box.

   The **Sign Keys** dialog box appears with the public key and fingerprint displayed in the text box.
3. Click the **Allow signature to be Exported** checkbox, to allow your signature to be exported with this key.

   An exportable signature is one that is allowed to be sent to servers and travels with the key whenever it is exported, such as by dragging it to an email message. The checkbox provides a shorthand means of indicating that you wish to export your signature.

   Or

   Click the **Advanced Options** button to configure preferences, such as signature type and signature expiration (Figure 4-4).



Sign Keys

By signing the selected user ID(s), you are certifying based on your own direct first-hand knowledge that the key(s) and attached user ID(s) actually belong to the identified user(s).

Before signing, make sure the key(s) were given to you in a secure manner by the owner, or you have verified the fingerprint with the owner.

Name	Fingerprint
Philip R. Zimmermann <prz@pgp.com>	17AF BAAF 2106 4E51 3F03 7E6E 63CB 691D FAEB D5FC

Signature Type

● Non-Exportable
○ Exportable
○ Meta-Introducer
○ Trusted Introducer

Domain Restriction:

Expiration

● Never
○ 08/03/1998

Figure 4-4. PGP Sign Keys dialog box (Advanced Options)

Choose a signature type to sign the public key with. Your choices are:

- **Non-exportable.** Use this signature when you believe the key is valid, but you don't want others to rely on your certification. This signature type cannot be sent with the associated key to a key server or exported in any way.
- **Exportable.** Use exportable signatures in situations where your signature is sent with the key to the key server, so that others can rely on your signature and trust your keys as a result. This is equivalent to checking the **Allow signature to be exported** checkbox on the **Sign Keys** menu.
- **Meta-Introducer Non-Exportable.** Certifies that this key and any keys signed by this key with a Trusted Introducer Validity Assertion are fully trusted introducers to you. This signature type is non-exportable.

  The **Maximum Trust Depth** option enables you to identify how many levels deep you can nest trusted-introducers. For example, if you set this to 1, there can only be one layer of introducers below the meta-introducer key.
- **Trusted Introducer Exportable.** Use this signature in situations where you certify that this key is valid, and that the owner of the key should be completely trusted to vouch for other keys. This signature type is exportable. You can restrict the validation capabilities of the trusted introducer to a particular email domain.

4. If you want to limit the Trusted Introducer's key validation capabilities to a single domain, enter the domain name in the **Domain Restriction** text box.
5. If you want to assign an expiration date to this signature, enter the date on which you want this signature to expire in the **Date** text box. Otherwise, the signature will never expire.
6. Click **OK**.

   The **Passphrase** dialog box appears.
7. Enter your passphrase, then click **OK**.

   An icon associated with your user name is now included with the public key that you just signed.

Granting trust for key validations

Besides certifying that a key belongs to someone, you can assign a level of trust to the owner of the keys indicating how well you trust them to act as an introducer for others, whose keys you may get in the future. This means that if you ever get a key from someone that has been signed by an individual whom you have designated as trustworthy, the key is considered valid even though you have not done the check yourself.

To grant trust for a key:

1. Open PGPkeys and select the key for which you want to change the trust level.

   NOTE: You must sign the key before you can set the trust level for it. If you have not already signed the key, see “Validating a public key” on page 50 for instructions.

2. Choose **Properties** from the **Keys** menu or click to open the **Properties** dialog box, as shown in Figure 4-2.
3. Use the Trust Level sliding bar to choose the appropriate level of trust for the key pair.

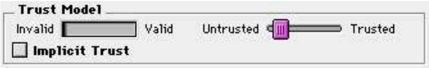


Figure 4-5. Trust Level dialog box

4. Close the dialog box to accept the new setting.

Changing your passphrase

It’s a good practice to change your passphrase at regular intervals, perhaps every three months. More importantly, you should change your passphrase the moment you think it has been compromised, for example, by someone looking over your shoulder as you typed it in.

To change your passphrase:

1. Open PGPkeys and select the key for which you want to change the passphrase.

   Choose **Properties** from the **Keys** menu or click to open the **Properties** dialog box.

   The **Properties** dialog box appears, as in Figure 4-2.

2. Click **Change Passphrase** from the **General** tab.

   The **Passphrase** dialog box appears.

   NOTE: If you want to change the passphrase for a split key, you must first rejoin the key shares. Click **Join** to collect the key shares. See “Signing and decrypting files with a split key” on page 108 for information about collecting key shares.

3. Enter your current passphrase in the space provided, then click **OK**.

   The **Confirmed Passphrase** dialog box appears.

4. Enter your new passphrase in the first text box. Press the TAB key to advance to the next text box and confirm your entry by entering your new passphrase again.

5. Click **OK**.

WARNING: If you are changing your passphrase because you feel that your passphrase has been compromised, you should wipe all backup keyrings and wipe your freespace.

Adding a new user name or address to your key pair

You may have more than one user name or email address for which you want to use the same key pair. After creating a key pair, you can add alternate names and addresses to the keys. You can only add a new user name or email address if you have both the private and public keys.

To add a new user name or address to your key:

1. Open PGPkeys and select the key pair for which you want to add another user name or address.
2. Choose **Add/Name** from the **Keys** menu.

   The **PGP New User Name** dialog box appears.
3. Enter the new name and email address in the appropriate fields, and then click **OK**.

   The **PGP Enter Passphrase** dialog box appears.
4. Enter your passphrase, then click **OK**.

   The new name is added to the end of the user name list associated with the key. If you want to set the new user name and address as the primary identifier for your key, select the name and address and then choose **Set as Primary Name** from the **Keys** menu.

IMPORTANT: When you add or change information in your key pair, always update it on the key server so that your most current key can be available to anyone. See "Updating your key on a key server" on page 87 for instructions.

Adding a photographic ID to your key

You can include a photographic user ID with your PGP keys.

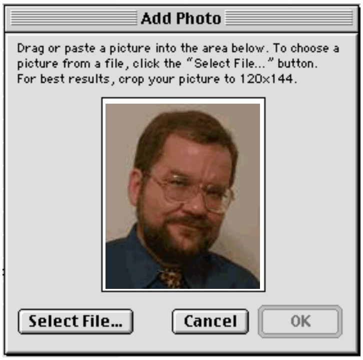
NOTE: This feature is available for Diffie-Hellman / DSS and RSA keys. The Photographic ID feature is not supported by RSA Legacy keys.

IMPORTANT: Although you can view the photographic ID accompanied with someone's key for verification, you should always check and compare the digital fingerprints. See "Verifying someone's public key" on page 61 for more information about authentication.

To add your photograph to your key:

1. Open PGPkeys and select your key pair and then choose **Add/Photo** from the **Keys** menu.

   The **Add Photo** dialog box opens.



Add Photo

Drag or paste a picture into the area below. To choose a picture from a file, click the "Select File..." button. For best results, crop your picture to 120x144.

2. Drag or paste your photograph onto the **Add Photo** dialog box or browse to it by clicking **Select File**.

   NOTE: The photograph can be from the Clipboard, a PICT file. For maximum picture quality, crop the picture to 120x144 pixels before adding it to the **Add Photo** dialog box. If you do not do this, PGP will scale the picture for you.

3. Click **OK**.

   The **Passphrase** dialog box opens.

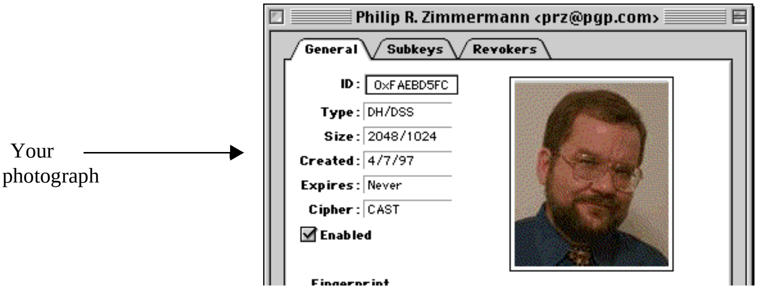
4. Enter your passphrase in the space provided, then click **OK**.

   Your photographic user ID is added to your public key and is listed in the PGPkeys window.

> **IMPORTANT:** When you add or change information in your key pair always update it on the key server so that your most current key can be available to anyone. See "Updating your key on a key server" on page 87 for instructions.

To replace your photographic ID:

1. Open PGPkeys and select the photograph which is listed under your keypair from the **Keys** menu, then click ▷ to view the list of items associated with your key.



ID: 0xFAEBD5FC
Type: DH/DSS
Size: 2048/1024
Created: 4/7/97
Expires: Never
Cipher: CAST
☑ Enabled
Fingerprint

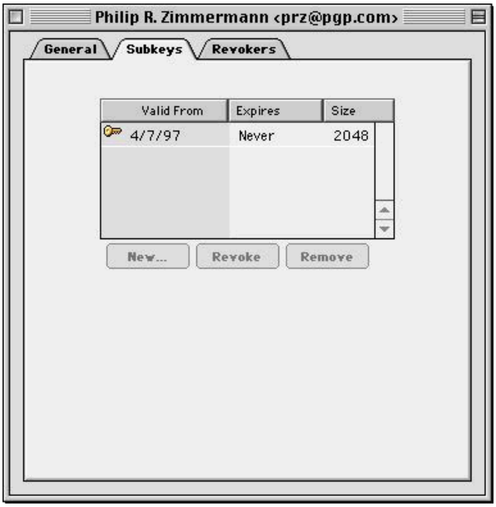
Figure 4-6. PGPkeys
(Example: Photographic User ID)

2. Choose **Delete** from the **Edit** menu.

3. Add your new photographic ID using the instructions outlined in "To add your photograph to your key:" on page 68.

Subkeys properties

To access the **Subkeys Properties** panel for a particular key, select the desired key and then choose **Properties** from the **Keys** menu. The **Key Properties** dialog box appears. Click the **Subkeys** tab. The **Subkeys** panel appears as shown in Figure 4-7.



Valid From	Expires	Size
4/7/97	Never	2048

Figure 4-7. Key Property dialog box (Subkeys panel)

Creating new subkeys

Every Diffie-Hellman / DSS and RSA key is actually two keys: a signing key and an encryption subkey. PGP Version 6.0 and above provides the ability to create and revoke new encryption keys without sacrificing your master signing key and the signatures collected on it. One of the most common uses for this feature is to create multiple subkeys that are set to be used during different periods of the key's lifetime. For example, if you create a key that will expire in three years, you might also create 3 subkeys and use each of them for one of the years in the lifetime of the key. This can be a useful security measure and provides an automatic way to periodically switch to a new encryption key without having to recreate and distribute a new public key.

NOTE: This feature is available for Diffie-Hellman / DSS and RSA keys. Subkeys are not supported by RSA Legacy keys.

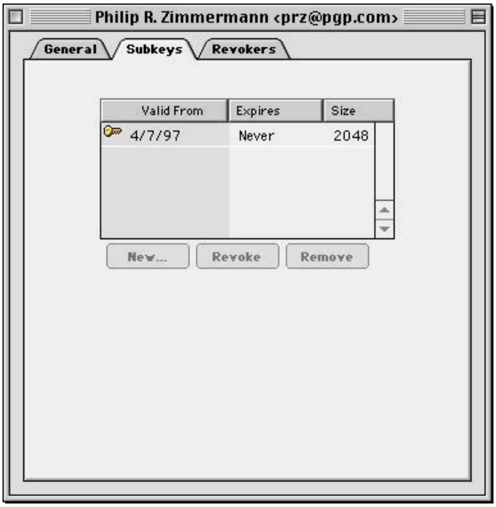
To create new subkeys:

1. Open PGPkeys and select your key pair, then choose **Properties** from the **Keys** menu, or click .

   The **Properties** dialog box appears.

2. Click the **Subkeys** tab.

   The **Subkeys** dialog box opens, as shown in Figure 4-8 on page 71.



Valid From	Expires	Size
4/7/97	Never	2048

Figure 4-8. PGP key property page (Subkeys dialog box)

3. To create a new subkey, click **New**.

   The **New Subkey** dialog box opens.

4. Enter a key size from 1024 to 3072 bits, or enter a custom key size from 1024 to 4096 bits.

5. Indicate the start date on which you want your subkey to activate.

6. Indicate when you want your subkey to expire. You can either use the default selection, which is **Never**, or you can enter a specific date after which the subkey will expire.

> **NOTE:** To avoid confusion when maintaining more than one subkey on your key pair, try not to overlap your subkeys start and expiration dates.

7. Click **OK**.

   The **Passphrase** dialog box appears.

8. Enter your passphrase and then click **OK**.

   Your new subkey is listed in the Subkey window.

> **IMPORTANT:** When you add or change information in your key pair, always update it on the key server so that your most current key can be available to anyone. See “Updating your key on a key server” on page 87 for instructions.

Designated revoker properties

To access the **Revokers** panel for a particular key, select the desired key and then choose **Properties** from the **Keys** menu. The **Key Properties** dialog box appears, as shown in Figure 4-2 on page 61. Click the **Revokers** tab. The **Revokers** panel appears as shown in Figure 4-9. (Note, if there are no designated revokers for the selected key, then the Revokers tab does not appear.)

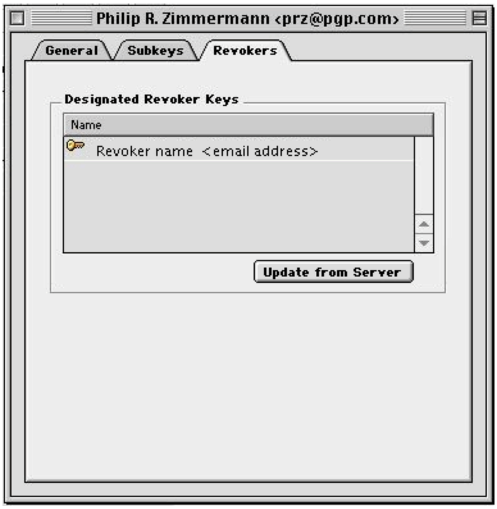


Figure 4-9. Key Property dialog box (Revokers panel)

The **Revokers** panel lists any keys that have the ability to revoke your PGP key, and provides a convenient means for updating a revokers' key with the **Update from Server** button.

If the key belonging to the revoker is not on your keyring, then "*Unknown Key*" followed by the keys' key ID displays instead of the user ID. Highlight the key ID, and click the **Update from Server** button to search for the key on a key server.

Appointing a designated revoker

It is possible that you might forget your passphrase someday or lose your private key (your laptop is stolen or your hard drive crashes, for example). Unless you are also using Key Reconstruction and can reconstruct your private key, you would be unable to use your key again, and you would have no way of revoking it to show others not to encrypt to it. To safeguard against this possibility, you can appoint a third-party key revoker. The third-party you designate is then able to revoke your key just as if you had revoked it yourself.

NOTE: For a key to appear revoked to another user, both the revoked key and the Designated Revoker key must be on his/her keyring. Thus, the designated revoker feature is most effective in a corporate setting, where all users' keyrings contain the company's Designated Revoker key. If the revokers' key is not present on a person's keyring, then the revoked key does not appear revoked to that user and he/she may continue to encrypt to it.

NOTE: This feature is available for Diffie-Hellman/DSS and RSA keys. Key revoking is not supported by RSA Legacy keys.

To add a designated revoker to your key:

1. Open PGPkeys and then select the key pair for which you want to add a revoker.
2. Select **Add/Revoker** from the **Keys** menu.

   A dialog box opens and displays a list of keys.
3. Select the key(s) in the User ID list that you want to appoint as a revoker.
4. Click **OK**.

   A confirmation dialog box appears.
5. Click **OK** to continue.

   The **Passphrase** dialog box appears.

6. Enter your passphrase, then click **OK**.

7. The selected key(s) is now authorized to revoke your key. For effective key management, distribute a current copy of your key to the revoker(s) or upload your key to the server. See "Distributing your public key" on page 43 for instructions.

Revoking a key

If the situation ever arises that you no longer trust your personal key pair, you can issue a revocation to the world telling everyone to stop using your public key. The best way to circulate a revoked key is to place it on a public key server.

To revoke a key:

1. Open PGPkeys and select the key pair you want to revoke.

2. Choose **Revoke** from the **Keys** menu.

   The **Revocation Confirmation** dialog box appears.

3. Click **OK** to confirm your intent to revoke the selected key.

   The **PGP Enter Passphrase** dialog box appears.

4. Enter your passphrase, then click **OK**.

   When you revoke a key, it is marked out with a red X to indicate that it is no longer valid.

5. Send the revoked key to the server so everyone will know not to use your old key.

Additional Decryption Key properties

To access the **ADK** panel for a particular key, select the desired key and then choose **Properties** from the **Keys** menu. The **Key Properties** dialog box appears, as shown in Figure 4-2 on page 61. Click the **ADK** tab. The **ADK** panel appears. (Note, if there are no Additional Decryption Keys associated with the selected key, then the ADK tab does not appear.)

The **ADK** panel lists all Additional Decryption Keys (ADKs) for the selected key. ADKs are keys that allow the security officers of an organization to decrypt messages that have been sent to or from people within your organization. There are two types of keys: incoming additional decryption keys and outgoing additional decryption keys.

NOTE: Although the security officer should not ordinarily use the Additional Decryption keys, there may be circumstances when it is necessary to recover someone's email. For example, if someone is injured and out of work for some time or if email records are subpoenaed by a law enforcement agency and the corporation must decrypt mail as evidence for a court case.

Adding an X.509 certificate to your PGP key

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

NOTE: The instructions in this section describe how to add an X.509 certificate to your key pair if you are using the Net Tools PKI Server. This process varies between Certificate Authorities and some of the terminology you must use when interacting with your CA is a policy decision. You may need to consult your company's PGP or PKI Administrator for instructions.

An X.509 digital certificate is a recognized electronic document used to prove identity and public key ownership over a communication network.

You can request an X.509 digital certificate and add it to your key pair using PGP menu preferences and your company's *Certificate Authority* (CA) or a public CA (for example, VeriSign).

There are four main steps to adding an X.509 certificate to your key pair:

1. Retrieve the Root CA certificate from the CA and add it to your PGP keyring (see Step 1).

2. Enter information about the CA in the **Certificate Authority** panel in the Preferences dialog box (see Step 2).

3. Request a certificate from the CA. Your X.509 certificate request is verified and signed by the CA (see Step 3). (The CA's signature on the certificate makes it possible to detect any subsequent tampering with the identifying information or the public key, and it implies that the CA considers the information in the certificate valid.)

4. Retrieve the certificate issued by the CA and add it to your key pair (see Step 4).

Each of these four steps is described in greater detail in the following sections.

To add an X.509 certificate to your PGP key pair:

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

1. Obtain and add the Root CA certificate to your PGP keyring.

   To do this, follow these steps:

   a. Open your Web browser and connect to the CA's enrollment site. If you do not know the URL, consult your company's PGP or PKI administrator.

   b. Locate and examine the Root CA certificate. This process varies between Certificate Authorities. For example, if your company were using the Net Tools PKI Server, you would click the **Download a CA Certificate link**, and then click the **Examine this Certificate** button.

   c. Copy the key block for the Root CA certificate and paste it into your **PGPkeys** window.

      The **Import Key** dialog box appears and imports the Root CA certificate into your keyring.

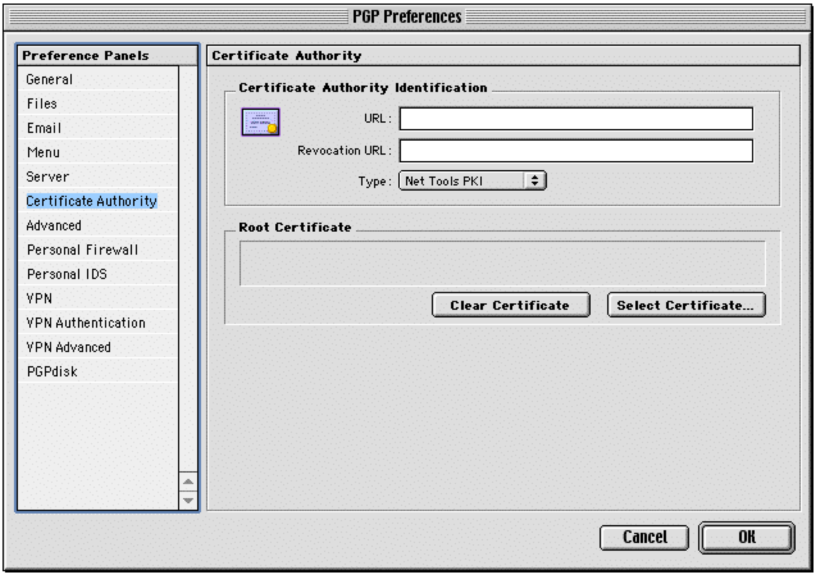
   d. Sign the Root CA certificate with your key to make it valid, then open the **Key Properties** and set the trust level. Trust must be set on the Root CA.

2. Configure **Certificate Authority** panel in the Preferences dialog box.

   To do this, follow these steps:

   a. Select **Preferences** from the PGPkeys **Edit** menu, then select **Certificate Authority**.

      The **Certificate Authority** panel appears, as shown in Figure 4-10 on page 78.



Type : Net Tools PKI

Figure 4-10. PGP Preferences dialog box (Certificate Authority Panel)

b. Enter the CA's URL in the **Certificate Authority Identification URL** field, for example, https://nnn.nnn.nnn.nnn:nnnnn (this is the same URL you used to retrieve the Root CA).

c. If there is a separate URL for retrieving certificate revocation lists (CRLs), enter it in the corresponding field.

If you do not know the URL for Revocation, leave this field blank or consult your company's PGP or PKI administrator.

d. In the **Type** box, specify the name of certificate authority you are using. Your choices are:

- Net Tools PKI
- VeriSign OnSite
- Entrust
- iPlanet CMS
- Windows 2000

e. Click the **Select Certificate** button, then select the Root CA certificate you just retrieved.

The **Root Certificate** text box displays information on the selected root CA certificate. The terminology for the certificate is a policy decision. Typically, the following terminology is true for X.509 certificates.

Term:	Description:
CN **(Common Name)**	Often a description of the type of certificate (e.g., “Root”).
EMAIL	The email address for the certificate holder.
OU **(Organizational Unit)**	The organization to which the certificate belongs (e.g.,“Accounting”).
O **(Organization)**	Typically the name of the company to which the certificate belongs (e.g.,“Secure Company”).
L **(Locality)**	The location of the holder of the certificate (e.g., “Santa Clara”).

f. Click **OK**.

3. Make a certificate request.

To do this, follow these steps:

a. Select **Add—>Certificate** from the **Keys** menu in PGPkeys.

The **Certificate Attributes** dialog box appears.

b. Verify the certificate attributes; use the **Add**, **Edit**, and **Remove** buttons to make any required changes, and click **OK**. The **PGP Enter Passphrase** dialog box appears.

c. Enter the passphrase for your key pair, then click **OK**.

The **PGP Server Progress** bar appears.

The certificate request is sent to the CA server. The server authenticates itself to your computer and accepts your request.

In a corporate setting, your company’s PGP or PKI administrator verifies your information in the request. The identifying information and public key are assembled and then digitally signed with the CA’s own certificate to create your new certificate.

The administrator sends you an email message stating that your certificate is ready for retrieval.

4. Retrieve your certificate and add it to your key pair.

   In a corporate setting, your certificate may be retrieved and added to your key pair automatically depending on the settings your administrator has configured. In this case, continue with Step c.

   If you do not have automatic certificate retrieval configured, you can retrieve your certificate and add it to your keyring manually. To do this, follow these steps:

   a. In PGPkeys, select the PGP key for which you made the certificate request.

   b. On the **Server** menu, select **Retrieve Certificate**.

      PGP contacts the CA server and automatically retrieves your new X.509 certificate and adds it to your PGP key.

   c. If you are running PGPnet, set this certificate as your X.509 authentication key in PGPnet (**View—>Preferences—> Authentication**).

> **IMPORTANT:** When you add or change information in your key pair, always update it on the key server so that your most current key can be available to anyone. See “Updating your key on a key server” on page 87 for instructions.

Splitting and rejoining keys

Any private key can be split into shares among multiple “shareholders” using a cryptographic process known as Blakely-Shamir key splitting. This technique is recommended for extremely high security keys. For example, Network Associates keeps a corporate key split between multiple individuals. Whenever we need to sign with that key, the shares of the key are rejoined temporarily.

> **NOTE:** Split keys are not compatible with versions of PGP Desktop Security previous to 6.0, or with versions of PGP e-Business Server or PGP Command Line products previous to 7.0.

Creating a split key

To split a key, select the key pair to be split and choose **Share Split** from the **Keys** menu. You are then asked to set up how many different shares will be required to rejoin the key. The shares are saved as files either encrypted to the public key of a shareholder or encrypted conventionally if the shareholder has no public key. After the key has been split, attempting to sign with it or decrypt with it will automatically attempt to rejoin the key. For information about rejoining a split key, see "Signing and decrypting files with a split key" on page 108.

To create a split key with multiple shares:

1. In PGPkeys, create a new key pair or select an existing key pair that you want to split. To learn how to create a new key pair, see "Making a key pair" on page 32.

2. On the **Keys** menu, choose Share Split.

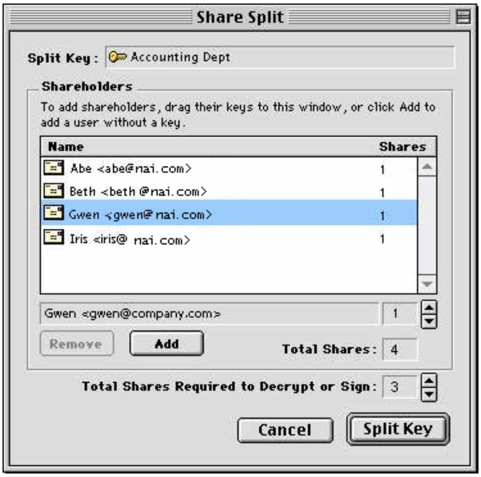
   The **Share Split** dialog box opens.

3. Add shareholders to the key pair by dragging their keys from PGPkeys to the **Shareholder** list in the **Share Split** dialog box.

   To add a shareholder that does not have a public key, click **Add** in the **Share Split** dialog box, enter the persons name and then allow the person to type in their passphrase.

4. When all of the shareholders are listed, you can specify the number of key shares that are necessary to decrypt or sign with this key.

   In Figure 4-11, for example, the total number of shares that make up the Group Key is four and the total number of shares required to decrypt or sign is three. This provides a buffer in the event that one of the shareholders is unable to provide his or her key share or forgets the passphrase.



Split Key: Accounting Dept

Shareholders

To add shareholders, drag their keys to this window, or click Add to add a user without a key.

Name	Shares
Abe <abe@nai.com>	1
Beth <beth @nai.com>	1
Gwen <gwen@ nai.com>	1
Iris <iris@ nai.com>	1

Gwen <gwen@company.com> 1

Total Shares: 4

Total Shares Required to Decrypt or Sign: 3

Figure 4-11. Share Split dialog box (Example)

By default, each shareholder is responsible for one share. To increase the number of shares a shareholder possesses, click the name in the shareholder's list to display it in the text field below. Type the new number of key shares or use the arrows to select a new amount.

5. Click **Split Key**.

   A dialog box opens and prompts you to select a directory in which to store the shares.

6. Select a location to store the key shares.

   The **Passphrase** dialog box appears.

7. Enter the passphrase for the key you want to split and then click **OK**.

   A confirmation dialog box opens.

8. Click **Yes** to split the key.

   The key is split and the shares are saved in the location you specified. Each key share is saved with the shareholder's name as the file name, as shown in the example below:

9. Distribute the key shares to the owners, then delete the local copies.

   Once a key is split among multiple shareholders, attempting to sign or decrypt with it will cause PGP to automatically attempt to rejoin the key. To learn how to rejoin a split key to sign or decrypt files, see "Signing and decrypting files with a split key" on page 108.

Rejoining split keys

Once a key is split among multiple shareholders, attempting to sign or decrypt with it will cause PGP to automatically attempt to rejoin the key. There are two ways to rejoin the key, locally and remotely.

Rejoining key shares locally requires the shareholders presence at the rejoining computer. Each shareholder is required to enter the passphrase for their key share.

Rejoining key shares remotely requires the remote shareholders to authenticate and decrypt their keys before sending them over the network. PGP's Transport Layer Security (TLS) provides a secure link to transmit key shares which allows multiple individuals in distant locations to securely sign or decrypt with their key share.

IMPORTANT: Before receiving key shares over the network, you should verify each shareholder's fingerprint and sign their public key to ensure that their authenticating key is legitimate. To learn how to verify a key pair, see "Verify with a digital fingerprint" on page 50.

To rejoin a split key:

1. Contact each shareholder of the split key. To rejoin key shares locally, the shareholders of the key must be present.

   To collect key shares over the network, ensure that the remote shareholders have PGP installed and are prepared to send their key share file. Remote shareholders must have:

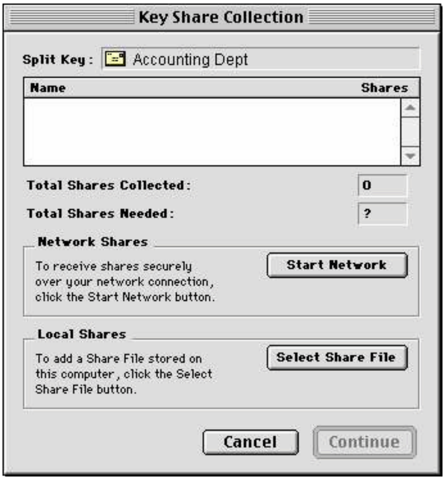
   - their key share files and passwords
   - a key pair (for authentication to the computer that is collecting the key shares)
   - a network connection
   - the IP address or Domain Name of the computer that is collecting the key shares

2. At the rejoining computer, use Finder to select the file(s) that you want to sign or decrypt with the split key.

   The **PGP Enter Passphrase for Selected Key** dialog box appears with the split key selected.

3. Click **OK** to reconstitute the selected key.

   The **Key Share Collection** dialog box appears, as shown in Figure 4-12.



Split Key : Accounting Dept

Total Shares Collected : 0

Total Shares Needed : ?

To receive shares securely over your network connection, click the Start Network button.

To add a Share File stored on this computer, click the Select Share File button.

Figure 4-12. Key Share Collection dialog box

4. Do one of the following:

    - **If you are collecting the key shares locally**, click **Select Share File** and then locate the share files associated with the split key. The share files can be collected from the hard drive, a floppy disk, or a mounted drive. Continue with Step 5.

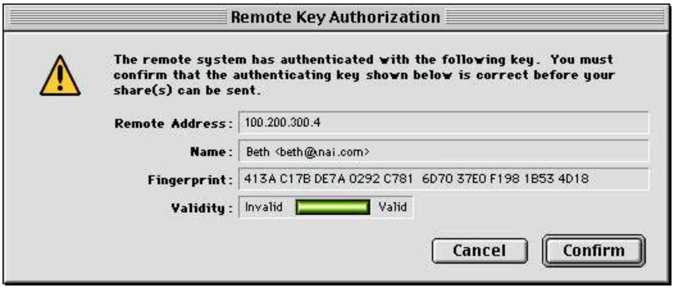
    - **If you are collecting key shares over the network**, click **Start Network**.

    The **Passphrase** dialog box opens. In the **Signing Key** box, select the key pair that you want to use for authentication to the remote system and enter the passphrase. Click **OK** to prepare the computer to receive the key shares.

    The status of the transaction is displayed in the **Network Shares** box. When the status changes to "Listening," the PGP application is ready to receive the key shares.

    At this time, the shareholders must send their key shares. To learn how to send key shares to the rejoining computer, see "To send your key share over the network:" on page 86.

    When a share is received, the **Remote Authentication** dialog box appears, as shown in Figure 4-13.



Remote Key Authorization

The remote system has authenticated with the following key. You must confirm that the authenticating key shown below is correct before your share(s) can be sent.

Remote Address: 100.200.300.4

Name: Beth <beth@nai.com>

Fingerprint: 413A C17B DE7A 0292 C781 6D70 37E0 F198 1B53 4D18

Validity: Invalid 🟩 Valid

Figure 4-13. Remote Authentication dialog box

If you have not signed the key that is being used to authenticate the remote system, the key will be considered invalid. Although you can rejoin the split key with an invalid authenticating key, it is not recommended. You should verify each shareholder's fingerprint and sign each shareholder's public key to ensure that the authenticating key is legitimate.

Click **Confirm** to accept the share file.

5. Continue collecting key shares until the value for **Total Shares Collected** matches the value for **Total Shares Needed** in the **Key Shares Collection** dialog box.

6. Click **OK**.

   The file is signed or decrypted with the split key.

To send your key share over the network:

1. When you are contacted by the person who is rejoining the split key, make sure that you have these items:

   - your key share file and password
   - your key pair (for authentication to the computer that is collecting the key shares)
   - a network connection
   - the IP address or Domain Name of the rejoining computer collecting the key shares

2. Choose Send Share File from the PGPkeys File menu.

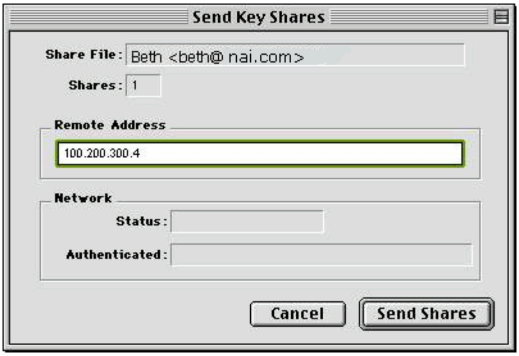
   The **Select Share File** dialog box appears.

3. Locate your key share and then click **Open**.

   The **PGP Enter Passphrase** dialog box appears.

4. Enter your passphrase and then click **OK**.

   The **Send Key Shares** dialog box appears, as shown in Figure 4-14 on page 86.



Send Key Shares

Share File: Beth <beth@ nai.com>

Shares: 1

Remote Address

100.200.300.4

Network

Status:

Authenticated:

Figure 4-14. Send Key Shares dialog box

5. Enter the IP address or the Domain Name of the rejoining computer in the **Remote Address** text box, then click **Send Shares**.

   The status of the transaction is displayed in the **Network Status** box. When the status changes to "Connected," you are asked to authenticate yourself to the rejoining computer.

   The **Remote Authentication** dialog box appears asking you to confirm that the remote computer is the one to whom you want to send your key share.

6. Click **Confirm** to complete the transaction.

   After the remote computer receives your key shares and confirms the transaction, a message box appears stating that the shares were successfully sent.

7. Click **OK**.

8. Click **Done** in the **Key Shares** window when you have completed sending your key share.

Updating your key on a key server

If you ever need to change your email address, or if you acquire new signatures, all you have to do to replace your old key is send a new copy to the server; the information is automatically updated. However, you should keep in mind that public key servers are only capable of adding new information and will not allow removal of user names or signatures from your key.

To remove signatures or user names from your key, see "Removing signatures or user names associated with your key" on page 87 for instructions.

If your key is ever compromised, you can revoke it; this tells the world to no longer trust that version of your key. See "Revoking a key" on page 75 for more details on how to revoke a key.

Removing signatures or user names associated with your key

At some point you may want to remove a subkey, a signature, or a user ID associated with a particular key.

Public key servers are only capable of adding new information and will not allow removal of user names or signatures from your key. To remove signatures or user names associated with your public key, you must first remove your key from the server, make the required change, then post your key back on the server.

If your **Server** settings in the Preferences dialog box are configured to synchronize keys with the key server when you add names/photos/revokers to your key, your key is automatically updated on the server. If, however, your keys do not automatically synchronize with the server, follow the instructions outlined below to manually update your key on the key server.

NOTE: When you delete a key, signature, or user name from a key, it is removed and not recoverable. Signatures and user names can be added again to a key, and an imported public key can be imported again to your keyring. However, a private key that exists only on that keyring cannot be created again, and all messages encrypted to its public key copies can no longer be decrypted.

To remove signatures or user names from your key on a key server:

IMPORTANT: This procedure is for removing signatures or user names associated with your key on LDAP key servers only. Additionally, the key server must be configured to allow this action.

1. Open PGPkeys.
2. Choose **Search** from the **Server** menu or click 🔍 in the PGPkeys menu.

   The PGPkeys **Search** window appears.
3. Choose the server you want to search from the **Search for Keys On** menu.
4. Specify your search criteria to locate your public key:

   The default is **User ID**, but you can click the arrows to select **Key ID**, **Key Status**, **Key Type**, **Key Size**, **Creation Date**, **or Expiration Date**. For example, you might search for all keys with the User ID of Fred.
5. To begin the search, click **Search**.

   The results of the search appear in the window.
6. Select the key that you want to remove from the server, then select **Delete** from the Server menu.

   The **Passphrase** dialog box appears.
7. Enter the passphrase for the key you want to remove from the server and then click **OK**.

   The **Confirmation** dialog box appears and the key is removed.

8. Update your key (remove the unwanted signatures or user names).

9. Copy the updated key to the server (see "Placing your public key on a key server" on page 43 for instructions).

   If the key server is configured to synchronize keys with other key servers, your key will be updated on the other servers automatically upon synchronization.

WARNING: If you delete your key from a key server, you should be aware that someone who has your public key on their keyring can upload it to the server again. You should check the server periodically to see if the key has reappeared—you may have to delete your key from the server more than once.

Reconstructing your key

If you ever lose your private key or you forget your passphrase, there is no way to recover from it unless you set up a key reconstruction policy, which includes setting up a key reconstitution server and enabling this feature in your PGP software. If this feature is enabled in your software, you would have provided recovery information—five secret questions and answers—and would have sent your key to the key reconstruction server. To learn how to send your key to the reconstruction server, see "To send your key to a key reconstruction server:" on page 41.

If you sent your key to a reconstruction server, you can restore your key pair at any time as long as you have your public key and can answer at least three of the five secret questions you created.

To reconstruct your key from a reconstruction server:

1. Open PGPkeys, then select the key that you want to reconstruct.

2. Select **Reconstruct Key** from the **Key** menu.

   If the reconstruction server is a PGP key server, the **Server User ID and Password** dialog box appears. Enter your user ID and password to log on to the server.

3. Click **OK**.

   The **Key Reconstruction** dialog box appears.

4. In the **Key Reconstruction** dialog box, enter answers in the **Answer** boxes to their corresponding questions. Keep in mind that your answers are case sensitive. You must be able to answer at least three questions to restore your key.

   You can use the **Hide Answers** checkbox to view or hide your answers.

5. Click **OK** to continue.

   The **PGP Enter Confirmed Passphrase** dialog box appears.

6. In the **Passphrase** box, enter a new string of characters or words you want to use as the new passphrase for your new key pair.

   > **NOTE:** Your passphrase should contain multiple words and may include spaces, numbers, and punctuation characters. Choose something that you can remember easily but that others won’t be able to guess. The passphrase is case sensitive, meaning that it distinguishes between uppercase and lowercase letters. The longer your passphrase, and the greater the variety of characters it contains, the more secure it is. Strong passphrases include upper and lowercase letters, numbers, punctuation, and spaces but are more likely to be forgotten. See “Creating a passphrase that you will remember” on page 38, for more information about choosing a passphrase.

   To confirm your entry, press the TAB key to advance to the next line, then enter the same passphrase again.

7. Click **OK**.

   Your key pair is reconstituted and appears in PGPkeys.

Part III: Securing Your Files and Communications

- **Chapter 5: Securing Email**
- **Chapter 6: Securing Files**

Securing Email 5

PGP provides the means for you to securely communicate through your email application with the use of the PGP plug-ins and utilities. This chapter explains how to secure email messages you send to others and decrypt and verify the messages others send to you.

Securing email communications

Sending email that is not encrypted is like sending a postcard: the message you write can easily be read by a person in between you and the recipient.

PGP offers an easy way to secure your messages against unauthorized reading. PGP also allows you to add your digital signatures to your messages to guarantee their authenticity and data integrity. To secure your email, PGP offers plug-ins to work along with your email applications and other utilities that encrypt, sign, decrypt, and verify email text. The PGP email plug-ins are available for seamless integration with Claris Emailer, Microsoft Exchange, Outlook and Express, and QUALCOMM Eudora.

PGP/MIME

If you are using an email application with one of the plug-ins that supports the PGP/MIME standard, and you are communicating with another user whose email application also supports this standard, both of you can automatically encrypt and decrypt your email messages and any attached files when you send or retrieve your email. All you have to do is turn on the PGP/MIME encryption and sign functions from the **Email** panel of the **PGP Preferences** dialog box, which can be opened from PGPtray or within PGPkeys.

When you receive email from someone who uses the PGP/MIME feature, the mail arrives with an icon in the message window indicating that it is PGP/MIME encoded.

To decrypt the text and file attachments in PGP/MIME encapsulated email and to verify any digital signatures, simply click the lock and quill icon. Attachments are still encrypted if PGP/MIME is not used, but the decryption process is usually more involved for the recipient.

Encrypting and signing email

The quickest and easiest way to secure email communications is by using an email application supported by the PGP plug-ins. If you are using an email application that is not supported by the PGP plug-ins, you can encrypt, sign, decrypt and verify the text of your email messages by using PGPmenu or PGPtools.

Encrypting and signing email using the PGP plug-ins

Although the procedure varies slightly between different email applications, you perform the encryption and signing process by clicking the appropriate buttons in the application's toolbar.

When you encrypt and sign with an email application that is supported by the PGP plug-ins, you have two choices, depending on what type of email application the recipient is using. If you are communicating with other PGP users who have an email application that supports the PGP / MIME standard, you can take advantage of a PGP / MIME feature to encrypt and sign your email messages and any file attachments automatically when you send them. If you are communicating with someone who does not have a PGP / MIME-compliant email application, you should encrypt your email with PGP / MIME turned off to avoid any compatibility problems. Refer to Table 5-1, "PGP Plug-in Features," for a list of plug-ins and their features.

Table 5-1. PGP Plug-in Features

	Eudora 3 - 4.0	Claris Emailer 2.0	Outlook Express 4.0
PGP/MIME	Yes	No	No
Auto-decrypt	No	decryption supported through PGPmenu	decryption supported through PGPmenu
Encrypt HTML	Yes	No	No
View decrypted HTML as an HTML document	Yes	No	No
Encrypt attachments	Yes	No	No
Encrypt/Sign defaults	No	No	No
Recipient matching	Yes	Yes	Yes

To encrypt and sign with supported email applications:

1. Use your email application to compose your email message as you normally would.

   TIP: If you are sending sensitive email, consider leaving your subject line blank or creating a subject line that does not reveal the contents of your encrypted message.

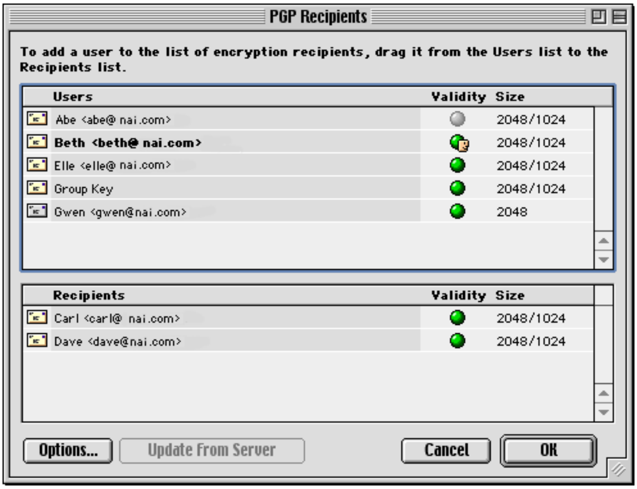
2. When you have finished composing the text of your email message, click the envelope and lock icon (🔏) to encrypt the text of your message, then click the paper and pen icon (📝) to sign your message.

   NOTE: If you know that you are going to use PGP / MIME regularly, you can leave this feature turned on by selecting the appropriate settings in the **Email** panel of the **Preferences** dialog box.

3. Send your message as you normally do.

   If you have a copy of the public keys for every one of the recipients, the appropriate keys are automatically used. However, if you specify a recipient for whom there is no corresponding public key or one or more of the keys have insufficient validity, the **PGP Recipient Selection** dialog box appears (Figure 5-1) so that you can specify the correct key.

   You can force the **PGP Recipient Selection** dialog box to appear, even if you have a valid copy of the public keys for every one of the recipients, by holding down the SHIFT KEY when you hit SEND. You should do this if you want to use the Secure Viewer or Conventional Encrypt features and you do not want your message to be sent automatically.



To add a user to the list of encryption recipients, drag it from the Users list to the Recipients list.

Users	Validity	Size
Abe <abe@ nai.com>	○	2048/1024
Beth <beth@ nai.com>	●	2048/1024
Elle <elle@ nai.com>	●	2048/1024
Group Key	●	2048/1024
Gwen <gwen@nai.com>	●	2048

Recipients	Validity	Size
Carl <carl@ nai.com>	●	2048/1024
Dave <dave@nai.com>	●	2048/1024

Figure 5-1. PGP Recipient Selection window

4. Drag the public keys for those who are to receive a copy of the encrypted email message into the **Recipients** list box. You can also double-click any of the keys to move it from one area of the screen to the other.

   The **Validity** icon indicates the minimum level of confidence that the public keys in the **Recipient** list are valid. This validity is based on the signatures associated with the key. See Chapter 4, “Managing Keys,” for details.

5. You can choose from the following encryption options depending on the type of data you are encrypting:

    - **Secure Viewer.** Select this option to protect the data from TEMPEST attacks upon decryption. If you select this option, the decrypted data is displayed in a special TEMPEST attack prevention font that is unreadable to radiation capturing equipment, and cannot be saved in decrypted format. For more information about TEMPEST attacks, see the section on vulnerabilities in *An Introduction to Cryptography*.

        NOTE: The **Secure Viewer** option may not be compatible with previous versions of PGP. Messages encrypted with this option enabled can be decrypted by previous versions of PGP, however this feature may be ignored.

    - **Conventional Encrypt.** Select this option to use a common passphrase instead of public key encryption. If you select this option, the message is encrypted using a session key, which encrypts (and decrypts) using a passphrase that you will be asked to choose.

        You can also use this feature without a passphrase to create compact Self-Extracting Archives (SEA) which are not encrypted. The resulting archives run on both PowerPC and 68K Macs.

6. Click **OK** to encrypt and sign your mail.

    If you have elected to sign the encrypted data, the **Signing Key Passphrase** dialog box appears, requesting your passphrase before the mail is sent.

7. Enter your passphrase and then click **OK**.

    WARNING: If you do not send your email immediately but instead store it in your outbox, you should be aware that when using some email applications the information is not encrypted until the email is actually transmitted. Before queuing encrypted messages you should check to see if your application does in fact encrypt the messages in your outbox. If it does not, you can use PGPmenu’s **Encrypt Now** option to encrypt your messages before queuing them in the outbox.

Encrypting and signing email without PGP plug-in support

If your email application does not support the PGP plug-ins, you can use PGPtools to encrypt the text of your message prior to sending it.

To encrypt and sign email without a PGP plug-in:

1. Use your email application to compose your email message as you normally would.

   TIP: If you are sending sensitive email, consider leaving your subject line blank or creating a subject line that does not reveal the contents of your encrypted message.

2. When you have finished composing the text of your email message, open PGPmenu and select **Encrypt**, **Sign**, or **Encrypt & Sign**.

   TIP: If these options are dimmed, you need to add the application to the **Menu** panel of the **Preferences** dialog box. For more information on adding an application, see “Setting menu preferences” on page 158.

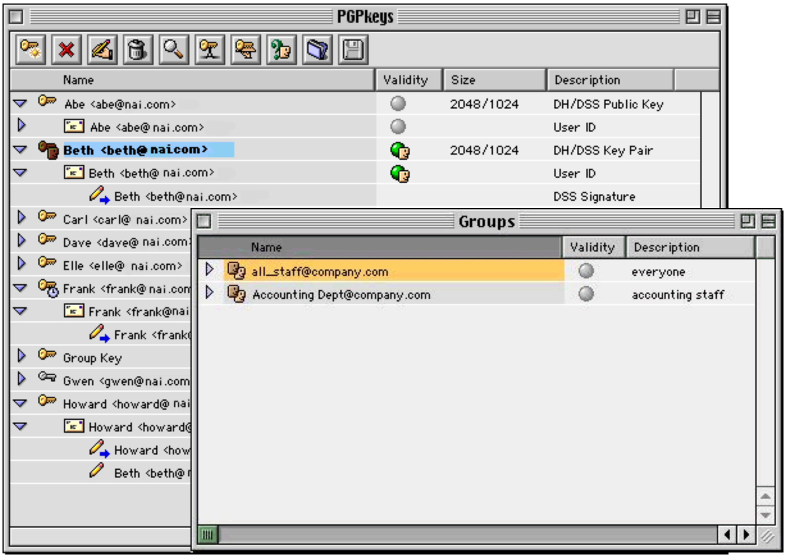
   Encrypted text appears in your email message window.

3. Continue with Step 3 on page 96 to complete your encrypting and signing task.

Encrypting email to groups of recipients

You can use PGP to create group distribution lists. For example, if you want to send encrypted mail to 10 people at usergroup@nai.com, you could create a distribution list with that name. The **Groups** menu in PGPkeys contains the **Show Groups** option that toggles the display of the **Groups** window in PGPkeys. The **Groups** window is displayed as in Figure 5-2.

NOTE: If you intend to encrypt information to all members of an existing email distribution list, you must create a PGP group by the same name as, and including the same members as, the email distribution list. For example, if there is a *usergroup@nai.com* list set up in your email application, you must create a usergroup@nai.com group in PGP.



Name	Validity	Size	Description
Abe <abe@nai.com>	●	2048/1024	DH/DSS Public Key
Abe <abe@ nai.com>	●		User ID
Beth <beth@ naicom>	🟢	2048/1024	DH/DSS Key Pair
Beth <beth@ nai.com>	🟢		User ID
Beth <beth@nai.com>			DSS Signature
Carl <carl@ nai.com>			
Dave <dave@ nai.com			
Elle <elle@ nai.com>			
Frank <frank@ nai.com			
Frank <frank@nai			
Frank <frank			
Group Key			
Gwen <gwen@nai.com			
Howard <howard@ nai			
Howard <howard@			
Howard <how			
Beth <beth@			

Name	Validity	Description
all_staff@company.com	●	everyone
Accounting Dept@company.com	●	accounting staff

Figure 5-2. PGPkeys with Groups window

Working with distribution lists

Use the Groups feature to create distribution lists and to edit the list of people to whom you want to send encrypted email.

To create a group (distribution list):

1. Choose **New Group** from the **Groups** menu.

2. Enter a name for the group distribution list. Optionally, enter a group description. For example, you can name the group “everyone@nai.com” with a description of “All employees.”

3. Click **OK** to create the distribution list.

   The group distribution list is added to your keyring and can be viewed in the **Groups** window.

To add members to a distribution list:

1. In the PGPkeys window, select the users or lists you want to add to your distribution list.

2. Drag the users from the PGPkeys window to the desired distribution list in the **Groups** window.

> **NOTE:** Members in a distribution list can be added to other distribution lists.

To add a distribution list to another distribution list:

1. Select the distribution list that you want to add to another list.

2. Drag the selected list into the list to which it will be added.

To delete members from a distribution list:

1. Within the distribution list, select the member to be deleted.

2. Press the DELETE key.

   PGP asks you to confirm your choice.

To delete a distribution list:

1. Select the distribution list to be deleted from the **Groups** window.

2. Press the DELETE key.

Sending encrypted and signed email to distribution lists

You can send encrypted email to groups of recipients once your PGP distribution lists are created. See "Working with distribution lists" on page 99 for more information about creating and editing distribution lists.

To send encrypted and signed email to a distribution list:

1. Address the mail to your mail distribution list.

   The name of your encryption distribution list must correspond to the name of the email distribution list.

2. Use your email application to compose your email message just as you normally would.

3. When you have finished composing the text of your email message, open PGPmenu and select **Encrypt**, **Sign**, or **Encrypt & Sign**.

   The **PGP Key Recipients** dialog box appears (Figure 5-1). Select the recipient's public keys for the text you are encrypting or signing. The options available are described in "To encrypt and sign with supported email applications:" on page 95.

4. Send the message.

Decrypting and verifying email

The quickest and easiest way to secure email communications is by using an email application supported by the PGP plug-ins. If you are using an email application that is not supported by the PGP plug-ins, you can encrypt, sign, decrypt and verify the text of your email messages by using PGPmenu or PGPtools.

Decrypting and verifying email using the PGP plug-ins

Although the procedure varies slightly between different email applications, when you are using an email application supported by the plug-ins, you can perform the decryption and verification operations by clicking the envelope icon in the message or your application's toolbar. In some cases you may need to select **Decrypt/Verify** from the menu in your email application. In addition, if you are using an application that supports the PGP / MIME standard, you can decrypt and verify your email messages as well as any file attachments by clicking an icon attached to your message.

If you are using an email application that is not supported by the PGP plug-ins, you will decrypt and verify your email messages via PGPmenu. In addition, if your email includes encrypted file attachments, you must decrypt them separately via PGPtools or PGPmenu.

To decrypt and verify from supported email applications:

1. Open your email message just as you normally do.

   You will see a block of unintelligible ciphertext in the body of your email message.

2. To decrypt and verify the message, click the locked envelope icon (✉).

   To decrypt and verify attached files, decrypt them separately using PGPtools or PGPmenu.

   The **PGP Enter Passphrase** dialog box appears, asking you to enter your passphrase.

3. Enter your passphrase, then click **OK**.

   The message is decrypted. If it has been signed and you have the sender's public key, a message appears indicating whether the signature is valid.

   If the message is encrypted with the **Secure Viewer** option enabled, an advisory message appears. Click **OK** to continue. The decrypted message appears on a secure PGP screen in a special TEMPEST attack prevention font.

4. You can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.

> **NOTE:** Messages encrypted with the **Secure Viewer** option enabled cannot be saved in their decrypted state.

Decrypting and verifying email without PGP plug-in support

If your email application does not support the PGP plug-ins, you can use PGPtools to decrypt the text of your message prior to sending it.

To decrypt and verify from non-supported email applications:

1. Open your email message just as you normally do.

   You will see a block of unintelligible ciphertext in the body of your email message.

2. In PGPmenu, select **Decrypt/Verify**.

   If the email message includes encrypted file attachments, decrypt them separately with PGPtools or PGPmenu.

   The **PGP Enter Passphrase** dialog box appears asking you to enter your passphrase.

3. Enter your passphrase, then click **OK**.

   The message is decrypted. If it has been signed, a message appears indicating whether the signature is valid.

   If the message is encrypted with **Secure Viewer** enabled, an advisory message appears. Click **OK** to continue. The decrypted message appears on a secure PGP screen in a special TEMPEST attack prevention font.

4. You can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.

> **NOTE:** Messages encrypted with the **Secure Viewer** option enabled cannot be saved in their decrypted state.

Securing Files 6

This chapter describes how to use PGP to securely maintain files. It describes how to use PGP to encrypt, decrypt, sign, and verify files either for email or for secure storage on your computer. It also describes the PGP Wipe and Free Space Wiper functions, which delete files by erasing their contents completely from your computer.

Securing your files and folders with PGP

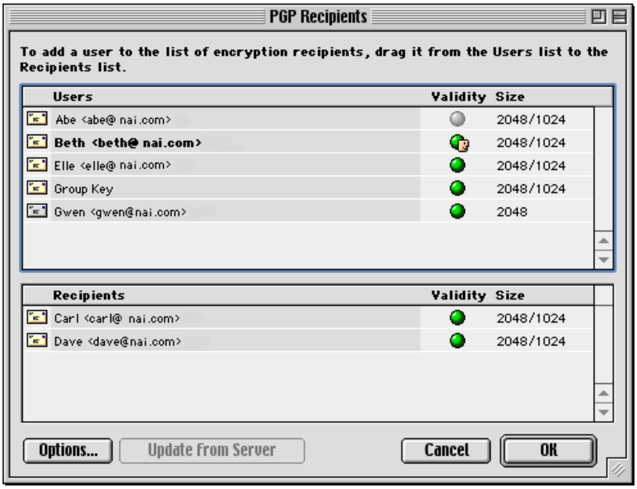
You can use PGP to encrypt and sign files to use as email attachments as well as decrypt and verify files or attachments that have been encrypted to you. You use the techniques described in this chapter to perform any of these PGP tasks.

Encrypting and signing files

Use the **Encrypt**, **Sign**, or **Encrypt and Sign** options available from PGPmenu, PGPtools, or the PGP contextual menu to secure your files and folders.

NOTE: For information about accessing PGPmenu, PGPtools, or the PGP contextual menu, refer to Chapter 2, “A Quick Tour of PGP”.

When you select **Encrypt** or **Encrypt and Sign**, the **PGP Key Selection** dialog box automatically appears, as shown in Figure 6-1 on page 106. This dialog box allows you to select the recipients public keys for the data you are encrypting.



To add a user to the list of encryption recipients, drag it from the Users list to the Recipients list.

Users	Validity	Size
Abe <abe@ nai.com>	○	2048/1024
Beth <beth@ nai.com>	●	2048/1024
Elle <elle@ nai.com>	●	2048/1024
Group Key	●	2048/1024
Gwen <gwen@nai.com>	●	2048

Recipients	Validity	Size
Carl <carl@ nai.com>	●	2048/1024
Dave <dave@nai.com>	●	2048/1024

Figure 6-1. PGP Key Selection dialog box

You select the public keys by dragging them to the **Recipients** list. You can choose additional encryption options by clicking the **Options** button. The options available to you depend upon the type of data that you are encrypting. Here are the possible options:

- **Text Output.** When sending files as attachments with some email applications, you may need to select the **Text Output** check box to save the file as ASCII text. This is sometimes necessary in order to send a binary file using older email applications. Selecting this option increases the size of the encrypted file by about 30 percent.
- **MacBinary**.
  - **Yes.** This is the recommended option for all encryptions when sending to another user of PGP Version 5.5 or above on any platform. This means that Mac OS users will receive the exact file that was intended.
  - **No.** Select this option when sending encrypted files to a PC using an older version of PGP if you know that the file you are sending can be read by Windows applications when no MacBinary is used.
  - **Smart.** Select this option when communicating with users who are not using PGP versions 5.5 or above.
- **Wipe Original.** Select this check box to overwrite the original document that you are encrypting, so that your sensitive information is not readable by anyone who can access your hard disk.

- **Secure Viewer.** Select this check box to protect text from TEMPEST attacks upon decryption. If you select this option, the data is displayed in a special TEMPEST attack prevention font that is unreadable to radiation capturing equipment upon decrypting, and your email can’t be saved in decrypted format. For more information about TEMPEST attacks, see the vulnerabilities section in *An Introduction to Cryptography*. This option is only available when encrypting text or text files.
- **Conventional Encrypt.** Select this check box to rely on a common passphrase rather than on public key cryptography. The file is encrypted using a session key, which encrypts (and decrypts) using a passphrase that you are asked to choose.
- **Self Decrypting Archive (SDA).** Select this check box to create a self decrypting executable file. If you select this option, the file is encrypted using a session key, which encrypts (and decrypts) using a passphrase that you are asked to choose. The resulting executable file can be decrypted by simply double-clicking on it and entering the appropriate passphrase. This option is especially convenient for users who are sending encrypted files to people who do not have PGP software installed. Note that sender and recipient must be on the same operating system.

  If you select this check box, you can also create non-encrypted self-extracting archive. To create a self-extracting archive with PGP, do not provide passphrase and click **OK**. The resulting executable file will have a .SEA extension.

If you are signing the files, you are asked to supply your passphrase. After encryption, if you look in the folder where the original file was located, you will find a file with the specified name represented by one of three icons:

encrypted with text output

encrypted with standard output

self decrypting archive output

If you are encrypting or signing a folder, the output may be in a new folder, depending on the options you selected.

Decrypting and verifying files

When someone sends you encrypted data in a file, you can unscramble the contents and verify any appended signature to make sure that the data originated with the alleged sender and that it has not been altered.

Use the **Decrypt & Verify** option available from PGPmenu, PGPtools, or the PGP contextual menu to decrypt your files and folders.

NOTE: For information about accessing PGPmenu, PGPtools, or the PGP contextual menu, refer to Chapter 2, “A Quick Tour of PGP”.

To decrypt and/or verify data that has been encrypted to your key, you must have your private key and passphrase to complete the task. If the file was encrypted with the **Secure Viewer** option enabled, the decrypted text appears on a secure PGP screen in a special TEMPEST attack prevention font. Otherwise, the message will appear in its original state.

NOTE: Messages encrypted with the **Secure Viewer** option enabled cannot be saved in their decrypted state. They are only viewable on the secure PGP screen after decryption.

Opening a self-decrypting archive

To open a self decrypting archive (SDA), double-click the executable file (the file should have a .SDA.EXE extension). Enter the correct password and specify a location in which to save the decrypted file.

Signing and decrypting files with a split key

Whenever you want to sign or decrypt files with a split key, you must rejoin the key before you can perform the signing or decrypting task. For detailed instructions on collecting and rejoining a split key, see “Rejoining split keys” on page 83.

Permanently erasing files and free disk space

As you create and delete sensitive files on your computer, fragments from the data contained in the files remain in the free disk space of your computer. When you delete a file normally by placing it in the Trash, the name of the file is removed from the file directory but the data in the file remains on the disk. Even when you empty the Trash the data is not completely erased until the operating system overwrites the free disk space. Also, many programs create temporary files while you edit the contents of your documents. These files are deleted when you close the documents but your data is also left behind in free disk space.

In essence, your sensitive files are never completely erased and with the proper tools someone could retrieve your previously deleted files and even gather personal information from the free disk space of your computer.

If you want to completely destroy your sensitive files without leaving fragments of their data behind, use the PGP Wipe utility. When you delete a file using Wipe, the file is immediately overwritten (even on systems with virtual memory) and all traces of the file are removed so that it cannot be retrieved even by using disk recovery software. To learn how to erase files with the Wipe utility, see “Using PGP Wipe to permanently delete a file” on page 110.

In addition, you can set file wiping preferences from the **General** panel of the **PGP Preferences** dialog box to enable Wipe to automatically wipe files when deleting them. To learn how to enable these settings, see “Setting general preferences” on page 152.

To erase the free disk space that contains data from previously deleted files and programs, use PGP Free Space Wiper. To ensure that your deleted data is irrecoverable, erase your free disk space periodically with the Free Space Wiper. To learn how to erase the free disk space on your computer, see “Using the PGP Wipe Free Space Wizard to clean free disk space” on page 111.

Using PGP Wipe to permanently delete a file

Use the **Wipe** feature available from PGPtools and the PGP contextual menu to permanently erase your files and folders.

NOTE: For information about accessing PGPtools, or the PGP contextual menu, refer to Chapter 2, “A Quick Tour of PGP”.

To permanently delete your files and folders:

1. Select the files or folders that you want to delete.
2. Choose **Wipe** from PGPtools or from the PGP contextual menu.

   A confirmation dialog box appears.
3. Click **OK** to permanently erase the file.

   To stop wiping the file before the task is completed, click **Cancel**.

   NOTE: Clicking **Cancel** during file wipe can leave remnants of the file behind.

   IMPORTANT: Many programs automatically save files in progress, so back-up copies of the file you deleted may exist. PGP Security, Inc. recommends that you run the Wipe utility on the back-up copies as well as the original file to thoroughly erase it from your hard disk.

Using the PGP Wipe Free Space Wizard to clean free disk space

Use the **Wipe Free Space** feature available from PGPtools to clean your free disk space.

NOTE: For information about starting the PGPtools application, refer to Chapter 2, “A Quick Tour of PGP”.

To wipe free space on your disks:

WARNING: Before running the PGP Free Space Wiper, file sharing must be turned off.

1. In PGPtools, click the Freespace Wipe button ( ) to start the Freespace Wipe Wizard.

   The **PGP Free Space Wiper Welcome** screen appears.

2. Read the information carefully, then click **Next** to advance to the next dialog box.

   The **PGP Free Space Wiper** prompts you to select the volume you want to wipe and the number of passes you want to perform.

3. In the **Volume** box, select the disk or volume that you want PGP to wipe. Then, select the number of passes that you want PGP to perform. The recommended guidelines are:

   - 3 passes for personal use.
   - 10 passes for commercial use.
   - 18 passes for military use.
   - 26 passes for maximum security.

   NOTE: Commercial data recovery companies have been known to recover data that has been over written up to 9 times. PGP uses highly sophisticated patterns during each wipe to ensure that your sensitive data cannot be recovered.

4. Click **Next** to continue.

   The **Perform Wipe** dialog box opens and displays statistical information about the drive or volume you selected.

5. Click the **Begin Wipe** button to start freespace wiping your disk or volume.

   The PGP Free Space Wiper scans and then wipes leftover fragments from your disk or volume.

6. When the wipe session ends, click **Finish**.

> **WARNING:** Clicking **Cancel** during file wipe can leave remains of the file on your computer.

Scheduling folder and free space wiping

You can use AppleScript to schedule periodic folder and free space wiping for selected folders. The AppleScript dictionary for this is located in PGPtools.

To schedule folder and free space wiping:

1. Open the Script Editor and choose **New Script** from the **File** menu.

> **TIP:** The Script Editor is located in the **AppleScript** folder in the **Apple Extras** folder on your startup disk.

   The new script window appears.

2. Enter a description for the script in the **Description** text box—for example, “Scheduled Free Space Wipe - 3 passes.”

3. Enter the following information into the AppleScript text box:

```
with timeout of X seconds

tell application “PGPtools”

activate

wipe free space volume “Your Macintosh HD” passes Y

end tell

end timeout
```

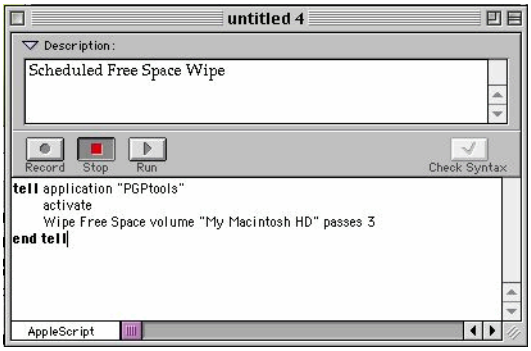
Where "*Your Macintosh HD*" is, enter the name of the hard disk in which you want to wipe freespace.

Where *X* is, enter the amount of time you want to allocate for the Free Space Wipe session. Wiping may take a long time to complete, depending on the amount of passes you specified and the speed of the computer you are using. If you are unsure, enter a high timeout number (for example, 60,000 seconds).

4. Click the **Check Syntax** button in the script window and navigate to the PGPtools application.

TIP: Use the PGPtools Dictionary to view a list of acceptable syntax. To open the PGPtools Dictionary, choose **Open Dictionary** from the **File** menu and navigate to PGPtools in your PGP folder.

When the syntax check is complete, the Script Editor formats the script, as shown in Figure 6-2.



Scheduled Free Space Wipe

```
tell application "PGPtools"
	activate
	Wipe Free Space volume "My Macintosh HD" passes 3
end tell
```

Figure 6-2. Script Editor window

5. Choose **Save** from the **File** menu.
6. When the **Save** dialog box appears select a location and specify a name for the script.
7. Open the **Kind** pop-up menu and choose **Application**.
8. Click **Save**.

You can customize your script to wipe additional hard disks or to run different or multiple wipe schedules. You can ensure periodic wiping by saving the compiled script in your Shutdown Items folder in the System folder.

Part IV: Securing Your Network Communications with PGPnet

PGPnet Basics 7

Learning about PGPnet

Today's technology has brought many changes to the workplace. The bulk of interoffice memos and reports traditionally placed in a mailbox and received in a few days is now sent electronically and received in a matter of seconds. Employees who work at home or travel can now make a phone call to transfer data to and from their local or home office.

Two by-products of these advances are an increased security threat to data transmitted over phone lines, and a significant rise in the cost of phone services. Companies saw the Internet as an answer to rising costs, but security remained an issue.

Fortunately, even newer technologies provide solutions to these problems. *Virtual Private Networks (VPNs)* allow corporations to transmit data securely over the Internet, reducing the security threat to transmitted data while sharply reducing the cost of phone services.

For an overview of the PGPnet user interface, refer to Chapter 8, "A Quick Tour of PGPnet."To learn how to configure the features of PGPnet, refer to Chapter 9, "Configuring PGPnet's VPN Feature."

What is a Virtual Private Network?

A Virtual Private Network (VPN) is a secure communications link over an insecure medium—generally the Internet. The link is secured by software installed on machines at both ends of the communications connection. The software requires user authentication and performs data encryption. With a VPN in place, only legitimate users can participate in secured data transactions, and no one can tamper with or read data in transit.

A VPN is useful any time you want to send or receive data via the Internet, and be confident that the data will not be read by others, changed by others, or sent by an imposter. For example:

- Remote hosts can use VPNs to communicate securely with a corporate network.
- Two corporate networks (perhaps belonging to the same organization) that are geographically separate can use a VPN to communicate as one network.
- Companies that install VPNs can use them to make their internal data available to trusted companies and individuals (for example, suppliers and consultants, or even specific individuals within the company).
- Individuals that want to communicate with each other privately via the Internet can do so using a VPN connection.

These are all examples where a VPN serves as a low-cost, secure means for transmitting data.

How does PGPnet's VPN feature work? Let's look at an example.

Let's say you are a user on the corporate network of Company A. Your boss tells you that you need to communicate with an off-site sales associate. These communications include information that is considered confidential. Not to worry—you can communicate with the sales associate via a Virtual Private Network.

Setting up VPN communications using PGPnet is straightforward:

1. Make sure that the remote computer (in this example, the computer belonging to the sales associate) can connect to the corporate network via a direct line or the Internet.
2. Make sure that both your computer and the remote computer are equipped with PGP Desktop Security (or a compatible product).
3. List the remote computer (by IP address) as a host you want to communicate with via a VPN connection.

4. Select a method for encrypting and authenticating your data; for example, a shared secret passphrase or an encryption key.

   (For more information on making keys, refer to Chapter 3, “Making and Exchanging Keys”.)

Once these basic criteria are met, secure communication between your computers can happen automatically. For detailed instructions on how to configure PGPnet’s VPN feature, refer to Chapter 9, “Configuring PGPnet’s VPN Feature.”

VPN terms

While VPN communication is fairly simple to set up, the behind-the-scenes negotiations between computers can get a bit more complex. The following is a list of terms and phrases that are used frequently in the context of virtual private networking. You may encounter these terms as you use PGPnet to secure your network communications. Reading this section is optional—do so if you are interested in learning more about VPN terminology.

- *IPsec* (Internet Protocol Security) is a protocol designed as the standard to ensure secure information transfer over insecure networks such as the Internet.
- A *secure host* is a machine running PGPnet or another IPsec-compatible peer-to-peer capable client software (that is, software that allows hosts to communicate directly with each other).
- A *gateway* is a machine that connects your computer or network to other networks.
- *Tunnel mode* is a VPN mode used to communicate with hosts or subnets that are behind a secure gateway.
- *Transport mode* is a VPN mode used for communications between two secure hosts that do not have a gateway between them (also called *peer-to-peer* communications).
- A *secure subnet* is a subnet (a network that forms part of a larger network) that has up to 254 machines behind it that are generally running PGPnet or a compatible client software. The secure subnet designation allows you (or your administrator, if applicable) to identify a number of machines in the same IP address range that are known to be IPsec-compatible. Note that secure subnets do not have to be behind gateways.
- An *insecure host* is a machine that is not running PGPnet or another IPsec-compatible peer-to-peer capable client software.

- An *insecure subnet* is one that has up to 254 machines behind it that are not running PGPnet or a compatible client software.
- A *Security Association (SA)* is an agreement that summarizes terms for secure communication between two machines. An SA is created the first time a local machine communicates with a remote machine, and it describes how the machines will communicate with one another (for example, the type of encryption, the duration of their association, and the method of authentication).

  PGPnet records and monitors all SAs that your machine initiates and that other machines initiate with your machine. When an SA that your machine initiated is close to expiration, PGPnet initiates another SA with the remote host.

  NOTE: You can view all active SAs on PGPnet's **Status** panel. For more information on the **Status** panel, see "Reviewing the status of existing SAs" on page 126.

- *IKE (Internet Key Exchange)* is a secure means for exchanging keys over the Internet.

A Quick Tour of PGPnet 8

This chapter gets you started using PGPnet and introduces you to PGPnet's user interface.

Displaying PGPnet

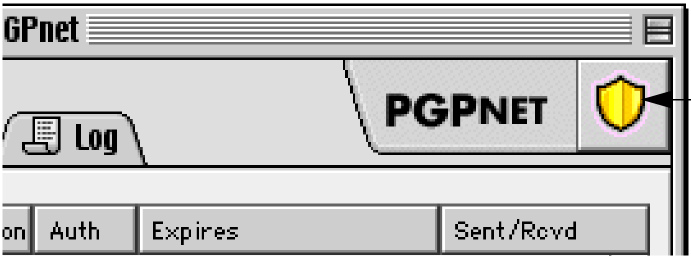
To display PGPnet, click **PGPmenu**, and then select **PGPnet** (the **PGPmenu** appears as an icon in the menu bar of the Finder).

Turning PGPnet on and off

When PGPnet is on, it is running in the background. To communicate with a machine, use your software (for example, email or web browser) as you normally would. PGPnet evaluates each communication and encrypts and tunnels as required.

Use the button in the upper-right corner of the main PGPnet window to turn PGPnet on and off. (See Figure 8-1.)

- If PGPnet is turned off and the machine is rebooted, PGPnet will be off after reboot.
- If PGPnet is turned off, all communication with all machines is allowed to pass through unmodified and unsecured.



Click here to turn on and off

Figure 8-1. Turning PGPnet on and off

Quitting PGPnet

To quit PGPnet, select **Quit** from PGPnet’s **File** menu.

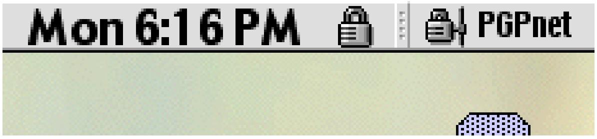
Note that exiting PGPnet does not disable the PGPnet service or terminate SAs.

PGPnet features

To:	See:
learn about PGPmenu’s icon	“PGPmenu’s icon” on page 123
understand the PGPnet window	“The PGPnet window (at a glance)” on page 123
review the status of existing SAs	“Reviewing the status of existing SAs” on page 126
establish and terminate SAs	“Establishing and terminating SAs” on page 128
block communications with other machines	“Blocking communications with other machines” on page 129
understand entries on PGPnet’s Log panel	“Reviewing PGPnet’s log entries” on page 133
change your TCP/IP configurations	“Changing your secure TCP/IP configurations” on page 134

PGPmenu’s icon

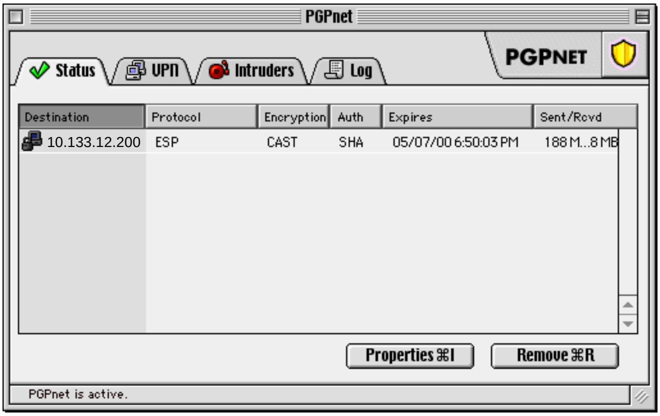
PGPmenu’s icon tells you the status of PGPnet.



PGPmenu’s icon

Figure 8-2. PGPmenu’s icon

The PGPnet window (at a glance)



Destination	Protocol	Encryption	Auth	Expires	Sent/Rcvd
10.133.12.200	ESP	CAST	SHA	05/07/00 6:50:03 PM	188 M...8 MB

PGPnet is active.

Menus

When PGPnet is active, there are four menus in the menu bar:

- **File** (**Open Hosts**, **Close**, **Save Hosts**, **Configurations**, and **Quit**)
- **Edit** (**Select All** and **Preferences**)
- **View** (**Status**, **VPN**, **Intruders**, and **Log**)
- **Help** (**PGP Help**)

Panels

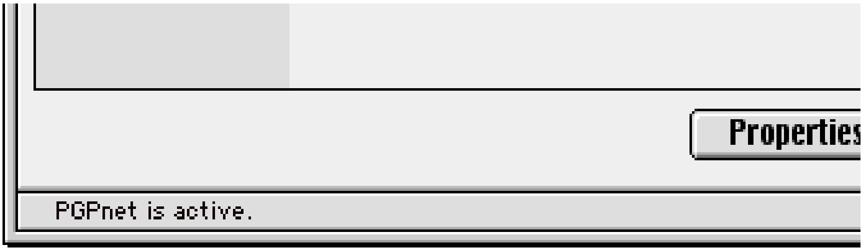
There are four panels on the PGPnet window:

- **Status panel**. Use to review the status of existing SAs (see "Reviewing the status of existing SAs" on page 126).
- **VPN panel**. Use to add, edit, or remove entries in PGPnet's host list, and to manually establish and terminate SAs. Note that once hosts are added to the host list, you can also establish and terminate SAs from PGPmenu in PGPtray.

  In addition to adding entries to the host list manually, you can drag and drop a PGPnet host list from the desktop to the **VPN** panel.

  If an arrow appears to the left of an entry in the host list, click the arrow to expand the display and view other entries associated with that entry. To edit a host entry, double-click on the host entry or select the entry and click **Properties**. Use the **Connect** and **Disconnect** button to establish and terminate SAs. (see "Establishing and terminating SAs" on page 128).
- **Intruders panel**. Use to review communications blocked by PGPnet's firewall and to add hosts to and remove hosts from the list of blocked hosts (see "Blocking communications with other machines" on page 129).
- **Log panel**. Use to review log entries for diagnostic purposes (see "Reviewing PGPnet's log entries" on page 133).

Status bar



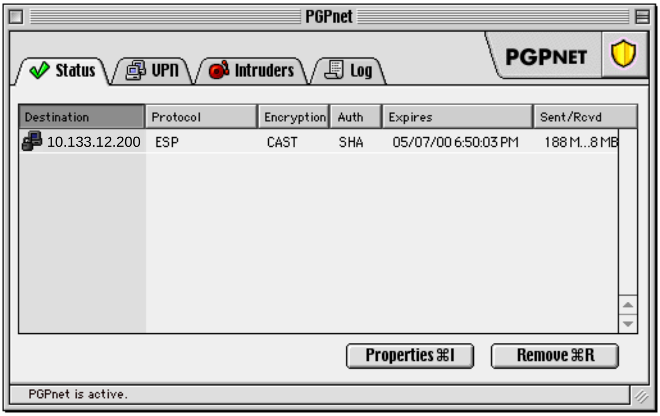
PGPnet is active.

Figure 8-3. PGPnet’s status bar

The messages in the status bar tell you if the PGPnet is active or inactive, and if the PGPservice (a background program) is running.

Message:	Description:
PGPnet is active	PGPnet is configured for the current TCP/IP configuration and is turned on.
PGPnet is inactive	PGPnet is not configured for the current TCP/IP configuration.
PGPnet is active but turned off	PGPnet is configured for the current TCP/IP configuration but is turned off.
PGPservice is not running	The PGPservice, a required program that runs in the background, is not running.

Reviewing the status of existing SAs



Destination	Protocol	Encryption	Auth	Expires	Sent/Rcvd
10.133.12.200	ESP	CAST	SHA	05/07/00 6:50:03 PM	188 M...8 MB

PGPnet is active.

Figure 8-4. The Status panel

The **Status** panel in the PGPnet window lists active PGPnet SAs (see Figure 8-4 on page 126). An SA may be terminated when it reaches a certain byte limit (for example, 4 MBs of data has been transmitted over the SA), or after a specific amount of time. The length of an SA is negotiated when it is initiated. When PGPnet negotiates the SA, it sets an expiration value and automatically creates a new SA when the SA reaches that value and expires. The SA expiration value is user-configurable; for more information, see "Setting automatic key renewal values" on page 171.

- If your machine initiated an SA and the SA is about to expire, PGPnet automatically initiates the negotiation of a new SA to replace the expiring SA. As a result, there may be times when the **Status** panel displays two SAs for the same machine.

- When you establish an SA with another host, PGPnet uses the most restrictive expiration values set by either of the two hosts. As a result, you may see an SA expire before your maximum expiration value is met because the other host has more restrictive expiration values set.

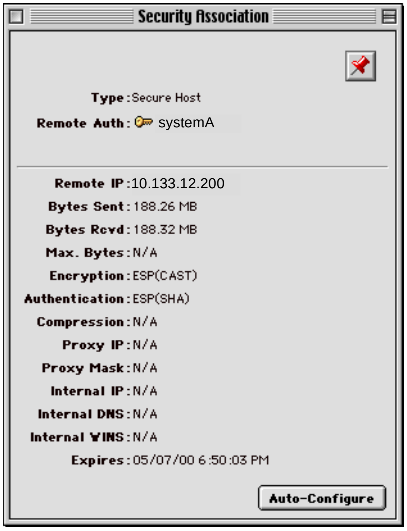
Use the **Remove** feature to remove an SA. Remove an SA when you think that it has been compromised, if you know that the target host is down, or for any reason that you think the connection should be terminated. Note that if PGPnet is turned off, this button is disabled.

Use the **Properties** feature to view the details of an SA, including IP address, bytes sent, type of encryption, and so on (the Security Association properties dialog). To view details, select the host and click **Properties** (Figure 8-5**)**. Click the pushpin in the upper right corner to keep the window displayed on your screen. When the window is open, click the X in the upper right corner to close the window or click **Close**.

Use the **Auto-Configure** feature to configure a host entry based on an existing SA.

- If the SA is for a configured host, PGPnet imports the SA's authentication key to your PGP keyring, and assigns this key as the authentication key for the configured host.
- If the SA is for an unconfigured host, PGPnet creates a new secure host entry in the host list, imports the SA's authentication key to your PGP keyring, and assigns this key as the authentication key for the configured host.

If the SA does not have an associated authentication key (that is, it uses shared secret for authentication), you cannot use this feature.

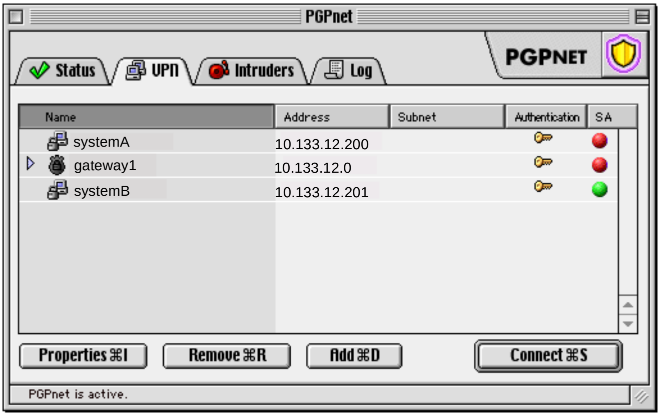


Type : Secure Host
Remote Auth : systemA

Remote IP : 10.133.12.200
Bytes Sent : 188.26 MB
Bytes Rcvd : 188.32 MB
Max. Bytes : N/A
Encryption : ESP(CAST)
Authentication : ESP(SHA)
Compression : N/A
Proxy IP : N/A
Proxy Mask : N/A
Internal IP : N/A
Internal DNS : N/A
Internal WINS : N/A
Expires : 05/07/00 6:50:03 PM

Figure 8-5. SA Properties dialog

Establishing and terminating SAs



Name	Address	Subnet	Authentication	SA
systemA	10.133.12.200		🔑	🔴
▷ gateway1	10.133.12.0		🔑	🔴
systemB	10.133.12.201		🔑	🟢

PGPnet is active.

Figure 8-6. The VPN panel

The **VPN panel** displays secure gateways, subnets, and hosts. If an arrow appears to the left of an item, click the arrow to expand the display and view other entries associated with that item. All buttons are disabled if PGPnet is turned off.

Use the **Connect** button to establish an SA with a configured host. Select the host, then click **Connect**. The **Connect** button is disabled when an inappropriate host entry is selected (for example, when you select a secure subnet or insecure host that is not behind a gateway).

Click **Properties** to edit an entry.

Use the **Disconnect** button to terminate an SA with a configured host. Select the host, then click **Disconnect**.

Opening a host list

There are two ways to open an existing PGPnet host list and add the hosts to the **VPN** panel:

- Drag the host list from the desktop to the PGPnet **VPN** panel.
- Select **Open Hosts** from PGPnet’s **File** menu, browse and select the file you want to open, and click **Open**.

Saving a host list

To save a host list:

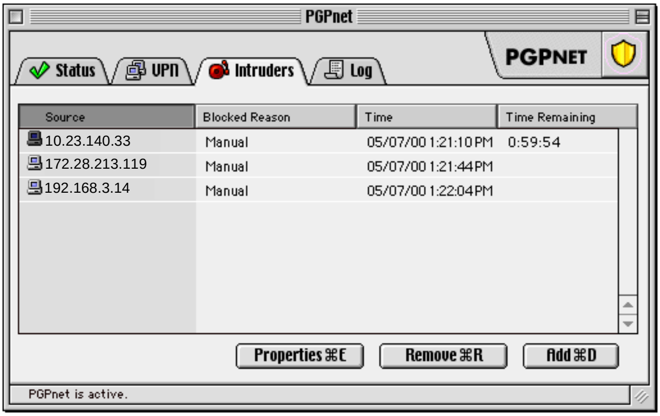
1. Select **Save Hosts** from PGPnet's **File** menu.
2. Name the file you want to save the hosts file to, then click **Save**.

Blocking communications with other machines

PGPnet's **Intruders** panel displays hosts that are blocked from communicating with your system, why they are blocked, and how long communication with the host will remain blocked.

Use this panel to block another system from communicating with your system, to use PGPnet's **Trace Source** feature (traces communication from you back to the source), or to remove a host from the blocked hosts list.

When a host attacks your system and you block further communication from that system, you can use the **Trace Source** feature to attempt to discover information about the attacker. For more information, see "Tracing an attacker" on page 131. Note that when a host is blocked, additional attacks are not reported.

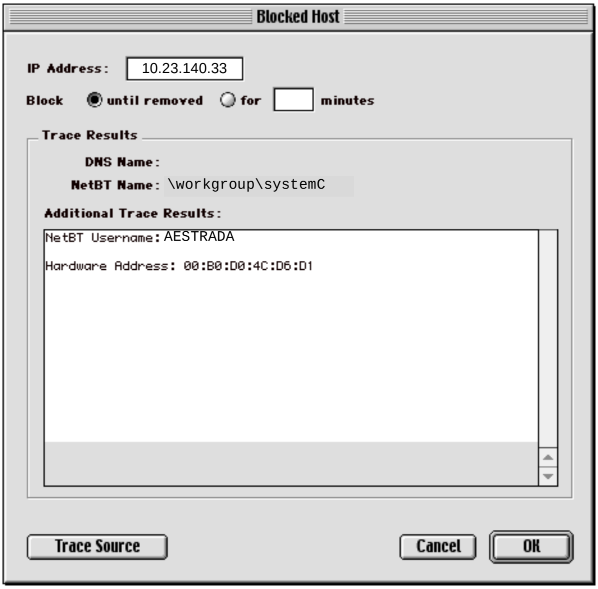


Source	Blocked Reason	Time	Time Remaining
10.23.140.33	Manual	05/07/00 1:21:10 PM	0:59:54
172.28.213.119	Manual	05/07/00 1:21:44 PM	
192.168.3.14	Manual	05/07/00 1:22:04 PM	

PGPnet is active.

Figure 8-7. The Intruders panel

Use **Properties** to view details regarding a blocked host. To do so, select the host and click **Properties**.



IP Address: 10.23.140.33

Block ● until removed ○ for minutes

DNS Name:

NetBT Name: \workgroup\systemC

Additional Trace Results:

NetBT Username: AESTRADA

Hardware Address: 00:B0:D0:4C:D6:D1

Figure 8-8. Intruders Properties window: Blocked Host

Use **Remove** to remove a host from the list of blocked hosts (see "Removing a host from the list of blocked hosts" on page 132).

Use **Add** to add a host to the list of blocked hosts (see "Blocking a host and tracing the source of communications" on page 131).

Use **DNS Lookup** to identify the IP address of a host.

Blocking a host and tracing the source of communications

To block communications from a specific IP address:

1. Click **Add**. PGPnet displays the **Blocked Host** dialog.
2. Enter the IP address of the computer that you want to block or click **DNS Lookup** to find the IP address.
3. Click **Until removed** or **for** and enter the number of minutes.
4. Click **OK**.

Tracing an attacker

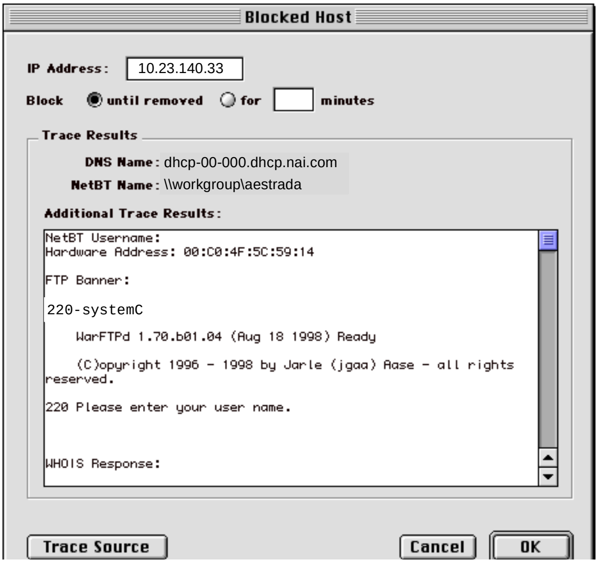
When a host attacks your system and becomes a blocked host, you can use PGPnet's **Trace Source** feature (see Figure 8-9 on page 132) to attempt to discover the following information about the attacker: DNS name, NetBIOS information, TELNET banner, HTTP server version, WHOIS, traceroute, FTP server banner, and SMTP banner. (A *banner* is a text string that the server software sends to a client when the client first contacts the server. Banners often have information in them that identifies the server or the operating system that the server is running.)

- If the Trace Source feature identifies the NetBIOS name, it attempts to identify network (MAC) addresses of that computer.
- If the Trace Source feature successfully identifies the DNS name, it queries the WHOIS database for information on the domain.
- If it cannot identify the DNS name, it attempts to identity the DNS names of adjacent IP addresses.

You can use this information to identify and locate the attacker and attempt to shut down the machine or reprimand the attacker.

To trace the source of the packets from an intruder:

1. Click the host entry on the **Intruders** panel and click **Properties**.
2. Click **Trace Source**. PGPnet displays captured information in the **Additional Trace Results** box. When the trace is complete, the **Trace Source** button is reactivated.



IP Address: 10.23.140.33

Block ● until removed ○ for ☐ minutes

Trace Results

DNS Name: dhcp-00-000.dhcp.nai.com

NetBT Name: \\workgroup\aestrada

Additional Trace Results:

```
NetBT Username:
Hardware Address: 00:C0:4F:5C:59:14

FTP Banner:

220-systemC

    WarFTPd 1.70.b01.04 (Aug 18 1998) Ready

    (C)opyright 1996 - 1998 by Jarle (jgaa) Aase - all rights
reserved.

220 Please enter your user name.


WHOIS Response:
```

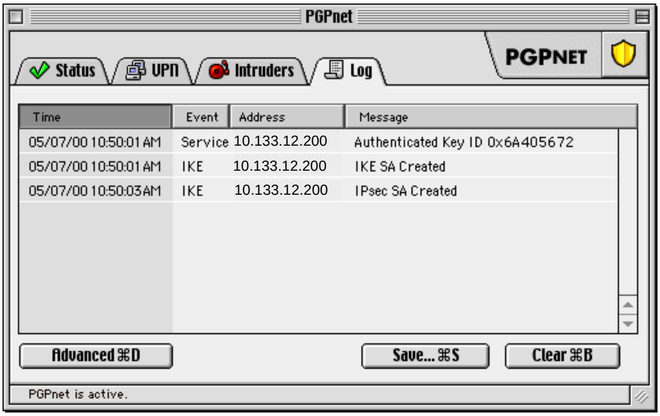
Figure 8-9. Blocked Host dialog: Trace Source feature

Removing a host from the list of blocked hosts

To remove a host from the list of blocked hosts:

1. Select the host.
2. Click **Remove**. PGPnet prompts, “Remove the selected host(s) from the blocked host list?”
3. Click **Yes**.

Reviewing PGPnet’s log entries



Time	Event	Address	Message
05/07/00 10:50:01 AM	Service	10.133.12.200	Authenticated Key ID 0x6A405672
05/07/00 10:50:01 AM	IKE	10.133.12.200	IKE SA Created
05/07/00 10:50:03AM	IKE	10.133.12.200	IPsec SA Created

PGPnet is active.

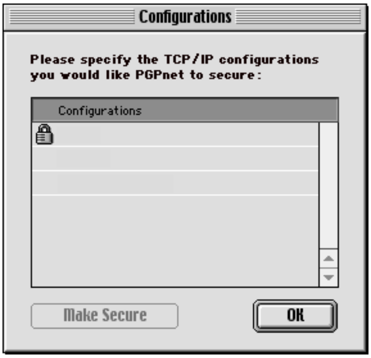
Figure 8-10. The Log panel

The **Log** panel shows **Service**, **IKE**, **IPsec**, **PGP**, **System**, and **Intrusion** events, when they occurred (date and time), and a description of the event or attack. Use this information to help resolve problems that occur (see Figure 8-10). Intrusion entries are highlighted in red.

Click **Advanced** to display the IKE log file. Note that when you close the Advanced IKE window, PGPnet does not save the data.

Click **Clear** to clear current log information from the log file and screen.

Changing your secure TCP/IP configurations



Configurations

Please specify the TCP/IP configurations you would like PGPnet to secure:

Figure 8-11. The Configurations dialog

To secure a different or additional TCP/IP configuration:

1. Select **Configurations** from the **File** menu. The PGPnet **Configurations** dialog is displayed on your screen listing all TCP/IP configurations.
2. To make a secure configuration insecure, click the configuration and click **Make Insecure**. To make an insecure configuration secure, click the configuration and click **Make Secure**.
3. Click **OK.**

Configuring PGPnet's VPN Feature 9

This chapter describes how to configure PGPnet's VPN feature. If you are in a corporate environment, your PGP or PGPnet administrator may have already configured this feature for you.

The following table identifies topics covered in this chapter.

To learn about:	See:
using PGPnet's VPN feature	"Configuring PGPnet's VPN feature" on page 136
remote authentication - requiring a host to present a specific key or certificate	"Remote Authentication" on page 145
shared secret	"Shared Secret" on page 145
adding a host, subnet, or gateway	"Adding a host, subnet, or gateway" on page 141
modifying a host, subnet, or gateway entry	"Modifying a host, subnet, or gateway entry" on page 144
removing a host, subnet, or gateway entry	"Removing a host, subnet, or gateway entry" on page 144
aggressive mode	"Using Aggressive Mode" on page 148

Configuring PGPnet's VPN feature

To start using PGPnet's VPN feature, you need to take the following steps:

1. Display PGPnet (see "Step 1. Displaying PGPnet" on page 136).
2. Secure your TCP/IP configurations (see "Step 2. Securing your TCP/IP configurations" on page 136).
3. Select your authentication key or certificate (see "Step 3. Selecting your authentication key or certificate" on page 137).
4. Open an existing host list (see "Step 4a. Importing a host list" on page 138) or add hosts to PGPnet (see "Step 4b. Adding a host, subnet, or gateway" on page 139).
5. Establish Security Associations (SAs) (see "Step 5. Establishing an SA" on page 139).

   Each of these steps is described in greater detail in the following sections.

Step 1. Displaying PGPnet

To display PGPnet, click **PGPmenu** and select **PGPnet** (the **PGPmenu** appears as an icon in the menu bar of the Finder).

Step 2. Securing your TCP/IP configurations

The first time you start PGPnet, a dialog asks you to select the TCP/IP configurations that you want to secure. Secure the configurations that you will use to communicate with other PGPnet hosts.

- If the network connection you want to secure is via ethernet, then PGPnet must be bound to the ethernet adapter (for example, "Connect via Ethernet").
- If the network connection you want to secure is via modem, then PGPnet must be bound to the modem adapter (also known as the Remote Access WAN Wrapper).
- If the network connection you want to secure is via AppleTalk, then PGPnet must secure the TCP/IP configurations that use AppleTalk.
- If the network connection you want to secure is via remote access dialup, PGPnet must secure the TCP/IP configuration that corresponds to the dialup connection (usually "Connect via PPP").

PGPnet can secure one or more TCP/IP configurations; as a result, you can elect to secure all TCP/IP configurations if desired.

You can change your selection at any time by selecting **Configurations** from the **File** menu.

Step 3. Selecting your authentication key or certificate

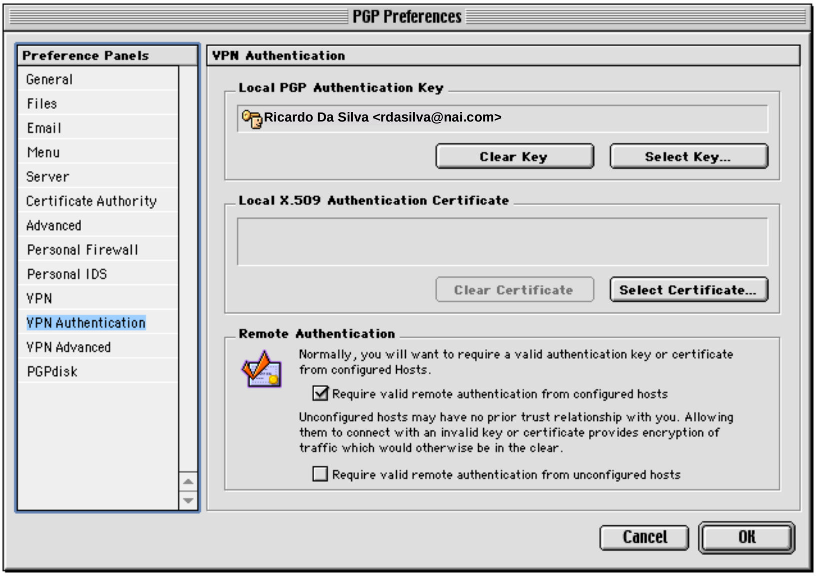
NOTE: X.509 authentication certificates are not supported in PGP Freeware.

Before you can use PGPnet, you must select the key and / or X.509 certificate that you will use for authentication purposes. If you do not have an existing keypair or X.509 certificate, see "Making and Exchanging Keys" on page 31.

To select your authenticating key and/or certificate:

1. Select **Preferences** from the **Edit** menu, then click **VPN Authentication**, as shown in Chapter 7, "PGPnet Basics".
2. Select the key and / or the certificate that you will use to authenticate (click **Select Key** or **Select Certificate**). Note that the key or certificate must be part of a key pair; you must have the private key.
3. Click **OK**. A dialog box asks you to enter the passphrase for the selected key.
4. Enter the passphrase and click **OK**.

IMPORTANT: If you are creating a VPN connection with another PGPnet host and using PGPkeys for authentication, you must both use the same type of PGP key. You cannot negotiate an SA if one side of the connection uses an RSA key and the other side uses a DH / DSS key.



VPN Authentication

Local PGP Authentication Key

Ricardo Da Silva <rdasilva@nai.com>

Local X.509 Authentication Certificate

Remote Authentication

Normally, you will want to require a valid authentication key or certificate from configured Hosts.

☑ Require valid remote authentication from configured hosts

Unconfigured hosts may have no prior trust relationship with you. Allowing them to connect with an invalid key or certificate provides encryption of traffic which would otherwise be in the clear.

□ Require valid remote authentication from unconfigured hosts

Figure 9-1. The VPN Authentication panel

Step 4a. Importing a host list

PGPnet includes a feature that allows you to import an existing list of hosts into PGPnet’s database, eliminating the need to add hosts manually. The host list must be one that you previously exported from PGPnet.

To open a host list and import it into PGPnet:

1. Select **Open Hosts** from PGPnet’s **File** menu.
2. Select the file that contains the host list. The hosts in the host file appear on the **VPN** panel.

Step 4b. Adding a host, subnet, or gateway

NOTE: This step is not required if you imported a host list.

To add a host, subnet, or gateway:

1. Click the **VPN** tab on the PGPnet window.
2. Click **Add**.
3. Enter the required information in the **Host/Gateway** dialog.

Step 5. Establishing an SA

To communicate with the hosts, subnets, and gateways that you added in step 3, you must create Security Associations.

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

To establish an SA with another host:

1. Verify that each system has a network connection.
2. Install PGPnet on both systems.
3. After installing PGPnet, reboot both systems.
4. Note the following:
   - If you are using PGP keys or X.509 certificates to authenticate, verify that each system has an authentication key or certificate set on the **VPN Authentication** panel (**Edit—>Preferences—>VPN Authentication**).
   - If you are using PGP keys to authenticate, then exchange, sign, and validate the public keys that each system is using for authentication. For more information, see Chapter 8, "A Quick Tour of PGPnet."
   - If you are using X.509 certificates to authenticate, then ensure that the Root CA for the remote party's X.509 certificate exists, is signed, and is fully trusted on both systems.

- If you are using PGP keys or X.509 certificates to authenticate, at least one user must create an entry in PGPnet’s host list for the other system (use **Add** on the **VPN** panel). If **Attempt** mode is set (**VPN** panel), you can now start communicating.

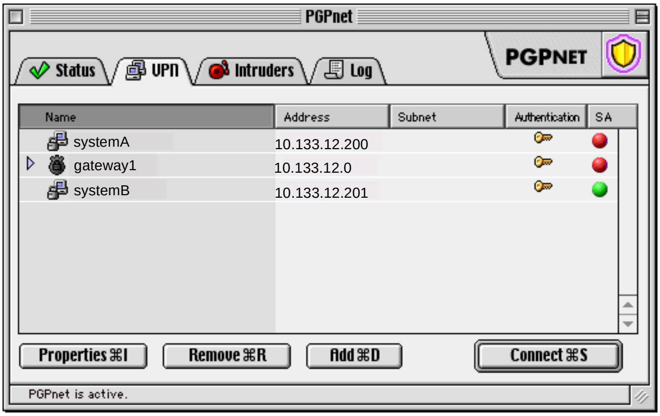
- If you are using *shared secret passphrase* for authentication, both users must create an entry in PGPnet’s host list for the other system, and you must agree on a shared secret passphrase. The passphrase can be a word or phrase.

5. Select the host’s entry on the **VPN** panel and click **Connect**. If the connection is successful, a green dot appears in the **SA** column.

Using the Host/Gateway dialog box

If you are in a corporate environment with a PGPnet administrator, many of the hosts, subnets, and gateways that you communicate with may have been preconfigured by your administrator. Each preconfigured host, subnet, and gateway is an entry in PGPnet’s host list. You can use PGPnet’s **Host/Gateway** dialog box to add additional entries to the host list.

If you do not have a PGPnet administrator or hosts, subnets, or gateways are not configured when you install PGPnet, use the **Host/Gateway** dialog box to add the necessary hosts, subnets, and gateways. You can view existing hosts, subnets, and gateways on the **VPN** panel.



Name	Address	Subnet	Authentication	SA
systemA	10.133.12.200		🔑	🔴
▷ gateway1	10.133.12.0		🔑	🔴
systemB	10.133.12.201		🔑	🟢

PGPnet is active.

Figure 9-2. The VPN panel

What you need to know

This section identifies the information that you need to add a host, subnet, or gateway.

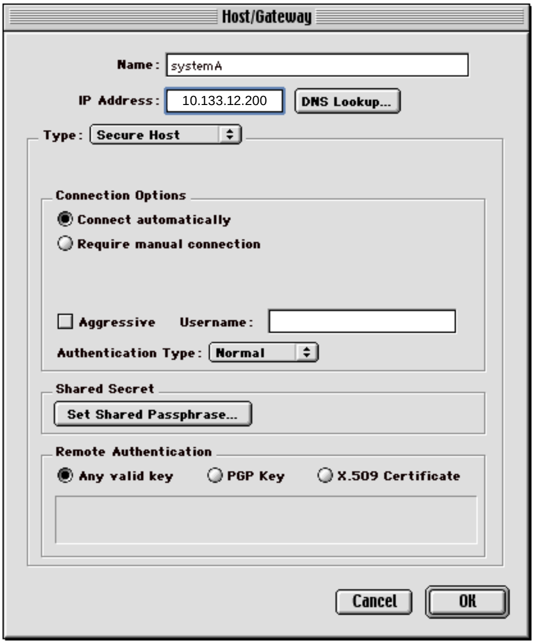
To:	You must know the:
Add a secure host	Host domain name or IP address
Add a subnet	IP address and subnet mask
Add a gateway	Host domain name or IP address
Add a host behind a configured gateway	Host domain name or IP address
Add a subnet behind a configured gateway	IP address and subnet mask

NOTE: You can have a secure gateway and a secure host (which is not behind a gateway) with the same IP address. When this occurs, the host entry is automatically set to **Manual connection** (that is, you must click the host in PGPtray’s PGPnet menu or click **Connect** on the **VPN** panel to connect to the host).

Adding a host, subnet, or gateway

Use PGPnet’s **Host/Gateway** dialog to add entries to the host list.

1. Click the **VPN** tab on PGPnet’s main window.
2. To add a host or subnet behind a configured gateway, click the gateway. To add a host behind a configured subnet, click the subnet.
3. Click **Add**. PGPnet displays the **Host/Gateway** dialog box.
4. Enter a descriptive name and IP address for the host, subnet, or gateway. If you do not know the IP address, click **DNS Lookup**. PGPnet displays a dialog box. Enter the domain name for the entity and click **OK**. PGPnet searches for the IP address.
   - If PGPnet finds the IP address, it displays the IP address; click **Use** to use the IP address in the **Host/Gateway** dialog.
   - If PGPnet does not find an IP address for the entity, it advises you.



Name: systemA

IP Address: 10.133.12.200

Type: Secure Host

● Connect automatically

○ Require manual connection

□ Aggressive Username:

Authentication Type: Normal

● Any valid key ○ PGP Key ○ X.509 Certificate

Figure 9-3. The Host/Gateway dialog

5. Select the type of host from the **Type** menu: **Insecure Host**, **Secure Host**, **Insecure Subnet**, **Secure Subnet**, or **Secure Gateway**. Note that the Connection Options differ depending on the type of host that you select.

   If you select **Insecure Subnet or Insecure Host**, click **OK**. PGPnet adds the entry to the **VPN** panel. Otherwise, proceed to the next step.

6. Select how you want to connect to this host:

   - **Connect automatically.** Select this option if you want PGPnet to connect automatically whenever traffic is exchanged with the host entry.

   - **Require manual connection.** Select this option if you use your machine from more than one site (for example, a corporate user who uses a laptop at home and at work). This feature allows you to communicate securely with the same hosts from either side of your corporate gateway using either of your machine’s adapters. Use the **Connect** button on the **VPN** panel to connect manually.

   If you are adding a gateway, click **OK** to add the entry to PGPnet’s host list. Otherwise, proceed to the next step.

7. If you are not using a shared secret for authentication, go to Step 9. If you are using a shared secret for authentication with this machine, click **Set Shared Passphrase**. PGPnet displays a dialog box.

8. Enter the passphrase that you intend to use for authentication; enter the passphrase a second time in the Confirmation box. Click **OK**. Note that both hosts must configure the same shared secret passphrase.

> **WARNING:** Unlike traditional PGP passphrases, Shared Secret passphrases are stored on your computer unencrypted. This presents a potential security risk.

9. The controls in the **Remote Authentication** section of the **Host/Gateway** dialog allow you to require the remote host to present a specific PGP key or X.509 certificate each time the host attempts to establish an SA with your machine. If the host attempts to establish a connection and does not present the specified key or certificate, your machine will refuse the connection. The default setting is **Any valid key**.

   - To identify a specific PGP key that the remote host must present for authentication, click **PGP Key**, select the key from the keys displayed in the pop-up dialog, and click **OK**. The key is displayed in the Remote Authentication section of the **Host/Gateway** dialog.

   - To identify a specific X.509 certificate that the remote host must present for authentication, click **X.509 Certificate**, select the certificate form the certificates displayed in the pop-up dialog, and click **OK**. The key is displayed in the Remote Authentication section of the **Host/Gateway** dialog.

10. Click **OK**.

Modifying a host, subnet, or gateway entry

There may be times when you need to modify the configuration of a host, subnet, or gateway. For example, when a IP address, subnet mask, or host domain name changes.

To modify a configuration:

1. Click the **VPN** tab.
2. Select the host, subnet, or gateway that you want to modify.
3. Click **Edit**. PGPnet displays the **Host/Gateway** dialog.

> **TIP:** Instead of selecting the host and clicking **Edit**, double-click the host in the host list.

4. Make the required edits.
5. Click **OK**.

   The PGPnet database is updated immediately. However, if the PGPnet service or driver are not operating normally, the PGPnet database is not updated until they are working properly. This may require a computer reboot.

Removing a host, subnet, or gateway entry

There may be times when you want to remove a configured host, subnet, or gateway. For example, when you feel that any entity is no longer secure.

To remove a host, subnet, or gateway:

1. Click the **VPN** tab.
2. Select the host, subnet, or gateway that you want to remove.
3. Click **Remove**.

Shared Secret

WARNING: Unlike traditional PGP passphrases, Shared Secret passphrases are stored on your computer unencrypted. This presents a potential security risk. To avoid this risk, use keys or certificates.

To use shared secret passphrase security, both users must create an entry in PGPnet's host list for the other system. You must know the other system's host name or IP address, and agree on a shared secret passphrase.

Remote Authentication

Requiring a host to present a specific key or certificate

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

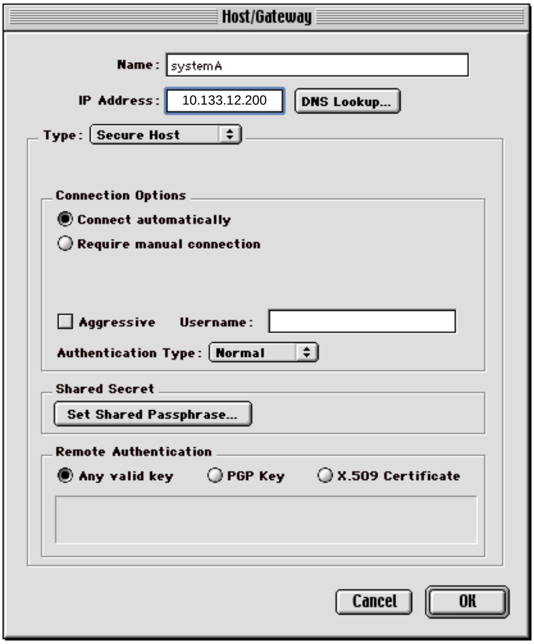
The controls in the **Remote Authentication** section of the **Host/Gateway** dialog box allow you to require the remote host to present a specific PGP key or X.509 certificate each time the host attempts to establish an SA with your host. If the host attempts to establish a connection and does not present the specified key or certificate, your machine will refuse the connection. The default setting is **Any valid key**.

You can add this requirement when you add a host using Expert Mode, or after you add a host by editing the host entry.

NOTE: Require them to present their public key, not your public key.

To require a host to present a specific key or certificate:

1. If you have not already done so, add the host, subnet, or gateway to PGPnet (for instructions,"Adding a host, subnet, or gateway" on page 141). PGPnet adds an entry to the host list on the **VPN** panel.
2. Select the entry on the **VPN** panel and click **Properties**. PGPnet displays the **Host/Gateway** dialog box. The **Remote Authentication** section is at the bottom of the dialog box.



Name: systemA

IP Address: 10.133.12.200

Type: Secure Host

Connection Options

● Connect automatically

○ Require manual connection

□ Aggressive Username:

Authentication Type: Normal

Shared Secret

Remote Authentication

● Any valid key ○ PGP Key ○ X.509 Certificate

Figure 9-4. Host/Gateway dialog

3. You can require the host, subnet, or gateway to present a specific PGP key or X.509 certificate to authenticate itself.

> **NOTE:** X.509 authentication certificates are not supported in PGP Freeware.

- To require a specific PGP key, click **PGP Key**. PGPnet displays the **Select Key** dialog box. Click the appropriate key and click **OK**. PGPnet displays the key in the **Remote Authentication** box. Click **OK** to close the **Host/Gateway** dialog box.
- To require a specific X.509 certificate, click **X.509 Certificate**. PGPnet displays the **Select X.509 Certificate** dialog box. Click the appropriate certificate and click **OK**. PGPnet displays the certificate in the **Remote Authentication** box. Click **OK** to close the **Host/Gateway** dialog box.

IMPORTANT: If you select a specific PGP key or X.509 certificate for a secure subnet entry, all users within that subnet must use the same key to authenticate themselves.

All key authentications appear on the **Log** panel, and each entry displays the key ID.

Authentication type

NOTE: PGP Freeware implements the Extended Authentication draft standard version 6. To take advantage of the **Authentication Type** feature, organizations must use a compatible gateway.

To change the authentication type you are using for a specific SA, double-click the host on the **VPN** panel to display the **Host/Gateway** dialog. The Authentication Type setting appears in the **Connection Options** section of the dialog.

The authentication type settings are:

- **Normal**. This is the default setting for **Authentication Type**. Each side of the SA authenticates itself to the other using either a shared passphrase, key, or certificate.
- **Extended**. This is an extension to the **Normal** setting. When you set **Authentication Type** to **Extended**, each side of the SA authenticates itself to the other using either a shared passphrase, key, or certificate. In addition, a legacy authentication exchange occurs which allows authentication via a number of other authentication methods, including RADIUS and SecurID.
- **Hybrid**. This is a modification to the **Extended** setting. This setting eliminates the client authentication via a shared passphrase, key, and certificate, but retains the server side authentication. Thus, this setting relies solely on the **Extended** authentication process to authenticate the client.

  For those who want to use legacy authentication, **Hybrid** is generally the ideal setting; it eliminates the need to establish a shared passphrase or generate a key or certificate. As a result, organizations can use their existing infrastructure of usernames and passwords or SecurID cards to authenticate themselves to the gateway.

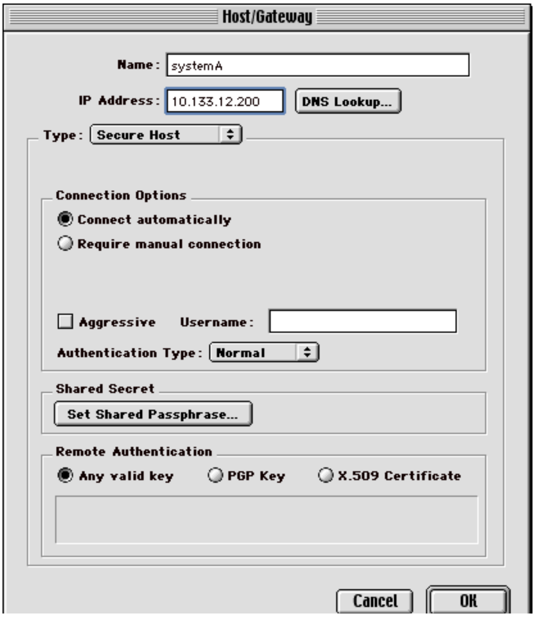
  Note that **Hybrid** support in gateways is far less common than **Normal** and **Extended** authentication.

Using Aggressive Mode

Use PGPnet’s aggressive mode feature with third-party VPN devices that require the use of Aggressive Mode IKE instead of normal Main Mode IKE.

To use aggressive mode:

1. If you have not already done so, add the host to PGPnet’s host list (for instructions, see “Adding a host, subnet, or gateway” on page 141).
2. Select the host on the **VPN** panel and click **Properties** to display the **Host/Gateway** dialog.
3. Click **Aggressive**.
4. If the following conditions are true, enter your user name to identify yourself to your third-party VPN gateway:
   - You are using a shared passphrase
   - You are using a dynamic IP address for your VPN client
5. Click **OK**.



Host/Gateway

Name: systemA

IP Address: 10.133.12.200

Type: Secure Host

Connection Options

● Connect automatically

○ Require manual connection

□ Aggressive Username:

Authentication Type: Normal

Shared Secret

Remote Authentication

● Any valid key ○ PGP Key ○ X.509 Certificate

Figure 9-5. PGPnet’s Host/Gateway Dialog

Part V: Appendices and Glossary

- **Appendix A: Setting Preferences**
- **Appendix B: Troubleshooting PGP**
- **Appendix C: Troubleshooting PGPnet**
- **Appendix D: Transferring Files between MacOS and Windows**
- **Appendix E: Biometric Word List**
- **Glossary**

Setting Preferences A

This chapter describes how to set your PGP preferences to suit your particular computing environment.

To set:	See:
General preferences	"Setting general preferences" on page 152
File preferences	"Setting file preferences" on page 155
Email preferences	"Setting email preferences" on page 156
Menu preferences	"Setting menu preferences" on page 158
Server preferences	"Setting server preferences" on page 161
Certificate Authority preferences	"Setting certificate authority preferences" on page 165
Advanced preferences	"Setting advanced preferences" on page 166
VPN preferences	"Setting VPN preferences" on page 169
VPN Authentication preferences	"Setting VPN authentication preferences" on page 172
VPN Advanced preferences	"Setting VPN advanced preferences" on page 174

Setting PGP preferences

PGP is configured to accommodate the needs of most users, but you have the option of adjusting some of the settings to suit your particular computing environment. You specify these settings through the **Preferences** dialog box.

There are several ways to access the **PGP Preferences** dialog box:

- From within all PGP utilities and plug-ins, click the gray lock icon (🔒) from PGPmenu, and then choose **Preferences**.
- From within PGPkeys and PGPnet, choose **Preferences** from the **Edit** menu.

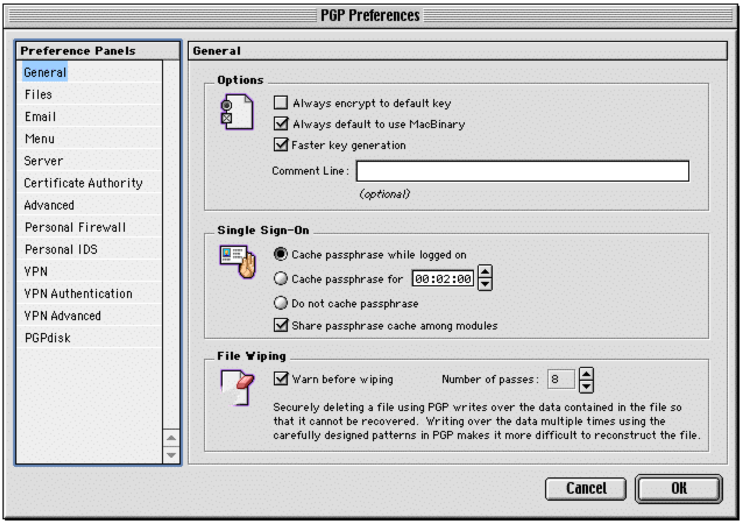
Setting general preferences

Use the **General** panel to specify your encrypting, signing, login, and file wiping preferences.

To set general PGP preferences:

1. Open the PGP **Preferences** dialog box.

   The **Preferences** dialog box opens with the **General** panel showing (Figure 9-1).



General

Options

□ Always encrypt to default key
☑ Always default to use MacBinary
☑ Faster key generation
Comment Line:
(optional)

Single Sign-On

● Cache passphrase while logged on
○ Cache passphrase for 00:02:00
○ Do not cache passphrase
☑ Share passphrase cache among modules

File Wiping

☑ Warn before wiping
Number of passes: 8

Securely deleting a file using PGP writes over the data contained in the file so that it cannot be recovered. Writing over the data multiple times using the carefully designed patterns in PGP makes it more difficult to reconstruct the file.

Figure 9-1. PGP Preferences dialog box (General panel)

2. Select from these PGP preferences:

Encryption Options

- **Always Encrypt to Default Key.** When this setting is selected, all the email messages and file attachments you encrypt with a recipient’s public key are also encrypted to you using your default public key. It is useful to leave this setting turned on so that, subsequently, you have the option of decrypting the contents of any email or files you encrypt.

- **Always Default to Use MacBinary.** When this setting is selected, Mac OS users will receive the exact file that was intended, and the Windows version will automatically decode the MacBinary and even append the appropriate file extension, such as .doc for Microsoft Word or .ppt for Microsoft PowerPoint. PGP recommends that you always select this setting. For more details, see Appendix D, "Transferring Files Between the MacOS and Windows."

- **Faster Key Generation.** When this setting is selected, less time is required to generate a new Diffie-Hellman / DSS key pair. This process is speeded up by using a previously calculated set of prime numbers rather than going through the time-consuming process of creating them from scratch each time a new key is generated. However, remember that fast key generation is only implemented for key sizes above 1024 and below 4096. Although it would be unlikely for anyone to crack your key based on their knowledge of these canned prime numbers, some may want to spend the extra time to create a key pair with the maximum level of security.

  The general belief in the cryptographic community is that using canned primes provides no decrease in security for the Diffie-Hellman / DSS algorithms. If this feature makes you uncomfortable, you may turn it off.

- **Comment Line.** You can add your comment text in this area. The text you enter here is always included in messages and files that you encrypt or sign. Comments entered in this field appear below the --BEGIN PGP MESSAGE BLOCK-- text header and PGP version number of each message.

Single Sign-On

NOTE: You must have the "multiple users" feature from MacOS 9 to use the **Cache Passphrases While Logged On** option.

- **Cache Passphrases While Logged On.** Automatically saves your passphrase in memory until you log off your computer. If you select this option, you are prompted for your passphrase once for each initial signing and decrypting task. You will not be prompted to enter it again for the same task until you log off your computer.

IMPORTANT: When this setting is selected, it is very important that you log off your computer before leaving it unattended. Your passphrase can remain cached for weeks if you never log off—anyone could read your encrypted messages or encrypt messages with your key while you are away from your computer.

- **Cache Passphrases For.** Automatically saves your passphrase in memory for the specified duration of time (in hours: minutes: seconds). If you select this option, you are prompted for your passphrase once for the initial signing or decrypting task. You are not prompted to enter it again until the allotted time you specify has lapsed. The default setting is 2 minutes.
- **Do not cache passphrase.** When this setting is selected, your passphrase is not stored in memory for any amount of time. Therefore, you are required to enter your passphrase for all PGPnet communications, as well as your encrypting, signing, and decrypting tasks.
- **Share Passphrase Cache Among Modules.** Automatically saves your passphrase in memory and shares it among other PGP modules. For example, if you enter your passphrase to sign using PGPtools, then you are not prompted for it to decrypt using PGPtray. Select this option with the **Cache Passphrases While Logged On** option and your passphrase is saved in memory until you log off your computer. Or, select this option with **Cache Passphrases For** and set the duration for which you want to save your passphrase.

File Wiping

- **Number of Passes**. This setting controls how many times the wipe utilities pass over the disk.
- **Warn Before Wiping.** When this setting is selected, a dialog box appears before you wipe a file to give you one last chance to change your mind before PGP securely overwrites the contents of the file and deletes it from your computer.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP **preferences**.

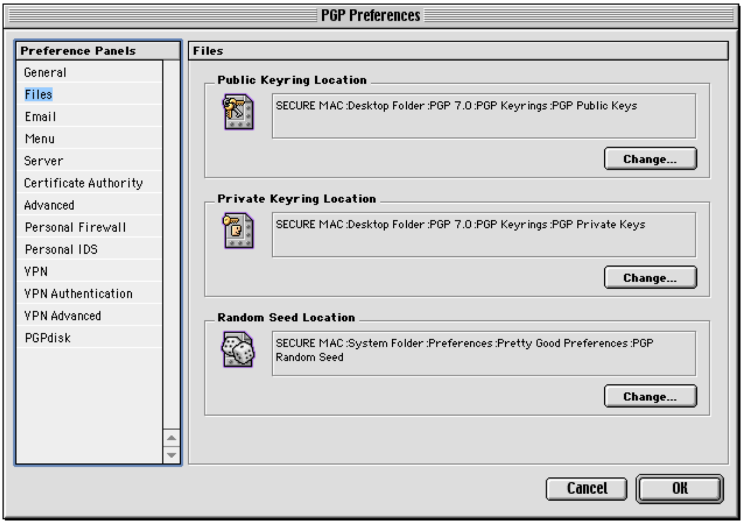
Setting file preferences

Use the **Files** panel to specify the location of the keyrings used to store your private and public keys.

To set PGP file preferences:

1. Open the PGP **Preferences** dialog box and select **Files**.

   The **Preferences** dialog box opens with the **Files** panel showing (Figure 9-2).



Public Keyring Location: SECURE MAC :Desktop Folder :PGP 7.0 :PGP Keyrings :PGP Public Keys

Private Keyring Location: SECURE MAC :Desktop Folder :PGP 7.0 :PGP Keyrings :PGP Private Keys

Random Seed Location: SECURE MAC :System Folder :Preferences :Pretty Good Preferences :PGP Random Seed

Figure 9-2. PGP Preferences dialog box (Files panel)

2. Use the buttons listed in the **Files** panel to set the appropriate location for your public and private keyrings, and / or random seed file:

Public Keyring Location

Shows the current location and name of the file where the PGP program expects to find your public keyrings. If you plan to store your public keys in some other location, you must specify this information here. The location you specify can also be used to store all automatic backups of the public keyring. See “Setting advanced preferences” on page 166 for more information about backing up your keyrings automatically.

Private Keyring Location

Shows the current location and name of the file where the PGP program expects to find your private keyrings. If you plan to store your private keys in some other location, you must specify this information here. Some users like to keep their private keyring on a floppy disk, which they insert like a key whenever they need to sign or decrypt mail. The location you specify can also be used to store all automatic backups of the public keyring.

Random Seed Location

Shows the location of the Random Seed file. Some users may wish to keep their Random Seed file in a secure location to prevent tampering. Given that this method of attack is very difficult, and has been anticipated by PGP, moving the Random Seed file from its default location is of marginal benefit.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

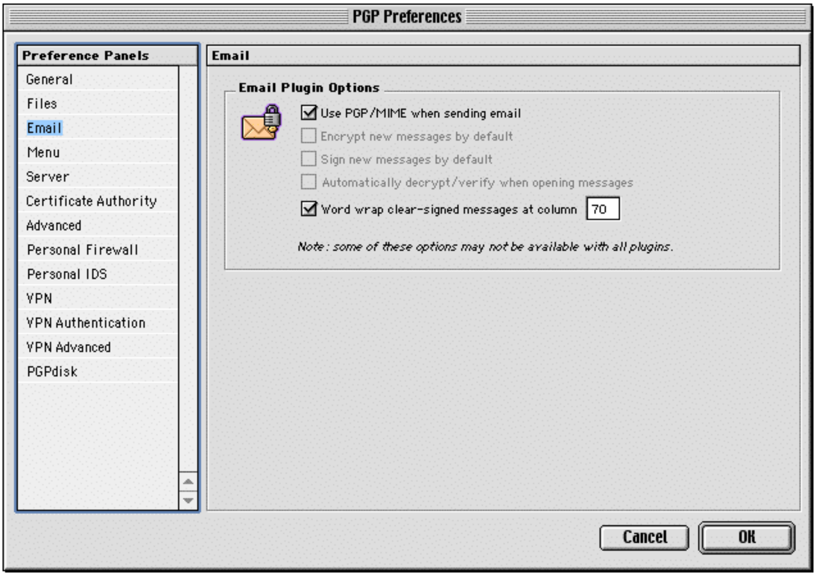
Setting email preferences

Use the **Email** panel to specify the preferences that affect the way PGP functions are implemented for your particular email application. Remember that not all of the selections may apply to your particular email application.

To set email preferences:

1. Open the PGP **Preferences** dialog box and select **Email**.

   The **Preferences** dialog box opens with the **Email** panel showing (Figure 9-3).



Email

Email Plugin Options

☑ Use PGP/MIME when sending email

□ Encrypt new messages by default

□ Sign new messages by default

□ Automatically decrypt/verify when opening messages

☑ Word wrap clear-signed messages at column 70

Note: some of these options may not be available with all plugins.

Figure 9-3. PGP Preferences dialog box (Email panel)

2. Select your email encryption preferences from the **Email** panel. Your choices are:

   - **Use PGP/MIME when sending mail.** If you are using Eudora and you enable this setting, all of your email messages and file attachments are automatically encrypted to the intended recipient. This setting has no effect on other encryptions you perform from PGPmenu, from the clipboard, or in the Finder and should not be used if you plan to send email to recipients who use email applications that are not supported by the PGP / MIME standard. Using Eudora, attachments will always be encrypted regardless of this setting, but if the recipient does not have PGP / MIME, the decryption process will be more manual.

   - **Encrypt new messages by default.** If you enable this setting, all of your email messages and file attachments are automatically encrypted. Some email applications cannot support this feature.

   - **Sign new messages by default.** If you enable this setting, you are prompted to sign all of your email messages. Some email applications cannot support this feature. This setting has no effect on other signatures you add from the clipboard. This setting has no effect on other signatures you add from PGPmenu.

- **Automatically decrypt/verify when opening messages.** If you enable this setting, all of your email messages and file attachments that are encrypted and/or signed are automatically decrypted and verified. Some email applications cannot support this feature.
- **Word wrap clear-signed messages at column [ ].** This setting specifies the column number where a hard carriage return is used to wrap the text in your digital signature to the next line. This feature is necessary because not all applications handle word wrapping in the same way, which could cause the lines in your digitally signed messages to be broken up in a way that cannot be easily read. The default setting is 70, which prevents problems with most applications.

WARNING: If you change the word-wrap setting in PGP, make sure that it is less than the word-wrap settings in your email application. If you set it to be the same or a greater length, carriage returns may be added that invalidate your PGP signature.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

Setting menu preferences

From the menu panel you can perform these tasks:

- **Add and remove PGPmenu for various applications.** To ensure easy access to PGP on your computer, you need to specify which applications on your computer that you want to integrate with PGP. For instructions, see "To add and remove PGPmenu for various applications:" on page 160.
- **Enable the Wipe Trash option.** When you delete a file normally by placing it in the Trash, the name of the file is removed from the file directory, but the data in the file stays on the disk and is recoverable. When this option is enabled, the **Empty Trash** option in the Finder changes to **Wipe Trash** and wipes the Trash so that your deleted items can no longer be recovered. To enable this option, check the **Wipe Trash** checkbox in the upper right-hand side of the **Menu** panel.

TIP: When this option is enabled, you can revert to the **Empty Trash** option in the Finder by holding down the COMMAND key.

- **View keyboard shortcuts for PGP functions.** PGPmenu also includes a set of keyboard shortcuts that gives you quick access to PGP's most common commands. The common commands include encrypting, signing, encrypting and signing, and decrypting and verifying data in the current open window.
- **Automatically lock your screen.** This option enables PGPScreen which allows you to lock down your computer with your PGPkey passphrase. This option is especially useful when you are working within PGPdisk volumes and must leave your computer unattended. PGPScreen locks-down your computer screen so that your PGPdisk volumes can remain open and secure while you are away from your computer.

  To enable this option, check the **Automatically lock your screen** check box and then specify the amount of idle time allowed to elapse before your screen is locked.

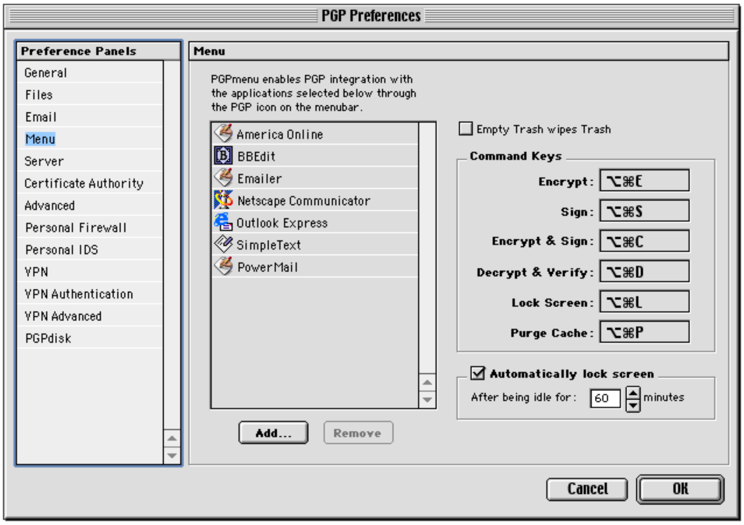
  If you enable this option in addition to passphrase caching (available in General **Preferences**), your passphrase is automatically saved in memory until you log off your computer or until PGP screen lock is invoked.

IMPORTANT: To unlock your computer screen, press the ESC key and then enter your PGP passphrase in the **PGP passphrase** dialog box.

To add and remove PGPmenu for various applications:

1. Open the **PGP Preferences** dialog box and select **Menu**.

   The **Preferences** dialog box opens with the **Menu** panel showing (Figure 9-4).



PGPmenu enables PGP integration with the applications selected below through the PGP icon on the menubar.

☐ Empty Trash wipes Trash

Command Keys

Encrypt: ⌥⌘E

Sign: ⌥⌘S

Encrypt & Sign: ⌥⌘C

Decrypt & Verify: ⌥⌘D

Lock Screen: ⌥⌘L

Purge Cache: ⌥⌘P

☑ Automatically lock screen

After being idle for: 60 minutes

Figure 9-4. PGP Preferences dialog box (Menu panel)

2. Click **Add** to add the PGP icon to the menu bar of the applications you select. For example, click the **Add** button and add Simpletext to the application list. The PGP icon is added to the **Simpletext** menu bar, so that you can sign, encrypt, decrypt, and verify the selected text in your documents.

   Double-click an application name in the PGPmenu preferences to open the **Advanced PGPmenu Preferences** dialog for that particular application, which contains settings that may help if you experience any compatibility problems using PGPmenu with a particular application.

   Click **Remove** to remove the PGP icon from the menu bar of applications you have previously selected.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

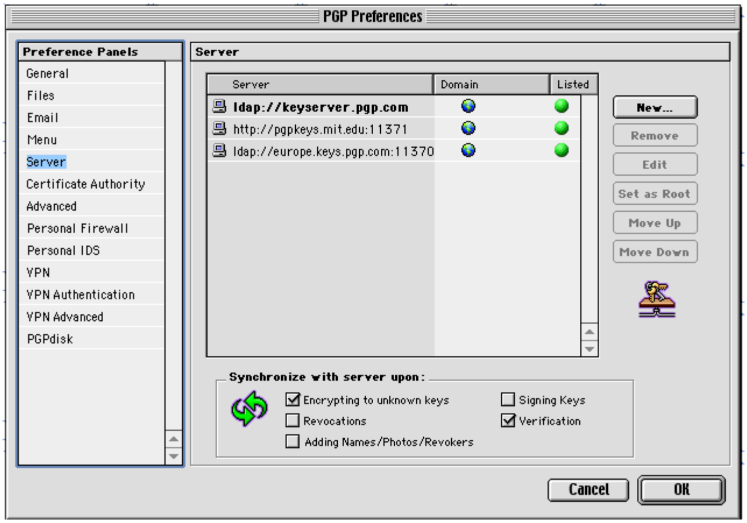
Setting server preferences

Use the **Server** panel to specify settings for the public key servers or directory servers that you are using to send and retrieve public keys, and with which you will automatically synchronize keys.

To set key server preferences:

1. Open the PGP **Preferences** dialog box and select **Server**.

   The **Preferences** dialog box opens with the **Server** panel showing (Figure 9-5).



Server	Domain	Listed
ldap://keyserver.pgp.com	🌐	●
http://pgpkeys.mit.edu:11371	🌐	●
ldap://europe.keys.pgp.com:11370	🌐	●

Synchronize with server upon:

☑ Encrypting to unknown keys
☐ Revocations
☐ Adding Names/Photos/Revokers
☐ Signing Keys
☑ Verification

Figure 9-5. PGP Preferences dialog box (Server panel)

2. To set your server preferences, use these buttons:

   - **New.** Adds a new server to your list.
   - **Remove.** Removes the currently selected server from your list.
   - **Edit.** Allows you to edit server information for the currently selected server.
   - **Set as root.** Identifies the root server that is used for specific corporate operations, such as updating group lists, sending group lists, updating introducers, etc. In corporate settings, your Security Officer will have already configured this.

- **Move Up** and **Move Down**. Use these buttons to arrange the servers in order of preference.

3. Select the options to use when synchronizing your private keyring with your key server(s). Your choices are:

Synchronize with server upon

- **Encrypting to unknown keys.** Select this option to have PGP automatically look up unknown recipients on the server to locate users that are not on your keyring when encrypting email.
- **Signing keys.** Select this option to allow keys to which you're adding your signature first to be updated from the server and then your changes sent to the server upon completion of the update.
- **Adding names/photos/revokers.** Select this option to allow keys to which you've added names, photographs, or revokers first to be updated from the server and then your changes sent to the server upon completion of the update. Updating the key beforehand ensures that, for example, the key has not been revoked since you last updated it.
- **Revocations.** Select this option to allow keys you revoke first to be updated from the server and then your changes sent to the server upon completion of the update.
- **Verification.** Select this option to have PGP automatically search and import from the key server when verifying a signed email message or file for which you do not have the sender's public key.

4. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

To add a key server to the server list:

1. Open the PGP **Preferences** dialog box and select **Server**.
2. Click the **New** button.

   The **Add New Server** dialog box appears.
3. In the **Type** box, select the type of server to use to access the key server. Your choices are:

   - **PGP Keyserver HTTP.** Select this option if you are using a Web-based PGP Keyserver to store and retrieve PGPkeys.
   - **PGP Keyserver LDAP.** Select this option if you are using a PGP Keyserver through LDAP to store and retrieve PGPkeys.
   - **PGP Keyserver LDAPS.** Select this option if you are using a PGP Keyserver through LDAPS to store and retrieve PGPkeys.
   - **PGP Directory LDAP.** Select this option if you are using a generic LDAP server—such as Netscape Directory Server or Microsoft Active Directory—to store and retrieve PGPkeys.
   - **PGP Directory LDAPS.** Select this option if you are using a generic LDAPS server—such as Netscape Directory Server or Microsoft Active Directory—to store and retrieve PGPkeys.
   - **X.509 Directory LDAP.** Select this option if you are using a generic LDAP directory server to store and retrieve X.509 certificates issued by iPlanet CMS or Microsoft Certificate Services.
   - **X.509 Directory LDAPS.** Select this option if you are using a generic LDAPS directory server to store and retrieve X.509 certificates issued by iPlanet CMS or Microsoft Certificate Services.
4. In the **Server Name** box, enter the domain name or IP address of the server. For example, server.nai.com or 123.45.67.89
5. Type the port number of the server in the **Port** box. For example 11371 is used for old-style HTTP key server, 389 is commonly used for LDAP key servers.
6. The **Key** box is for LDAPS servers. The server key is used by the server to authenticate the connection. (Key information is not displayed until you connect to the server.)

7. Under **Serves Key for Domain**, select the **Any Domain** option to allow PGP to send keys from any domain to this key server. This option is enabled by default.

   If you want PGP to send only keys from a specific domain to this key server, select the option below **Any Domain**. Then, enter the domain name in the space provided. For example, if you specify the domain nai.com, only those keys whose email address ends in nai.com will be sent to this server.

8. Select the **List in Search Window** checkbox if you want this key server listed in the **PGPkeys Search** window.

Accessing HTTP servers through a proxy server

If your Macintosh is behind a firewall with an HTTP proxy server, you can access HTTP key servers through the proxy by configuring the proxy server address in the Internet control panel.

To access HTTP key servers through a proxy server:

1. Open the Internet control panel.

2. Choose **User Mode** from the Internet control panel **Edit** menu.

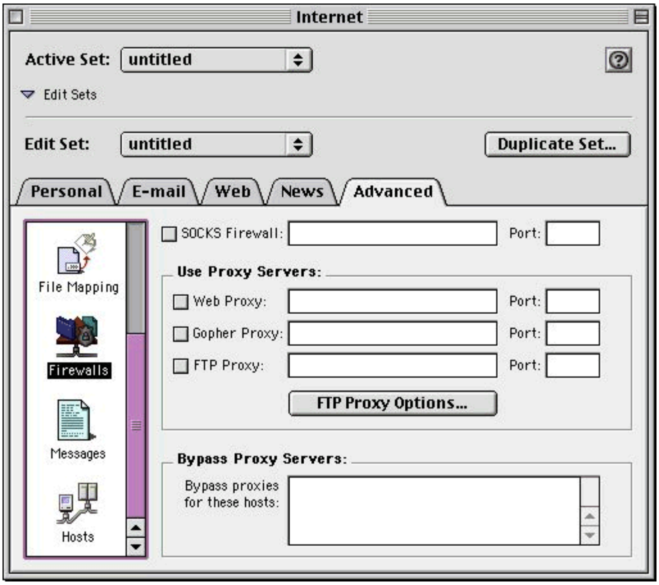
   The **User Mode** dialog box appears.

3. Select **Advanced** or **Administration**, and then click **OK**.

4. On the Internet control panel, click the **Advanced** tab.

5. Click the **Firewalls** icon on the left side of the **Advanced** panel.

   The Firewall options are displayed in the **Advanced** panel, as shown in Figure 9-6.



Active Set: untitled

Edit Set: untitled

□ SOCKS Firewall: Port:

Use Proxy Servers:

□ Web Proxy: Port:

□ Gopher Proxy: Port:

□ FTP Proxy: Port:

Bypass Proxy Servers:

Bypass proxies for these hosts:

Figure 9-6. Internet control panel
(Advanced Firewall Preferences)

6. Select the **Web Proxy** check box.

7. Type the name of the proxy server in the **Web Proxy** text box, then enter the port number for the proxy server in the **Port** text box.

   If you do not know the name of the proxy server or the port number, contact your System Administrator.

8. Choose **Save Settings** from the **File** menu.

9. Reboot your system for the changes to take effect.

Setting certificate authority preferences

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

Use the **Certificate Authority** panel to add your X.509 certificate to your PGP key. Before you can add your X.509 certificate however, you must first obtain the Root CA certificate from key server. For instructions about setting **certificate authority** preferences and adding your X.509 certificate to your key, see "Adding an X.509 certificate to your PGP key" on page 76.

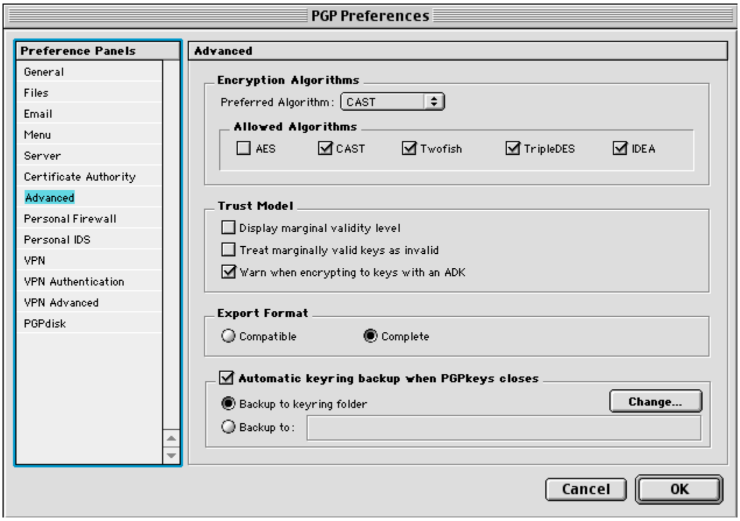
Setting advanced preferences

Use the **Advanced** panel to select your preferred encryption algorithm, the allowed algorithms, key trust options, key export format, and automatic keyring back up options.

To set advanced preferences:

1. Open the PGP **Preferences** dialog box and select **Advanced**.

   The **Preferences** dialog box opens with the **Advanced** panel showing (Figure 9-7).



Advanced

Encryption Algorithms

Preferred Algorithm: CAST

Allowed Algorithms

□ AES ☑ CAST ☑ Twofish ☑ TripleDES ☑ IDEA

Trust Model

□ Display marginal validity level

□ Treat marginally valid keys as invalid

☑ Warn when encrypting to keys with an ADK

Export Format

○ Compatible ● Complete

☑ Automatic keyring backup when PGPkeys closes

● Backup to keyring folder Change...

○ Backup to:

Figure 9-7. PGP Preferences dialog box (Advanced panel)

2. Select your PGP advanced preferences:

Encryption Algorithms

You can select from these encryption algorithms to use for your encryption operations:

- **CAST** (the default). CAST is a 128-bit block cipher. It is a strong, military-grade encryption algorithm, which has a solid reputation for its ability to withstand unauthorized access.

- **AES.** (If you want to use AES, then you must make the selection before you generate your keys.) The new Advanced Encryption Standard (AES) chosen by the National Institute of Standards and Technology (NIST) is Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen. It is considered to be both faster and smaller than its competitors. The key size and block size can be 128-bit, 192-bit, or 256-bit in size and either can be increased by increments of 32 bits.
- **IDEA.** (If you want to use IDEA, then you must make the selection before you generate your keys.) IDEA is the algorithm used for all RSA Legacy keys generated by PGP.
- **Triple-DES.** (If you want to use Triple-DES, then you must make the selection before you generate your keys.) Triple-DES is a U.S. Government algorithm that has withstood the test of time. It's an encryption configuration in which the DES algorithm is used three times with three different keys.
- **Twofish.** Twofish is a new 256-bit block cipher, symmetric algorithm created by Bruce Schneier. Twofish is one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) is considering as a replacement for the current Advanced Encryption Standard (AES).

For more information about these algorithms, see "The PGP Symmetric algorithms" in *An Introduction to Cryptography*.

The **Preferred Algorithm** choice affects the following:

- When using conventional encryption, the preferred cipher is used to encrypt.
- When creating a key, the preferred cipher is recorded as part of the key so that other people will use that algorithm when encrypting to you.

The **Allowed Algorithm** choice affects the following:

- When creating a key, the allowed ciphers are recorded as part of the key so that other people will use one of those algorithms when encrypting to you if the preferred algorithm is not available to them.

NOTE: Encrypting to a public key will fail if neither the Preferred Algorithm nor any of the Allowed Algorithms are available to the person encrypting the message.

WARNING: Clear the CAST, IDEA, Twofish, and Triple-DES check boxes only if you have suddenly learned that a particular algorithm is insecure. For example, if you become aware that Triple-DES has been broken, you can deselect that check box and all new keys you generate will have a record that Triple-DES may not be used when encrypting to you.

Trust Model

For a better understanding of the concepts of trust and validity, see *An Introduction to Cryptography*.

PGP gives you the option to select and / or change how key trust is displayed, and whether or not you wish to be warned whenever you encrypt a message to a public key that has an associated Additional Decryption Key. In the Trust Model section, choose from these options:

- **Display marginal validity level.** Use this check box to specify whether to display marginally valid keys as such, or simply to show validity as on or off. Marginal validity appears as bar icons having differing shading patterns. On / off validity appears as circle icons; green for valid, gray for invalid (the key has not been validated; it has not been signed by either a trusted introducer or by you).

- **Treat marginally valid keys as invalid.** Use this check box to specify whether to treat all marginally valid keys as invalid. Selecting this option causes the **Key Selection** dialog box to appear whenever you encrypt to marginally valid keys.

- **Warn when encrypting to an ADK.** Use this check box to specify whether to issue a warning whenever an encrypt-to key has an associated Additional Decryption Key.

Export format

- **Compatible:** Exports keys in a format compatible with previous versions of PGP.

- **Complete:** Exports the new key format, which includes photographic IDs and X.509 certificates.

Automatic keyring back up when PGP closes

Select this check box to back up your public and private keyrings automatically when you close PGP.

- **Back up to keyring folder.** Select this option to store your keyring back up files in the default PGP keyring folder.
- **Back up to.** Select this option to specify the location in which you want to store your backup files.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

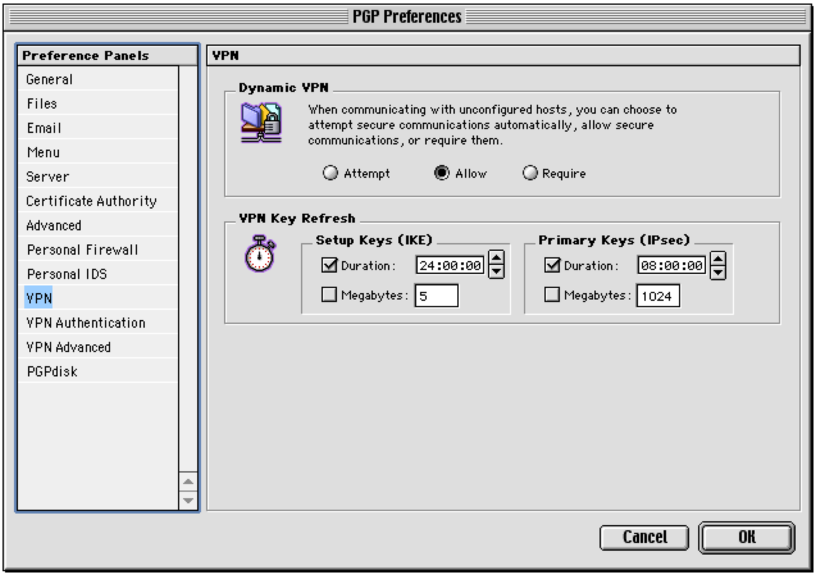
Setting VPN preferences

Use the **VPN** panel to control automatic key renewal, and how you communicate with unconfigured hosts.

To set VPN preferences:

1. Open the PGP **Preferences** dialog box and select **VPN**.

   The **Preferences** dialog box opens with the **VPN** panel showing (Figure 9-8).



Dynamic VPN

When communicating with unconfigured hosts, you can choose to attempt secure communications automatically, allow secure communications, or require them.

○ Attempt ● Allow ○ Require

VPN Key Refresh

Setup Keys (IKE)

☑ Duration: 24:00:00

□ Megabytes: 5

Primary Keys (IPsec)

☑ Duration: 08:00:00

□ Megabytes: 1024

Figure 9-8. PGP **Preferences** dialog box (VPN panel)

2. Choose from the following options:

Dynamic VPN

The Dynamic VPN feature allows you to communicate with anyone else who has PGPnet installed. PGPnet automatically encrypts and establishes an SA without any prior configuration. You do not even need to run PGPnet, as long as the Dynamic VPN **Attempt** setting is active (box is checked) and your local authentication key is set.

For example, assume that your machine, machine1, and your friend's machine, machine2, both have PGPnet installed and running, both have the Dynamic VPN **Attempt** setting active, but neither of you have the other machine configured (that is, you don't have machine2 in your host list, and your friend doesn't have machine1 in his host list). If machine1 contacts machine2, PGPnet discovers that machine2 supports IKE, and, as a result, negotiates an SA. Note that between the time that machine1 begins to communicate with machine2, and the time that the SA is negotiated, your communication is not protected by PGPnet.

PGPnet uses the three Dynamic VPN settings (**Attempt**, **Allow**, and **Require**) to control how you communicate with unconfigured hosts:

- **Attempt**. If you start to communicate with an unconfigured host (that is, the host is not in the host list and thus, there is no SA), PGPnet allows communications to continue while it attempts to create an SA.

  If PGPnet cannot negotiate an SA, communication continues insecurely.

  If PGPnet can negotiate an SA, the communication is encrypted. Note that when communicating with unconfigured hosts, some packets may pass in the clear or unencrypted before the connection is encrypted. This delay is usually about one to three seconds.

- **Allow**. This setting allows other hosts to connect to your machine securely, but you do not initiate SAs with unconfigured hosts.

- **Require**. Secure communications are required and all insecure traffic is dropped unless the host is configured as insecure.

VPN Key Refresh

You can change the automatic key renewal values for **Setup Keys (IKE)** and **Primary Keys (IPsec)**. These keys are responsible for creating your Security Associations. The default settings will work fine for most users. However, if you frequently send or receive large files, you may want to increase the key renewal values to prevent the need for frequent rekeying.

Values for Setup Keys (IKE) can be set in time (**Duration**); values for Primary Keys (IPsec) can be set in time (**Duration**) or data size (**Megabytes**).

- **Duration** is displayed in the following manner:

  2d, 08h, 04m (key expires in 2 days, 8 hours, and 4 minutes)

- **Megabytes** is displayed in the following manner:

  99 (key expires after 99 megabytes of data are transferred)

Note that when you establish an SA with another host, PGPnet uses the most restrictive key renewal values set by either of the two hosts. As a result, you may see an SA expire before your renewal value is met.

WARNING: Lowering the default value for Megabytes may result in multiple rekeyings when transmitting large files, which may, in turn, cause temporary interruption of normal network function.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

Setting automatic key renewal values

To change the automatic renewal values for Setup Keys (IKE):

1. Display the **VPN** panel **(Edit—>Preferences)**. The **Automatic Key Renewal** information appears in the bottom section of the **VPN** panel.
2. To set a duration for Setup Keys, select the check box next to **Duration**. Use the up and down arrows next to the **Duration** field to set the appropriate time limit or enter a numeric value in each field: hh:mm:ss.
3. Click **OK**.

To set automatic renewal values for Primary Keys (IPsec):

1. Display the **VPN** panel **(Edit—>Preferences)**. The **Automatic Key Renewal** information appears in the bottom section of the **VPN** panel.
2. To set a duration for Primary Keys, select the check box next to **Duration**. Use the up and down arrows next to the **Duration** field to set the appropriate time limit or enter a numeric value in each field: hh:mm:ss.

3. To set a data value in **Megabytes** for Primary Keys, select the check box next to **Megabytes**. Enter a numeric value.

4. Click **OK**.

Setting VPN authentication preferences

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

Use the **VPN Authentication** panel to perform the following tasks:

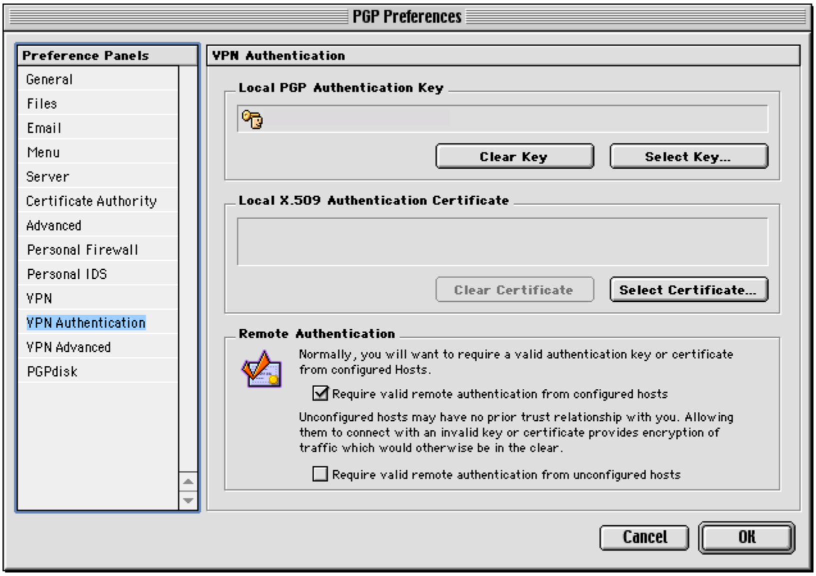
- Select a PGP key to authenticate your local machine (**PGP Authentication**).
- Select an X.509 certificate to authenticate your local machine (**X.509 Authentication**).
- Control remote authentication.

To set VPN authentication preferences:

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

1. Open the PGP **Preferences** dialog box and select **VPN Authentication**.

   The **Preferences** dialog box opens with the **VPN Authentication** panel showing (Figure 9-9).



Normally, you will want to require a valid authentication key or certificate from configured Hosts.

☑ Require valid remote authentication from configured hosts

Unconfigured hosts may have no prior trust relationship with you. Allowing them to connect with an invalid key or certificate provides encryption of traffic which would otherwise be in the clear.

□ Require valid remote authentication from unconfigured hosts

Figure 9-9. PGP Preferences dialog box (VPN Authentication panel)

2. Select your VPN authentication options:

Authenticating your Connection

To set your authentication key or certificate, use the following buttons:

- **Select key.** Displays a dialog box. Use this dialog box to select your key pair. You must then enter the passphrase for the selected key.
- **Clear Key.** Clears the selected key.
- **Select Certificate.** Displays a dialog box. Use this dialog box to select your X.509 private certificate on the keyring. You must then enter the passphrase for the selected certificate.
- **Clear Certificate.** Clears the selected X.509 certificate.

When you click **OK**, you are asked to enter the passphrase for the selected authentication key or certificate. Enter the passphrase and click **OK**. You are asked to enter this passphrase each time you login to PGPnet.

Remote Authentication

Normally you will want to require a valid authentication key or certificate from configured hosts. To do so, click **Require valid remote authentication from configured hosts**.

Unconfigured hosts may have no prior trust relationship with you. Allowing them to connect with an invalid key or certificate provides encryption of traffic which would otherwise be in the clear.

- To allow connection from unconfigured hosts with an invalid key or certificate, clear the **Require valid remote authentication from unconfigured hosts** box.

- To require valid remote authentication from unconfigured hosts, click **Require valid remote authentication from unconfigured hosts**.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

Setting VPN advanced preferences

WARNING: The default settings on this panel allow you to communicate with PGPnet, strong-crypto GVPN users, and many other IPsec products. Do not change the settings unless you are an experienced IPsec user.

The **VPN Advanced** panel displays the **Allowed Remote Proposals** and IKE and IPsec **Proposals**.

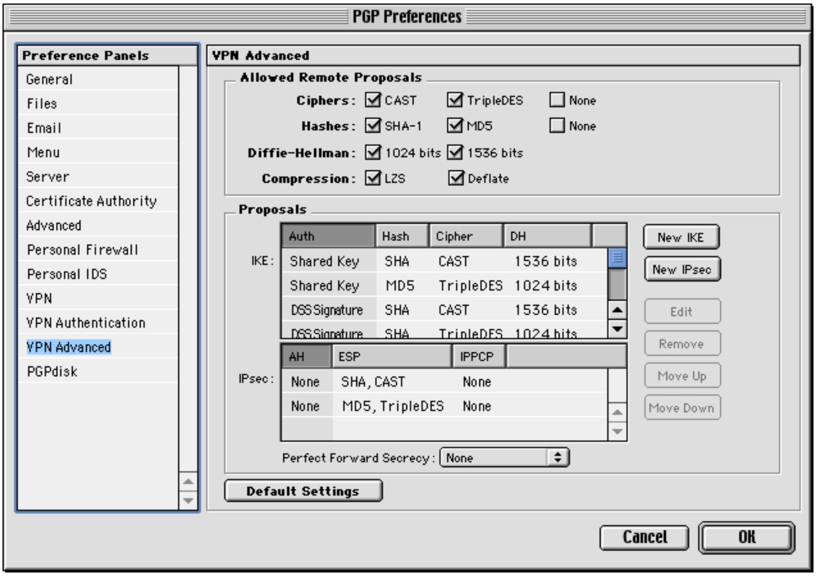
- The **Allowed Remote Proposals** section tells PGPnet to accept any proposal from other users that includes any item checked (allowed) in these boxes. The exceptions to this are the **None** items for **Cipher** and **Hashes**. Use the **None** items with extreme caution or not at all. If you check **None** for **Ciphers** (encryption), PGPnet accepts proposals that do not include encryption. If you check **None** for **Hashes** (authentication), PGPnet accepts proposals that do not include authentication.

- The IKE and IPsec **Proposals** sections identify the proposals that you make to others. Other users must accept exactly what is specified in at least one of your proposals for IKE and for IPsec.

To set VPN advanced preferences:

1. Open the PGP **Preferences** dialog box and select **VPN Advanced**.

   The **Preferences** dialog box opens with the **VPN Advanced** panel showing (Figure 9-10).



Ciphers: ☑ CAST ☑ TripleDES □ None

Hashes: ☑ SHA-1 ☑ MD5 □ None

Diffie-Hellman: ☑ 1024 bits ☑ 1536 bits

Compression: ☑ LZS ☑ Deflate

IKE:

Auth	Hash	Cipher	DH
Shared Key	SHA	CAST	1536 bits
Shared Key	MD5	TripleDES	1024 bits
DSS Signature	SHA	CAST	1536 bits
DSS Signature	SHA	TripleDES	1024 bits

IPsec:

AH	ESP	IPPCP
None	SHA, CAST	None
None	MD5, TripleDES	None

Perfect Forward Secrecy: None

Figure 9-10. PGP Preferences dialog box (VPN Advanced panel)

2. Select your VPN advanced preferences:

Allowed Remote Proposals

The **Allowed Remote Proposals** portion of this panel identifies the types of ciphers, hashes, compression, and Diffie-Hellman keys that PGPnet allows.

NOTE: Only experienced IPsec users should make any changes to the settings on this panel.

- **Ciphers.** Ciphers are algorithms used to encrypt and decrypt. To allow a specific type of cipher (CAST or TripleDES), place a check in the box to the left of the cipher. Check None with extreme caution or not at all, as it tells PGPnet to accept proposals that do not include encryption from other users.
- **Hashes.** A hash function takes a variable-sized input string and converts it to a fixed-sized output string. To allow a specific type of hash (SHA-1 or MD5), place a check in the box to the left of the hash function. Check None with extreme caution or not at all, as it tells PGPnet to accept proposals that do not include authentication from other users.
- **Diffie-Hellman.** Diffie-Hellman is a key agreement protocol. To allow a specific key size (1024 or 1536), place a check in the box to the left of the key size.
- **Compression.** A compression function takes a fixed-sized input and returns a shorter, fixed sized output. There are two types of compression: LZS and Deflate. To allow a specific type of compression, place a check in the box to the left of the compression type.

NOTE: LZS and Deflate increase performance for low-speed communications such as modems and ISDN. LZS and Deflate decrease performance for fast-speed communications (for example, cable modem, DSL, T-1, and T-3). This is due to the overhead of the compression routines.

For instructions on how to add and remove allowed remote proposals, see “Adding and removing Allowed Remote proposals” on page 179.

Proposals

Use the Proposals portion of the **VPN Advanced** panel to add, edit, remove, or reorder your existing proposals. The IKE and IPsec proposals tell PGPnet what proposals to make to other users; proposals must be accepted exactly as specified. Note that PGPnet allows a minimum of one and maximum of 16 proposals for both IKE and IPsec proposals.

NOTE: Only experienced IPsec users should make any edits to this panel.

The types of information used in IKE proposals are:

- **Authentication.** Authentication is a means of verifying information, such as identity.There are three types of authentication: shared key (a secret key shared by two or more users), DSS signature (a Digital Signature Standard signature, and RSA signature.
- **Hash.** A hash function takes a variable-sized input string and converts it to a fixed-sized output string. There are two types of hash: SHA (Secure Hash Algorithm) and MD5 (Message-Digest Algorithm).
- **Ciphers.** Ciphers are algorithms used to encrypt and decrypt. There are two types available: CAST and TripleDES.
- **Diffie-Hellman.** Diffie-Hellman is a key agreement protocol. There are two sizes of Diffie-Hellman keys available: 1024 and 1536.

The types of information used in IPsec Proposals are:

- **AH.** Enables Authentication Header (AH). AH is included for backward compatibility with older IPsec products. AH does not provide encryption. AH authenticates your IP addresses. This can, however, create problems. Since NAT translates your IP addresses, AH's authentication of your IP address can result in packet authentication failure.

  To use AH, you must select Ciphers **None** on the **VPN Advanced** panel, add an IPsec proposal that includes AH, and move that proposal to the top of the proposals list.

  There are two types available: SHA and MD5.
- **ESP.** Enables Encapsulating Security Payload (ESP), a sub-protocol of IPsec that handles both encryption and authentication.

  To allow remote proposals to initiate ESP **None** you must check the Ciphers **None** check box on the **VPN Advanced** panel. You must also add a proposal to your IPsec proposals that includes ESP None and move that proposal to the top of your IPsec proposal list.

  There are three hash types: None, SHA, and MD5. There are three cipher types: None, CAST, and TripleDES.
- **IPPCP.** Enables IP Payload Compression Protocol (IPPCP). Use for dial-up connections only. Involves major overhead.

To use IPPCP, you must create a new IPsec proposal that includes IPPCP on the **VPN Advanced** panel, move the proposal to the top of the proposals list, and turn on IPPCP and LZS or Deflate. Deflate has much higher overhead than LZS, so LZS is recommended.

Compression algorithms take a fixed-sized input and create a smaller fixed-sized output.

If another machine proposes IPPCP to PGPnet, PGPnet accepts the proposal, unless LZS and Deflate are turned off in the Remote Proposals section of the **VPN Advanced** panel.

There are two types of IPPCP: Deflate and LZS.

NOTE: LZS and Deflate increase performance for low-speed communications such as modems and ISDN, and decrease performance for fast-speed communications (for example, cable modem, DSL, T-1, and T-3). This is due to the overhead of the compression routines.

For more information on how to add, edit, reorder, or remove IKE and IPsec proposals, see “Working with IKE and IPsec proposals” on page 179.

Perfect Forward Secrecy

All IPsec proposals use the same **Perfect Forward Secrecy** Diffie-Hellman setting: **None**, **1024**, or **1536** bits.

If **Perfect Forward Secrecy** is on, PGPnet generates the keys for a particular connection and then disposes of the key material used to generate the key.

If an attacker were able to brute-force attack a specific SA, it would not help the attacker brute-force past or future connections.

If PFS is on (that is, you select **1024** or **1536**), it must be turned on on all machines that you communicate with.

PFS requires additional Diffie-Hellman key exchanges which takes additional processing time. This can become an issue on a gateway that handles hundreds of SA negotiations a minute if everyone is using PFS.

If PFS is turned on on your machine but it is off on a gateway, you cannot negotiate an SA with that gateway.

Default Settings button

Use this button to restore the default settings for all fields on this screen. In most cases, the default settings will be sufficient to establish SAs and use PGPnet.

3. Click **OK** to save your changes or choose another panel to continue configuring your PGP preferences.

Adding and removing Allowed Remote proposals

To add an item to the Allowed Remote Proposals:

1. Display the **Preferences** dialog box **(Edit —>Preferences)**
2. Click the **VPN Advanced** panel.
3. Select the check box to the left of the item.
4. Click **OK**.

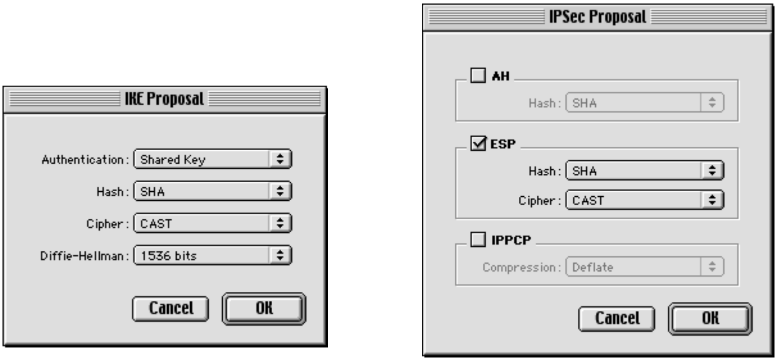
To remove an item from the Allowed Remote Proposals:

1. Display the **Preferences** dialog box **(Edit—>Preferences)**
2. Click the **VPN Advanced** panel.
3. Clear the check box to the left of the item.
4. Click **OK**.

Working with IKE and IPsec proposals

To add an IKE or IPsec proposal:

1. Display the **Preferences** dialog box **(Edit—>Preferences)**.
2. Click the **VPN Advanced** panel.
3. Click **New**, and select **IKE** or **IPsec**.
4. Make the appropriate selections in the **IKE** or **IPsec Proposal** dialog box (Figure 9-11).



IKE Proposal

Authentication: Shared Key

Hash: SHA

Cipher: CAST

Diffie-Hellman: 1536 bits

IPSec Proposal

□ AH

Hash: SHA

☑ ESP

Hash: SHA

Cipher: CAST

□ IPPCP

Compression: Deflate

Example IKE Proposal

Example IPsec Proposal

Figure 9-11. IKE and IPsec Proposal dialog boxes

5. Click **OK**.
6. If you are adding an IPsec proposal, select the appropriate Diffie-Hellman setting (**None**, **1024**, and **1536**) in the **Perfect Forward Secrecy** setting. All IPsec proposals use the same Diffie-Hellman setting.
7. Click **OK**.

To edit an IKE or IPsec proposal:

1. Display the **Preferences** dialog box **(Edit—>Preferences)**.
2. Click the **VPN Advanced** panel.
3. Select the Proposal.
4. Click **Edit**.
5. Make the appropriate changes in the **IKE** or **IPsec Proposal** dialog box (Figure 9-11 on page 180).
6. Click **OK**.
7. Review the setting displayed in the **Perfect Forward Secrecy** box. Note that all IPsec proposals use the same Diffie-Hellman setting. Change the setting if required.
8. Click **OK** on the **VPN Advanced** panel.

To remove an IKE or IPsec proposal:

1. Display the **Preferences** dialog box **(Edit—>Preferences)**.
2. Click the **VPN Advanced** panel.
3. Click the proposal.
4. Click **Remove**.
5. Click **OK**.

To reorder IKE or IPsec proposals:

1. Display the **Preferences** dialog box **(Edit—>Preferences)**.
2. Click the **VPN Advanced** panel.
3. Select the proposal.
4. To move the proposal up, click **Move Up**. To move the proposal down, click **Move Down**.
5. Click **OK**.

Troubleshooting PGP B

This appendix presents information about problems you may encounter while using PGP and suggests solutions. The following table lists PGP errors, a possible cause for the error, and a solution.

Error	Cause	Solution
Authentication rejected by remote SKEP connection	The user on the remote side of the network share file connection rejected the key that you provided for authentication.	Use a different key to authenticate the network share file connection, or contact the remote user to assure them that the key you're using is valid.
The PGP memory page locking driver is not functioning correctly.	Could be the result of an incorrect installation, a system failure, or tampering with your system.	Reinstall PGP.
Cannot perform the requested operation because the output buffer is too small.	The output is larger than the internal buffers can handle.	If you are encrypting or signing, you may have to break up the message and encrypt/sign smaller pieces at a time. If you are decrypting or verifying, ask the sender to encrypt/sign smaller pieces and re-send them to you.
Could not encrypt to specified key because it is a sign-only key.	The selected key can only be used for signing.	Choose a different key, or generate a new key that can encrypt data.
Could not sign with specified key because it is an encrypt-only key.	The selected key can only be used for encrypting.	Choose a different key, or generate a new key that can sign data.
Error in domain name systemic	The destination address you provided is incorrect, or your network connection is misconfigured.	Check to make sure that the destination address you provided is the correct one. If you are sure of this, check your connection to the network.

Error	Cause	Solution
Identical shares cannot be combined	You attempted to combine the same share twice.	If you received the shares from a share file, try choosing a different share file. If you received the shares from the network, you may need to contact the user at the remote location and tell them to send a different set of shares
No secret keys could be found on your keyring.	There are no private keys on your keyring.	Generate your own pair of keys in PGPkeys.
Socket is not connected	The network connection to the PGP key server or to the network share file connection has been broken.	Try re-establishing the connection by repeating the procedure you used to start the connection. If that fails, check your connection to the network.
The action could not be completed due to an invalid file operation.	The program failed to read or write data in a certain file.	The file is probably corrupt. Try altering your PGP Preferences to use a different file, if possible.
The evaluation time for PGP encrypting and signing has passed. Operation aborted.	The product evaluation time has expired.	Download the freeware version or buy the commercial version of the product.
The keyring contains a bad (corrupted) PGP packet.	The PGP message that you are working with has been corrupted, or your keyring has been corrupted.	Ask the sender to re-send the message if it's a message that you're working with. If it's your keyring, try restoring from your backup keyring.
The keyring file is corrupt.	The program failed to read or write data in a certain file.	There is a file that is probably corrupt or missing. It may or may not be the keyring file. Try using a different file name or path, if possible.
The message/data contains a detached signature.	The signature for the message/file is located in a separate file.	Double-click on the detached signature file first.
The passphrase you entered does not match the passphrase on the key.	The passphrase you entered is incorrect.	You may have the CAPS LOCK on, or you simply may have mis-typed the passphrase. Try again.
The PGP library has run out of memory.	The operating system has run out of memory.	Close other running programs. If that doesn't work, you may need more memory in your machine.

Error	Cause	Solution
The specified user ID was not added because it already exists on the selected key.	You can't add a User ID to a key if there is one just like it already on the key.	Try adding a different user ID, or delete the matching one first.
The specified key could not be found on your keyring.	The key needed to decrypt the current message is not on your keyring.	Ask the sender of the message to re-send the message and make sure they encrypt the message to your public key.
The specified input file does not exist.	The file name typed in does not exist.	Browse to find the exact name and path of the file you want.
There is not enough random data currently available.	The random number generator needs more input in order to generate good random numbers.	When prompted, move the mouse around, or press random keys, in order to generate input.
There was an error during the writing of the keyring or the exported file.	The program failed to write data to a certain file.	Your hard drive may be full, or if the file is on a floppy, the floppy is not present in the floppy drive.
There was an error opening or writing the keyring or the output file.	A file that was needed couldn't be opened.	Make sure the settings in your PGP Preferences is correct. If you've recently deleted files in the directory that you installed PGP, you may need to re-install the product.
This key is already signed by the specified signing key.	You can't sign a key that you have already signed.	You may have accidentally picked the wrong key. If so, choose a different key to sign.
Unable to perform operation because this file is read-only or otherwise protected. If you store your keyring files on removable media the media may not be inserted.	A file that was needed is set to read-only or is being used by another program.	Close other programs that may be accessing the same files as the program you are running. If you keep your keyring files on a floppy disk, make sure that the floppy disk is in the floppy drive.

Troubleshooting PGPnet C

This appendix contains explanations for error messages that may appear on PGPnet's Log panel, tells you how to solve problems that may occur with PGPnet, and includes additional information about PGPnet features that you can use to troubleshoot problems with PGPnet.

PGPnet error messages

The following table lists PGPnet error messages, a possible cause of the error message, and a solution to the problem.

Error	Cause	Solution
Invalid exchange	Trying to communicate on a Phase 1 exchange that no longer exists. Phase 1 was established; however, one side has shut down. This may also occur when you delete an SA. Some products do not notice that the SA has been terminated, so those products continue to send information (this is generally harmless).	Re-establish the SA.
No SPI Found	One machine in the SA goes down, and the other machine doesn't know it. The errors appear on the machine that doesn't know that the SA has gone down.	Re-establish the SA.
No SA Found	Most likely an internal error in the PGP program.	Report this problem to NAI.
Unequal payload length	Usually caused by shared secret mismatch. Can also be caused by network packet corruption (packet says it's 5 Kb, but it's 4 Kb.).	Verify that you are using the same shared secret as the other machine.
No proposal chosen	Can occur when machine A and machine B have different configuration settings.	Compare the other machine's configuration with your own configuration (**VPN Advanced** Preferences panel).

Error	Cause	Solution
Invalid cookie	Cookie is no longer valid between machine A and machine B. One machine is attempting to communicate via an SA that has been terminated. Generally harmless.	Re-establish the SA.
Response timeout	1) Routing problem. IP protocols 50 and 51 UDP 500 for IKE. 2) You are sending requests to a machine that is configured incorrectly.	Find out if there is a firewall or Network Address Translation (NAT) device preventing connection.
NAT incompatibility is detected	There is a Network Address Translation (NAT) device preventing connection.	Remove the NAT device. NAT is incompatible with many Internet protocols, including IPsec.

Additional tips

- You can use IKE log for troubleshooting. To access the IKE log, click **Advanced** on the **Log** panel.
- In a corporate setting, Administrators can “lock” their users PGPnet configurations settings. See the *PGP Administrator’s Guide* for details.
- If communications are really slow, check the compression setting on the PGP **VPN Advanced** panel. You may not want to use compression. Note that compression is only useful for dial-up connections.
- If you are having trouble creating an SA, verify that the TCP/IP configuration that you are using is secured by PGPnet.
- If you can create an SA with a machine (a green light appears in the SA column) but you cannot send or receive traffic, make sure PGPnet and your Network Address Translation (NAT) have the same device or adapter.

  You may be bound to the wrong adapter. Check your TCP/IP configurations.

Understanding authentication

The **VPN Authentication** panel controls how you authenticate yourself with other machines. It also controls if other machines, configured or unconfigured, must present valid remote authentication to communicate with your machine.

The **Remote Authentication** option on the **Host/Gateway** dialog controls how a specific host authenticates itself to your machine.

The VPN Authentication panel

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

Use the **PGP Authentication** and **X.509 Authentication** boxes to identify how you want to authenticate your local machine when you communicate with other machines. When you attempt to create an SA, PGPnet uses the selected key or certificate to tell the other machine who you are.

Use the **Remote Authentication** options to tell PGPnet how you want configured and unconfigured machines to authenticate themselves.

Configured hosts. Normally you will want to require a valid authentication key or certificate from configured hosts. To do so, click **Require valid remote authentication from configured hosts**. If you want a configured host to present a specific PGP key or X.509 certificate, use the **Remote Authentication** option on the **Host/Gateway** dialog.

Unconfigured hosts. These hosts may have no prior trust relationship with you. Allowing them to connect with an invalid key or certificate provides encryption of traffic which would otherwise be in the clear.

- To allow connection from unconfigured hosts with a key or certificate that is not considered valid on your keyring (but which may, of course, be a completely valid key), clear the **Require valid remote authentication from unconfigured hosts** box.
- To require valid remote authentication from unconfigured hosts, click **Require valid remote authentication from unconfigured hosts**. When this setting is used, the user authenticates the key that the server presents and authenticates with his own anonymous certificate. This is similar to how most e-commerce web-sites work; the server is authorized, but the client is anonymous.

Host/Gateway dialog: Remote Authentication

NOTE: X.509 authentication certificates are not supported in PGP Freeware.

The controls in the **Remote Authentication** section of the **Host/Gateway** dialog allow you to require the remote host to present a specific PGP key or X.509 certificate each time the host attempts to establish an SA with your host. If the host attempts to establish a connection and does not present the specified key or certificate, your machine will refuse the connection.

You can add this requirement when you add a host using Expert Mode, or after you add a host by editing the host entry.

NOTE: The key that you require them to present should be their public key, not your public key.

IMPORTANT: If you select a specific PGP key or X.509 certificate for a secure subnet entry, all users within that subnet must use the same key to authenticate themselves. This would be an unusual configuration.

All key authentications appear on the **Log** panel, and each entry displays the key ID.

Transferring Files Between the MacOS and Windows

D

Transferring files to and from MacOS is a classic problem in using almost any kind of data exchange software, such as email applications, FTP, compression utilities, and PGP. This appendix is intended to document how this problem has finally been solved by PGP version 5.5.x and above, and to discuss how to communicate with previous versions of PGP.

The MacOS stores files differently from other operating systems. Even the text file format of the MacOS is different. MacOS files are really two files consisting of a Data segment and a Resource segment. In order to send a file from MacOS to Windows without losing data, the two segments must be merged into one. The standard method by which a MacOS file is converted into a single file so that it can be transferred to another Macintosh or PC without losing either of its halves is called MacBinary.

The problem is that, without special software, Windows and other platforms cannot inherently understand the MacBinary format. If a situation occurs where the receiving software fails to convert a MacBinary format file into a Windows file, the resulting file is unusable. Third-party utilities exist on Windows to convert it after the fact into a usable file, but that can be rather inconvenient.

Versions of PGP prior to 6.0 and many utilities available on the market today generally try to ignore this problem as much as possible and leave all decisions up to the user as to whether or not to encode a file with MacBinary when sending from MacOS. This places the burden of deciding to send with MacBinary, and not risk losing any data, or send without MacBinary, with hope that no important data will be lost on the user, who often has no idea what the correct decision is. The decision should generally be based on whether the file is being sent to Windows or MacOS. But what about if you're sending to both at the same time? There is no good solution to that problem with older versions of PGP and many other utilities. This has resulted in great confusion and inconvenience for users.

The reverse, sending a file from Windows to the MacOS, has also been a major problem. Windows uses filename extensions, such as .doc, to identify the type of a file. This is meaningless to the MacOS. These files are sent to a Macintosh computer without any file type or creator information. The process of making them readable after receipt generally involves various arcane motions in the Open dialog of the creator application, or in many cases requires the user to understand MacOS lore of creator and type codes by setting them manually in a third-party utility. Fortunately, the latest version of PGP (versions 5.5 and above) leads the way out of this confusion.

Sending from the MacOS to Windows

On the MacOS, there are three options when encrypting or signing a file:

- **MacBinary: Yes.** This is the recommended option for all encryptions when sending to another user of PGP Version 5.5 or above on any platform. This means that MacOS users will receive the exact file that was intended, and the Windows version will automatically decode the MacBinary and even append the appropriate file extension, such as .doc for Microsoft Word or .ppt for Microsoft PowerPoint. PGP includes information on most popular application filename extensions and Macintosh-creator codes. In cases where the type is unknown or known to be a MacOS-only file such as a MacOS application, the file remains in MacBinary format so that it can later be forwarded to a Macintosh fully intact.

- **MacBinary: No.** If you are communicating with users who have an older version of PGP, the decision of whether to send with MacBinary generally ends up in the sender's hands as in most other programs and in previous versions of PGP for MacOS. When sending to a PC using an older version, if you know that the file you are sending can be read by Windows applications when no MacBinary is used, select this option. This includes most files that are generally cross-platform such as those created by the Microsoft Office applications, graphics files, compressed files, and many others. The sender or the recipient will have to manually rename the file to have the correct filename extension on Windows. This is required because the Windows recipient does not have the creator information normally encoded with MacBinary.

- **MacBinary: Smart.** There are some very limited cases where this option can be useful when communicating with users who are not using later versions of PGP. This option makes a decision as to whether to encode with MacBinary based on an analysis of the actual data in the file. If the file is one of the following types, it will not be encoded with MacBinary, thereby making it readable on a PC with any version of PGP:
  - PKzip compressed file
  - Lempel-Ziv compressed file
  - MIDI music format file
  - PackIt compressed file
  - GIF graphics file
  - StuffIt compressed file
  - Compactor compressed file
  - Arc compressed file
  - JPEG graphics file

As shown, only a limited selection of files will result in a readable file by old versions of PGP on other platforms using the Smart option. Any other file received on a PC with an older version of PGP will be unreadable without stripping the MacBinary encoding with a third-party utility. Also, the file will not have the correct filename extension on the PC unless that extension was manually added by the user on the sending side. Using Smart mode, the resulting file may not be the same as the original when sent to a Macintosh, because it may lose its creator and type codes. This mode remains in the product mostly due to the fact that it was in PGP Version 5.0 and some users may only have a need to send the above file types. This option is not recommended in most cases.

In summary, if you are sending only to versions 6.x or above, always select MacBinary: Yes (the default). Thus, no thought is required if your environment is using PGP version 6.x or above exclusively. When sending to users with older versions, you should select MacBinary: No for cross-platform file types and MacBinary: Yes for files which simply wouldn't be readable to PC users anyway (such as a MacOS application).

> **NOTE:** PGP Version 5.0 did not have a MacBinary: No option. In order to send file types without MacBinary, which are not included in the MacBinary: Smart list to a PC using 5.0, the file must be manually set to one of the creator and type codes on the Smart list before sending.

Receiving Windows files on the MacOS

When decrypting, PGP version 5.5.x and later automatically attempts to translate filename extensions for non-MacBinary files into MacOS creator and type information. For example, if you receive a file from Windows with an extension of .doc, the file will be saved as a Microsoft Word document. The same list of applications used when adding filename extensions upon receipt of a MacBinary file on Windows is used to translate filename extensions back into the MacOS equivalent when received on a Macintosh computer. In almost all cases, this results in files which are immediately readable and double-clickable on MacOS.

Previous versions of PGP for MacOS do not have this feature. The user will have to manually determine that a file named “report.doc” is a Microsoft Word file. After determining the creator application, in the case of Microsoft Word, one can simply use the Open dialog to open the file by selecting Show All Files from the popup menu. Many other applications also have this feature, but some don't. If the document cannot be opened from within the application, the user must find out what the appropriate Macintosh creator and type codes are for the file and manually set them with a third-party utility. There are many free utilities to do this. Upgrading to version 6.x or above is probably the easiest option in this case, as it eliminates this problem.

Supported applications

The following list of major applications produce documents which are automatically translated by PGP when sent from Windows to MacOS and vice versa. You can add items to this list by editing the PGPMacBinaryMappings.txt file in the \WINDOWS directory. On the Mac side, remove the .txt suffix on the filename—PGPMacBinaryMappings is located in System Folder / Preferences / Pretty Good Preferences.

- PhotoShop (GIF, native Photoshop documents, TGA, JPEG)
- PageMaker (Versions 3.X, 4.X, 5.X, 6.X)
- Microsoft Project (project and template files)
- FileMaker Pro
- Adobe Acrobat
- Lotus 123
- Microsoft Word (text, RTF, templates)
- PGP
- Microsoft PowerPoint

- StuffIt
- QuickTime
- Corel WordPerfect
- Microsoft Excel (many different types of files)
- Quark XPress

The following general filename extensions are also converted:

.cvs	.arj	.ima	.eps	.mac	.cgm
.dl	.fli	.ico	.iff	.img	.lbm
.msp	.pac	.pbm	.pcs	.pcx	.pgm
.plt	.pm	.ppm	.rif	.rle	.shp
.spc	.sr	.sun	.sup	.wmf	.flc
.gz	.vga	.hal	.lzh	.Z	.exe
.mpg	.dvi	.tex	.aif	.zip	.au
.mod	.svx	.wav	.tar	.pct	.pic
.pit	.txt	.mdi	.pak	.tif	.eps

Biometric Word Lists E

Biometric Word Lists

By Philip Zimmermann and Patrick Juola

PGP uses a special list of words to convey binary information in an authenticated manner over a voice channel, such as a telephone, via biometric signatures. The human voice that speaks the words, if recognized by the listener, serves as a means of biometric authentication of the data carried by the words. The word list serves the same purpose as the military alphabet, which is used to transmit letters over a noisy radio voice channel. But the military alphabet has 26 words, each word representing one letter. For our purposes, our list has 256 carefully selected phonetically distinct words to represent the 256 possible byte values of 0 to 255.

We created a word list for reading binary information over the phone, with each word representing a different byte value. We tried to design the word list to be useful for a variety of applications. The first application we had envisioned was to read PGP public key fingerprints over the phone to authenticate the public key. In that case, the fingerprint is 20 bytes long, requiring 20 words to be read aloud. Experience has shown it to be fairly tedious and error prone to read that many bytes in hexadecimal, so it seems worth using a word list to represent each byte by a word.

Some applications may require transmitting even lengthier byte sequences over the phone, for example, entire keys or signatures. This may entail reading more than a hundred bytes. Using words instead of hex bytes seems even more justified in that case.

When reading long sequences of bytes aloud, errors may creep in. The kinds of error syndromes you get on human-spoken data are different than they are for transmitting data through a modem. Modem errors usually involve flipped bits from line noise. Error detection methods for modems usually involve CRCs to be added, which are optimized for detecting line noise bursts. However, random sequences of spoken human words usually involves one of three kinds of errors: 1) transposition of two consecutive words, 2) duplicate words, or 3) omitted words. If we are to design an error detection scheme for this kind of data transmission channel, we should make one that is optimized for these three kinds of errors. Zhahai Stewart suggested a good scheme (in personal conversation with me in 1991) for error detection of these errors.

Stewart's scheme for error detection while reading aloud long sequences of bytes via a word list entails using not one, but two lists of words. Each list contains 256 phonetically distinct words, each word representing a different byte value between 0 and 255. The two lists are used alternately for the even-offset bytes and the odd-offset bytes in the byte sequence.

For example, the first byte (offset 0 in the sequence) is used to select a word from the even list. The byte at offset 1 is used to select a byte from the odd list. The byte at offset 2 selects a word from the even list again, and the byte at offset 3 selects from the odd list again. Each byte value is actually represented by two different words, depending on whether that byte appears at an even or an odd offset from the beginning of the byte sequence. For example, suppose the word “adult” and the word “amulet” each appears in the same corresponding position in the two word lists, position 5. That means that the repeating 3-byte sequence 05 05 05 is represented by the 3-word sequence “adult, amulet, adult.”

This approach makes it easy to detect all three kinds of common errors in spoken data streams: transposition, duplication, and omission. A transposition will result in two consecutive words from the even list followed by two consecutive words from the odd list (or the other way around). A duplication will be detected by two consecutive duplicate words, a condition that cannot occur in a normal sequence. An omission will be detected by two consecutive words drawn from the same list.

To facilitate the immediate and obvious detection by a human of any of the three error syndromes described above, without computer assistance, we made the two lists have one obviously different property: The even list contains only two-syllable words, while the odd list contains only three-syllable words. That suggestion came from Patrick Juola, a computational linguist.

PGPfone was the application that precipitated the actual development of the word list by Juola and Zimmermann. PGPfone is an application that turns your computer into a secure telephone. We used it to authenticate PGPfone's initial Diffie-Hellman key exchange without using digital signatures and public key infrastructures. We knew we would end up using it for authenticating PGP key fingerprints when we applied it to PGP later.

The idea behind building the word lists was to develop a metric to measure the phonetic distance between two words, then use that as a goodness measure to develop a full list. Grady Ward provided us with a large collection of words and their pronunciations, and Patrick Juola used genetic algorithms to evolve the best subset of Ward's list.

To briefly summarize what he did, he made a large population of guesses and let the population “sexually reproduce” by exchanging words with other guesses -- and, like biological evolution, the better guesses survived into the next generation. After about 200 generations, the list had mostly stabilized into a best guess, with far greater phonetic distance between the words than what we started with in the initial guess lists.

The first major hurdle was the development of the metric. Linguists have studied sound production and perception for decades, and there is a standard feature set used to describe sounds in English. For example, say the words “pun,” “fun,” “dun,” and “gun” (go ahead, try it), and notice how your tongue keeps moving back in your mouth on each word. Linguists call this the “place of articulation,” and noises that are very different in this feature sound different to English speakers. Combining the features of all the sounds in a word gives us a representation of the sound of the entire word -- and we can compute the phonetic distance between a pair of words.

Actually, it wasn't that simple. We didn't know how to weight the various features, certain word-level features like accents were hard to represent, and the feature-based analysis simply fails for certain sounds. There were also a few other more subtle criteria; for example, we wanted the words to be common enough to be universally recognizable, but not so common as to be boring --and we didn't want confusing words like “repeat” or “begin” or “error”. Some sound features are less perceptible to non-native-English speakers, for example, some Japanese speakers might hear and pronounce “r” and “l” the same way. It would be nice if the words were short enough that you could fit enough of them on a small LCD display. Large consonant clusters (“corkscrew” has five pronounced consonants in a row) are sometimes hard to say, especially to non-English speakers. One way or another, we tried to incorporate all these criteria into a filter on the initial dictionary list or into the distance metric itself.

After the computer evolved the winning list, we looked at it. Yes, the words were phonetically distinct. But many of them looked like a computer picked them, not a human. A lot of them were just ugly and dumb. Some were repugnant, and some were bland and wimpy. So we applied some “wetware” augmentation to the list. Some words were deleted, and replaced by some human-chosen words. We had the computer check the new words against the list to see if they were phonetically distant from the rest of the list. We also tried to make the words not come too close to colliding phonetically with the other words in the larger dictionary, just so that they would not be mistaken for other words not on the list.

There were a variety of selection criteria that Juola used in his algorithms. He published a paper on it that goes into more detail. This document is just a brief overview of how we built the list.

I'm not entirely happy with the word list. I wish it had more cool words in it, and less bland words. I like words like “Aztec” and “Capricorn”, and the words in the standard military alphabet. While we'd like to reserve the right to revise the list at some future time, it's not likely, due to the legacy problems that this initial version will create. This version of the list was last modified in September 1998.

Two Syllable Word List

aardvark
absurd
accrue
acme
adrift
adult
afflict
ahead
aimless
Algol
allow
alone
ammo
ancient
apple
artist
assume
Athens
atlas
Aztec
baboon
backfield
backward
banjo
beaming
bedlamp
beehive
beeswax
befriend
Belfast
berserk
billiard
bison
blackjack
blockade
blowtorch
bluebird
bombast
bookshelf
brackish
breadline
breakup
brickyard
briefcase
Burbank
button
buzzard
cement
chairlift
chatter
checkup
chisel
choking
chopper
Christmas
clamshell
classic
classroom
cleanup
clockwork
cobra
commence
concert
cowbell
crackdown
cranky
crowfoot
crucial
crumpled
crusade
cubic
dashboard
deadbolt
deckhand
dogsled
dragnet
drainage
dreadful
drifter
dropper
drumbeat
drunken
Dupont
dwelling
eating
edict
egghead
eightball
endorse
endow
enlist
erase
escape
exceed
eyeglass
eyetooth
facial
fallout
flagpole
flatfoot
flytrap
fracture
framework
freedom
frighten
gazelle
Geiger
glitter
glucose
goggles
goldfish
gremlin
guidance
hamlet
highchair
hockey
indoors
indulge
inverse
involve
island
jawbone
keyboard
kickoff
kiwi
klaxon
locale
lockup
merit
minnow
miser
Mohawk
mural
music
necklace
Neptune
newborn
nightbird
Oakland
obtuse
offload
optic
orca
payday
peachy
pheasant
physique
playhouse
Pluto
preclude
prefer
preshrunk
printer
prowler
pupil
puppy
python
quadrant
quiver
quota
ragtime
ratchet
rebirth
reform
regain
reindeer
rematch
repay
retouch
revenge
reward
rhythm
ribcage
ringbolt
robust
rocker
ruffled
sailboat
sawdust
scallion
scenic
scorecard
Scotland
seabird
select
sentence
shadow
shamrock
showgirl
skullcap
skydive
slingshot
slowdown
snapline
snapshot
snowcap
snowslide
solo
southward
soybean
spaniel
spearhead
spellbind
spheroid
spigot
spindle
spyglass
stagehand
stagnate
stairway
standard
stapler
steamship
sterling
stockman
stopwatch
stormy
sugar
surmount
suspense
sweatband
swelter
tactics
talon
tapeworm
tempest
tiger
tissue
tonic
topmost
tracker
transit
trauma
treadmill
Trojan
trouble
tumor
tunnel
tycoon
uncut
unearth
unwind
uproot
upset
upshot
vapor
village
virus
Vulcan
waffle
wallet
watchword
wayside
willow
woodlark
Zulu

Three Syllable Word List

adroitness
adviser
aftermath
aggregate
alkali
almighty
amulet
amusement
antenna
applicant
Apollo
armistice
article
asteroid
Atlantic
atmosphere
autopsy
Babylon
backwater
barbecue
belowground
bifocals
bodyguard
bookseller
borderline
bottomless
Bradbury
bravado
Brazilian
breakaway
Burlington
businessman
butterfat
Camelot
candidate
cannonball
Capricorn
caravan
caretaker
celebrate
cellulose
certify
chambermaid
Cherokee
Chicago
clergyman
coherence
combustion
commando
company
component
concurrent
confidence
conformist
congregate
consensus
consulting
corporate
corrosion
councilman
crossover
crucifix
cumbersome
customer
Dakota
decadence
December
decimal
designing
detector
detergent
determine
dictator
dinosaur
direction
disable
disbelief
disruptive
distortion
document
embezzle
enchanting
enrollment
enterprise
equation
equipment
escapade
Eskimo
everyday
examine
existence
exodus
fascinate
filament
finicky
forever
fortitude
frequency
gadgetry
Galveston
getaway
glossary
gossamer
graduate
gravity
guitarist
hamburger
Hamilton
handiwork
hazardous
headwaters
hemisphere
hesitate
hideaway
holiness
hurricane
hydraulic
impartial
impetus
inception
indigo
inertia
infancy
inferno
informant
insincere
insurgent
integrate
intention
inventive
Istanbul
Jamaica
Jupiter
leprosy
letterhead
liberty
maritime
matchmaker
maverick
Medusa
megaton
microscope
microwave
midsummer
millionaire
miracle
misnomer
molasses
molecule
Montana
monument
mosquito
narrative
nebula
newsletter
Norwegian
October
Ohio
onlooker
opulent
Orlando
outfielder
Pacific
pandemic
Pandora
paperweight
paragon
paragraph
paramount
passenger
pedigree
Pegasus
penetrate
perceptive
performance
pharmacy
phonetic
photograph
pioneer
pocketful
politeness
positive
potato
processor
provincial
proximate
puberty
publisher
pyramid
quantity
racketeer
rebellion
recipe
recover
repellent
replica
reproduce
resistor
responsive
retraction
retrieval
retrospect
revenue
revival
revolver
sandalwood
sardonic
Saturday
savagery
scavenger
sensation
sociable
souvenir
specialist
speculate
stethoscope
stupendous
supportive
surrender
suspicious
sympathy
tambourine
telephone
therapist
tobacco
tolerance
tomorrow
torpedo
tradition
travesty
trombonist
truncated
typewriter
ultimate
undaunted
underfoot
unicorn
unify
universe
unravel
upcoming
vacancy
vagabond
vertigo
Virginia
visitor
vocalist
voyager
warranty
Waterloo
whimsical
Wichita
Wilmington
Wyoming
yesteryear
Yucatan

Glossary

AES (Advanced Encryption Standard) NIST approved encryption standards, usually used for the next 20 - 30 years. Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen, was chosen as the new AES in October 2000.

AH (Authentication Header) a security protocol that provides authentication services. AH is embedded in the data to be protected. AH can be used either by itself or with Encryption Service Payload (ESP).

Algorithm (encryption) a set of mathematical rules (logic) used in the processes of encryption and decryption.

Algorithm (hash) a set of mathematical rules (logic) used in the processes of message digest creation and key/signature generation.

Anonymity of unknown or undeclared origin or authorship, concealing an entity's identification.

ANSI (American National Standards Institute) develops standards through various Accredited Standards Committees (ASC). The X9 committee focuses on security standards for the financial services industry.

ASCII-armored text binary information that has been encoded using a standard, printable, 7-bit ASCII character set, for convenience in transporting the information through communication systems. In the PGP program, ASCII armored text files are given the default filename extension, and they are encoded and decoded in the ASCII radix-64 format.

Asymmetric keys a separate but integrated user key-pair, comprised of one public key and one private key. Each key is one way, meaning that a key used to encrypt information can not be used to decrypt the same data.

Authentication the determination of the origin of encrypted information through the verification of someone's digital signature or someone's public key by checking its unique fingerprint.

Authorization certificate an electronic document to prove one's access or privilege rights, also to prove one is who they say they are.

Authorization to convey official sanction, access or legal power to an entity.

Automatic Key Renewal the Setup Keys (IKE) and Primary Keys (IPsec) are responsible for creating your Security Associations. They are automatically renewed based on the Automatic Key Renewal values that appear on the VPN Options panel for Windows or the VPN Key Refresh option for Mac.

Backdoor a cipher design fault, planned or accidental, which allows the apparent strength of the design to be easily avoided by those who know the trick. When the design background of a cipher is kept secret, a back door is often suspected.

Back Orifice a backdoor program for Windows 9x written by a group calling themselves the Cult of the Dead Cow. This backdoor allows remote access to the machine once installed, allowing the installer to run commands, get screen shots, modify the registry, and perform other operations. Client programs to access Back Orifice are available for Windows and UNIX.

Blind signature ability to sign documents without knowledge of content, similar to a notary public.

Block cipher a symmetric cipher operating on blocks of plain text and cipher text, usually 64 bits.

CA (Certificate Authority) a trusted third party (TTP) who creates certificates that consist of assertions on various attributes and binds them to an entity and/or to their public key.

CAPI (Crypto API) Microsoft’s crypto API for Windows-based operating systems and applications.

CAST a 64-bit block cipher using 64-bit key, six S-boxes with 8-bit input and 32-bit output, developed in Canada by Carlisle Adams and Stafford Tavares.

Certificate (digital certificate) an electronic document attached to a public key by a trusted third party, which provides proof that the public key belongs to a legitimate owner and has not been compromised.

Certification endorsement of information by a trusted entity.

Certify to sign another person's public key.

Certifying authority one or more trusted individuals who are assigned the responsibility of certifying the origin of keys and adding them to a common database.

Ciphertext plaintext converted into a secretive format through the use of an encryption algorithm. An encryption key can unlock the original plaintext from ciphertext.

Clear-signed message messages that are digitally signed but not encrypted.

Clear text characters in a human readable form or bits in a machine-readable form (also called *plain text*).

Compression function a compression function takes a fixed-sized input and returns a shorter, fixed sized output.

Corporate signing key a public key that is designated by the security officer of a corporation as the system-wide key that all corporate users trust to sign other keys.

Conventional encryption encryption that relies on a common passphrase instead of public key cryptography. The file is encrypted using a session key, which encrypts using a passphrase that you will be asked to choose.

Cryptanalysis the art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

CRYPTOKI same as PKCS #11.

Cryptography the art and science of creating messages that have some combination of being private, signed, unmodified with non-repudiation.

Cryptosystem a system comprised of cryptographic algorithms, all possible plain text, cipher text, and keys.

Data integrity a method of ensuring information has not been altered by unauthorized or unknown means.

Decryption a method of unscrambling encrypted information so that it becomes legible again. The recipient's private key is used for decryption.

denial of service attack an assault, usually planned, that seeks to disrupt Web access. A denial of service attack overwhelms an Internet server with connection requests that cannot be completed. In so doing, it causes the server to become so busy attempting to respond to the attack that it ignores legitimate requests for connections.

DES (Data Encryption Standard) a 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for over 20 years, adopted in 1976 as FIPS 46.

Dictionary attack a calculated brute force attack to reveal a password by trying obvious and logical combinations of words.

Diffie-Hellman the first public key algorithm, invented in 1976, using discrete logarithms in a finite field.

Digital cash electronic money that is stored and transferred through a variety of complex protocols.

Direct trust an establishment of peer-to-peer confidence.

Digital signature see signature.

DSA (Digital Signature Algorithm) a public key digital signature algorithm proposed by NIST for use in DSS.

DSS (Digital Signature Standard) a NIST proposed standard (FIPS) for digital signatures using DSA.

ECC (Elliptic Curve Cryptosystem) a unique method for creating public key algorithms based on mathematical curves over finite fields or with large prime numbers.

EES (Escrowed Encryption Standard) a proposed U.S. government standard for escrowing private keys.

Elgamal scheme used for both digital signatures and encryption based on discrete logarithms in a finite field; can be used with the DSA function.

Encryption a method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt it to read it.

ESP (Encapsulating Security Payload) IPsec header that encrypts the contents of an IP packet.

Fingerprint a uniquely identifying string of numbers and characters used to authenticate public keys. This is the primary means for checking the authenticity of a key. See *Key Fingerprint*.

FIPS (Federal Information Processing Standard) a U.S. government standard published by NIST.

Firewall a combination of hardware and software that protects the perimeter of the public/private network against certain attacks to ensure some degree of security.

Hash function a one way function that takes an input message of arbitrary length and produces a fixed length digest.

Hierarchical trust a graded series of entities that distribute trust in an organized fashion, commonly used in ANSI X.509 issuing certifying authorities.

HTTP (HyperText Transfer Protocol) a common protocol used to transfer documents between servers or from a server to a client.

Hexadecimal hexadecimal describes a base-16 number system. That is, it describes a numbering system containing 16 sequential numbers as base units (including 0) before adding a new position for the next number. (Note that we're using “16” here as a decimal number to explain a number that would be “10” in hexadecimal.) The hexadecimal numbers are 0-9 and then

use the letters A-F.

IDEA (International Data Encryption Standard) a 64-bit block symmetric cipher using 128-bit keys based on mixing operations from different algebraic groups. Considered one of the strongest algorithms.

IKE (Internet Key Exchange) provides a secure means of key exchange over the Internet. IKE is also a candidate for IPSec security archetecture.

IKE and IPsec proposals The IKE and IPsec proposals tell PGPnet what proposals to make to other users. Proposals must be accepted exactly as specified. PGPnet allows a minimum of one and maximum of 16 proposals for both IKE and IPsec proposals.

Implicit trust Implicit trust is reserved for key *pairs* located on your local keyring. If the private portion of a key pair is found on your keyring, PGP assumes that you are the owner of the key pair and that you implicitly trust yourself.

Integrity assurance that data is not modified (by unauthorized persons) during storage or transmittal.

Introducer a person or organization who is allowed to vouch for the authenticity of someone’s public key. You designate an introducer by signing their public key.

IP Payload Compression Protocol (IPPCP) a protocol to reduce the size of IP datagrams. This protocol will increase the overall communication performance between a pair of communicating hosts/gateways (“nodes”) by compressing the datagrams, provided the nodes have sufficient computation power and the communication is over slow or congested links. IPPCP is very useful over slow links such as a modem, but it is not recommended over fast links.

IP spoofing the act of inserting a false sender IP address into an Internet transmission in order to gain unauthorized access to a computer system.

IPsec a TCP/IP layer encryption scheme under consideration within the IETF.

ISO (International Organization for Standardization) responsible for a wide range of standards, like the OSI model and international relationship with ANSI on X.509.

Key a digital code used to encrypt and sign and decrypt and verify messages and files. Keys come in key pairs and are stored on keyrings.

Key escrow/recovery a practice where a user of a public key encryption system surrenders their private key to a third party thus permitting them to monitor encrypted communications.

Key exchange
a scheme for two or more nodes to transfer a secret session key across an unsecured channel.

Key fingerprint
a uniquely identifying string of numbers and characters used to authenticate public keys. For example, you can telephone the owner of a public key and have him or her read the fingerprint associated with their key so you can compare it with the fingerprint on your copy of their public key to see if they match. If the fingerprint does not match, then you know you have a bogus key.

Key ID
a legible code that uniquely identifies a key pair. Two key pairs may have the same user ID, but they will have different Key IDs.

Key length
the number of bits representing the key size; the longer the key, the stronger it is.

Key management
the process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic key to authorized recipients in a secure manner.

Key pair
a public key and its complimentary private key. In public-key cryptosystems, like the PGP program, each user has at least one key pair.

Keyring
a set of keys. Each user has two types of keyrings: a private keyring and a public keyring.

Key splitting or “secret sharing”
the process of dividing up a private key into multiple pieces, and share those pieces among a group of people. A designated number of those people must bring their shares of the key together to use the key.

LDAP (Lightweight Directory Access Protocol)
a simple protocol that supports access and search operations on directories containing information such as names, phone numbers, and addresses across otherwise incompatible systems over the Internet.

Message digest
a compact “distillate” of your message or file checksum. It represents your message, such that if the message were altered in any way, a different message digest would be computed from it.

Meta-introducer
a trusted introducer of trusted introducers.

MIC (Message Integrity Check)
originally defined in PEM for authentication using MD2 or MD5. Micalg (message integrity calculation) is used in secure MIME implementations.

MIME (Multipurpose Internet Mail Extensions)
a freely available set of specifications that offers a way to interchange text in languages with different character sets, and multimedia email among many different computer systems that use Internet mail standards.

Non-repudiation preventing the denial of previous commitments or actions.

One-way hash a function of a variable string to create a fixed length value representing the original pre-image, also called message digest, fingerprint, message integrity check (MIC).

Passphrase an easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

Password a sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification.

PFS (Perfect Forward Secrecy) for a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

PGP/MIME an IETF standard (RFC 2015) that provides privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC1847, currently deployed in PGP 5.0 and later versions.

Phase 1 and Phase 2 the IKE negotiation occurs in two phases. Phase 1 authenticates the two parties and sets up a key management Security Association for protecting the data that is passed during the negotiation. In this phase, the key management policy is used to secure the negotiation messages. Phase 2 negotiates data management Security Association, which uses the data management policy to set up IP Security tunnels in the kernel for encapsulating and decapsulating data packets.

PKCS (Public Key Crypto Standards) a set of *de facto* standards for public key cryptography developed in cooperation with an informal consortium (Apple, DEC, Lotus, Microsoft, MIT, RSA, and Sun) that includes algorithm-specific and algorithm-independent implementation standards. Specifications defining message syntax and other protocols controlled by RSA Data Security Inc.

PKI (Public Key Infrastructure) a widely available and accessible certificate system for obtaining an entity’s public key with some degree of certainty that you have the “right” key and that it has not been revoked.

Plaintext normal, legible, un-encrypted, unsigned text.

Primary Keys (IPsec) IPsec keys responsible for creating your Security Association. Values can be set in time or data size.

Private key the secret portion of a key pair-used to sign and decrypt information. A user's private key should be kept secret, known only to the user.

Private keyring a set of one or more private keys, all of which belong to the owner of the private keyring.

Public key one of two keys in a key pair-used to encrypt information and verify signatures. A user's public key can be widely disseminated to colleagues or strangers. Knowing a person's public key does not help anyone discover the corresponding private key.

Public keyring a set of public keys. Your public keyring includes your own public key(s).

Public-key cryptography cryptography in which a public and private key pair is used, and no security is needed in the channel itself.

Random number an important aspect to many cryptosystems, and a necessary element in generating a unique key(s) that are unpredictable to an adversary. True random numbers are usually derived from analog sources, and usually involve the use of special hardware.

Revocation retraction of certification or authorization.

RFC (Request for Comment) an IETF document, either FYI (For Your Information) RFC sub-series that are overviews and introductory or STD RFC sub-series that identify specify Internet standards. Each RFC has an RFC number by which it is indexed and by which it can be retrieved (www.ietf.org).

Rijndael a block cipher designed by Joan Daemen and Vincent Rijmen, chosen as the new Advanced Encryption Standard (AES). It is considered to be both faster and smaller than its competitors. The key size and block size can be 128-bit, 192-bit, or 256-bit in size and either can be increased by increments of 32 bits.

RSA short for RSA Data Security, Inc.; or referring to the principals - Ron Rivest, Adi Shamir, and Len Adleman; or referring to the algorithm they invented. The RSA algorithm is used in public key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.

SA (Security Association) a relationship between two or more entities that describes how the entities will use security services to communicate securely.

secret sharing see Key Splitting.

secure channel a means of conveying information from one entity to another such that an adversary does not have the ability to reorder, delete, insert, or read (SSL, IPSec, whispering in someone’s ear).

self-signed key a public key that has been signed by the corresponding private key for proof of ownership.

session key the secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session.

Setup Keys (IKE) IKE keys responsible for creating your Security Association. Values can be set in time.

sign to apply a signature.

signature a digital code created with a private key. Signatures allow authentication of information by the process of signature verification. When you sign a message or file, the PGP program uses your private key to create a digital code that is unique to both the contents of the message and your private key. Anyone can use your public key to verify your signature.

S/MIME (Secure Multipurpose Mail Extension) a proposed standard developed by Deming software and RSA Data Security for encrypting and/or authenticating MIME data. S/MIME defines a format for the MIME data, the algorithms that must be used for interoperability (RSA, RC2, SHA-1), and the additional operational concerns such as ANSI X.509 certificates and transport over the Internet.

SSL (Secure Socket Layer) developed by Netscape to provide security and privacy over the Internet. Supports server and client authentication and maintains the security and integrity of the transmission channel. Operates at the transport layer and mimics the “sockets library,” allowing it to be application independent. Encrypts the entire communication channel and does not support digital signatures at the message level.

symmetric algorithm a.k.a., conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another. Two sub-categories exist - Block and Stream.

subkey a subkey is a Diffie-Hellman encryption key that is added as a subset to your master key. Once a subkey is created, you can expire or revoke it without affecting your master key or the signatures collected on it.

TCP session hijacking when a hacker takes over a TCP session between two machines. Since most authentication only occurs at the start of a TCP session, this allows the hacker to gain access to a machine.

Text standard, printable, 7-bit ASCII text.

Timestamping recording the time of creation or existence of information.

TLS (Transport Layer Security)

an IETF draft, version 1 is based on the Secure Sockets Layer (SSL) version 3.0 protocol, and provides communications privacy over the Internet.

TLSP (Transport Layer Security Protocol)

ISO 10736, draft international standard.

Triple DES

an encryption configuration in which the DES algorithm is used three times with three different keys.

Trusted

a public key is said to be trusted by you if it has been validated by you or by someone you have designated as an introducer.

Trusted introducer

someone whom you trust to provide you with keys that are valid. When a trusted introducer signs another person’s key, you trust that the person’s key is valid, and you do not need to verify the key before using it.

Twofish

a new 256-bit block cipher, symmetric algorithm created by Bruce Schneier. Twofish is one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) is considering as a replacement for the current Advanced Encryption Standard (AES).

User ID

a text phrase that identifies a key pair. For example, one common format for a user ID is the owner's name and email address. The user ID helps users (both the owner and colleagues) identify the owner of the key pair.

VPN Key Refresh

the Setup Keys (IKE) and Primary Keys (IPsec) are responsible for creating your Security Associations. They are automatically renewed based on the VPN Key Refresh values that appear on the VPN Options panel on Mac.

Validity

indicates the level of confidence that the key actually belongs to the alleged owner.

Verification

the act of comparing a signature created with a private key to its public key. Verification proves that the information was actually sent by the signer, and that the message has not been subsequently altered by anyone else.

Virtual Identity

PGPnet’s Virtual Identity is based on the config-mode draft standard from the IETF IPsec working groups. It is also knows as phase 1.5 and transaction exchange.

This feature can retrieve an IP address and other configuration information for your computer from a secure gateway. Since the gateway gives your machine an address, all of the machines behind that gateway view you as part of their network and will communicate with you freely.

VPN (Virtual Private Network) allows private networks to span from the end-user, across a public network (Internet) directly to the Home Gateway of choice, such as your company’s Intranet.

Web of trust a distributed trust model used by PGP to validate the ownership of a public key where the level of trust is cumulative, based on the individuals’ knowledge of the introducers.

X.509 an ITU-T digital certificate that is an internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer’s name, the user’s identifying information, and the issuer’s digital signature, as well as other possible extensions.

Index