December 2006

PGP® Desktop 9.5 for Mac OS X User's Guide

Rest Secured™

Version Information

PGP Desktop 9.5 for Mac OS X User's Guide. PGP Desktop version 9.5.2. Released December 2006.

Copyright Information

Trademark Information

Licensing and Patent Information

The IDEA cryptographic cipher described in U.S. patent number 5,214,703 is licensed from Ascom Tech AG. The CAST encryption algorithm is licensed from Northern Telecom, Ltd. PGP Corporation has secured a license to the patent rights contained in the patent application Serial Number 10/655,563 by The Regents of the University of California, entitled Block Cipher Mode of Operations for Constructing a Wide-blocksize block Cipher from a Conventional Block Cipher. PGP Corporation may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents.

Acknowledgments

The Zip and ZLib compression code in PGP Desktop was created by Mark Adler and Jean-Loup Gailly; the Zip code is used with permission from the free Info-ZIP implementation. The BZip2 compression code in PGP Desktop was created by Julian Seward.

Export Information

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restricts the export and re-export of certain products and technical data.

Limitations

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement provided with the software. The information in this document is subject to change without notice. PGP Corporation does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by PGP Corporation.

About PGP Corporation

Recognized worldwide as a leader in enterprise encryption technology, PGP Corporation develops, markets, and supports products used by more than 30,000 enterprises, businesses, and governments worldwide, including 90% of the Fortune® 100 and 75% of the Forbes® International 100. PGP products are also used by thousands of individuals and cryptography experts to secure proprietary and confidential information. During the past 15 years, PGP technology has earned a global reputation for standards-based, trusted security products. It is the only commercial security vendor to publish source code for peer review. The unique PGP encryption product suite includes PGP Universal—an automatic, self-managing, network-based solution for enterprises—as well as desktop, mobile, FTP/batch transfer, and SDK solutions. Contact PGP Corporation at www.pgp.com or +1 650 319 9000.

Contents

Introduction

The *PGP Desktop for Mac OS X User's Guide* explains how to use PGP Desktop for Mac OS X, a software product from PGP Corporation that uses encryption to protect data while it is on your system and while it is in transit.

Who Should Read This User's Guide

This Guide is for anyone who is going to be using the PGP Desktop for Mac OS X software to protect their data.

If you are new to cryptography and would like an overview of the terminology and concepts in PGP Desktop, please refer to *An Introduction to Cryptography* (it was installed onto your computer when you installed PGP Desktop).

What's New in This Version of PGP Desktop?

This release of PGP Desktop for Mac OS X introduces the following new features:

PGP Whole Disk Encryption

Changes in this release

PGP Whole Disk Encryption introduces encryption of hard disks for Mac OS X, including multiple-user support and compatibility with PGP Whole Disk Encrypted disks from PGP Desktop for Windows. This feature supports all removable and non-boot fixed disks, and is compatible with HFS+, FAT, and FAT32 filesystems. NTFS is also supported, as read-only.

Benefits

PGP Whole Disk Encryption (WDE) locks down the entire contents of removable and non-boot fixed disks, external drives, and USB flash drives. Encryption runs as a background process that is transparent to you, automatically protecting valuable data without requiring you to take additional steps.

Where to find

Open PGP Desktop and click the PGP Disk item.

For more information

See "Using PGP Whole Disk Encryption" on page 51.

Intel Mac Support

Changes in this release

PGP Desktop 9.5 is a Universal application that runs on both Intel- and PowerPC-based Macintosh computers.

Benefits

Unified Window Interface adoption of Apple's new Unified interface provides a cleaner, more integrated look under Tiger.

PGP Virtual Disk—Resizable Virtual Disks

Changes in this release

Resizable PGP Virtual Disks now automatically expand to fit their contents. A PGP Virtual Disk can automatically expand as files are copied to it to the maximum size of the physical media on which the disk file resides. A PGP Virtual Disk can also be compacted down to the minimum size of the enclosed files.

Benefits

You can now use PGP Virtual Disk without worrying about running out of space on the Virtual Disk.

Where to find

Open PGP Desktop and click the PGP Disk item.

For more information

See "Using PGP Virtual Disks" on page 67.

PGP Zip Editing

Changes in this release

PGP Zip Editing allows PGP Zip files to be opened after creation for editing. File contents and encryption recipients can be changed at any time.

Benefits

You can now easily manage the contents of your PGP Zip files.

Where to find

Open PGP Desktop and click the PGP Zip item.

For more information

See "PGP Zip" on page 89.

Directory Authentication Enrollment

Changes in this release

Directory Authentication Enrollment with PGP Universal is now supported in addition to the previous email enrollment process.

Benefits

You now have another way to participate in a PGP Universal-managed environment.

PGP Messaging Policy Enhancements

Changes in this release

This release provides the following new policies in the Messaging Policy Editor:

- **Send Signed policy** action has been added to support signing messages without encryption, even when a key is found.
- **Message Size** policies are now available to execute actions based on whether a message is greater than or less than specific sizes.
- **Search keys.domain and** policy has been added to allow implicit keys.domain lookup prior to searching any of the configured keyservers. This is now configured in all default policies.

For PGP Universal-managed environments, this release now allows the local keyring to be used for key lookups. The local keyring is queried when this option is on before all other key sources.

Benefits

Unmanaged users continue to have full control over their messaging policy, with additional granular control over how and when to apply encryption policy. In managed environments, messaging policies can be centrally configured and distributed across an organization.

Where to find

To access PGP Messaging, click the PGP Messaging item.

Click a policy to view its settings.

For more information

See "Services and Policies" on page 25.

PGP Universal Server HTTPS Proxy Support

Changes in this release

This feature enables policy connections from PGP Desktop to a PGP Universal server via HTTPS proxies.

Benefits

In a PGP Universal-managed environment, this feature allows the PGP administrator to configure the proxy settings used by PGP Desktop for connecting to the PGP Universal server.

Notifiers

Changes in this release

The PGP Notifier feature displays information about what PGP Desktop is doing to protect your data, fading into view in a selectable corner of your screen. For outgoing messages, it shows how the message will be sent to each recipient, enabling you to decide whether or not to send the message. Inbound messages also show notifications, including details about the signature on the message. A Notifier also displays the results of automated key lookups.

Other functions such as PGP Whole Disk Encryption are also fully integrated with the Notifier to provide a view into the actions taken by PGP Desktop.

Benefits

Notifiers for PGP Messaging describe exactly how a message is being processed: which messages are encrypted, which go out in the clear, and so on, according to the defined mail policy. In environments where mail policy allows messages to be sent in the clear, this feature also provides the option to prevent a message from being sent unencrypted if a recipient's key is not found.

Where to find

1 Open PGP Desktop, and then from the **PGP** menu, select **Preferences**.

2 Click the **Notifications** tab.

For more information

See "Notifications Preferences" on page 161.

Network Key and Group Selection

Changes in this release

The Network Key and Group Selection screen for PGP Zip, PGP Whole Disk, PGP Virtual Disk has been completely redesigned to support selection of keys from all local keyrings, smart keyrings, and keyservers. Additionally, this new interface fully integrates with LDAP directories on both Windows and Mac OS X to select groups or mailing lists—when configured for policy synchronization with PGP Universal 2.5—allowing easy encryption of files, messages, and disks to defined groups in your enterprise directory.

Benefits

This provides easy encryption of files, messages, and disks to defined groups in your enterprise directory.

Where to find Begin the process of creating, for example, a new PGP Zip archive. On the **Security** tab, click the plus-sign icon. The new **Network Key and Group Selection** screen appears.

Mailing List Expansion

Changes in this release In Active Directory environments, PGP Desktop automatically expands each mailing list to list all individual recipients for encryption, enabling creation of secured mailing lists when PGP Desktop is configured for policy synchronization with both PGP Universal Server 2.5 and a configured directory server.

Benefits Allows end-to-end encryption of content to individual recipients who are part of a distribution list.

PGP Universal Migration

Changes in this release PGP Universal migration allows PGP Desktop software stamped from PGP Universal Server to be installed on top of an unstamped installation of PGP Desktop; this stamped version of PGP Desktop will reset the policies and bind the existing installation to the policies set on the server.

Benefits This enables easy migration from a standalone deployment of PGP Desktop to a managed deployment of PGP Desktop.

PGP Universal Server Messaging Policy

Changes in this release PGP Universal Server Messaging Policy extends PGP Desktop messaging policy to support the new PGP Universal 2.5 content filtering system.

Benefits In PGP Universal-managed environments, a PGP administrator can control when and how email encryption is applied by PGP Desktop, enabling centralized control and enforcement of your organization's security policy.

International Character Support Enhancements

Changes in this release International character support in messages has been enhanced significantly in this release.

Benefits Ensures interoperability with international message encoding standards and international character sets.

Signing Subkeys

Changes in this release

Signing Subkeys treats your master key as a subkey authorizer, to authorize sets of signing and encryption subkeys over time.

Benefits

This mode helps to ensure compliance with local laws and corporate policies in some areas requiring that signing keys must not leave the control of the end user while ensuring that encryption keys can be escrowed.

Where to find

1. Open PGP Desktop, then click the **Keys** item.
2. Double click a private key to open its **Key Info** screen.
3. Click the **Subkeys** heading near the bottom of the screen (if the subkeys section is not already open). The subkeys on the selected key appear.

For more information

See "Viewing Subkeys" on page 136.

Bundle Keys

Changes in this release

Bundle Keys allows you to import multiple X.509 certificates, including those on smartcards, as subkeys onto a new PGP key so as to retain the integrated identity inherent in such certificate collections. Additionally, X.509 certificates can be imported from PKCS 12 or PFX files as subkeys of existing PGP keys. Export as certificates is also supported.

Benefits

This feature provides greater support for X.509 certificates with PGP Desktop.

Preferred Encoding

Changes in this release

Preferred encoding is a new key property that can be configured on your private keys. Preferred encoding states whether you can receive PGP/MIME, PGP Partitioned, or both encoding formats. All components of the PGP Desktop 9.5/PGP Universal 2.5 product suite observe this property.

Benefits

Lets you specify what encodings should be used if the preferred method is not clear.

FIPS 140-2 Integrity Checking

Changes in this release

FIPS 140-2 integrity checking provides a comprehensive test suite used to verify the PGP SDK for NIST FIPS validation that can now be executed whenever PGP Desktop starts up.

Benefits This test suite verifies PGP Corporation's signatures on each PGP SDK binary and verifies the algorithmic integrity of each FIPS-validated cipher and public key algorithm. This activates the FIPS power-up and operational self-tests to ensure the integrity of cryptographic operations in accordance with FIPS standards.

Where to find From the **Tools** menu, select **PGP Options**, and then click **Advanced**.

For more information See "Advanced Preferences" on page 163.

FIPS 186-3 (Read Only)

Changes in this release This feature provides support for verification of signatures from the newly defined DSA key sizes of 2048 and 3072.

Benefits This feature provides support for emerging standards.

Using this Guide

This Guide provides information on configuring and using the components within PGP Desktop. Each chapter of the guide is devoted to one of the components of PGP Desktop.

"Managed" versus "Unmanaged" Users

A PGP Universal Server can be used to control the policies and settings used by components of PGP Desktop. This is often the case in enterprises using PGP software. PGP Desktop users in this configuration are known as *managed* users, because the settings and policies available in their PGP Desktop software are pre-configured by a PGP administrator and managed using a PGP Universal Server. If you are part of a managed environment, your company may have specific usage requirements. For example, managed users may or may not be allowed to send plaintext email, or may be required to encrypt their disk with PGP Whole Disk Encryption.

Users not under the control of a PGP Universal Server are called *unmanaged* or *standalone* users.

This Guide describe how PGP Desktop works in both situations; however, managed users may discover while working with the product that some of the settings described in this document are not available in their environments. See "Appendix C, PGP Desktop and PGP Universal" for more information.

Symbols Used in This Guide

Notes, Cautions, and Warnings are used in the following ways.

Notes are extra, but important, information. A Note calls your attention to important aspects of the product. You will be able to use the product better if you read the Notes.

Cautions indicate the possibility of loss of data or a minor security breach. A Caution tells you about a situation where problems could occur unless precautions are taken. Pay attention to Cautions.

Warnings indicate the possibility of significant data loss or a major security breach. A Warning means serious problems are going to happen unless you take the appropriate action. Please take Warnings very seriously.

About PGP Desktop Licensing

A *license* is used within the PGP software to enable the functionality you purchased, and sets the expiration of the software. Depending on the license you have, some or all of the PGP Desktop family of applications will be active. Once you have entered the license, you must then authorize the software with PGP Corporation, either manually or online.

To license PGP Desktop:

Do one of the following:

- If you are a managed user, you are most likely already using a licensed copy of PGP Desktop. Check your license details as described in "Checking License Details" on page xiv. If you have questions, please contact your PGP administrator.
- If you are an unmanaged user, or a PGP administrator, check your license details as described in "Checking License Details". If you need to authorize your copy of PGP Desktop, do so as described in "Authorizing PGP Desktop for Mac OS X".

Checking License Details

To see the details of your PGP Desktop license:

1 Open PGP Desktop.

2 From the **PGP** menu, select **License**.

The **License Information** window appears, showing the following information:

Item	Description
Name	The name your license is registered to.
Organization	The organization your license is registered to.

Item	Description
Email	The email address associated with your license.
Type	The type of license you have, Enterprise or Home.

3 Click **Details**.

The details of your license appear:

Item	Description
Expiration Date	The date your license expires.
Number of Seats	The number of seats available for this license.
Enabled Features	Which components are active in your license.
Disabled Features	Those components that are **not** active in your license.

If you do not authorize your copy of PGP Desktop, only limited features will be available to you (PGP Zip and Keys).

Authorizing PGP Desktop for Mac OS X

If you need to change to a new license number, or if you skipped the license authorization process during configuration, follow these instructions to authorize your software.

Make sure your Internet connection is active before proceeding. If you have no Internet connection, you must submit a request for a manual authorization.

Before you begin:

If you purchased PGP Desktop, you received an email order confirmation with an attached PDF file.

1 Make a note of the name, organization, and license number you received in the email order confirmation. These are shown in the section titled **Important Note** in the PDF. You will need these details during the licensing process.

During configuration of your PGP Desktop software, you must type the name, organization, email address, and license number to authorize your copy of PGP Desktop with PGP Corporation's authorization server.

Your license number also appears on the download page of your PGP product.

2 Open PGP Desktop.

3 From the **PGP** menu, select **License**.

4 Click **Change License**.

5 Type the **Name** and **Organization** exactly as specified in your PGP email order confirmation PDF. These will be shown in the section titled **Important Note** in the .PDF. If the **Important Note** section does not exist in your PDF, your first authorization attempt will set the name and organization permanently.

6 Type the **Email** address you wish to assign to the licensing of the product.

If you have previously authorized the same license number, you must enter the same Name, Organization, and Email Address as you did the previous time. If you enter different information, authorization will fail.

7 Do one of the following:

– Type your 28-character license number in the **License Number** fields (for example, DEMO1-DEMO2-DEMO3-DEMO4-DEMO5-ABC).

To avoid typing errors and make the authorization easier, copy the entire license number, put the cursor in the first "License Number" field, and paste. Your license number will be correctly entered into all six "License Number" fields.

– To request a one-time, 30-day evaluation of PGP Desktop, select **Try for 30 Days**. When you purchase a license, you can enter it any time before the end of the 30-day evaluation period. If you don't enter a valid license, PGP Desktop will revert to unlicensed functionality when the 30-day evaluation period is over.

– To purchase a PGP Desktop license, select **Purchase Now.** A Web browser will open and take you to the online PGP Store.

8 Click **Authorize**.

9 When your license is authorized, click **OK** to complete the process.

Resolving License Authorization Errors

If you receive any error messages while authorizing your software, the ways to resolve this issue vary based on the error message. See the **HOWTO: License PGP Desktop 9.x** section in the PGP Support Portal at https://pgp.custhelp.com for suggestions.

Resources

Refer to these sections for additional resources about PGP Desktop.

Getting product information

Unless otherwise noted, the product documentation is provided as Adobe Acrobat PDF files that are installed with PGP Desktop. Release notes are also available, which may have last-minute information not found in the product documentation.

Once PGP Desktop is released, additional information regarding the product is entered into the online Knowledge Base available on PGP Corporation's Support Portal.

Contact information

- To learn about PGP support options and how to contact PGP Technical Support, please visit http://www.pgp.com/support.
- To access the PGP Support forums, please visit http://forums.pgpsupport.com.
- To access the PGP Support Knowledge Base or request PGP Technical Support, please visit http://support.pgp.com.

  You must have a valid support agreement to request Technical Support.
- For any other contacts at PGP, please go to the Contact Us page on the PGP website at http://www.pgp.com/company/contact.
- For general information about PGP Corporation, please visit the PGP website at http://www.pgp.com.

1 PGP Desktop Basics

Getting started with PGP Desktop

PGP Desktop is a security tool that uses cryptography to protect your data against unauthorized access.

It protects your data being sent by email or by instant messaging (IM). It lets you encrypt entire external drives (or external drive partitions) so everything is protected all the time. You can also protect portions of any drive, creating a secure virtual disk on which you can store your sensitive data. PGP Desktop lets you put any combination of files and folders into an encrypted, compressed package for easy distribution or backup. And, you can use PGP Desktop to shred (secure delete) sensitive files, so that no one can retrieve them.

PGP Desktop lets you create PGP keypairs and manage both your personal keypairs and the public keys of others. It is available for both the Mac OS X and Windows platforms.

Some high-level conceptual information is presented in these topics:

- "PGP Desktop Terminology" on page 1
- "Using PGP Desktop for the First Time" on page 4

PGP Desktop Terminology

To make the most of PGP Desktop, you should be familiar with the following terms:

PGP Product Component Terms

- **PGP Desktop:** A software tool that uses cryptography to protect your data against unauthorized access. PGP Desktop is available for Mac OS X and Windows.
- **PGP Global Directory:** A free, public keyserver hosted by PGP Corporation. The PGP Global Directory provides quick and easy access to the universe of PGP keys. It uses next-generation keyserver technology that verifies the email address on a key (so that the keyserver doesn't get clogged with unused keys) and lets users manage their own keys. Using the PGP Global Directory significantly enhances your chances of finding a valid public key of someone to whom you want to send secured messages. PGP Desktop is designed to work closely with the PGP Global Directory.
- **PGP Keys:** A feature of PGP Desktop that gives you complete control over both your own PGP keys, and the keys of those persons with whom you are securely exchanging email messages.
- **PGP Messaging:** A feature of PGP Desktop that automatically and transparently supports all of your email clients through policies you control. PGP Desktop accomplishes this using a new proxy technology; the older plugin technology is also available. PGP Messaging also protects many IM clients, such as AIM and iChat (both users must have PGP Messaging enabled).

- **PGP Shred:** A feature of PGP Desktop that lets you securely delete data from your system. PGP Shred overwrites files so that even file recovery software cannot recover them.
- **PGP Universal:** A tool for enterprises to automatically and transparently secure email messaging for their employees. If you are using PGP Desktop in a PGP Universal-protected environment, your messaging policies and other settings may be controlled by your organization's PGP administrator.
- **PGP Virtual Disk volumes:** PGP Virtual Disk volumes are a feature of PGP Desktop that let you use part of your hard drive space as an encrypted virtual disk. You can protect a PGP Virtual Disk volume with a key or a passphrase. You can even create additional users for a volume, so that people you authorize can also access the volume. The PGP Virtual Disk feature is especially useful on portables, such as PowerBooks, MacBooks, and iBooks, because if your computer is lost or stolen, the sensitive data stored on the PGP Virtual Disk is protected against unauthorized access.
- **PGP Whole Disk Encryption:** Whole Disk Encryption is a feature of PGP Desktop that on Mac OS X encrypts an entire external drive or drives, or external drive partitions, to protect your files when you aren't using them. Volumes that are encrypted using the PGP Whole Disk Encryption and PGP Virtual Disk features can be used on the same drive. You can use a passphrase, or keypair on a USB token, for added security when protecting drives with the PGP Whole Disk Encryption feature.
- **PGP Zip:** A feature of PGP Desktop that lets you put any combination of files and folders into a single encrypted, compressed package for convenient transport or backup. You can encrypt a PGP Zip archive to a PGP key or to a passphrase, allowing you to send the archive to someone who doesn't even have PGP Desktop on their system.
- **Separate Signing Subkey:** A PGP keypair consists of a master key for signing, and a subkey for encryption. You can also generate a separate subkey for signing. Among other uses, this feature is needed in regions where separate subkeys for signing are required for legally-binding digital signatures.

PGP Product Concepts

- **Conventional cryptography:** Uses the same passphrase to encrypt and decrypt data. Conventional cryptography is great for data that isn't going anywhere (because it encrypts and decrypts quickly). However, conventional cryptography is not as well suited for situations where you need to send encrypted data to someone else, especially if you want to send encrypted data to someone you have never met.
- **Decrypting:** The process of taking encrypted (scrambled) data and making it meaningful again. When you receive data that has been encrypted by someone using your public key, you use your private key to decrypt the data.
- **Encrypting:** The process of scrambling data so that if an unauthorized person gets access to it, they cannot do anything with it. The data is so scrambled, it's meaningless.

- **Public-key cryptography:** Public-key cryptography uses two keys (called a keypair) for encrypting and decrypting. One of these two keys is your private key; and, like the name suggests, you need to keep it private. Very, very private. The other key is your public key, and, like its name suggests, you can share it with the general public. In fact, you're supposed to share.

  So how does public-key cryptography work? Let's say you and your cousin in another state want to exchange private messages. Both of you have PGP Desktop. First, you both need to create your keypair: one private key and one public key. Your private key you keep secret, your public key you send to a public keyserver like the PGP Global Directory (keyserver.pgp.com), which is a public facility for distributing public keys. (Some companies have their own private keyservers.)

  Once the public keys are on the PGP Global Directory, you can go back to the PGP Global Directory and get your cousin's public key, and she can go to the keyserver and get yours (there are other ways to exchange public keys; refer to Chapter 10, PGP Keys for more information). This is important because to send an encrypted email message that only your cousin can decrypt, **you encrypt it using your cousin's public key.** What makes this work is that only your cousin's private key can decrypt a message that was encrypted using her public key. Even you, who have her public key, cannot decrypt the message once it has been encrypted using her public key. **Only the private key can decrypt data that was encrypted with the corresponding public key.**

- **Signing:** The process of applying a digital signature to data using your private key. Because data signed by your private key can be verified only by your public key, the ability to verify signed data with your public key proves that your private key signed the data and thus proves the data is from you.

- **Verifying:** The process of proving that the private key was used to digitally sign data by using that person's public key. Because data signed by a private key can only be verified by the corresponding public key, the fact that a particular public key can verify signed data proves the signer was the holder of the private key.

PGP Product Terms

- **Keypair:** A private key/public key combination. When you create a PGP "key", you are actually creating a keypair. As your keypair includes your name and your email address, in addition to your private and public keys, it might be more helpful to think of your keypair as your digital ID—it identifies you in the digital world as your driver's license or passport identifies you in the physical world.

- **Keyserver:** A repository for keys. Some companies host keyservers for the public keys of their employees, so other employees can find their public keys and send them protected messages. The PGP Global Directory (https://keyserver.pgp.com/) is a free, public keyserver hosted by PGP Corporation.

- **Private key:** The key you keep very, very private. Only your private key can decrypt data that was encrypted using your public key. Also, only your private key can create a digital signature that your public key can verify.

Do not give your private key, or its passphrase, to anyone!

- **Public key:** The key you distribute to others so that they can send protected messages to you (messages that can only be decrypted by your private key) and so they can verify your digital signature. Public keys are meant to be widely distributed.

  Your public and private keys are mathematically related, but there's no way to figure out your private key if someone has your public key.

For more terms, see the Glossary on page 171.

Using PGP Desktop for the First Time

PGP Corporation recommends the following procedure for getting started with PGP Desktop:

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

If you are a corporate user, your PGP administrator may have specific installation instructions for you to follow or may have configured your PGP installer with certain settings. Either way, this is the first step.

2 **Run the Setup Assistant**.

The Setup Assistant will get you up and running by helping you to create a keypair (if you don't have one) and publish your public key to the PGP Global Directory.

3 **Exchange public keys with others**.

After you have created a keypair, you can begin sending and receiving secure messages with other PGP Desktop users (once you have exchanged public keys with them). You can also use the PGP Desktop disk-protection features.

Exchanging public keys with others is an important first step. To send them secure messages, you need a copy of their public key, and to reply with a secure message, they need a copy of your public key. If you did not upload your public key to the PGP Global Directory using the Setup Assistant, do so now. If you do not have the public key for someone to whom you want to send messages, the PGP Global Directory is the first place to look. PGP Desktop does this for you—when you send email, it finds and verifies the keys of other PGP Desktop users automatically. It then encrypts your message to the recipient public key, and sends the message.

4 **Validate the public keys you get**.

When you get a public key from an untrusted keyserver, try to make sure that it has not been tampered with, and that the key really belongs to the person it names. To do this, use PGP Desktop to look at the Key Info of the key you received, and compare the key's unique fingerprint with the fingerprint of that person's keypair (a good way to do that is by telephoning the key's owner and having them read you the fingerprint information so that you can compare it). Keys from trusted keyservers like the PGP Global Directory have already been verified.

5 **Start securing your email, files, and instant messaging**.

After you generate your keypair and exchange public keys, you can begin encrypting, signing, decrypting, and verifying your email messages and files. The secure IM chat session feature generates its own keys automatically, so you can use this feature even before you generate your keypair. The only requirement is that you must be chatting with another PGP Desktop user for the chat session to be secured.

6 **Watch for information boxes from the PGP Desktop Notifier feature to appear**.

As you send or receive messages, or perform other PGP Desktop functions, the PGP Desktop Notifier feature displays information boxes that appear in whichever corner of the screen you wish. These PGP Notifier boxes tell you the action that PGP Desktop took, or will take. After you grow familiar with the process of sending and receiving messages, you can change options for the PGP Notifier feature—or turn it off.

7 **After you have sent or received some messages, check the messaging logs to make sure everything is working correctly**.

If you want more information than the Notifier feature displays, the Messaging Log provides detailed information about all messaging operations.

8 **Modify your messaging policies, if necessary**.

Email messages are sent and received—automatically and seamlessly—if PGP Desktop messaging policies are configured correctly. If your message recipient has a key on the PGP Global Directory, the default PGP Desktop policies provide *opportunistic* encryption. Opportunistic encryption means that, if PGP Desktop has what it needs (such as the **verified** recipient public key) to encrypt the message automatically, then it does so. Otherwise, it sends the message in *clear text* (unencrypted). The default PGP Desktop policies also provide optional *forced* encryption. This means that, if you include the text "[PGP]" in the Subject line of a message, then the message **must** be sent securely. If verified keys cannot be found, then the message is not sent, and (if set to do so in PGP Options) a PGP Desktop Notifier box alerts you.

9 **Start using PGP Desktop's other features**.

Along with its messaging features, you can also use PGP Desktop to secure the disks that you work with:

- Use the **PGP Whole Disk Encryption** feature to encrypt an external disk or disk partition. All files on the external disk or partition are secured, and are encrypted and decrypted on the fly as you use them. The process is completely transparent to you.
- Use the **PGP Virtual Disk** feature to create a secure "virtual hard disk." You can use this virtual disk like a bank vault for your files. Use PGP Desktop or the Mac OS X Finder to unmount (and therefore lock) the virtual disk, and your files are secure—even if your computer is currently being used.
- Use the **PGP Zip** feature to create compressed and encrypted PGP Zip archives. These archives offer an efficient way to transport or store files securely.
- Use the **PGP Shredder** feature to delete sensitive files that you no longer need. PGP Shredder removes them completely, eliminating any possibility of recovery.

2 The PGP Desktop User Interface

Accessing PGP Desktop features

This section describes the PGP Desktop user interface. It contains the following topics:

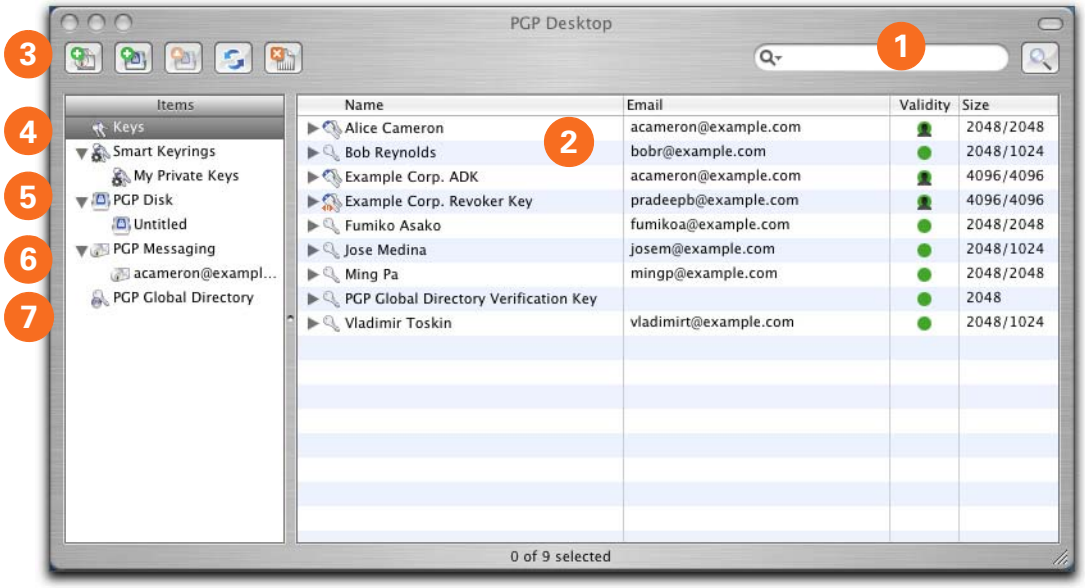
Accessing PGP Desktop Features

There are four primary ways to access PGP Desktop features:

- Launch the PGP Desktop application from the Mac OS X Finder or Dock, then work directly from PGP Desktop.
- Use the PGP Desktop menu in the Mac OS X Menu Bar in the upper-right corner of the screen.
- From the Desktop or a Finder window, Ctrl-click a file or folder (or right-click it if you have two-button mouse) then select **PGP** from the context menu that appears.
- Use the PGP Desktop icon in the Mac OS X Dock in any of these ways, then select from the menu that appears:
  - Click the PGP Desktop Dock icon and hold the mouse button down.
  - Ctrl-click the Dock icon.
  - Right-click the Dock icon, if you are using a two-button mouse.

PGP Desktop Main Screen

PGP Desktop's main screen is your main interface to the product.



	Interface Element
1	Search field
2	Work area: The Keys work area is currently visible.
3	Toolbar
4	Keys
5	PGP Disk
6	PGP Messaging
7	Keyservers

The PGP Desktop main screen includes:

- **The search field**. Lets you search for keys on the local keyring. Simply enter characters and the names and email addresses on the local keyring that include those characters will display. Click the **Advanced Search** button for more search criteria.
- **The PGP Desktop Work area**. Displays information about and actions you can take for the selected item.
- **The Toolbar**. Provides access to frequently used features.

  You can:

  – Create a new PGP Zip archive.

  – Create a new PGP Virtual Disk.

  - Mount an existing PGP Virtual Disk.
  - Synchronize keys.
  - Shred files.

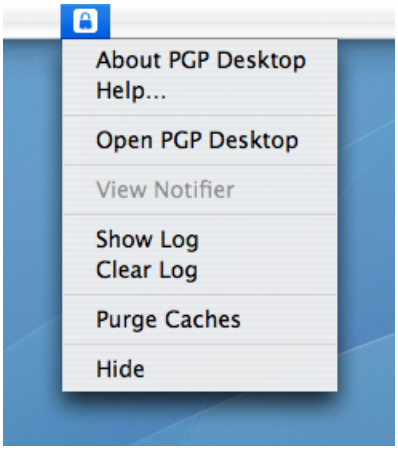
- **The Keys item**. Gives you control over the PGP keys that PGP Desktop is managing for you.
- **The PGP Zip item.** Use this item to view and manage PGP Zip archives.
- **The PGP Disk item**. Use this item to view and manage PGP Virtual Disk volumes. Also, you can use this item to create new PGP Virtual Disk volumes, as well as encrypting an entire non-boot disk using the PGP Whole Disk Encryption feature.
- **The PGP Messaging item**. Use this item to manage PGP Messaging services. You can also use this item to create new services and policies, and manage existing services and policies.
- **The Keyservers item**. Use this item to view and manage keyservers.

The PGP Desktop Icon in the Menu Bar

One way to access many PGP Desktop features is from the PGP Desktop icon in the Menu Bar.

The PGP Desktop icon in the Menu bar

When you click the PGP Desktop icon in the Menu Bar, you can access these things:



- **About PGP Desktop**. Displays a window with information about the version of PGP Desktop you are using, licensing information, and a list of the people who helped create PGP Desktop. This window also has a button that you can use to uninstall PGP Desktop.
- **Help**. Opens the PGP Desktop integrated online help.
- **Open PGP Desktop.** Opens the PGP Desktop main screen.
- **View Notifier.** Displays the PGP Desktop Notifier box, so you can review the Notifier messages that have appeared.
- **Show Log.** Displays the PGP Desktop Messaging Log.
- **Clear Log.** Clears the PGP DesktopMessaging Log.
- **Purge Caches.** Purges the PGP Desktop internal IMAP and POP message caches, the key cache, and the passphrase cache.
- **Hide.** Removes the PGP icon from the Menu Bar, but leaves the background parts of the application running.

  The **Hide** command becomes the **Quit** command if you hold down the **Option** key before clicking the PGP Desktop icon. This removes the PGP Desktop icon from the Menu Bar **and causes the background parts of PGP Desktop to quit.** Context-menu functionality continues to work.

If you use the Option key and the PGP Menu Bar icon to **quit** the background parts of PGP Desktop, email messages are no longer encrypted, decrypted, signed, or verified. You may also not be able to decrypt messages received while the background parts of PGP Desktop were not running, even after they are started again. Finally, no key management is done while the background parts of the software is not running. For these reasons, it is recommended that you keep the PGP Desktop background processes running at all times.

To restart the background processes of PGP Desktop if the application is not running:

1 Locate the PGP Desktop application on your system.

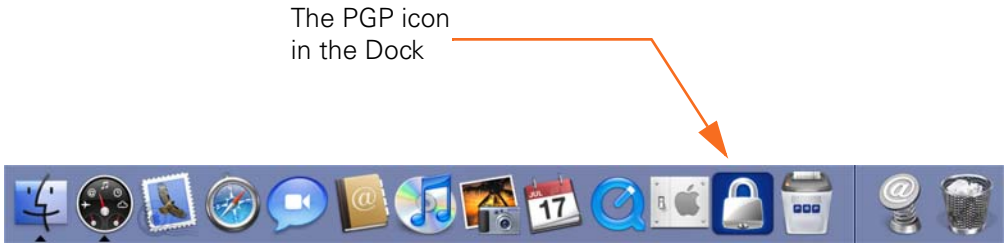
  The default location is in the Applications folder.

2 Double-click the PGP Desktop application icon.

  PGP Desktop starts and its icon appears in the Menu Bar.

The PGP Dock Icon

One way to access many PGP features is from the PGP Dock icon.



The PGP Desktop icon appears in the Dock when the application is open, or when you have put the PGP Desktop icon into the Dock manually.

When you click and hold the PGP Desktop icon in the Dock when the application is already open (or Ctrl-click it, or use the right mouse button if you are using a two-button mouse), a menu appears giving you access to the following commands:

- **Any currently-open PGP Desktop windows:** If PGP Desktop is currently running, any of its windows that you have open appear at the top of this menu.
- **About PGP Desktop**: Displays the PGP Desktop **About** box. The **About** box shows the PGP Desktop credits, what version you are currently using, and has a button that you can use to uninstall the PGP Desktop software.
- **Preferences**: Opens the PGP Desktop Preferences.
- **Clipboard**: Lets you Encrypt, Sign, Encrypt & Sign, or Decrypt/Verify the contents of the Clipboard.
- **Check For Updates**: Checks for newer versions of PGP Desktop. If a newer version is found, you have the option of downloading it.
- **Purge Caches:** Clears the portion of memory that the PGP Desktop software uses to store passphrases, stored keys, and other data.

The remaining menu items, in the lowest section of the menu, are standard Mac OS X Dock items:

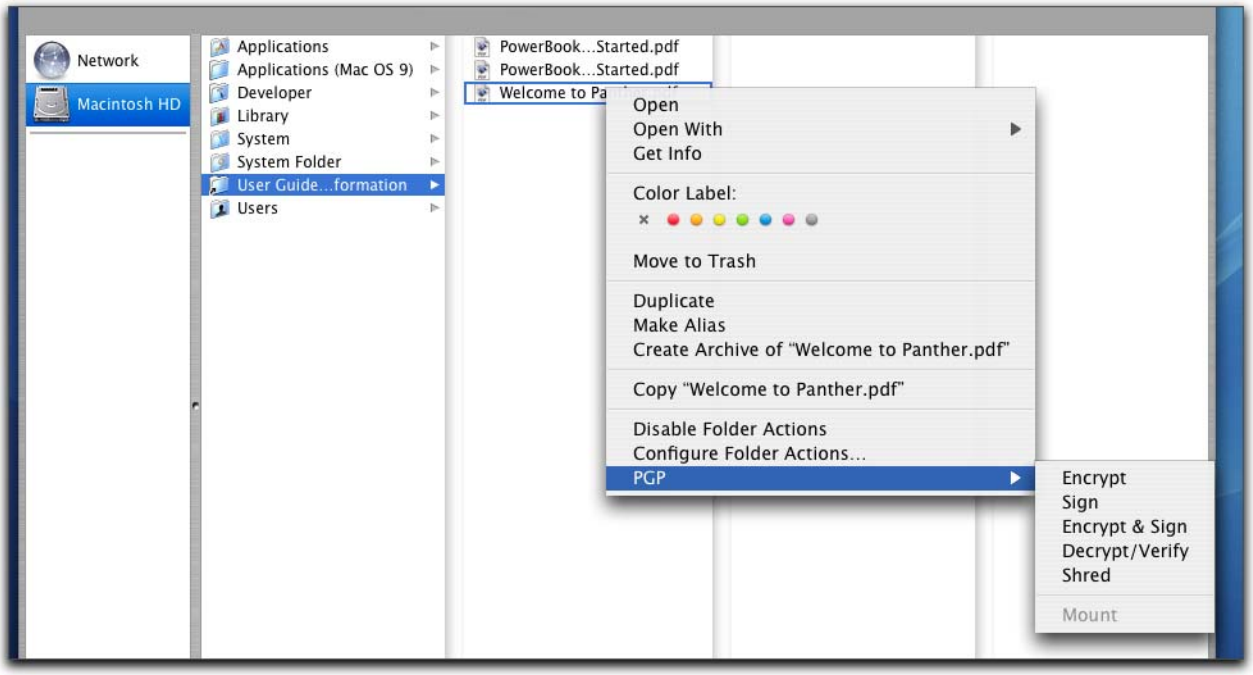
- **Remove from Dock**: Removes the PGP Desktop icon in the Dock.
- **Open at Login:** Sets your Mac OS X Account System Preference so that PGP Desktop launches when you log on to your computer.
- **Show In Finder**: Shows the location of the PGP Desktop application in a Finder window.
- **Hide**: Hides any PGP Desktop application screens.
- **Quit**: Quits the PGP Desktop application.

If you click and hold the PGP Desktop icon in the Dock when the application is not open, you only see the standard Mac OS X Dock items.

Mac OS X Finder

You can also access PGP Desktop functions from the Mac OS X Finder:

1. Open a Finder window
2. Ctrl-click (or right-click, if you are using a two-button mouse) the desired file or folder
3. Select the appropriate action from the context menu that appears.



PGP Desktop Notifier alerts

The PGP Desktop Notifier feature displays a small information box that tells you the status of incoming and outgoing email messages, as well as instant messaging sessions.

PGP Desktop Notifier Features for Messaging

The PGP Desktop Notifier feature informs and assists you as you use email and instant message chats with PGP Desktop:

- It displays information about incoming email, such as decryption and signature status, as well as sender, subject, and encryption key.
- For outgoing email, it displays encryption and signature status. It also offers a way that you can stop an email message from being sent if the encryption options are not what you want.
- It provides a way that you can review (at any time) the statuses of previous incoming or outgoing messages for that Mac OS X session.
- At the start of a chat session with another PGP Desktop user who has the PGP Desktop Notifiers feature enabled, it informs you that the chat session is secured.

You can use the PGP Desktop Notifier feature to monitor all of your incoming email, or some of it. You can also maintain precise control over every outgoing message, or only some of them. You can set various Notifier options, or turn the PGP Desktop Notifier feature off if you prefer.

You can delay a message from being sent by moving your cursor over the Notifier box. If you do not do this within 4 seconds (you can set this interval in preferences for the Notifier feature) the message is sent unencrypted, and the Status field reflects that.

If you do move your cursor over the message, **Block** and **Send** buttons appear in the Notifier box. You can click **Block** to stop the message from being transmitted, or **Send** to send the message.

If you send an email to more than one recipient, and PGP Desktop is able to find keys for some recipients but not others, the Notifier informs you of the status, and gives you two options:

- Send the email encrypted to those with keys, and unencrypted to those without them.
- Block the message so it is sent to no one.

The PGP Desktop Notifier feature then informs you of the resulting status. You can click **More** to see more details.

Some additional points about the PGP Desktop Notifier feature:

- For message notifications, you can use left and right arrow buttons in the upper-right corner of the Notifier box to scroll Notifier messages forward or backward. This way, you can review messages that came before or after the message you are viewing currently.

- When they first display, Notifier message boxes have a partially transparent appearance to prevent obscuring anything on your screen. Notifier message boxes become opaque if you move your cursor over them, and become translucent again when you move your mouse away from them.
- Unless the pointer is over them, Notifier messages display for approximately seven seconds. If you need more time to read a Notifier, move your pointer over the Notifier and it remains on your display.
- If you completely miss reading a Notifier, or you would like to review previous ones, choose **View Notifier** from the PGP Desktop icon in the Mac OS X Menu Bar. This restores the PGP Desktop Notifier box.

You can close a Notifier box by clicking the **x** in the upper left corner.

For information about setting PGP Desktop Notifier preferences, see "Notifications Preferences" on page 161.

Incoming PGP Desktop Notifier messages

PGP Desktop Notifier messages for incoming emails help you determine whether:

- Messages you are receiving were encrypted to a public key for which you have the corresponding private key.
- The Signature(s) within an email you are receiving can be verified.
- Information about who sent the email to you.

Outgoing PGP Desktop Notifier messages

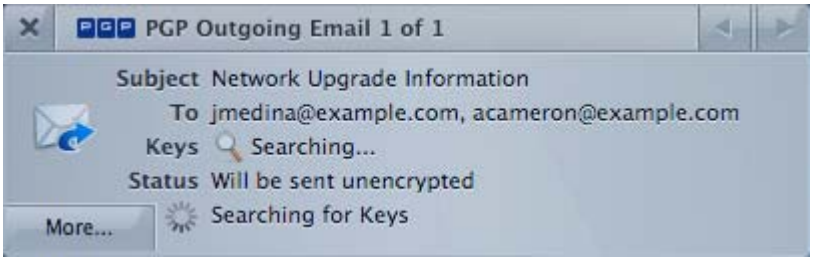
The PGP Desktop Notifier feature displays messages to help you monitor—before they are sent—whether your emails are going to be sent encrypted or unencrypted.

Following are some example Notifier messages.

Incoming Email

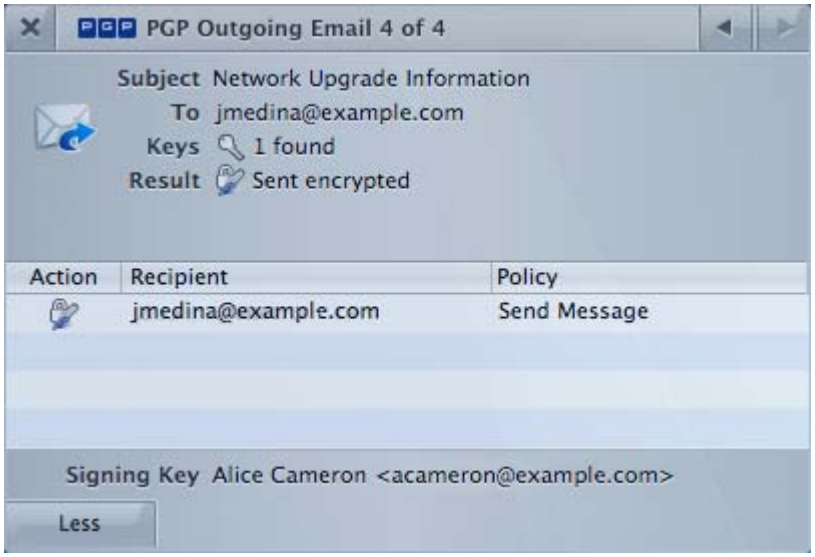
This Notifier message appears after PGP Desktop has decrypted an email successfully and verified that it came from the recipient.

Outgoing Email



This Notifier message appears as PGP Desktop is searching for the public keys of the persons in the To line. When the appropriate keys are found, the Status line will change to say that the message will be sent encrypted. If the appropriate keys cannot be found, PGP Desktop will follow policy and, in this case, send the message unencrypted.

Outgoing Email with All Information Visible



This Notifier message appears after a message has been sent encrypted and you click on More to see the details of how PGP Desktop handled the message.

It is not necessary for you to view this additional information unless you want to see it. To hide the additional information again, click **Less**.

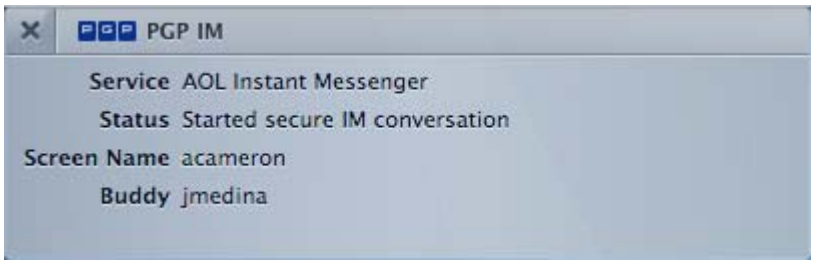
PGP Notifier for Instant Messaging

If you have PGP Desktop installed on your computer, and if you have opted for Notifiers for Instant Messaging to appear (under the **Notifications** tab in PGP Desktop Preferences), then PGP Desktop Notifiers alert you when the AOL Instant Messenger (AIM) sessions that you have with other PGP Desktop users are protected.

For more information on proper configuration, as well as the use of the secure instant message chat feature, see Chapter 5, Securing Instant Messaging.

When you use the secure instant messaging feature, a Notifier displays at the beginning of the chat session to inform you that your chat is secure, and a padlock icon displays next to your "buddy name" with most AIM-compliant instant messaging clients.

Instant Messaging Notifier



Once you have finished your chat session with another PGP Desktop user, and you close the chat window, a final Notifier message informs you that the secure session has ended.

3 Installation

Installing PGP Desktop on your system

This section describes how to install PGP Desktop onto your computer and how to get up started and running after installation. The following topics are covered here.

Before you Install

This section describes the minimum system requirements for installing PGP Desktop on your Mac OS X system.

System Requirements

Minimum system requirements to install PGP Desktop are:

- Operating System—Mac OS X 10.4.0 through 10.4.6.
- Free memory—128 MB physical RAM.
- Free disk space—20 MB hard disk space.

Installing PGP Desktop for Mac OS X

The PGP Desktop installer walks you through the installation process.

To install PGP Desktop on your Mac OS X system:

1. Quit all other applications.
2. Mount the PGP DiskCopy image.
3. Double-click PGP.pkg.
4. Follow the on-screen instructions.

If you are in a domain protected by a PGP Universal Server, your PGP administrator may have preconfigured your PGP Desktop installer with specific features and/or settings.

Upgrading the Software

You can upgrade to PGP Desktop 9.5 for Mac OS X from a previous version of PGP Desktop for Mac OS X, or PGP Universal Satellite for Mac OS X.

PGP Desktop 9.0 for Mac OS X or greater, and PGP Universal Satellite 2.0 for Mac OS X or above, **cannot** both be installed in the same system. The installers for both products will detect the presence of the other program and end the install.

To upgrade to PGP Desktop 9.5 for Mac OS X:

- **From PGP Desktop 8.x or 9.x for Mac OS X**, begin the installation process for PGP Desktop 9.5 for Mac OS X.

  The existing version of PGP Desktop for Mac OS X is automatically uninstalled, then PGP Desktop 9.5 for Mac OS X is installed. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version.

- **From a version of PGP Desktop for Mac OS X *prior* to Version 8.0**, you must manually uninstall the existing software before beginning the installation of PGP Desktop 9.5 for Mac OS X. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version.

- **From PGP Universal Satellite 1.2 or previous for Mac OS X**, begin the installation process for PGP Desktop 9.5 for Mac OS X.

  Existing versions of PGP Universal Satellite for Mac OS X are automatically uninstalled, then PGP Desktop 9.5 for Mac OS X is installed. Existing settings are retained.

Installing any version of PGP Universal Satellite 1.x on top of PGP Desktop 9.5 for Mac OS X is an unsupported configuration. Neither program will work correctly. Uninstall both programs and then reinstall only PGP Desktop.

- **From PGP Desktop for Mac OS X (version 8.x) and PGP Universal Satellite:** Follow the install process for PGP Desktop 9.5 for Mac OS X.

  PGP Desktop for Mac OS X and PGP Universal Satellite for Mac OS X are both automatically uninstalled, then PGP Desktop 9.5 for Mac OS X is installed. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version, as are existing PGP Universal Satellite for Mac OS X settings.

Licensing PGP Desktop

Refer to the PGP Desktop *Release Notes* for license information for this release.

Running the Setup Assistant

The Setup Assistant displays a series of screens that ask you questions—then uses your answers to configure PGP Desktop for you.

If you have questions about any of the content on the Setup Assistant screens, click **Help** on the screen.

PGP key reconstruction is not available in this version of PGP Desktop for Mac OS X; it is scheduled to be included in an upcoming release. If your security policies require the use of key reconstruction, please use PGP Desktop for Windows in a PGP Universal environment.

The Setup Assistant does not configure all PGP Desktop settings. When you finish going through the Setup Assistant screens, you can then configure those settings not covered in the Setup Assistant.

Integrating with Entourage 2004

The PGP Desktop for Macintosh installation package includes scripts so you can integrate PGP with Entourage. Once the scripts are copied to the required folders, the Scripts menu in Entourage will include a PGP menu option. Use the Entourage scripts if you want to encrypt email text without having to use an email proxy.

To integrate PGP scripts with Entourage:

1 If it is running, quiit Entourage.

1 Open the PGP Desktop for Macintosh download.

2 In the PGP Desktop download folder, open the Extras folder.

3 In the Extras folder, open the Entourage folder.

4 Double-click the file `EntourageScripts.zip` to extract the following scripts from the zip file:

- Decrypt & Verify\mod
- Encrypt & Sign\\mac
- Encript\moe
- Sign\mos

5 Copy and paste the scripts to the following folders:

- Documents
- Microsoft User Data
- Entourage Script Menu items
- PGP

6 Start Entourage. The Scripts menu now includes a PGP menu option.

Uninstalling PGP Desktop

To uninstall PGP Desktop:

1 In PGP Desktop, from the **PGP** menu, select **Uninstall**.

A confirmation dialog appears.

2 Click **Yes** to continue with the uninstall process.

3 You are prompted to authenticate as the administrative user of the Mac OS X system from which you are uninstalling PGP Desktop.

4 Enter the appropriate password, then click **OK**.

The PGP Desktop software is removed from your system.

Your keyring and PGP Virtual Disk files are not removed from your system, in case you decide to reinstall PGP Desktop in the future.

Moving Your PGP Desktop Installation From One Computer to Another

Moving a PGP Desktop installation from one computer to another is not a difficult process, although there are a few crucial steps which must be completed successfully. The process consists of the following steps:

- Uninstall PGP Desktop from the old computer,
- Transfer the public and private keyring files from the old computer to the new computer,
- Install PGP Desktop on the new computer,
- Configure PGP Desktop to use the keyring files transferred from the old computer, and finally,
- License PGP Desktop on the new computer.

To transfer your PGP Desktop installation to another computer:

1. Uninstall PGP Desktop, To do this, in PGP Desktop from the **PGP** menu, select **Uninstall**.

   Note that this step does not remove the keyring files.

2. Transfer the keyrings. To do this, copy the keyring files (both `pubring.pkr` and `secring.skr`) from the old computer to removable media such as a flash drive, and then copy them to the new computer. The default location for the keyring files is in the PGP folder.

   If PGP Desktop has never been installed on the new computer, create this folder first before copying the keyring files to the computer.

3. Install PGP Desktop on the new computer. To do this, download PGP Desktop by clicking the download link in your original PGP order confirmation email.

4. During the installation process, do the following:

   – During the PGP Desktop setup wizard on the new computer select **No, I have existing keyrings** and specify the location where you copied the keyring files to on the new computer.

   – Use the same name, organization, and license number used when PGP Desktop was originally authorized.

4 Securing Email Messages

Using PGP Desktop to protect your email

This chapter describes how to use PGP Desktop to automatically and transparently secure your email messages.

How PGP Desktop Secures Email Messages

When secure email messaging is enabled, PGP Desktop monitors the email traffic between your email client and your mail server. Depending on the circumstances, PGP Desktop will intercede on your behalf to encrypt, sign, decrypt, or verify messages.

How this happens is different for incoming and outgoing messages.

For incoming messages, PGP Desktop automatically evaluates all incoming email messages and takes the appropriate actions as described in "Incoming Messages" on page 24.

In some cases, such as if you have stored encrypted email messages using versions of PGP Desktop prior to 9.x, the current PGP Desktop email proxy, which decrypts messages as they are received by the computer, cannot decrypt them. To decrypt such legacy email messages, the PGP Desktop plug-in permits the decryption of these messages created by technology used in previous versions of PGP Desktop.

For outgoing messages, there are a range of actions that PGP Desktop can take on your behalf based on configured policies (a policy is a set of instructions that tells PGP Desktop what to do in specific situations). PGP Desktop comes pre-configured with a set of

policies that suit the needs of the vast majority of users. However, you are also provided with fine-grained control over these policies should you wish to change them. A policy is a set of one or more instructions, generally of a form like: "In this circumstance, do this." By combining these instructions, policies can be tailored to meet all of your email security requirements.

By default, when you are sending an outgoing message, PGP Desktop looks for a key it can trust to encrypt the message. It will look first on the local keyring for the public key of the recipient. If it does not find such a key, it will, again by default, check the PGP Global Directory for a trusted key for the recipient. If it does not find a trusted key there, and no other policies apply, the default Opportunistic Encryption policy will be applied, which means the message will be sent in the clear; that is, unencrypted. This default behavior strikes a balance between protecting outgoing messages and making sure they get sent.

Creating new policies is covered in detail in "Creating a New Security Policy" on page 36.

If you are in a PGP Universal-protected domain, your local PGP Desktop policies determine how your messages are encrypted and when. For more information, consult with your organization's PGP

Incoming Messages

PGP Desktop manages incoming mail messages based on the content of the message. **These scenarios assume standalone PGP Desktop, not in a domain protected by a PGP Universal server** (in which case mail action policies set by your PGP Universal administrator can apply):

- **Message not encrypted nor signed.** PGP Desktop does nothing to the content of these messages; it simply passes the message along to your email client.
- **Message encrypted, but not signed.** When PGP Desktop sees a message coming to you that is encrypted, it will attempt to decrypt it for you. To do this, PGP Desktop will check the local keyring for the private key that can decrypt the message. If the private key is not on the local keyring, PGP Desktop will not be able to decrypt it; the message will be passed to your email client still encrypted. If the private key **is** on the local keyring, PGP Desktop will decrypt it immediately if the passphrase for the private key is in memory (cached). If the passphrase is not cached, PGP Desktop will prompt you for the passphrase and decrypt the message when you supply the correct passphrase. Once a message is decrypted, PGP Desktop passes it to your email client.

  If the PGP Desktop messaging proxy is turned off, PGP Desktop will not be able to decrypt incoming encrypted messages; it will pass them along to your email client still encrypted. It is recommended that you leave your messaging proxy on all the time if you expect to be sending and receiving encrypted messages. On is the default setting.
- **Message signed, but not encrypted.** PGP Desktop will search the local keyring for a public key that can be used to verify the signature. If PGP Desktop cannot find the appropriate public key on the local keyring, it will try to search for a keyserver at keys.domain (where **domain** is the domain of the sender of the message), then the PGP Global Directory (at keyserver.pgp.com), and finally any other configured keyservers. If PGP Desktop finds the right public key at any of these locations, it

verifies the signature (or not, if the signature is bad) and passes the message to your email client annotated with information about the signature—information is also put into the Messaging Log. If PGP Desktop cannot find the appropriate public key, it passes the message to your email client unverified.

- **Message encrypted and signed.** PGP Desktop goes through both of the processes described above: first finding the private key to decrypt the message and then finding the public key to verify the signature. However, if a message cannot be decrypted, then it cannot be verified.

If PGP Desktop is unable to either decrypt or verify a message, you might want to consider contacting the sender of the message. If the message couldn't be decrypted, make sure the sender was using your real public key. If the message couldn't be verified, ask the sender to publish their key on the PGP Global Directory—older PGP versions or other OpenPGP products can access the web version of this directory at https://keyserver.pgp.com, or ask them to send their public key to you directly by email.

PGP Desktop only encrypts by default to keys that are known to be valid. If you didn't get a key from the PGP Global Directory, you may need to verify its fingerprint with the owner and sign it for it to be used.

Outgoing Messages

Email messages that you send can be encrypted, signed, both, or neither. Because you probably have different combinations for different recipients or email domains, you need to create policies for all of your outgoing email message possibilities. Once correct policies are in place, your email messages are protected automatically and transparently.

If you are in a PGP Universal-protected domain, your local PGP Desktop policies are controlled by the policies specified by your PGP Universal Server.

Services and Policies

To understand how to use PGP Desktop to automatically and transparently protect your outgoing messages, you need to understand two terms: service and policy.

- **Service**. Information about one email account on your system and the policies that apply to that account. In most cases, PGP Desktop will automatically create and configure a service for each email account on your system. In some circumstances, you may want to create and configure a service manually.
- **Policy**. A set of one or more instructions that tell PGP Desktop what to do in specific situations. Policies are associated with services—often more than one (a policy can be reused by different services). Conversely, a service can (and usually does) have more than one policy.

When deciding how to handle a specific outgoing email message, PGP Desktop checks the policies configured for the service one at a time (from the top of the list going down). When it finds a policy that applies, it stops checking policies and implements the one that applies.

All new services are created with the following default policies:

- **Mailing List Admin Requests**. Specifies that administrative requests to mailing lists are sent in the clear; that is, not encrypted or signed.
- **Mail List Submissions**. Specifies that submissions to mailing lists are sent signed (so they can be authenticated) but not encrypted.
- **Require Encryption: [PGP] Confidential**. Specifies that any message flagged as confidential in your email client or containing the text "[PGP]" in the subject line **must** be encrypted to a valid recipient public key or it cannot be sent.
- **Opportunistic Encryption**. Specifies that any message for which a key to encrypt cannot be found should be sent without encryption (in the clear). Having this policy as the **last** policy in the list ensures that your messages will always be sent, albeit in the clear, even if a key to encrypt it to the recipient cannot be found.

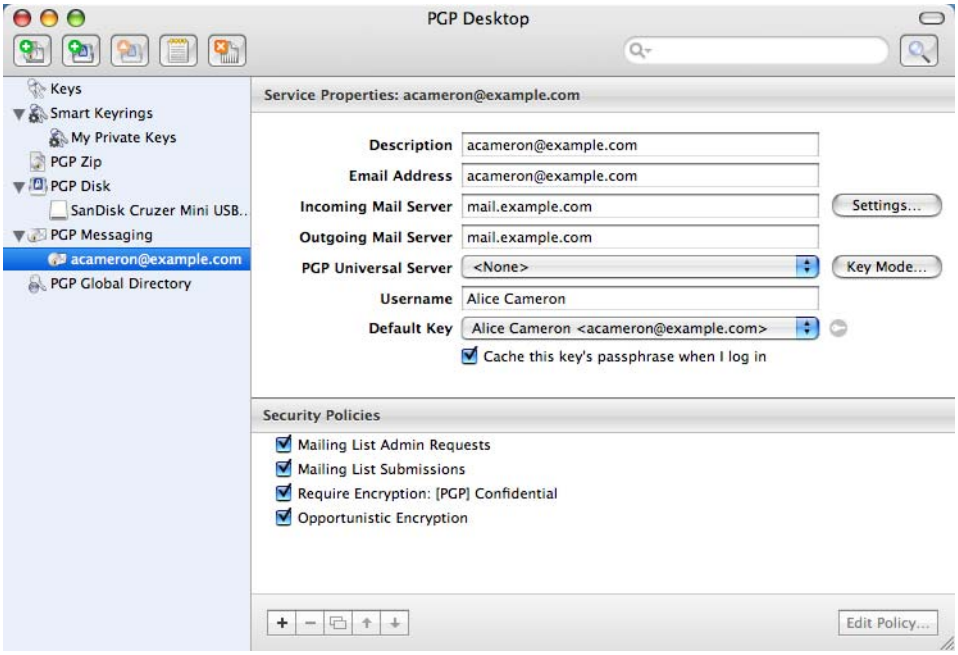
  Do not put Opportunistic Encryption first in the list of policies (or anywhere but last, for that matter) because when PGP Desktop finds a policy that matches, and Opportunistic Encryption matches everything, it stops searching and implements the matching policy. So if a policy is lower on the list than Opportunistic Encryption, it will never be implemented.

The default policies can be modified, but not deleted. Alternatively, they can be disabled, then moved up or down in the list of policies.

To view services and policies:

1. Open PGP Desktop.
2. Click a service listed under the PGP Messaging item.

   The Service Properties for that service appear in the PGP Desktop main screen.



Creating a Service and Editing Account Properties

A service is information about an email account, as well as the security policies that are to be applied to outgoing messages for that email account.

In most cases, PGP Desktop creates services for you as you use your email accounts to send or receive messages. If you need to create a service yourself, make sure to read and understand these instructions. Incorrect configuration of a service could result in problems sending or receiving email messages.

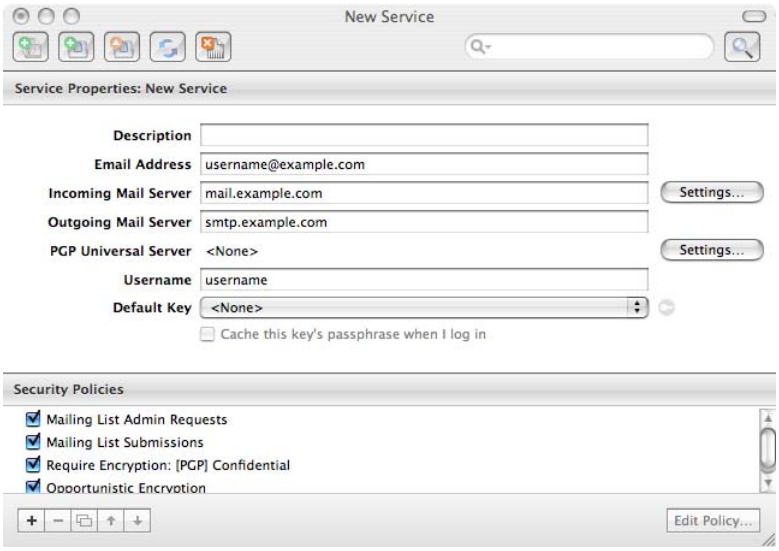
To create a new service:

1 Open PGP Desktop and click the PGP Messaging item.

The PGP Messaging screen appears.

2 Click the **Create New Service** button. Or, from the **Messaging** menu, select **New Service**.

The **New Service** screen appears. The **Service Properties** section shows default settings and the Security Policies section displays default security policies.

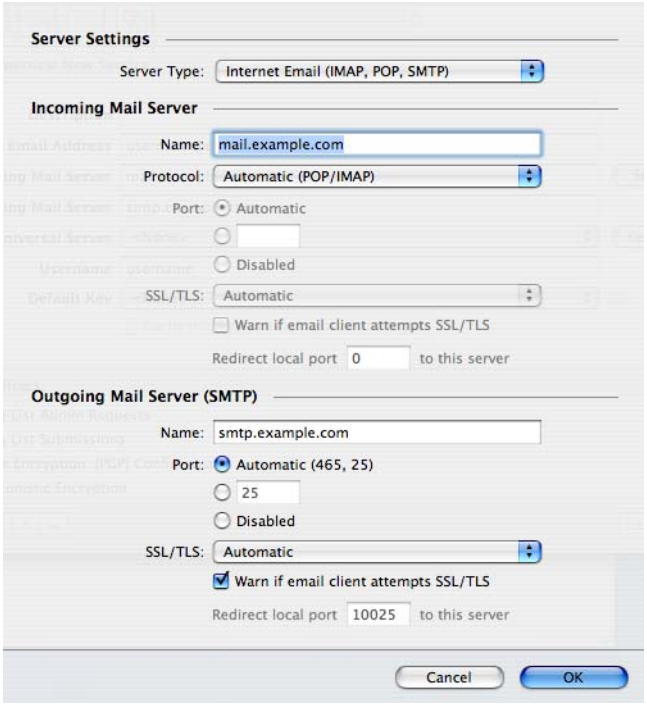


3 In the **Description** field, enter a descriptive name for this service. (This step is optional, but helpful when you work with multiple services).

4 In the **Email Address** field, enter the email address associated with this service. For example, **acameron@example.com**.

5 Type the name of your incoming and outgoing email servers, or click **Server Settings** if you want to set advanced options.

If you chose to set advanced options, the **Server Settings** dialog appears.



6 Enter the appropriate settings:

- **Server Type:** Select the type of server that the new service will be using:

  PGP Universal Server—for PGP Desktop users who are in a PGP Universal-managed environment. Contact your PGP administrator for more details on correct settings. If you are using PGP Desktop in a PGP Universal-managed environment, the correct settings for the Server Settings screen were automatically downloaded.

  Internet Mail—for standalone PGP Desktop users who have a POP or IMAP mail connections.

- **Name**: Enter the name of the mail server that handles *incoming* messages.

- **Protocol**: Select the protocol used to pick up messages on the incoming mail server.

  The **Automatic** setting can automatically detect either POP or IMAP connections.

- **Port**: Keep **Automatic** (the default) or specify a port to connect to on the incoming mail server to pick up messages (if you have selected either the **Internet Mail** or **PGP Universal** settings and either **POP** or **IMAP**—not **Automatic**).

- **SSL/TLS**: Specify how PGP Desktop interacts with your mail server:

  Automatic: PGP will do its best to provide SSL/TLS protection. It first tries the alternate port, then it attempts STARTTLS (if supported by the server), finally, if the above fails, it connects to the server unprotected.

  Require STARTTLS: PGP Desktop requires the server honor the STARTTLS command.

  Require SSL: PGP Desktop requires that the server honor SSL-protected connections on the specified alternate port.

  Do Not Attempt: PGP Desktop does not attempt any SSL/TLS protection of the connection with the mail server.

- **Warn if email client attempts SSL/TLS:** When selected, PGP Desktop displays a warning dialog if the email client attempts SSL/TLS, as this is a condition that is incompatible with PGP Desktop proxying your email. (This option is selected by default.)

This option should only be enabled if you are certain your mail server supports SSL. It ensures that PGP Desktop will not fall back to sending or receiving messages with the mail server over an unprotected connection if, for example, a problem occurs while negotiating SSL protection for the connection. **If you enable this option and your mail server does not support SSL, PGP Desktop will not send or receive any of your messages.**

- **Name**: Enter the name of the mail server that handles *outgoing* messages.

- **Port**: Keep **Automatic (465, 25)** or specify another port to connect to on the outgoing mail server to send messages.

This option is only available for the outgoing mail server if your settings permitted choosing it for the incoming mail server.

– **SSL/TLS**: Specify how PGP Desktop interacts with your mail server:

Automatic: PGP will do its best to provide SSL/TLS protection. It first tries the alternate port, then it attempts STARTTLS (if supported by the server), finally, if the above fails, it connects to the server unprotected.

Require STARTTLS: PGP Desktop requires that the server honor the STARTTLS command.

Require SSL: PGP Desktop requires that the server honor SSL-protected connections on the specified alternate port.

Do Not Attempt: PGP Desktop does not attempt any SSL/TLS protection of the connection with the mail server.

– **Warn if email client attempts SSL/TLS:** When selected, PGP Desktop displays a warning dialog if the email client attempts SSL/TLS, as this is a condition that is incompatible with PGP Desktop proxying your email. (This option is selected by default.)

7 Click **OK** when you are finished.

8 In the **Universal Server field,** select the name of the PGP Universal Server protecting the email domain you are in. **<None>** appears if you are not in an email domain protected by a PGP Universal Server. If your domain is protected by a PGP Universal Server, but it is not listed, select **<Add Server>** to enter the name of your PGP Universal Server. Check with your PGP Universal administrator for more information.

9 If you want to change your existing key mode, click **Key Mode**.

The **Key Mode** dialog box appears, displaying your current key mode. If necessary, click **Reset Key,** which begins the process of resetting your account and choosing a different key mode. You can only reset your key and choose a different key mode if you are in an email domain protected by a PGP Universal Server. Refer to "Working with the Security Policy List" on page 43 for more information about key modes.

10 Click **OK**.

11 In the **Username** field, enter the username on the email account.

12 In the **Default Key** field, the current key displays.

– If you are using PGP Desktop as a standalone product, you can either keep the default key, or select another one from the menu (if another key is available).

– If you are using PGP Desktop in a PGP Universal-managed environment, the default key is displayed and you cannot change it. If you need to change your key, you must click **Key Mode** and go through the procedure to reset your key.

13 Enable **Cache this key's passphrase when I log in** (by selecting the checkbox) if you want to cache the passphrase for the keypair you just selected when you log in.

If you don't cache the key's passphrase, you will be prompted for it when you are sending signed messages or receiving encrypted messages.

14 In the **Security Policies** section, the current policies that apply to the selected service are displayed.

If you are using PGP Desktop as a standalone product, you can view the default security polices, disable the default security policies, or add new policies. If you are using PGP Desktop in a PGP Universal-managed environment, you must use the policies from the PGP Universal Server.

See "Creating a New Security Policy" on page 36 for more information about creating a new policy or editing existing ones.

15 When you are done with the security policies, the account is ready. It is not necessary to click a button to save your information. It was saved as soon as you entered it.

To make changes to the account properties of an existing service:

1 Open PGP Desktop and click the **PGP Messaging** item.

2 Click on the name of the service whose account properties you want to edit.

The settings for the selected service appear in the PGP Messaging Work area.

3 Make the desired changes to the account properties of the service.

Disabling, Enabling, and Deleting a Service

If you want to stop a service from working, but you don't want to delete the service because you might need it again, you can disable the service. This is useful if you only want PGP Desktop to process mail on particular accounts, but not others. If you are certain that you won't need the service again, delete it.

To disable an existing service:

1 Under the **PGP Messaging** item, select the name of the service you want to disable.

The settings for the service appear. Confirm that you have selected the correct service.

2 From the **Messaging** menu select **Disable Service**.

You can also Ctrl-click the name of the service (or right-click it if you are using a two-button mouse) and select **Disable Service** from the context menu that appears.

The service is disabled.

To enable a disabled service:

1 Under the **PGP Messaging** item, select the name of the service you want to enable.

The settings for the service appear. Confirm that you have selected the correct service.

2 Click to select the name of the service again, only this time hold down the Ctrl key as you click. You can also right-click the name of the service if you are using a two-button mouse.

A context menu appears.

3 From the context menu, select **Enable Account**.

The service is enabled.

PGP Desktop alerts you that the change may not take place until you restart your email client.

To delete a service:

1 Under the **PGP Messaging** item, select the name of the service you want to enable.

The settings for the service appear. Confirm that you have selected the correct service.

2 Click to select the name of the service again, only this time hold down the Ctrl key as you click. You can also right-click the name of the service if you are using a two-button mouse.

A context menu appears.

3 From the context menu, select **Clear**.

The service is deleted.

PGP Desktop and SSL

When you use PGP Desktop, PGP Corporation's goal is for your data to be automatically protected whenever possible. This includes protecting your data in transit between your email client and your mail server.

SSL stands for Secure Sockets Layer, which is a cryptographic protocol that secures communications between two devices; in this case, between your email client or PGP Desktop and your mail server.

PGP Desktop protects your data to and from your mail server in different ways depending on the circumstances. The following information applies only if you selected **Automatic** (the default) for the SSL/TLS setting in the server settings dialog:

- **When the connection is not SSL protected.** If the connection between your email client and your mail server is not SSL protected, PGP Desktop will automatically attempt to upgrade that connection to SSL (it will negotiate with your mail server and upgrade the connection if the mail server supports it).

  If the mail server does not support SSL, the message(s) PGP Desktop sends and receives during the session will be over an unprotected connection. Whether or not those messages will be encrypted/decrypted by PGP Desktop does not affect the

attempt by PGP Desktop to upgrade the connection. Messages encrypted by PGP Desktop can be sent or received over a connection protected by SSL or not protected by SSL.

PGP Desktop always attempts to upgrade an unprotected connection to the mail server to SSL protection because an SSL-protected connection not only protects any non-PGP-encrypted messages on their way to the mail server or coming from it, but it also protects your mail server authentication passphrase when it is sent to the mail server.

- **When the connection *is* protected by SSL.** If you have SSL protection turned on in your email client for the connection to your mail server, you must turn it off if you want PGP Desktop to encrypt or decrypt your messages; PGP Desktop cannot process your messages if they are already SSL-encrypted.

  Turning off SSL protection in your email client does not mean that your non-PGP-encrypted messages are now unprotected going to or coming from your mail server. As with any connection that is not SSL protected, PGP Desktop will automatically attempt to upgrade the connection to SSL protection if the mail server supports it. If the mail server does not support SSL connections, the messages PGP Desktop sends during the session will be over an unprotected connection.

  The only time your messages will be sent in the clear to your mail server is if the messages are not PGP encrypted and the connection to the mail server cannot be upgraded to SSL protected.

- **When you can't have messages sent in the clear.** Some security policies require that only protected messages can be sent; in other words, unprotected messages must never be sent. If necessary, you can easily configure PGP Desktop to support this kind of security policy.

  Select the applicable PGP Messaging service, access the Server Settings dialog (click the name of the server currently in the Server field of the Account Properties for the service), and select the option "Require SSL/TLS when communicating with these servers" (located at the bottom of the dialog).

  When this option is enabled, PGP Desktop will only send messages to or receive messages from your mail server if the connection between them is SSL protected. If an SSL-protected connection cannot be established, PGP Desktop will not interact with the server.

  This option should only be enabled if you are certain your mail server supports SSL. It ensures that PGP Desktop will not fall back to sending or receiving messages with the mail server over an unprotected connection if, for example, a problem occurs while negotiating SSL protection for the connection. If you enable this option and your mail server does not support SSL, PGP Desktop will not send or receive any of your messages.

- **When you want SSL enabled in your email client.** If you want to use PGP Desktop with SSL enabled in your email client, you can do that; you just have to tell PGP Desktop that you are doing it by selecting the option "Ignore SSL/TLS with this server" for your incoming or outgoing mail server, or both. When you enable this option for a connection to a mail server, PGP Desktop will ignore traffic coming in from or going out over that connection when the connection is protected by SSL.

PGP Desktop will monitor the connections to and from this server, ignoring traffic sent or received on SSL-protected connections. If, however, PGP Desktop detects a non-SSL-protected connection, it will handle the traffic like any other unprotected connection; it will attempt to upgrade the connection to SSL and it will apply applicable policies to messages.

Multiple Services

Some email services and Internet Service Providers use multiple mail servers for a single DNS name in a "round-robin" fashion such that PGP Desktop may create multiple messaging services for a single email account, seeing each mail server as separate and thus requiring its own messaging service.

PGP Desktop ships with wildcard support for common email services, such as ***.yahoo.com** and ***.mac.com**. However, if you are using a less-common email service or if the services change their mail server configurations, you could run into this problem.

If you see PGP Desktop create multiple services for a single email account, and you check the settings and see they are the same except the mail server for the first service is **mail1.example.com**, the mail server for the second service is **mail2.example.com**, and the mail server for the third is **mail3.example.com**, and so on, then you need to manually edit one of the services.

The best solution is to set one of the services such that the mail server entry for that service can support **multiple** mail servers being used round-robin. For the example cited above, you could manually change the server name on the Server Settings screen for one of the services to **mail*.example.com**, then delete the other services.

Some round-robin setups may be more complicated, requiring a slightly different solution. For example, if PGP Desktop were to create services with mail servers of **pop.frodo.example.com**, **smtp.bilbo.example.com**, and **mail.example.com**, then the best wildcard solution would be ***.example.com**.

Troubleshooting PGP Messaging Services

By default, PGP Desktop automatically determines your email account settings and creates a PGP Messaging service that proxies messaging for that email account.

Because of the large number of possible email account settings and mail server configurations, on some occasions a messaging service that PGP Desktop automatically creates may not work quite right.

If PGP Desktop has created a messaging service that isn't working right for you, one or more of the following items may help correct the problem:

- Verify that you can both connect to the Internet and send and receive email with PGP Services stopped. With the Option key held down, select **Quit** from the PGP Desktop icon in the Menu bar.

- Read the PGP Desktop Release Notes for the version of PGP Desktop you are using to see if your problem is a known issue.
- Make sure SMTP authentication is enabled for the email account (in your email client). This is **required** for PGP Desktop to proxy your messaging.
- Open the Messaging Log to see if the entries offer any clues as to what the problem might be.
- If SSL/TLS is enabled in your email client, you must disable it there if you want PGP Desktop to proxy your messaging. (This does **not** leave the connection to and from your mail server unprotected; PGP Desktop automatically attempts to upgrade any unprotected connection to SSL/TLS protection. The mail server must support SSL/TLS for the connection to be protected.)
- If either "Require STARTTLS" or "Require SSL" are enabled (at the bottom of the Server Settings screen for the messaging service) your mail server **must** support SSL/TLS or PGP Desktop won't send or receive any messages.
- If your email account uses non-standard port numbers, make sure these are included in the settings of your messaging service.
- If PGP Desktop is creating multiple messaging services for the same email account, see "Multiple Services" on page 34 for instructions how to create a wildcarded mail server name.
- Delete the PGP Messaging service that is not working correctly, then send/receive email. PGP Desktop then regenerates the messaging service.

If none of these items help correct the problem, try the following:

1. Delete the PGP Messaging service that isn't working right.
2. Stop all PGP Desktop services. With the **Option** key held down, select **Quit** from the PGP Desktop icon in the Menu bar. If PGP Desktop is open, doing this causes it to Quit.
3. Verify that you have Internet connectivity and can send and receive email with PGP Messaging services stopped.
4. Open your email client and write down your email account settings (including username, email address, incoming and outgoing mail server, incoming mail server protocol, and any non-standard mail server port numbers).
5. Close your email client and restart PGP Desktop, which restarts PGP services (either restart Mac OS X or open PGP Desktop).
6. Manually create a PGP Messaging service using the account settings you wrote down.
7. Open your email client and begin sending and receiving messages.

If you continue to have problems with a PGP Messaging service, access any of the following for assistance:

- The PGP Corporation website: www.pgp.com

- The PGP Support website: www.pgp.com/support
- The PGP Support forums: forums.pgpsupport.com

Creating a New Security Policy

Security policies are what control how PGP Desktop handles outgoing email messages.

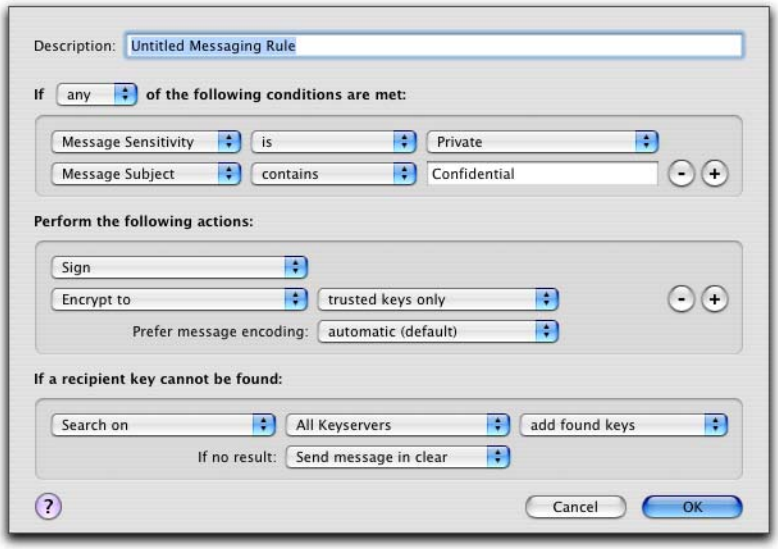
To create a new security policy:

1 In the **PGP Messaging** item, click on the name of the service for which you want to create a new security policy.

The settings for the service appear, including the list of existing security policies.

2 Click the plus-sign icon (**+**) at the bottom of the screen.

The **Untitled Messaging Rule** screen appears.



If your email domain is protected by a PGP Universal Server, and you look at the Message Policy settings for a policy from a PGP Universal Server, the fields may be different from the fields shown above.

3 In the **Description** field, enter a descriptive name for the policy you are creating.

4 In the **If** field, select:

- **If any**. The policy applies when any condition is met.
- **If all**. The policy only applies when all conditions are met.
- **If none**. The policy only applies if none of the conditions are met.

5 In the first condition field, select:

- **Recipient**. The policy applies only to messages to the specified recipient.
- **Recipient Domain**. The policy applies only to email messages in the specified recipient domain.
- **Sender.** The policy applies only to messages with the specified sender address.
- **Message.** The policy applies only to messages which have the specified signed and/or encrypted state.
- **Message Subject**. The policy applies only to messages with the specified message subject.
- **Message Header**. The policy applies only to messages for which the specified header meets the specified criterion.
- **Message Body**. The policy applies only to messages with the specified message body.
- **Message Size.** The policy applies only to messages of the specified size (in bytes).
- **Message Priority**. The policy applies only to messages with the specified message priority.
- **Message Sensitivity**. The policy applies only to messages with the specified message sensitivity.

6 In the second condition field, select:

- **is**. The condition is met when text in the first condition field *matches* the text entered in the text box.
- **is not**. The condition is met when text in the first condition field *does not match* the text entered in the text box.
- **contains**. The condition is met when text in the first condition field *contains* the text entered in the text box.
- **does not contain**. The condition is met when text in the first condition field *does not contain* the text entered in the text box.
- **begins with**. The condition is met when text in the first condition field *begins with* the text entered in the text box.
- **ends with**. The condition is met when text in the first condition field *ends with* the text entered in the text box.
- **matches pattern**. The condition is met when text in the first condition field *matches the pattern* entered in the text box.
- **is less than**. The condition is met when message size is *less than* the text entered in the text box.
- **is greater than**. The condition is met when message size is *greater than* the text entered in the text box.

7 In the third condition field, select:

- **text entry box**. Enter text for the matching criteria.
- **signed**. Matching criteria for Message is *signed*.
- **encrypted**. Matching criteria for Message is *encrypted*.
- **encrypted to key ID**. Matching criteria for Message is *encrypted to key ID* that matches the key ID entered in the text entry box that appears.
- **none**. Matching criteria for Message Sensitivity is *none*.
- **Personal**. Matching criteria for Message Sensitivity is *Personal*.
- **Private**. Matching criteria for Message Sensitivity is *Private*.
- **Confidential**. Matching criteria for Message Sensitivity is *Confidential*.
- **Low**. Matching criteria for Message Priority is *Low*.
- **Normal**. Matching criteria for Message Priority is *Normal*.
- **High**. Matching criteria for Message Priority is *High*.

You can create more condition lines by clicking the plus-sign icon.

8 In the first action field, select:

- **Send In Clear**. Specifies that the message should be sent in the clear; that is, not signed nor encrypted.
- **Sign**. Specifies that the message should be signed.
- **Encrypt to**. Specifies that the message should be encrypted.

9 In the second action field, select:

- **recipient's verified key**. Ensures the message can be encrypted only to a verified key of the intended recipient.
- **recipient's unverified key**. Allows the message to be encrypted to an unverified key of the intended recipient.
- **recipient's verified end-to-end key**. Ensures the message can be encrypted only to a verified end-to-end key of the intended recipient. An end-to-end key is a key in sole possession of the individual recipient. In a PGP Universal-managed environment, this is a Client Key Mode key as opposed to a Server Key Mode key, where the PGP Universal Server is in possession of the key. (Whether the key is end-to-end or not is shown on the **Key Info** screen in the **Group** field—**No** means that it *is* end-to-end (is not part of a group), and **Yes** means that it *is not* end-to-end.)
- **recipient's unverified end-to-end key**. Allows the message to be encrypted to an unverified end-to-end key of the intended recipient.
- **a list of keys**. Specifies that the message can only be encrypted to keys on the list.

You can create more action lines by clicking the plus-sign icon.

10 In the prefer message encoding field, select:

- **automatic**. Lets PGP Desktop choose the message encoding format. This is almost always the best option unless you know exactly why you need to use one of the other message encoding formats explicitly.
- **PGP Partitioned**. Sets PGP Partitioned as the preferred message encoding format. This format is the most backwards compatible with older PGP and OpenPGP products.
- **PGP/MIME**. Sets PGP/MIME as the preferred message encoding format. PGP/MIME is able to encrypt and sign the entire message including attachments in one pass and is usually therefore faster and better able to reproduce the full message fidelity.
- **S/MIME**. Sets S/MIME as the preferred message encoding format. Choose S/MIME if, for some reason, you need to force messages to be S/MIME even if the user has a PGP key.

11 In the first recipient key not found field, select:

- **Search keys.domain and.** Specifies a search that includes both keys.domain as well as another server you specify.
- **Search.** Specifies a keyserver to search on.
- **Clear-sign message.** Specifies that the message should be sent in the clear, but signed.
- **Send message unsecured.** Specifies that the message be sent in the clear.
- **Block message.** Stops message from being sent.

12 In the second recipient key not found field, select:

- **All keyservers**. Allows all keyservers, including the PGP Global Directory, to be searched for an appropriate key. Note that keyservers other than the PGP Global Directory may provide unverified keys that cannot be used if you require verified keys in the policy. Unless you know exactly why you need to search another keyserver and are prepared to find those keys manually to verify them when necessary, search only on the PGP Global Directory.
- **PGP Global Directory**. Specifies that only the PGP Global Directory is searched.

13 In the third recipient key not found field, specify:

- **ask to save found keys**. Specifies that PGP Desktop should ask if you want to save to your local keyring a particular found key.
- **save found keys**. Specifies that found keys should automatically be saved to your local keyring.
- **temporarily cache found keys**. Specifies that a found key should be temporarily saved in memory. Keys in this cache will automatically be used when verifying signed messages, and will be used for encryption if they have been verified.

14 In the If no result field, select:

- **Clear-sign message.** Sign message but send it in the clear.
- **Send message unsecured.** Do not encrypt message.
- **Block message.** Stop message from being sent.

15 Click **OK** when the policy settings are configured.

The new policy appears in the list of security policies.

Wildcards and Regular Expressions in Policies

PGP Desktop supports the use of wildcards and regular expressions in security policies in text entry boxes.

Using wildcards and regular expressions lets you match multiple text strings using a single text string.

In addition to the following examples, PGP Desktop also supports broader regular expressions that adhere to standard formats. The "Matches Pattern" criteria actually means "matches regular expression."

For example, you can use the following:

- *****: matches any number of characters, including zero characters. For example, **a*c** would match **ac**, **abc**, **abbc**, and **almnopqrstuvc**. The asterisk is referred to as a wildcard.
- **?**: matches any single character. For example, **a?c** would match **acc**, **abc**, and **aYc**, but not **abbc**.
- **character**: matches itself only, except for "*" and "?". For example, **abcd** matches only **abcd**.
- **\character**: matches itself only, including "*" and "?". For example, use ***** if you need to match on an asterisk.

Security Policy Information and Examples

When you create a new service, four security policies are automatically created. These policies can be disabled, but they cannot be deleted or modified. This section describes how two of these default security policies work (Opportunistic Encryption and Require Encryption: [PGP] Confidential). It also describes two situations for which you might want to create a security policy, and explains how to configure them.

Opportunistic Encryption

Opportunistic Encryption is one of the two default security policies that PGP Desktop automatically creates for a service.

The settings for Opportunistic Encryption are:

If: any

Conditions: Recipient Domain / is / *

Actions: Sign / Encrypt to / recipient's verified key

Prefer message encoding: automatic (default)

Key Not Found: Search keys.domain and / PGP Global Directory / temporarily cache found keys

If no result: Send message unsecured

Opportunistic Encryption causes those messages for which a trusted key cannot be found to be delivered signed but not encrypted. This ensures your messages get signed and sent, although some may be unencrypted (sent in the clear).

Opportunistic Encryption was designed to go last in your list of security policies, as it will match any message sent. If placed above a policy in the list, PGP Desktop will never reach that policy, thus rendering it useless.

Require Encryption: [PGP] Confidential

Require Encryption: Confidential is one of the two default security policies that PGP Desktop automatically creates for a service.

The settings for Require Encryption: Confidential are:

- **If**: any
- **Conditions**: Message Subject / contains / [PGP]
  Message Sensitivity / is / Confidential
- **Actions**: Sign
  Encrypt to / recipient's verified key
- **Prefer message encoding**: automatic (default)
- **Key Not Found**: Search keys.domain and / All Keyservers / temporarily cache found keys
- **If no result**: Block message

Require Encryption: [PGP] Confidential causes those messages with subjects that contain [PGP] or are set as confidential in your email client to require encryption to a trusted key in order to be sent. If a trusted key cannot be found, the message is *not* sent.

Require Encryption to <Domain>

If you use Opportunistic Encryption with its default settings and you put it at the bottom of the list of policies, it will cause those messages for which a trusted key cannot be found to be delivered in the clear. This ensures that your messages get sent, but it also means that some may be sent in the clear.

If there are specific domains to which sending in the clear is not an option, you can create a security policy that calls for encrypting and/or signing or the message is *not* sent. When you create this policy, make sure it is higher in the list than Opportunistic Encryption.

The settings for such a policy are:

- **If**: any
- **Conditions**: Recipient Domain / is / example.com
- **Actions**: Sign
  Encrypt to / recipient's verified key
- **Prefer message encoding**: automatic (default)
- **Key Not Found**: Search / All Keyservers / temporarily cache found keys
- **If no result**: Block message

This security policy is similar to Require Encryption: Confidential in that it requires a message be encrypted or the message is not sent, but the criteria is not whether the message is marked confidential but rather that the email domain of the recipient is **example.com**. Using this policy ensures all messages to example.com are encrypted with a trusted key or they are not sent.

Sign and Send in the Clear to <Domain>

If you regularly send email to a domain for which you want to sign all messages but not encrypt them, you should set up a policy for that domain. Your messages will be processed faster if you don't wait for the final policy, Opportunistic Encryption, to send the messages in the clear.

The settings for such a policy are:

- **If**: any
- **Conditions**: Recipient Domain / is / example.com
- **Actions**: Sign
- **Prefer message encoding**: automatic (default)
- **Key Not Found**: Send message unsecured
- **If no result**: n/a

Working with the Security Policy List

There are several important things you can do to the security policies in the list of security policies, such as edit a policy, add a new policy (described in "Creating a New Security Policy" on page 36), delete a policy, and change the order of policies in the list.

Editing a Security Policy

To edit an existing security policy:

1 Open PGP Desktop and click the **PGP Messaging** item.

The **PGP Messaging** screen appears.

2 Click the name of the service with the security policy you want to edit.

The properties for the service you selected appear.

3 Select the security policy that you want to edit, then click **Edit Policy.**

The **Messaging Rule** screen appears, displaying the settings for the specified policy.

Two of the default policies, **Require Encryption: [PGP] Confidential** and **Opportunistic Encryption**, can be viewed and disabled, but not modified or deleted.

4 Make the desired changes to the policy.

Refer to "Creating a New Security Policy" on page 36 and "Security Policy Information and Examples" on page 40 for information about the fields on the **Message Policy** dialog.

5 When you have made the desired changes, click **OK** to close the **Message Policy** dialog.

The specified security policy is changed.

Deleting a Security Policy

To delete an existing security policy:

1. Click the name of the service with the security policy you want to delete.

   The properties for the service you selected appear.

2. Deselect the checkbox next to the policy you want to delete.

   The checkbox is deselected.

3. Click the name of the policy you want to delete (not its checkbox).

   The specified policy highlights.

4. Click **[-]** at the bottom of the **Security Policies** area.

   A confirmation dialog appears.

5. Click **Remove** to delete the policy.

   The specified security policy is deleted from the list.

Changing the Order of Policies in the List

To change the order of policies in the **Security Policy** list:

1. In the **PGP Messaging** item, select the name of the service that has the security policy whose order you want to change.

   The properties for the service you selected appear.

2. From the **Security Policies** list, click on the name of the policy whose order in the list you want to change.

   The specified policy highlights.

3. Click the **Up Arrow** or **Down Arrow** at the bottom of the **Security Policies** window until the policy is in the desired location in the list.

   Make sure **Opportunistic Encryption** is at the bottom of the list. Any policy below it is not implemented.

Key Modes

If you are using PGP Desktop in a PGP Universal-managed environment, PGP Desktop will have a key mode.

The information in this section applies *only* to users of PGP Desktop in an email domain protected by a PGP Universal Server.

Available key modes are:

- **Server Key Mode (SKM):** Keys are generated on and managed by the PGP Universal Server; they are only shared with the computer on which you are running PGP Desktop as needed. Your private key is stored only on the PGP Universal Server, which also handles all private key management. The PGP Universal administrator has complete access to your private key and can thus access all messages you encrypt. This key mode is **not** compatible with Smart Cards.

PGP Corporation recommends that PGP Desktop users ***not*** use SKM, as you will not have control over your private key, which is required for most other PGP Desktop features.

- **Client Key Mode (CKM):** Keys are generated on and managed by the computer on which you are running PGP Desktop; private keys are not shared with the PGP Universal Server. All cryptographic operations (encrypt, decrypt, sign, verify) are also handled by the computer on which you are running PGP Desktop. This key mode is compatible with Smart Cards.
- **Guarded Key Mode (GKM):** Very similar to CKM, except that an ***encrypted*** copy of the private key is stored on the PGP Universal Server, which you can access if you change computers. As the key is encrypted, the PGP Universal administrator cannot access this private key, only you can. This key mode is compatible with Smart Cards as long as the key is not generated directly on the Smart Card; that is, as long as the key is copied to the Smart Card.
- **Server Client Key Mode (SCKM):** Also very similar to CKM, except that a copy of the private *encryption* key is stored on the PGP Universal Server; private *signing* keys never leave the computer on which you are running PGP Desktop. This key mode ensures compliance with laws and corporate policies that require that the private signing key not leave the control of the user, while making sure that the private encryption key is stored in case of emergency. This key mode is compatible with Smart Cards as long as the key is not generated directly on the Smart Card. SCKM requires a key with a separate signing subkey, which can be created for a new key with PGP Desktop 9.5 or greater or added to an older PGP key using PGP Desktop 9.5 or greater.

Depending on how your PGP administrator configured your copy of PGP Desktop, you may or may not be able to choose your key mode. Also, you may or may not be able to change your key mode.

Please contact your PGP administrator if you have additional questions about your key mode.

Determining Key Mode

Remember that only PGP Desktop users in a PGP Universal-protected environment will have a key mode; standalone PGP Desktop users do not have a key mode.

To determine your key mode:

1 Open PGP Desktop and select the **PGP Messaging** service whose key mode you want to determine.

The account properties and security policies for the selected service appear.

2 In the **PGP Universal Server** field, the key mode for the selected service is shown in parentheses after the name of the PGP Universal Server.

For example: **keys.example.com (GKM)**

This tells you that the key mode for the selected service is Guarded Key Mode and that the associated PGP Universal Server is keys.example.com.

Changing Key Mode

Depending on how your PGP administrator configured your copy of PGP Desktop, you may not be able to change your key mode.

To change your key mode:

1 Open PGP Desktop and select the **PGP Messaging** service whose key mode you want to determine.

The account properties and security policies for the selected service appear.

2 Click **Key Mode**.

The **PGP Universal Key Mode** screen appears, describing your current key management mode.

3 Click **Reset Key**.

The **PGP Key Setup Assistant** appears.

4 Read the text, then click **Next**.

The **Key Management Selection** screen appears.

5 Select the desired key mode.

Depending on how your PGP Universal administrator configured your copy of PGP Desktop, some key modes may not be available.

6 Click **Next**.

The **Key Source Selection** screen appears.

7 Choose one of the following:

- **New Key**. You will be prompted to create a new PGP key, which will be used to protect your messaging.
- **PGP Desktop Key**. You will be prompted to specify an existing PGP key to use to protect your messaging.
- **Import Key**. You will be prompted to import a PGP key, which will be used to protect your messaging.

8 Make the desired selection, then click **Next**.

9 If you selected **New Key**:

   a Enter a passphrase for the key, then click **Next**.

   b When the key is generated, click **Next**.

   c Click **Finish**.

10 If you selected **PGP Desktop Key**:

   a Select the key from the local keyring that you want to use, then click **Next**.

   b Click **Finish**.

11 If you selected **Import Key**:

   a Locate the file that holds the PGP key you want to import (it must contain a private key), then click **Next**.

   b Click **Finish**.

Viewing the PGP Messaging Log

The PGP Messaging Log is a handy way of seeing what actions the PGP Messaging feature is taking to secure your messaging.

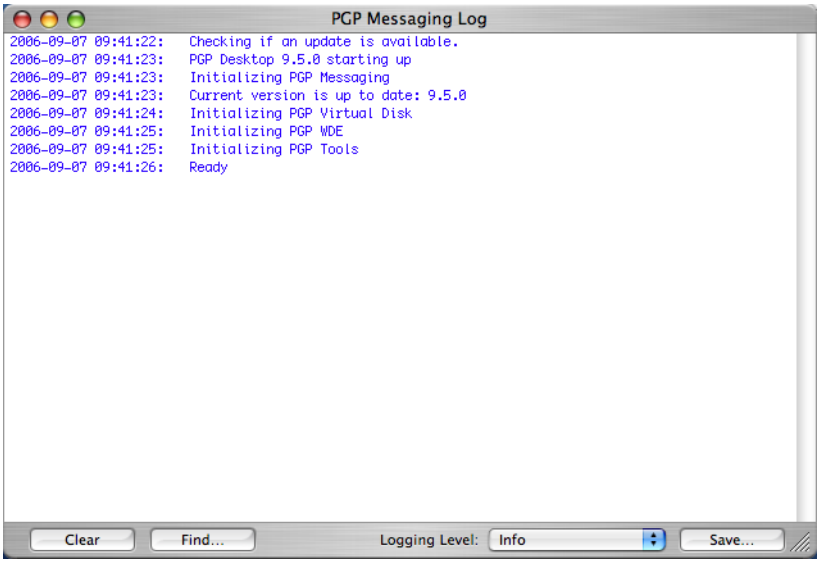
To view the PGP Messaging Log:

1 Open PGP Desktop and click the **PGP Messaging** item.

   The PGP Messaging screen appears.

2 From the **Messaging** menu, select **Show Log**.

   The PGP Messaging Log appears.



3 Click **Clear** to clear all of the entries in the PGP Messaging Log. You will be prompted to confirm that you want to clear all entries in the log; click **Yes**.

4 Click **Find** to search the entries in the PGP Messaging Log. Enter the search terms and click **Next**.

5 **Logging level** lets you select the minimum information level of log entries you wish to view: **Info** or **Verbose**. Note that **Verbose** can result in large log files.

6 Click **Save** to save a copy of the entries in the log. Specify a filename, location, and format (the default is a plain text file) for the log file, then click **Save**.

7 Click the red circle in the upper left corner of the screen to close the **PGP Messaging Log** screen.

5 Securing Instant Messaging

Using PGP Desktop to secure your instant messages

The following topics are available on how to use PGP Desktop to secure your instant messaging (IM) sessions:

About PGP Desktop's Instant Messaging Support

PGP Desktop automatically encrypts your IM sessions if the following conditions are met:

- Both users in the IM session have PGP Desktop 9.0 or greater up and running on the system on which they are doing the IM session. You can confirm that you are using PGP Desktop 9.0 or greater by clicking the PGP menu and selecting **About PGP Desktop** from the menu.
- Both users have the **Encrypt instant messages** setting enabled in their Preferences. You can confirm that **Encrypt instant messages** is enabled on your system by pulling down the PGP menu, selecting Preferences, clicking on the Messaging icon, and verifying that **Encrypt instant messages** is selected.
- Both users are using supported IM clients.
- The AIM address of the initiator of the IM session *must* be on the Buddy List of the recipient of the session. If it isn't, the session won't be encrypted.

Audio and video connections are not encrypted by PGP Desktop.

The following IM clients are currently supported on Mac OS X: iChat 2.1 and 3.0, AOL Instant Messenger 4.7. Encryption of file transfers and direct connections require iChat 2.1.

PGP Desktop's secure IM feature uses Perfect Forward Secrecy for enhanced security. All keys used to secure your IM sessions are generated at the beginning of the connection and then destroyed when you disconnect; completely new sets of keys are used for every IM session. This adds an extra level of security to your IM sessions.

About the Keys Used for Encryption

A 1024-bit RSA key is generated each time you log onto your IM software, and is destroyed when you log out. This key is used to exchange randomly generated seed data with anyone with whom you communicate. The seed data is combined and hashed to allow each participant in the communication to generate a set of symmetric keys used for that particular communication (one for each direction). The symmetric keys are used to encrypt all the messages with AES256.

Some of that data is also used to generate keyed-hash message authentication code, or HMAC, for each message so that the message integrity can be checked.

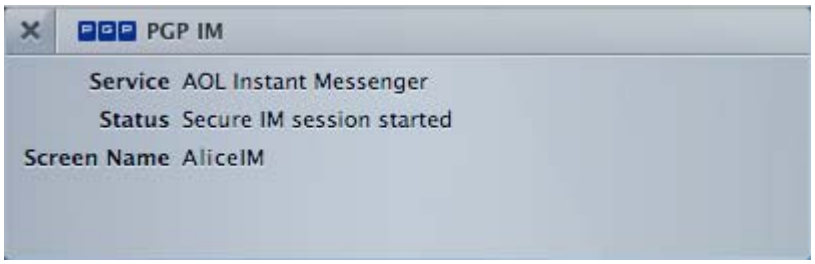
The keys used for secure IM communication are not user configurable.

Encrypting your IM Sessions

Once you have met the conditions described above to support encrypted IM sessions, simply start your IM session normally. Your IM session will be automatically and transparently protected.

There are multiple ways to verify that your IM session is being protected:

- When you log in to your IM client, a notification message appears.



- When the IM session begins, the first message you see from the other user in the session will have extra text appended that says: "Conversation encrypted by PGP Desktop."
- If you open the Messaging Log after you have started your IM session, it will have entries noting that the IM session is being proxied, that the session is being encrypted, and so on.

  For example:

  ```
  2006-09-15 11:39:49 Proxying AIM connection from AliceIM using Apple iChat.

  Initiating PGP Desktop encrypted AIM sessin with JMedinaX using your key with id 0x0910D29E.

  Encrypted AIM session with JMedinaX established.
  ```

6 Using PGP Whole Disk Encryption

Protecting external disks and partitions

You can use the PGP Whole Disk Encryption feature of PGP Desktop to encrypt entire portions of some kinds of external disks or external disk partitions. This section includes the following topics:

About PGP Whole Disk Encryption

You can use the PGP Whole Disk Encryption feature to fully encrypt a Windows-formatted external disk. You can also use it to fully encrypt external Mac OS HFS-type disk partitions. (For more information about HFS-formatted disks, see the Apple Support website: http://www.apple.com/support.)

When you encrypt an entire external disk or external disk partition using the PGP Whole Disk Encryption feature, every sector is encrypted: application files, data files, free space, and temp files.

When you use these encrypted files, they are decrypted and opened automatically as needed. With most modern computers, after the disk is completely encrypted, there is no noticeable slowdown of your activities.

The PGP Virtual Disk feature (formerly called *PGP Disk*) is different from the PGP Whole Disk Encryption feature. PGP Virtual Disks perform like additional volumes on your system that can be locked, even while you are using your computer. These volumes are like a vault where you can store files needing protection. There is no actual physical disk, only the virtual one that the PGP Virtual Disk feature creates and manages. PGP Whole Disk Encryption protects your entire external hard disk or partition. Both products work independently of each other, so you can use them at the same time. For more information, see Chapter 7, Using PGP Virtual Disks.

The PGP Whole Disk Encryption feature protects the contents of the following types of non-boot disks (either partitions, or the entire disk):

- external disks
- removable disks
- USB flash disks

When you shut down a system with an encrypted external boot disk or partition, or if you remove an encrypted removable disk from the system, all files on the disk or partition remain encrypted and fully protected—data is never written to the disk or partition in an unencrypted form. Proper authentication (passphrase or private key) is required to make the files accessible again.

Once you unlock a disk or partition, its files are available to you—as well as anyone else who can physically use your system. Your files are unlocked until you lock them again by shutting down your computer. Use a PGP Virtual Disk volume for files that need to be secured even while your computer is in use. See Chapter 7, Using PGP Virtual Disks.

Authentication Options

When you encrypt an external disk or partition using PGP Whole Disk Encryption, you choose between these two forms of protection:

- **Passphrase**. With passphrase authentication, you specify a passphrase to use when you reboot a computer with an encrypted boot disk or partition, or if you attempt to access any other encrypted disk or partition.
- **Public key**. With public-key authentication, you specify a public key when encrypting an external disk or partition using PGP Whole Disk Encryption. Only the holder of the corresponding private key can access the contents of the disk or partition. To do that, they must provide the passphrase of their private key.

Licensing PGP Whole Disk Encryption

To use the PGP Whole Disk Encryption feature, your copy of PGP Desktop must have a license that supports it. Go to the PGP Corporation website (http://www.pgp.com) for more information about adding the PGP Whole Disk Encryption feature to your license.

Whole Disk Recovery Tokens

In a PGP Universal-managed environment, before encrypting a disk or partition using PGP Whole Disk Encryption, PGP Desktop creates a recovery token that can be used to access the disk or partition in case the passphrase or authentication token is lost.

This recovery token is automatically sent to the PGP Universal Server managing security for the disk or partition protected by PGP Whole Disk Encryption.

If you are in a PGP Universal-managed environment, and you lose the passphrase or authentication token used to protect a disk or partition with PGP Whole Disk Encryption, you should contact your PGP administrator for assistance using the recovery token.

The recovery token can be used only once to access a disk or partition that has been protected using PGP Whole Disk Encryption. After a recovery token is used, the PGP Desktop user is prompted to create a new, different recovery token.

Consider re-encrypting disks or partitions protected by PGP Whole Disk Encryption if security is compromised, by passphrase exposure for example. This process re-encrypts the disk or partition with the same encryption algorithm, but with a different underlying encryption key. The result is as if you decrypted the disk or partition and encrypted it again, but is much faster.

Moving Removable Disks to Other Systems

You can move removable **Windows-formatted** disks to another Mac OS X system that has PGP Desktop 9.5 installed, and access the encrypted files on the other system.

You must be able to authenticate to access the contents of the disk.

To protect a disk using the PGP Whole Disk Encryption feature, you must have the appropriate PGP Desktop license. However, if you have protected a removable Windows-formatted disk with PGP Whole Disk Encryption, you can use that removable disk on another computer with PGP Desktop 9.5 installed—even if the other system does not have a PGP Desktop license that supports Whole Disk Encryption.

Uninstalling PGP Desktop from Encrypted Disks or Partitions

If you have any disks or partitions on your system that are protected by PGP Whole Disk Encryption, these disks or partitions become inaccessible once PGP Desktop is uninstalled.

For this reason, PGP Corporation recommends decrypting any disks or partitions on your system that are protected using PGP Whole Disk Encryption ***prior*** to uninstalling PGP Desktop.

If you do accidentally uninstall PGP Desktop and then cannot access the data on a whole disk encrypted disk or partition, reinstall PGP Desktop to regain access.

Preparing to Encrypt with PGP Whole Disk Encryption

Here are some things to consider before you begin using PGP Whole Disk Encryption:

- The larger the disk or partition being encrypted, the longer the encryption process takes. Other factors that may affect encryption speed are, among others:
  - the size of the disk or partition
  - the processor speed and number of processors
  - the number of system processes running on the computer
  - the number of other applications running on the system
  - the amount of processor time those other applications require

  Generally, with an average system, an 80 GB disk or partition takes approximately three hours to encrypt using PGP Whole Disk Encryption (when no other applications are running). A very fast system, on the other hand, can easily encrypt such a disk or partition in less than an hour.
- Your system is somewhat slower than usual during the encryption process, although it is fully usable. It returns to normal operation when the encryption process is complete.

  PGP Desktop automatically slows the encryption process if you are using the system. The encryption process is faster if you avoid using your computer during the initial encryption.

  If you decide to run other applications during the encryption process, those applications will probably run slightly slower than normal until the encryption process is over.
- You can hide PGP Desktop during encryption. This does not affect the process.
- To stop the encryption process for a short time, use the **Stop** button, then click **Pause** in the dialog box. You need to authenticate after you click **Resume**.
- If you need to shut down your system before the encryption process is over, be sure to pause the process. When you restart, the encryption process resumes where it left off.
- Back up the disk before you encrypt it. Before you encrypt your disk, be sure to back it up so that you won't lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk. Also be sure to make regular backups of your disk.
- Encryption cannot begin on removable disk connected to a laptop computer if the laptop is running on battery power. It **must** be running on AC power. If a laptop computer goes on battery power during the initial encryption process (or a later decryption or re-encryption process) the activity is paused. When AC power is restored, the encryption, decryption, or re-encryption process resumes automatically.

- Regardless of the type of computer you are working with, your system must not lose power, or otherwise shut down unexpectedly, during the encryption process. Do not remove the power cord from the system before the encryption process is over.

Protecting a Disk or Partition with PGP Whole Disk Encryption

Before you encrypt your disk, be sure to back it up so that you won't lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk.

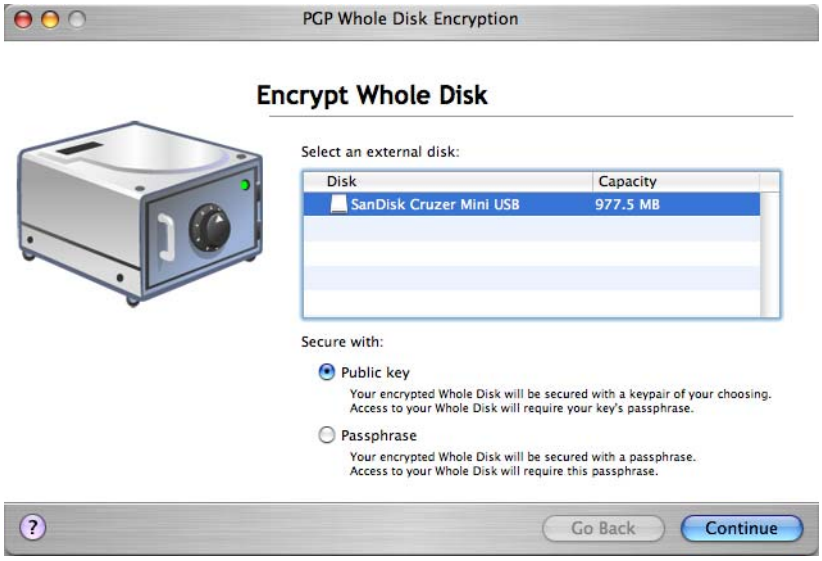
To protect a disk or partition using the PGP Whole Disk Encryption feature:

1 Open PGP Desktop and click on the PGP Disk item.

The **PGP Disk** screen appears.

2 Click **Encrypt a Disk**.

The **Encrypt Whole Disk** screen appears, showing a listing of disks on your system that can be protected.



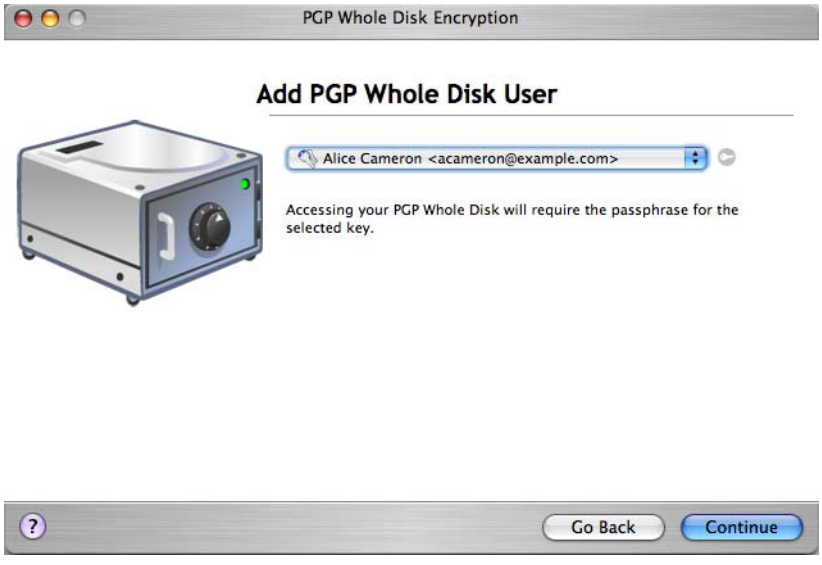
3 From the **Select an external disk** list, click on the disk or partition you want to protect.

4 In the **Secure with** section, specify how you want to access your protected disk or partition:

Public Key User. If you want to protect your disk or partition with a public key:

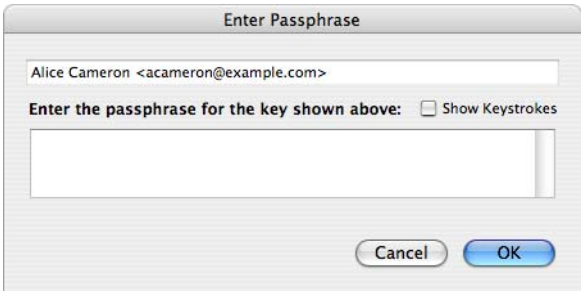
a Select **Public Key**, then click **Continue**.

The **Add PGP Whole Disk User** screen appears.



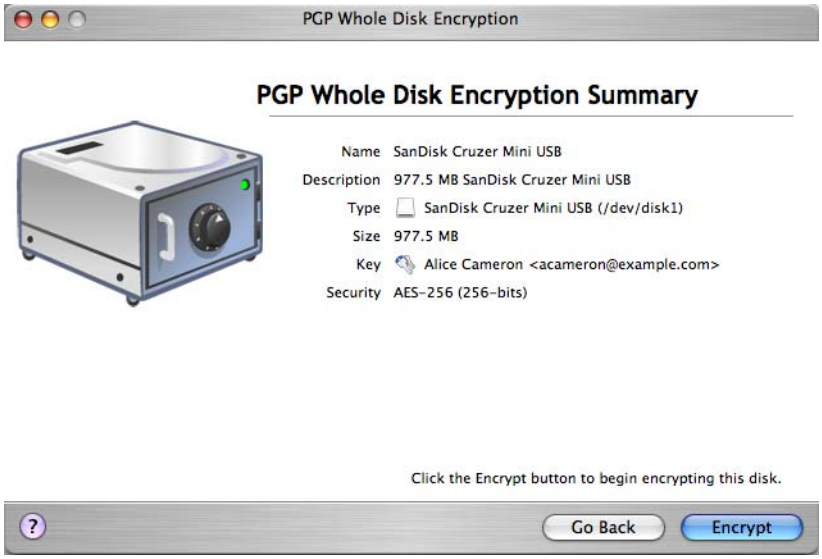
b Select a key from the drop-down list, then click **Continue**.

The **Enter Passphrase** dialog appears.



c Type the passphrase for the key you selected, then click **OK**.

The **PGP Whole Disk Encryption Summary** screen displays, showing you a summary of how your disk is going to be encrypted.



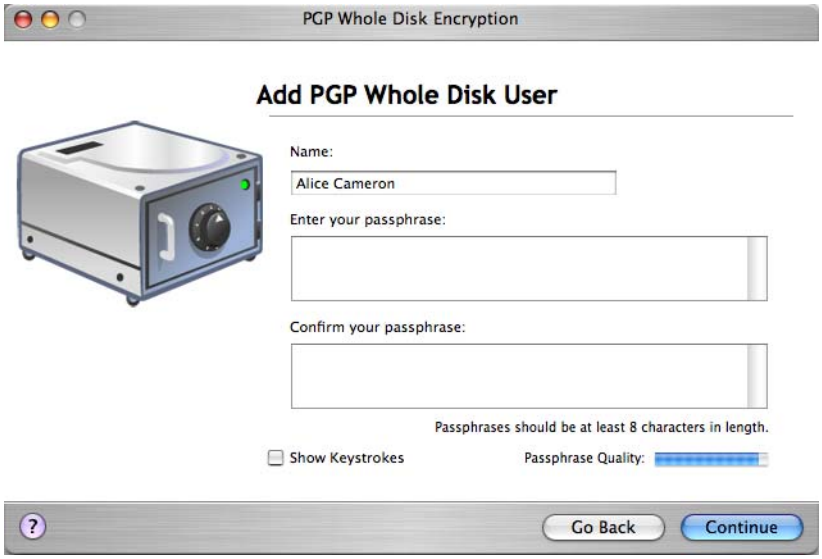
d Review the information, then click **Encrypt.**

The encryption process begins.

Passphrase User. If you want to protect your disk or partition with a passphrase:

a Select **Passphrase,** then click **Continue.**

The **Add PGP Whole Disk User** screen appears.



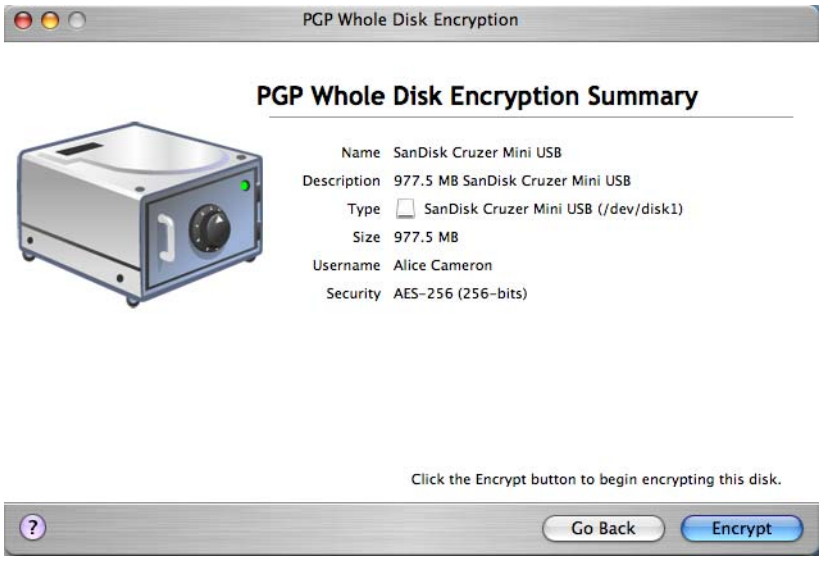
b Type a **Name** (or accept the default name), then type the desired passphrase in the **Enter your passphrase** field, and then type it again in the **Confirm your passphrase** field.

To see your passphrase as you type, select **Show Keystrokes**.

The Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating by comparing the estimated amount of entropy in the passphrase you enter against a true 128-bit random string (the same amount of entropy in an AES128 key). Filling the Passphrase Quality bar should give you a strong passphrase that could take *billions* of years to brute-force decrypt. Refer to "The Passphrase Quality Bar" on page 166 for more information.

c Click **Continue**.

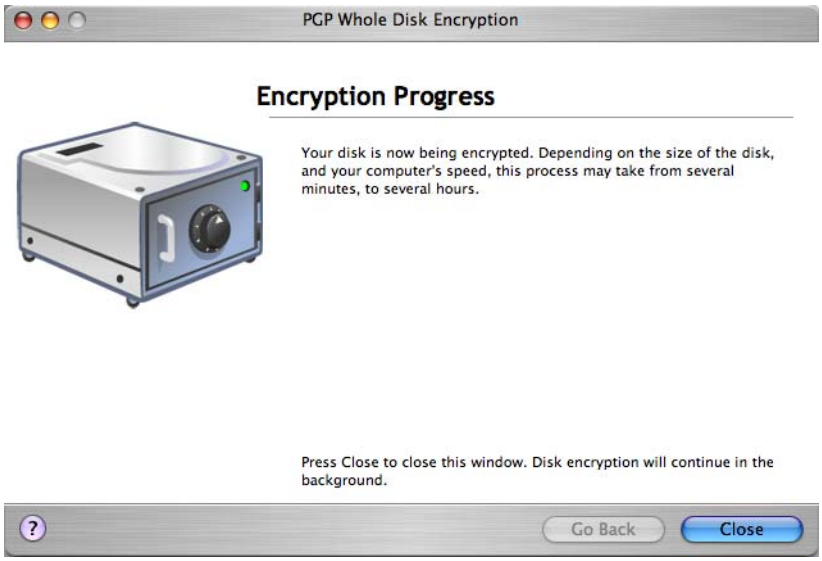
The **PGP Whole Disk Encryption Summary** screen appears, showing you a summary of how your disk is going to be encrypted.



d Review the information, then click **Encrypt.**

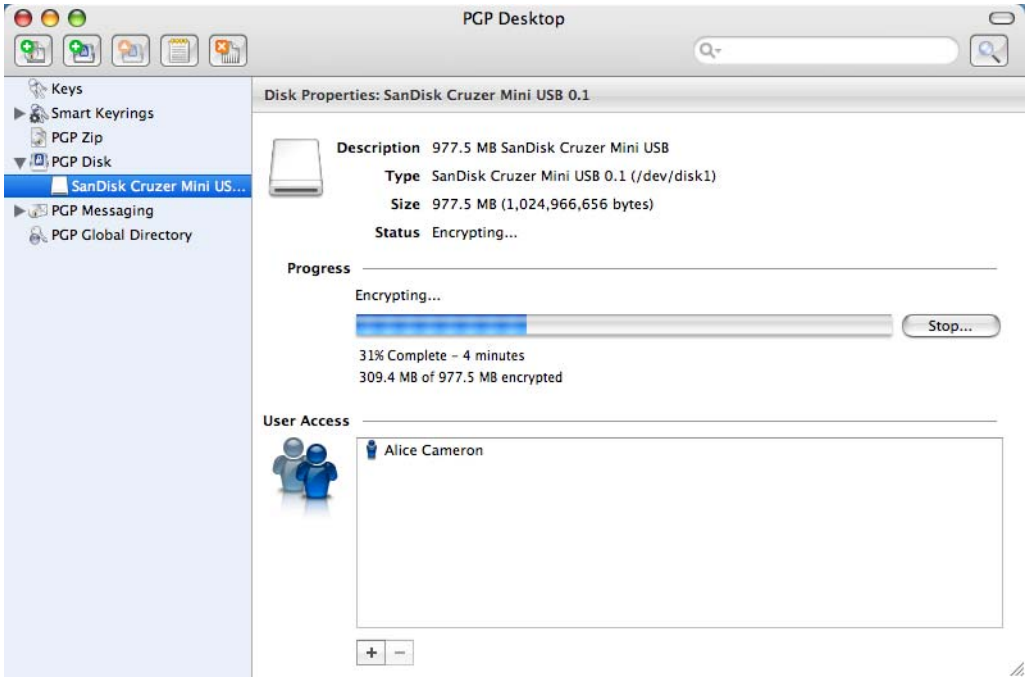
The encryption process begins.

5 The **Encryption Progress** screen appears.



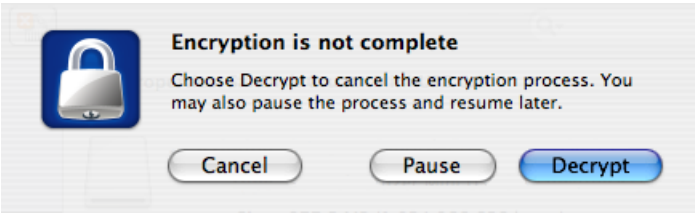
6 Click **Close**.

The PGP Desktop screen appears; the encryption process continues in the background.



7 You can click **Stop** during the encryption process to temporarily stop the process.

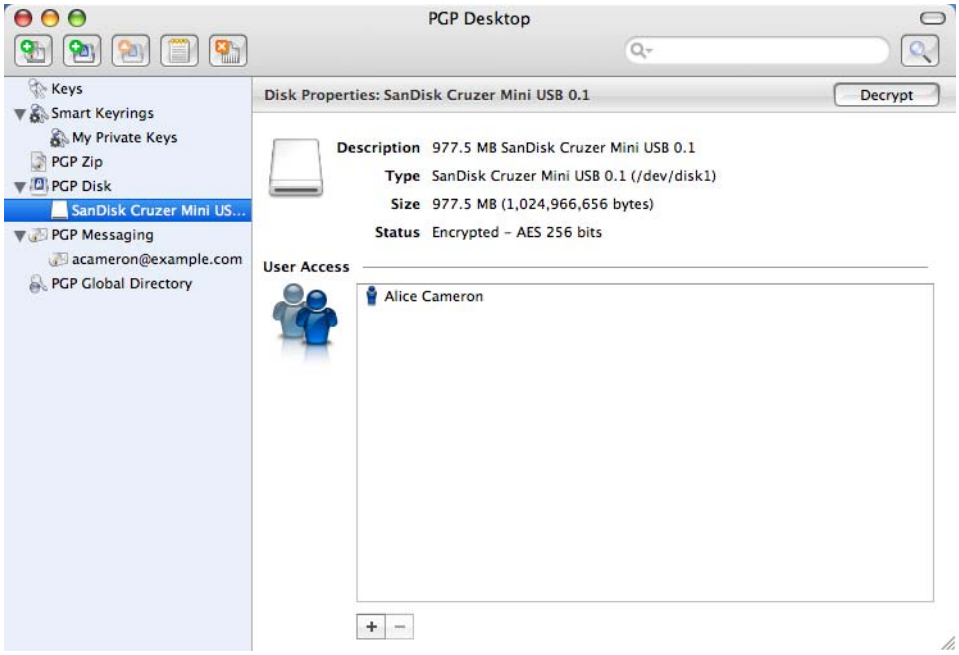
The **Encryption is not complete** dialog appears.



8 You can elect to **Pause** the encryption process, **Decrypt** the portion of the disk/partition that is already encrypted, or **Cancel** to close the dialog and continue with the encryption process.

If the encryption process stops and PGP Desktop indicates a disk read/write error, it means that PGP Desktop has encountered bad sectors on your disk or partition during the encryption process. Immediately reverse the encryption process by *decrypting* the portion of the disk or partition that has been encrypted. Then use your disk verification tools to find and resolve the problem.

When the encryption process completes, the disk properties for the encrypted disk/partition appear.


PGP Desktop
Keys
Smart Keyrings
My Private Keys
PGP Zip
PGP Disk
SanDisk Cruzer Mini US...
PGP Messaging
acameron@example.com
PGP Global Directory
Disk Properties: SanDisk Cruzer Mini USB 0.1
Decrypt
Description 977.5 MB SanDisk Cruzer Mini USB 0.1
Type SanDisk Cruzer Mini USB 0.1 (/dev/disk1)
Size 977.5 MB (1,024,966,656 bytes)
Status Encrypted – AES 256 bits
User Access
Alice Cameron

Adding Users to an Encrypted Disk or Partition

The user who creates an encrypted disk or partition can make it available to others. These additional users can access the encrypted disk or partition using their own unique passphrase or private key.

Having multiple users who can access a disk or partition protected by PGP Whole Disk Encryption serves as a backup in case one person forgets their passphrase. Users configured for an encrypted disk or partition can authenticate to the PGP Whole Disk Encryption log-in screen to unlock any protected disk or partition on that system.

To add additional users to a disk or partition protected by PGP Whole Disk Encryption:

1. Select the encrypted disk or partition to which you want to add another user.
2. Click the plus sign icon (**+**) below the **User Access** list.
3. Select **Add Public Key User** or **Add Passphrase User**, from the list that appears.

   If you select **Add Public Key User**, you are prompted to select the public key of the user(s) you want to add.

   a. Drag the users you want to add from the **Key Source** column into the **Keys to Add** column, then click **OK**.

      You are prompted for the passphrase of the encrypted disk.

   b. Enter the passphrase of the encrypted disk, then click **OK**.

      The specified public key user(s) is added.

   If you select **Add Passphrase User**, you are prompted for a username and a passphrase for the user you want to add.

   a. In the **Username** field, enter a username for the user you are adding.

   b. In the **Enter a passphrase for this user** field, enter a passphrase.

   c. In the **Confirm user's passphrase** field, enter the same passphrase again.

      To see your passphrase as you type, select **Show Keystrokes**.

   d. Click **OK**.

      You are prompted for the passphrase of the encrypted disk.

   e. Enter the passphrase of the encrypted disk, then click **OK**.

      The specified passphrase user is added.

Deleting Users From an Encrypted Disk or Partition

At some point you may want to remove the ability of a user to access an encrypted disk or partition.

To remove a user from an encrypted disk or partition:

1. Select the encrypted disk or partition from which you want to remove a user.
2. From the **User Access** list, select the name of the user you want to remove.
3. Click the minus sign icon (**–**) below the **User Access** list.

   You are prompted for the passphrase of the encrypted disk.
4. Enter the passphrase of the encrypted disk, then click **OK**.

   The alternate user is removed.

You cannot remove all users from an encrypted disk or partition; when only one user is listed in the User Access list, you cannot remove that user.

Changing User Passphrases

To change the passphrase of a passphrase user on an encrypted disk or partition:

1. Select the encrypted disk or partition with the user whose passphrase you wish to change.
2. In the **User Access** list, either Ctrl-click the user's name or right-click it if you have a two-button mouse.
3. From the context menu that appears, select **Change User Passphrase.**

   You are prompted for the passphrase of the encrypted disk.
4. Enter the passphrase of the encrypted disk, then click **OK**.

   The **Confirm Passphras**e screen appears.
5. Type a new passphrase in the **Enter your new passphrase** box, move to the **Confirmation** box and type the new passphrase again, then click **OK**.

   The passphrase is changed.

Viewing Key Information

To view key information of a public key user on an encrypted disk or partition:

1. Select the encrypted disk or partition with the public key user whose key information you wish to view.
2. In the **User Access** list, either Ctrl-click the user's name or right-click it if you are have a two-button mouse.
3. From the context menu that appears, select **Show Key Info.**

   The **Key Info** screen for the specified key appears.

Re-Encrypting an Encrypted Disk or Partition

Consider re-encrypting a protected disk or partition that you suspect of having a passphrase that has been compromised.

To re-encrypt a disk or partition, the PGP Whole Disk Encryption feature uses the same encryption algorithm (AES256)—but a different underlying encryption key—to encrypt the disk or partition again. The result is as if you decrypted the disk or partition and encrypted it again, but much faster.

To re-encrypt an encrypted disk or partition:

1. Select the encrypted disk or partition you would like to re-encrypt.
2. From the **Disk** menu, select **Re-Encrypt Disk**.

   You are prompted for the passphrase of the encrypted disk.
3. Enter the passphrase of the encrypted disk, then click **OK**.

   The re-encryption process begins.

Special Security Precautions Taken by PGP Desktop

PGP Desktop has features that help avoid security problems with the PGP Whole Disk Encryption feature. These precautions also apply to PGP Virtual Disk volumes.

Passphrase Erasure

When you enter a passphrase, PGP Desktop uses it only for a brief time, then erases it from memory. PGP Desktop also avoids making copies of the passphrase. The result is that your passphrase typically remains in memory for only a fraction of a second. Without this critically important feature, someone could search for your passphrase in your computer memory while you were away from the system. You would not know it, but they would then have full access to data protected by this passphrase.

Virtual Memory Protection

Your passphrase or other keys could be written to disk as part of the virtual memory system swapping memory to disk. PGP Desktop takes care that the passphrases and keys are never written to disk. This feature prevents a potential intruder from scanning the virtual memory file looking for passphrases.

Memory Static Ion Migration Protection

When you protect a disk or partition with PGP Whole Disk Encryption, your passphrase is turned into a key. This key is used to encrypt and decrypt the data on the encrypted disk or partition. While the passphrase is erased from memory immediately, the key (from which your passphrase cannot be derived) remains in memory.

This key is protected from virtual memory; however, if a certain section of memory stores the exact same data for extremely long periods of time without being turned off or reset, that memory tends to retain a static charge, which could be read by attackers. If your encrypted disk or partition is decrypted for long periods, over time, detectable traces of your key could be retained in memory. Devices exist that could recover the key. You won't find such devices at your neighborhood electronics shop, but major governments are likely to have a few.

PGP Desktop protects against this by keeping two copies of the key in RAM, one normal copy and one bit-inverted copy, and inverting both copies every few seconds.

Other Security Considerations

In general, the ability to protect your data depends on the precautions you take, and no encryption program can protect you from sloppy security practices.

For instance, if you leave your computer on with sensitive files open when you leave your desk, anyone can access that information—even if the disk or partition is protected using PGP Whole Disk Encryption.

Here are some tips for maintaining optimal security:

- Make sure that you save and close files on an encrypted disk or partition when you leave your computer. The contents are safely encrypted until you are ready to access the file again.
- When you are away from your desk, use a screen saver with a password to deter others from accessing your computer or viewing your screen.
- Make sure that your encrypted disks or partitions are not available to other computers on a network. You may need to arrange this with the network management staff within your organization. Once you have unlocked your disk or partition, PGP Whole Disk Encryption can no longer protect the files. They can be seen by anyone with network access to them. Consider the PGP Virtual Disk feature for storing files that need to be locked even while you are using your computer.
- Never write down your passphrase. Pick something you can remember. If you have trouble remembering your passphrase, use something to jog your memory, such as a poster, a song, a poem, or a joke—just do not write it down.
- If you use PGP Desktop at home and share your computer with other people, they will probably be able to see your open files on a disk or partition that is protected using PGP Whole Disk Encryption. As long as you shut down a system with a whole disk encrypted external boot disk or partition, or if you remove an encrypted removable disk from the system, all files on the disk or partition remain encrypted and fully protected.

7 Using PGP Virtual Disks

Creating a protected area on your computer

This chapter describes the PGP Virtual Disk feature of PGP Desktop. These topics are available in this chapter:

Overview

A PGP Virtual Disk is an area of space, on any disk connected to your computer, that is set aside and encrypted. PGP Virtual Disks are much like a bank vault, and are very useful for protecting sensitive files while the rest of your computer is unlocked for work.

PGP Virtual Disks were called *PGP Disks* in previous versions of PGP Desktop. The phrase *PGP Disk* now includes both the PGP Virtual Disk and the PGP Whole Disk Encryption features.

If you are using PGP Desktop in a PGP Universal-managed environment, you may be required to create a PGP Virtual Disk after installing PGP Desktop. If so, the size, filesystem, and algorithm may have been specified. Refer to Appendix C, PGP Desktop and PGP Universal for more information.

A PGP Virtual Disk looks and acts like an additional hard disk, although it is actually a single file that can reside on any of your computer disks. It provides storage space for your files—you can even install applications, or save files to a PGP Virtual Disk—but it can also be locked at any time without affecting other parts of your computer. When you need to use the applications or files that are stored on a PGP Virtual Disk, you can unlock the disk and make the files accessible again.

PGP Virtual Disks are unlocked and locked by mounting and unmounting them from your computer. PGP Desktop helps manage this operation for you.

Although you can specify a fixed size for your PGP Virtual Disk, you can also create a dynamically-sizing disk, one that grows larger as needs require it. The size you specify when you are creating the disk is the maximum size the disk can become.

When a PGP Virtual Disk is mounted, you can:

- Move/copy files into or out of the mounted PGP Virtual Disk.
- Save files to the mounted PGP Virtual Disk.
- Install applications within the mounted PGP Virtual Disk.

Files and applications on a PGP Virtual Disk are stored encrypted. If your computer crashes while a PGP Virtual Disk is mounted, the contents remain safely encrypted.

When a PGP Virtual Disk is unmounted, it does not appear within the Mac OS X Finder, and it is inaccessible to anyone without proper authentication.

For information about the PGP Options that affect PGP Virtual Disk volumes, see "Disk Preferences" on page 159.

Creating a New PGP Virtual Disk

To create a new PGP Virtual Disk:

1 Open PGP Desktop and select the **PGP Disk** item.

The **PGP Disk** screen appears.

2 Click **New PGP Virtual Disk.**

The New PGP Disk screen appears.

3 In the **Enter your desired PGP Disk size** field, type the amount of space that you want to reserve for the new PGP Virtual Disk. Use whole numbers, with no decimal places. You can also use the arrows to increase or decrease the number displayed in the field. Choose **KB** (Kilobytes), **MB** (Megabytes), or **GB** (Gigabytes) from the menu.

4 Specify the type of authentication you want to use for the primary user of this PGP Virtual Disk:

- **Public key**. If you want to protect your PGP Virtual Disk with your keypair, select **Public Key**.
- **Passphrase user.** If you want to protect your PGP Virtual Disk with a passphrase, select **Passphrase user**.

5 If you want to view or change the advanced options settings, select the Advanced Options checkbox.

The **Automatically resize PGP Virtual Disk as necessary** checkbox appears, as well as the **Cipher** and **Format** menus.

The default **Advanced Options** settings are appropriate for most users. Avoid changing these settings if you are unfamiliar with them.

6 Select the **Automatically resize PGP Virtual Disk as necessary** checkbox if you want PGP Desktop to manage the size of the new **PGP Virtual Disk** automatically. As you add or delete files, the disk size changes appropriately.

You can only select (or not select) the **Automatically resize PGP Virtual Disk as necessary** option when you are creating a PGP Virtual Disk. Once the disk is created, you can neither change a PGP Virtual Disk from a fixed disk to a resizable one, or vice-versa.

7 From the **Cipher** menu, select the encryption algorithm that you would like to use to protect your PGP Virtual Disk:

- **AES-256 (256 bits)**
- **CAST5 (128-bits)**.

Refer to "The PGP Virtual Disk Encryption Algorithms" on page 85 for more information about these encryption algorithms.

8 From the **Format** menu, select the disk format that you would like to use with your PGP Virtual Disk:

- **MS-DOS**. Use if you intend to share this PGP Virtual Disk with someone using PGP Desktop 9.5 for Windows.
- **Mac OS Extended**. The default format (also the modern Mac OS file-system format); supports large PGP Virtual Disk volumes. The minimum size is 4 MB. The Mac OS Extended format is also called HFS+.

- **Mac OS Extended (Journaled)**. Use if Journaling is enabled on your system. (Journaling causes a copy of everything written to disk to be written a second time in a private area of the filesystem, making disk recovery easier if necessary.)
- **Mac OS Extended (Case-sensitive, Journaled)**. Use if case-sensitive Journaling is enabled on your system.
- **Mac OS Standard**. For backwards compatibility with older Mac OS operating systems. The minimum size is 512 KB.
- **UNIX File System**. Use if you intend to share this PGP Virtual Disk volume with someone using a UNIX file system. The minimum size is 128 KB.

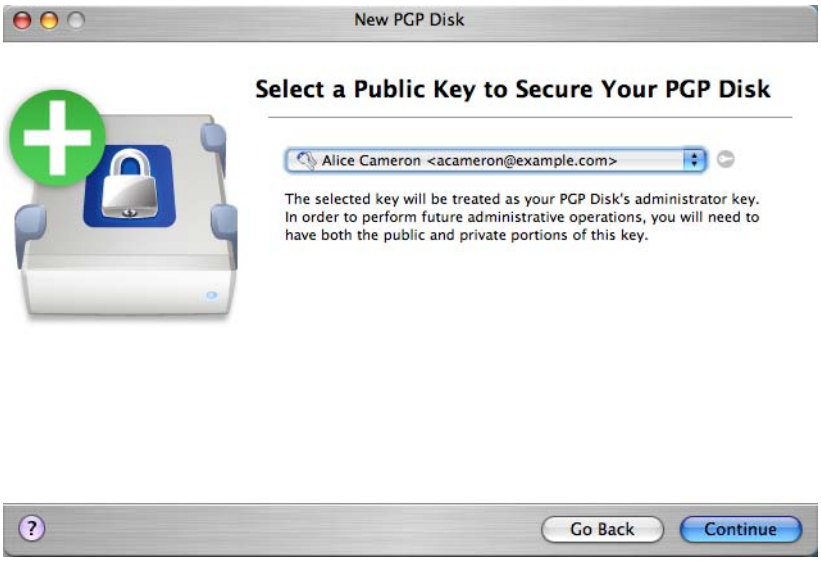
You can see format of an existing Mac OS X drive by selecting the drive, then selecting **Get Info** from the **File** menu.

9 Click **Continue**.

10 The next step depends on whether you chose public key or passphrase authentication.

For public key access:

a The **Select a Public Key to Secure Your PGP Disk** screen appears, displaying the public keys you can use for authenticating to the PGP Virtual Disk that you are creating.

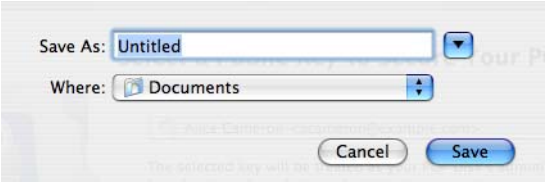


b Select a key from the list, then click **Continue**.

You are prompted for the passphrase of the key you selected (unless the passphrase is already cached, in which case this step is skipped).

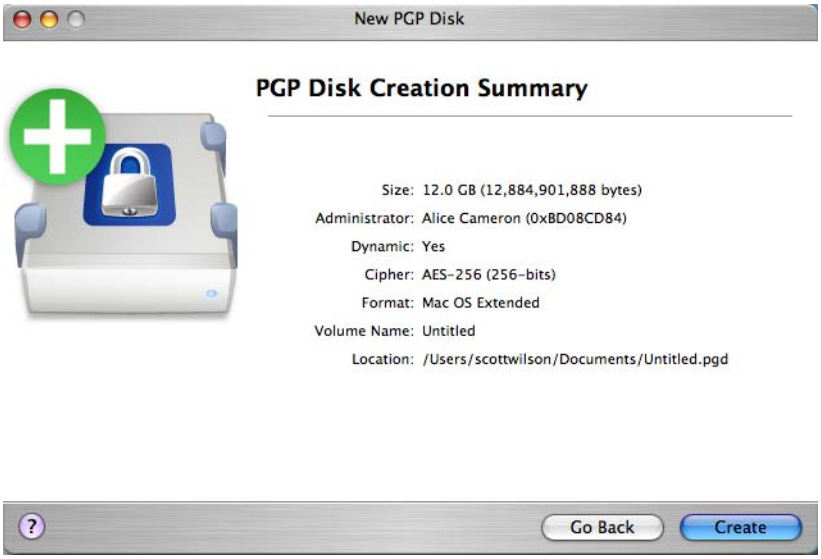
c Enter the appropriate passphrase, then click **OK**.

The **Save As** dialog appears.



d Select a file name and location for the PGP Virtual Disk, then click **Save.**

The **Summary** screen appears.



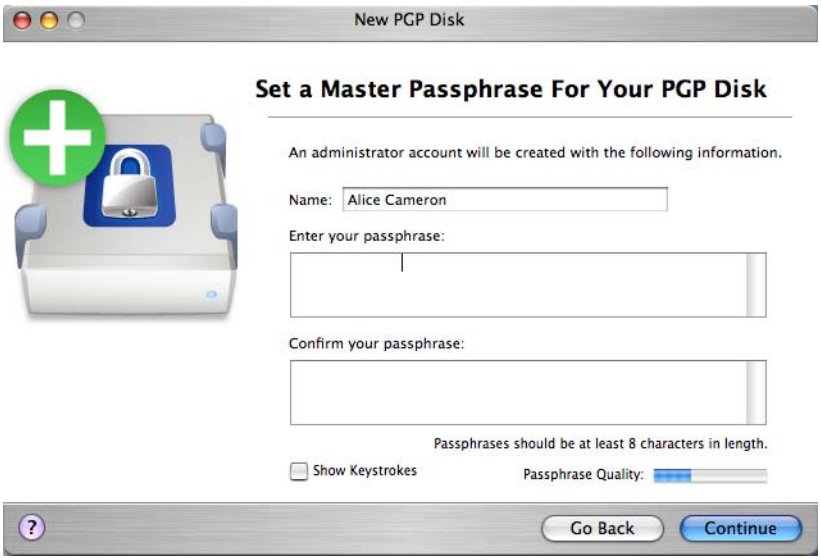
e Review the information on the PGP Disk Creation Summary screen. When you are finished, click **Create**.

The **Congratulations** screen appears.

f Click **Finish**.

For passphrase access:

a The **Set a Master Passphrase For Your PGP Disk** screen appears.



b In the **Name** field, type the name that you would like to assign to the primary PGP Virtual Disk user (or administrator).

c In the **Enter your passphrase** field, type the passphrase that you would like to use.

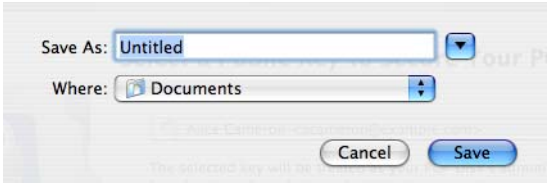
The **Passphrase Quality** bar indicates the strength of the passphrase that you have typed.

Select the **Show Keystrokes** checkbox if you would like to see the characters that you are typing, and you are certain that no one else can see what you are typing.

d In the **Confirm your passphrase** field, re-type the passphrase that you would like to use.

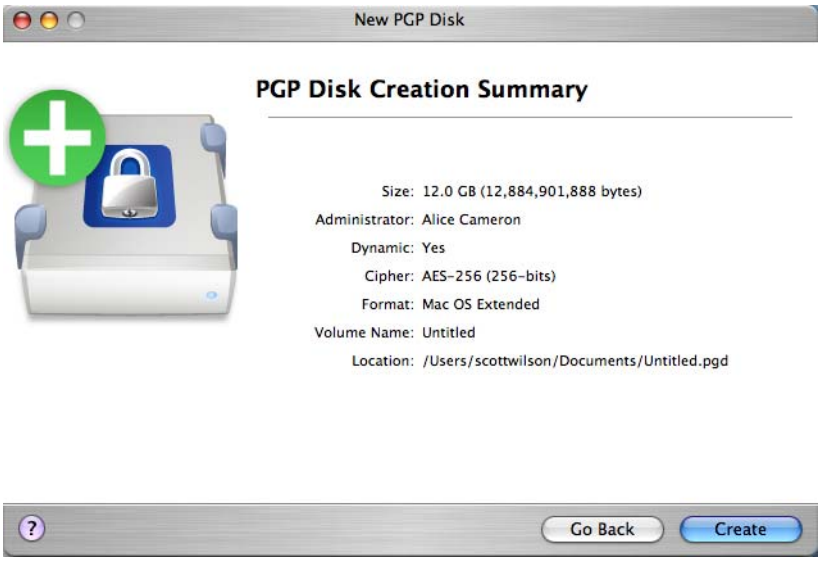
e Click **Continue.**

The **Save As** dialog box appears.

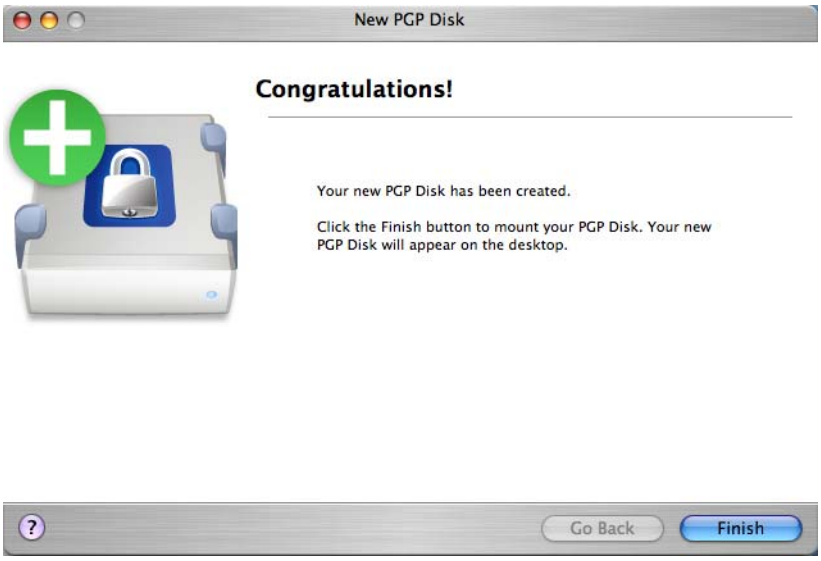


f Select a file name and location for the PGP Virtual Disk, then click **Save**.

g Review the information on the **PGP Disk Creation Summary** screen. When you are finished, click **Create**.



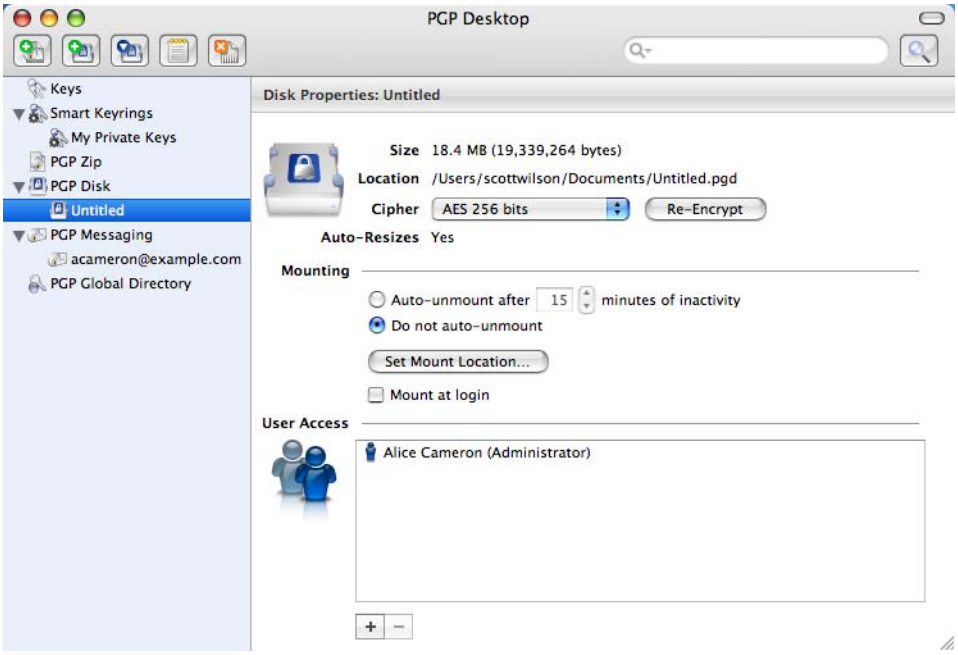
The **Creating your PGP Virtual Disk** screen appears, showing you progress as your PGP Virtual Disk is created. Once the disk is created, the **Congratulations** screen appears.



h Click **Finish**.

11 Your new PGP Virtual Disk is mounted automatically, and information about it appears in a Finder window.

The name of the disk also appears under the **PGP Disk** item.



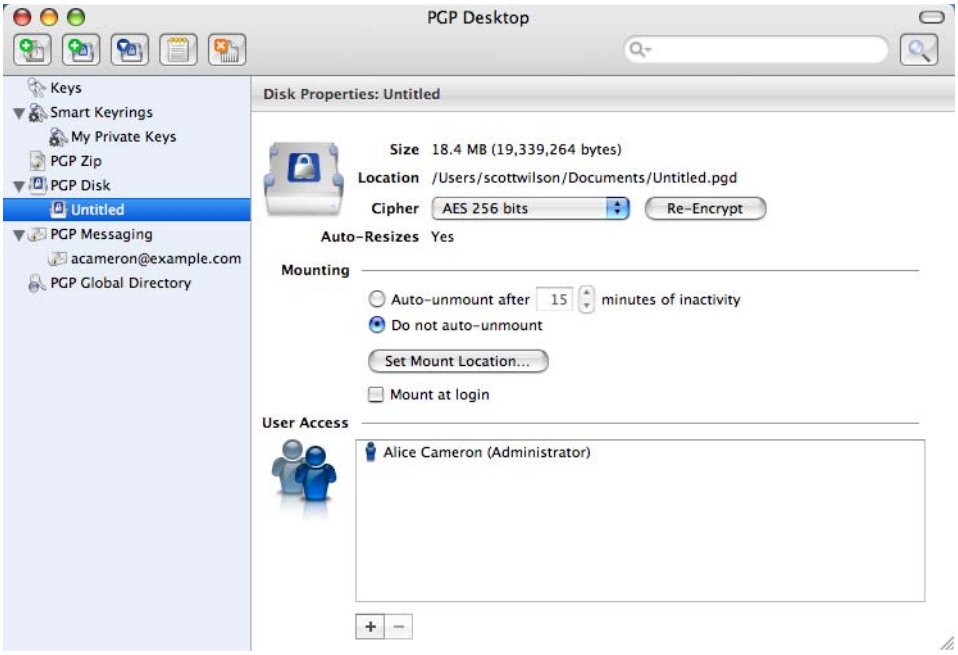
Viewing Properties of a PGP Virtual Disk

Once a PGP Virtual Disk has been created, there is information about the disk and settings you can change that are accessible from the Disk Properties screen.

To view the properties of a PGP Disk volume:

1 Click on the name of the disk in the **PGP Disk** item.

The Disk Properties screen appears.



Mounting a PGP Virtual Disk

When you create a new PGP Virtual Disk, it is automatically mounted so you can begin using it to store your files.

To secure the contents of a volume, you must unmount it. Once a volume is unmounted, its contents remain secured in an encrypted file where they are inaccessible until the volume is mounted once again.

There are several ways to mount a PGP Virtual Disk:

- On the Disk Properties screen for a PGP Virtual Disk, enable **Mount at login**. The PGP Virtual Disk will automatically mount at startup.
- Select the PGP Virtual Disk you want to mount under the PGP Virtual Disk item, then from the **Disk** menu select **Mount**.
- Click the **Mount Disk** icon on the Toolbar.
- In the Finder, Ctrl-click the PGP Disk volume file, or right-click if you are using a two button mouse, then from the context menu that appears select **PGP > Mount**.

Mounted PGP Virtual Disk volumes appear as empty drives in the Finder.

Using a Mounted PGP Virtual Disk

You can create, copy, move, and delete files and folders on a PGP Virtual Disk, just as you normally do with any other disk on your system.

Anyone else who has access to the volume (either on the same computer or over the network) can also access the data stored there. It is not until you unmount the volume that the data is protected.

Although each PGP Virtual Disk file is encrypted and cannot be accessed by anyone without proper authorization, it can still be deleted from your system. Anyone with access your system could delete the encrypted file containing the PGP Virtual Disk. For this reason, keeping a backup copy of the encrypted file is an excellent safety measure, as is keeping your computer locked when you step away from it.

Unmounting a PGP Virtual Disk

You lock a PGP Virtual Disk by unmounting it. Once a PGP Virtual Disk is unmounted, its contents are locked in the encrypted file associated with the volume. Its contents are inaccessible until the volume is mounted once again.

There are several ways to unmount a PGP Virtual Disk volume:

- Select the PGP Virtual Disk you want to mount under the **PGP Disk** item, then from the **Disk** menu select **Unmount**.
- Click the **Unmount Disk** icon on the Toolbar.
- In the Finder, Ctrl-click (or right-click if you are using a two-button mouse) the PGP Virtual Disk file, then from the context menu that appears select **PGP > Unmount**.
- Drag the icon of the mounted PGP Virtual Disk volume to the **Trash**.

Adding Alternate User Accounts to a PGP Virtual Disk

The administrator of a PGP Virtual Disk can make it available to other users. Those users can access the volume using their passphrases or private keys.

To add alternate user accounts to a PGP Virtual Disk:

1. Under the PGP Disk item, click the name of the PGP Virtual Disk to which you want to add an alternate user.
2. Click the plus-sign icon under the User Access list of the Disk Properties screen; select **Add Public Key User** or **Add Passphrase User,** depending on what kind of alternate user account you want to add.

   If you clicked **Add Public Key User**

   a. Select the public key of the alternate user you want to add by dragging their key from the **Key Source** column to the **Keys to Add** column.

      You can add multiple alternate users if you like.

   b. Click **OK**.

      The **Disk Properties** screen re-appears; the alternate public-key user appears in the **User Access** list.

   If you clicked **Add Passphrase User**:

   a. Select the public key of the alternate user you want to add by dragging their key from the **Key Source** column to the **Keys to Add** column.

The **Add a user to your PGP Disk** dialog appears.

b In the **Name** field, type a name for the alternate user you are adding.

c In the **Enter a passphrase for this user** field, type a passphrase for the user.

d In the **Confirm user's passphrase** field, re-type the passphrase.

The **Passphrase Quality** bar indicates the strength of the passphrase that you have typed.

e Select the **Show Keystrokes** checkbox if you would like to see the characters you are typing.

f Click **OK**.

The **Disk Properties** screen re-appears; the alternate passphrase user appears in the **User Access** list.

Deleting Alternate User Accounts From a PGP Virtual Disk

At some point you may want to remove the ability of an alternate user to access a PGP Virtual Disk.

To remove an alternate user account from a PGP Virtual Disk:

1. Under the **PGP Disk** item, click the name of the PGP Virtual Disk from which you want to remove an alternate user.
2. In the **User Access** list, select the alternate user you wish to remove.

   You cannot remove the Administrator.
3. Click the minus-sign icon under the **User Access** list.

   A confirmation dialog appears.
4. Click **Remove**.

   The alternate user is deleted.

Disabling Alternate User Accounts

To prevent access to a PGP Virtual Disk for an alternate user without deleting their account entirely, you can instead temporarily disable their access.

To disable an alternate user account from a PGP Virtual Disk:

1. Under the **PGP Disk** item, click the name of the PGP Virtual Disk with the alternate user you want to disable.
2. In the **User Access** list, select the alternate user you wish to disable.

You cannot disable the Administrator.

3 From the **Disk** menu, select **Disable User**.

A confirmation dialog appears.

4 Click **Disabled**.

The alternate user is disabled. They appear in the User Access list greyed out.

Changing Read/Write and Read-Only Status

Users of a PGP Virtual Disk can have either full read/write privileges, or read privileges only. You can change these privileges for a user at any time.

To change privileges for a user of a PGP Virtual Disk:

1 Select the **PGP Disk** control box on the left pane of the PGP Desktop main screen, then select the appropriate PGP Virtual Disk.

2 Make sure the selected PGP Virtual Disk is **not** mounted. You cannot toggle privileges if the volume is mounted.

3 In the User Access list, select the name of the alternate user whose read/write status you want to change.

4 The next step depends on the current status of the user. From the **Disk** menu select:

- **Set Read-Only Access** to change the user read-only access.
- **Allow Write Access** to change the user to read/write access.

The **Enter Passphrase** dialog box appears.

5 Type the passphrase for the PGP Virtual Disk administrator, then click **OK**.

The privileges of the selected user are changed.

Granting Administrator Status to an Alternate User

You can change the status of a user account from alternate to administrator:

1 Select the **PGP Disk** control box on the left pane of the PGP Desktop main screen, then select the appropriate PGP Virtual Disk volume.

2 From the **Disk** menu, select **Set as Disk Administrator.**

You can also Ctrl-click (or right-click if you have a two-button mouse) and select **Set as Disk Administrator** from the context menu.

The **Enter Passphrase** dialog box appears.

3 Type the passphrase for the PGP Virtual Disk administrator, then click **OK**.

The selected user account is changed to administrator.

You can only grant Administrator status to one user account at a time. By granting Administrator status to one account, you also remove it from another.

Changing User Passphrases

To change a user passphrase for a PGP Virtual Disk:

1. Select the **PGP Disk** control box on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk on which you are a user.
2. Select the name of a passphrase user from the User Access list, then select **Change User Passphrase** from the **Disk** menu.

   You can also Ctrl-click (or right-click if you have a two-button mouse) and select **Change User Passphrase** from the context menu.

   The **Enter Passphrase** dialog box appears.
3. Type the passphrase for the PGP Virtual Disk administrator, then click **OK**.
4. Type a new passphrase, move to the **Confirmation** box and enter the same passphrase again, then click **OK**.

   The passphrase is changed.

Set Mount Location

You can specify where the PGP Virtual Disk is mounted (located):

1. Select the **PGP Disk** control box on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk for which you want to set the mount location.
2. Click **Set Mount Location**.

   The **Set your PGP Disk's mount point** dialog box appears.
3. Select:

   – **Desktop (Default)**. Select this option to mount your PGP Disk volume on the Desktop. This is where the PGP Virtual Disk is mounted if you do not specify another location.

   – **At the following location**. Select this option to mount your PGP Virtual Disk at a location that you specify. Click **Browse,** then navigate to the location at which you would like your PGP Virtual Disk mounted. Click **Open** to confirm your choice.
4. Click **OK**.

The mount location for your PGP Virtual Disk is established.

Re-Encrypting PGP Virtual Disks

You can re-encrypt all data stored on a PGP Virtual Disk. You might do this for either (or both) of two reasons:

- You want to change the encryption algorithm currently being used to protect the volume.
- You suspect there has been a security breach.

With re-encryption, you can encrypt your PGP Virtual Disk again, but with a different underlying encryption key.

Adept users may be able to search the memory of a computer for the underlying encryption key of a PGP Virtual Disk. They could use the key to access the volume even after being removed from the user list. Re-encrypting the disk changes this underlying key and prevents this kind of intrusion.

To re-encrypt a PGP Virtual Disk:

1. Select the **PGP Disk** control box on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk that you want to re-encrypt.
2. If the PGP Virtual Disk is mounted, unmount it.
3. Click **Re-Encrypt**.

   A confirmation dialog box displays.
4. Review the information it contains, then click **Re-Encrypt.**

   The **Enter Passphrase** dialog box appears.
5. Type the passphrase for the PGP Virtual Disk administrator, then click **OK**.

   The PGP Disk is re-encrypted. A progress bar appears during the process.
6. When the current status displays Done, click **Next**.
7. Click **Finish** to complete the re-encryption process.

Deleting PGP Virtual Disks

At some point you may decide you no longer need a particular PGP Virtual Disk.

When you delete a PGP Virtual Disk, all data on it is also deleted. **There is no way to retrieve the data once you delete a PGP Virtual Disk.** Make sure that you have copied any data that you wish to save to another location **before deleting a PGP Virtual Disk.**

To delete a PGP Virtual Disk:

1. In PGP Desktop, Ctrl-click (or right-click if you have a two-button mouse) the PGP Disk you want to delete.
2. Select **Reveal in Finder** from the contextual menu.

   A Finder window appears with the PGP Virtual Disk file selected. If you have opted to have Mac OS X display file extensions, the PGP Virtual Disk is a .pgd file.
3. Drag the file to the Trash, then select **Empty Trash** from the File menu in the Finder.
4. In PGP Desktop, Ctrl-click (or right-click if you have a two-button mouse) the PGP Disk volume you want to delete and select **Clear** from the contextual menu.

   The PGP Disk is deleted from your system, as well as from PGP Desktop.

Maintaining PGP Virtual Disks

This section describes how to take proper care of the PGP Virtual Disks that you use with your computer.

Mounting PGP Virtual Disks on a Remote Server

You can place PGP Virtual Disk volumes on a Windows or UNIX remote server. The volumes can then be mounted by anyone with a Mac OS X system and PGP Desktop.

The first person to mount the PGP Virtual Disk locally has read-write access to the disk. No one else is then able to access the disk. If you want others to be able to access files within the volume, you must mount the volume in read-only mode (applies to FAT and FAT32 filesystem formats only). All users of the volume then have read-only access.

If the PGP Virtual Disk volume is stored on a Windows server, you can also mount the volume remotely on the server and allow people to share the mounted volume. However, this action provides no security for the files within the volume.

Backing up PGP Virtual Disk Volumes

Backing up the contents of your PGP Virtual Disk is the best way to safeguard your information from hardware failure or other loss.

It is not advisable to back up the contents of a mounted (and therefore, decrypted) PGP Virtual Disk just as you would any other volume. The contents are not encrypted, and are accessible to anyone who can restore the backup. Instead, instead make a backup copy of the encrypted volume.

To back up PGP Virtual Disks in encrypted form:

1. Unmount the PGP Virtual Disk.
2. In the Finder, locate the PGP Virtual Disk file. If you have opted to have Mac OS X display file extensions, the PGP Virtual Disk filename ends with.pgd.

   You can find the PGP Virtual Disk file easily by Ctrl-clicking (or right-clicking if you have a two-button mouse) the disk in the PGP Disk of the PGP Desktop side panel. Select **Reveal in Finder** from the contextual menu that appears.
3. Copy the unmounted encrypted PGP Virtual Disk file to a CD, DVD, tape, removable cartridge, or floppy disk just as you would any other file.

Even if some unauthorized person has access to the backup, they cannot decipher its contents.

When making backups of encrypted PGP Virtual Disk files, keep these issues in mind:

- Backing up encrypted files to a network drive gives others plenty of opportunity to guess at a weak passphrase. It is much safer to back up only to devices over which you have physical control.
- A lengthy, complicated passphrase helps further improve the security of your data.
- If you are on a network, make sure that any network back up system does not back up the files from your **mounted** PGP Virtual Disk. (You may need to discuss this with your System Administrator.) Once a PGP Virtual Disk is mounted, its files are decrypted and can be copied to a network backup system that vulnerable state.

Exchanging PGP Virtual Disks

You can exchange PGP Virtual Disks with other users who have PGP Desktop installed on their computers. You do that by sending them a copy of the PGP Virtual Disk data file, which contains the encrypted data. Here are some of the ways you might exchange PGP Virtual Disks:

- As mail attachments
- On a removable disk or CD
- Over a network

Once the other user has the PGP Virtual Disk file, they can mount it on a system running PGP Desktop and use the correct passphrase to access it. If the volume was encrypted to their public key, they use their private key for access.

Public key is the most secure protection method when adding alternate users to a PGP Virtual Disk because: (1) You don't need to exchange a passphrase with the alternate user which, depending on your method, could be intercepted or overheard. (2) The alternate user doesn't need to memorize another passphrase which could be forgotten. (3) It is easier to manage a list of alternate users if each uses their own private key to unlock the volume.

About PGP Virtual Disk Volumes

You can use PGP Virtual Disks to organize your work, keep similarly named files separate, or keep multiple versions of the same documents or programs separate.

Although the PGP Virtual Disks you create with PGP Desktop function just as any other volume you are accustomed to working with, the data is actually stored in one large encrypted file. Only when you mount the file are its contents presented in the form of a volume.

It is important to realize that all your data remains secure in the encrypted file and is only deciphered when you access one of the files. Having the data for a volume stored in this manner makes it easy to manipulate and exchange PGP Virtual Disks with others but it also makes it easier to lose data if the file is somehow deleted. It is wise to keep a back up copy of these encrypted files so that the data can be recovered if something happens to the original.

The PGP Virtual Disk Encryption Algorithms

Encryption employs a mathematical formula to scramble your data so that no one else can use it. When you apply the correct mathematical key, you unscramble the data. The PGP Virtual Disk encryption formula uses random data for part of the encryption process. The PGP Desktop application offers strong algorithm options for protecting your PGP Virtual Disks: AES-256, CAST, and Twofish.

The Advanced Encryption Standard (AES) is the NIST-approved encryption standard. The underlying cipher is Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen. The AES replaces the previous standard, the Data Encryption Standard (DES). PGP Virtual Disks can be protected with the strongest variation of AES, AES-256 (that is, AES with a key size of 256 bits).

CAST is considered an excellent block cipher because it is fast and very difficult to break. Its name is derived from the initials of its designers, Carlisle Adams and Stafford Tavares of Northern Telecom (Nortel). Nortel has applied for a patent for CAST, but they have made a commitment to make CAST available to anyone on a royalty-free basis. CAST appears to be exceptionally well-designed by people with good reputations in the field.

The design is based on a very formal approach, with a number of formally provable assertions that give good reasons to believe that it probably requires key exhaustion to break its 128-bit key. CAST has no weak keys. There are strong arguments that CAST is

immune to both linear and differential cryptanalysis, the two most powerful forms of cryptanalysis in the published literature, both of which have been effective in cracking the Data Encryption Standard (DES).

Twofish is a relatively new, but well regarded 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the new Advanced Encryption Standard (AES). .

Special Security Precautions Taken by PGP Virtual Disk

PGP Desktop takes special care to avoid security problems with PGP Virtual Disks that other programs may not take. These precautions also apply to whole disk encrypted drives.

Passphrase Erasure

When you type a passphrase, PGP Desktop uses it only for a brief time, then erases it from memory. PGP Desktop also avoids making copies of the passphrase. The result is that your passphrase typically remains in memory for only a fraction of a second.

This feature is crucially important—if the passphrase remained in memory, someone could search for it in your computer memory while you were away from the computer. You would not know it, but they would then have full access to any PGP Virtual Disks protected by this passphrase.

Virtual Memory Protection

Your passphrase or other keys could be written to disk as part of the virtual memory system swapping memory to disk. PGP Desktop takes care that the passphrases and keys are never written to disk. This feature is important because someone could scan the virtual memory file looking for passphrases.

Memory Static Ion Migration Protection

When you mount a PGP Virtual Disk volume, your passphrase is turned into a key. This key is used to encrypt and decrypt the data on your PGP Virtual Disk. While the passphrase is erased from memory immediately, the key (from which your passphrase cannot be derived) remains in memory while the disk is mounted.

This key is protected from virtual memory; however, if a certain section of memory stores the exact same data for extremely long periods of time without being turned off or reset, that memory tends to retain a static charge, which could be read by attackers. If your PGP Virtual Disk is mounted for long periods, over time, detectable traces of your key could be retained in memory. Devices exist that could recover the key. You won't find such devices at your neighborhood electronics shop, but major governments are likely to have a few.

PGP Desktop protects against this by keeping two copies of the key in RAM, one normal copy and one bit-inverted copy, and inverting both copies every few seconds.

Other Security Considerations

In general, the ability to protect your data depends on the precautions you take, and no encryption program can protect you from sloppy security practices. For instance, if you leave your computer running with sensitive files open when you leave your desk, anyone can access that information or even obtain the key used to access the data.

Here are some tips for maintaining optimal security:

- Unmount PGP Virtual Disks when you leave your computer. This way, the contents will be safely stored in the encrypted file associated with the volume until you are ready to access it again.
- Use a screen saver with a password so that it is more difficult for someone to access your computer or view your screen when you are away from your desk.
- Make sure that your PGP Virtual Disks cannot be seen by other computers on the network. You may need to talk to your network management people to guarantee this. The files in a mounted PGP Virtual Disk can be accessed by anyone who can see them on the network.
- Never write down your passphrases. Pick something you can remember. If you have trouble remembering your passphrase, use something to jog your memory, such as a poster, a song, a poem, a joke, but do not write down your passphrases.
- If you use PGP Desktop at home and share your computer with other people, they will probably be able to see your PGP Virtual Disk files. As long as you unmount the PGP Virtual Disks when you finish using them, no one else will be able to read their contents.
- If another user has physical access to your computer, that person can delete your PGP Virtual Disk files as well as any other files or volumes. If physical access is an issue, try either backing up your PGP Virtual Disk files or keeping them on an external device over which only you have physical control.
- Be aware that copies of your PGP Virtual Disk use the same underlying encryption key as the original. If you exchange a copy of your PGP Virtual Disk with another and both change your master passwords, both of you are still using the same key to encrypt the data. While it is not a trivial operation to recover the key, it is not impossible.

  You can change the underlying key by re-encrypting the volume.

8 PGP Zip

Creating secure archives

This chapter describes the PGP Zip feature of PGP Desktop and how you can use it to create encrypted and compressed packages, called PGP Zip archives, that can hold any combination of files and/or folders. The following topics are available:

Overview

PGP Zip is a feature of PGP Desktop that lets you put any combination of files and folders into an encrypted, compressed package for secure, convenient transport or backup. You can encrypt a PGP Zip archive to a PGP key or to a passphrase for recipients who have PGP Desktop

When you are creating a PGP Zip archive, you have the option of automatically deleting the original files from your system when the archive has been created. When you receive a PGP Zip archive, you can either extract all of the files and/or folders in the archive or just the ones you want.

PGP Zip archives are encrypted to the preferred cipher for PGP Desktop (if configured by a PGP administrator) or to AES256.

PGP Zip archives can be freely moved between the Mac OS X and Windows platforms, so long as PGP Desktop is installed on the system to which the PGP Zip archive is being moved.

PGP Zip archives can be either of two types:

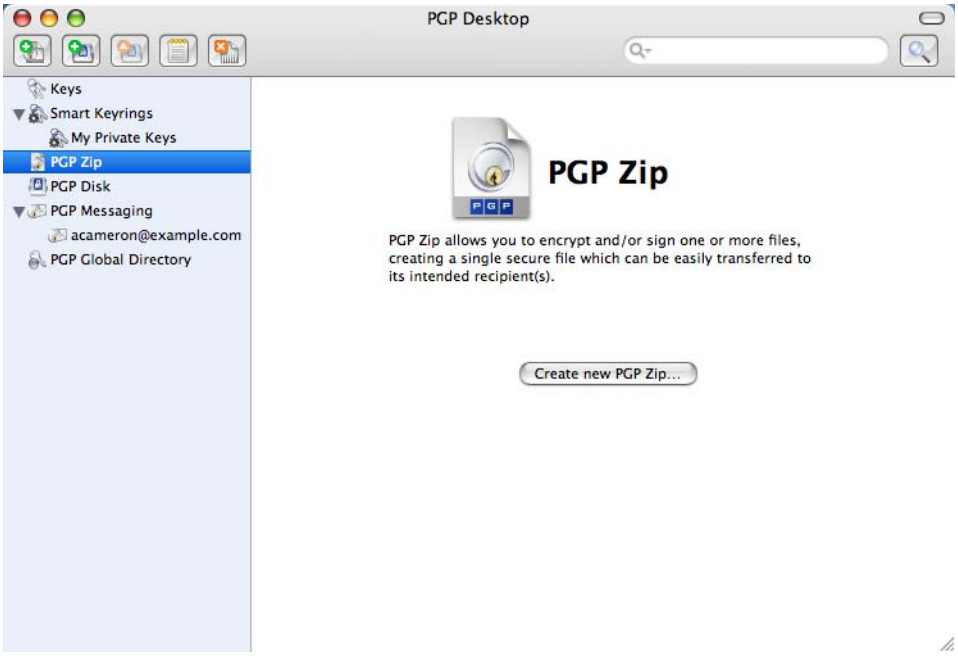
- **PGP Zip archives encrypted to a public key**. If you are sending the PGP Zip archive to one or more persons whose public keys you have, you should encrypt the archive to their public keys; thus, only the intended recipients can open the archive. The recipients must have PGP Desktop installed.
- **PGP Zip archives encrypted to a passphrase**. If you prefer to encrypt to a passphrase or you're sending the archive to multiple recipients, some of whom you don't have their public key, you can specify conventional encryption and encrypt the archive using a passphrase. In this case, you will need to communicate the passphrase to the recipients for them to be able to open the archive.The recipients must have PGP Desktop installed.

Creating PGP Zip Archives

To create a new PGP Zip archive:

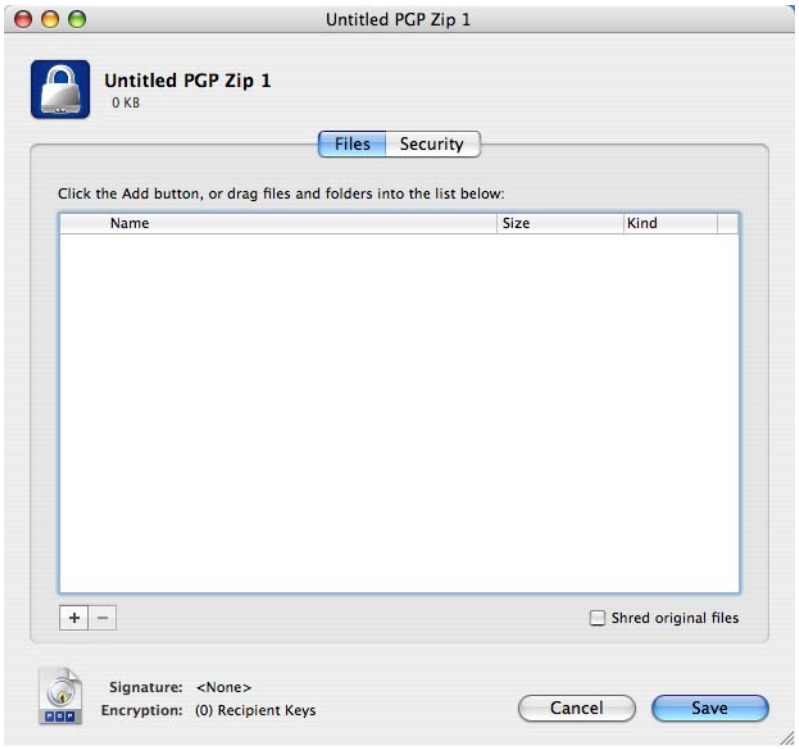
1 Open PGP Desktop and select the **PGP Zip** item.

The **PGP Zip** screen appears.



2 Click **Create new PGP Zip**.

The Untitled PGP Zip screen appears.



By default, the **Files** tab is selected. If it is not, click on **Files** to select it.

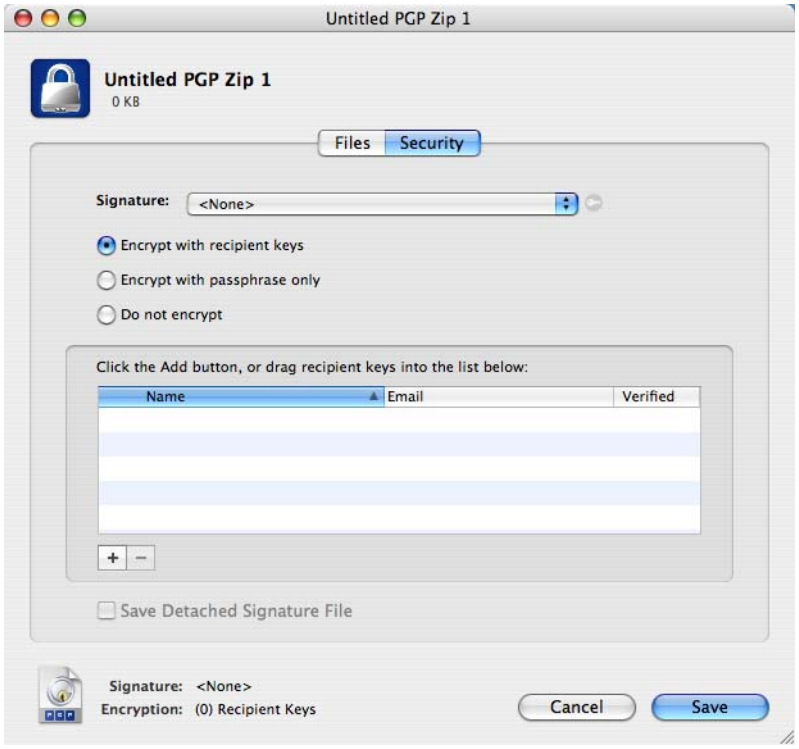
3 Specify what files and/or folders you want to be part of the PGP Zip archive you are creating. You can do this in either of two ways:

- Drag and drop the files/folders into the box.
- Click the plus-sign (**+**) icon below the box, then select the files and/or folders you want to be part of the PGP Zip archive in the dialog that appears. Click **Add** to add the files to the list.

If you add a file or folder you later decide you do not want, select the file or folder in the list and click the minus-sign (**–**) icon under the box. The file or folder is removed from the list.

4 Select **Shred original files** if you would like to securely delete from your system the files/folders you are putting into the PGP Zip archive.

5 When you are done specifying what files/folder should go into the PGP Zip archive, click the **Security** tab.



6 If desired, specify a private key from your keyring to provide a **Signature** for the PGP Zip archive you are creating.

This specified private key will be used to digitally sign the PGP Zip archive being created. The recipient(s) will be able to verify who the archive is from by verifying the digital signature using the corresponding public key.

To view the properties of the selected signing key, click the key icon to the right of the user ID of the key. Close the **Key Info** dialog when you are done.

7 Select the desired type of encryption:

– **Encrypt with recipient keys**. Lets you encrypt the PGP Zip archive to the public keys of the recipient(s). This ensures that only those recipient(s) can open the archive.

If you select public-key encryption, either drag and drop the public keys of the recipients onto the box or click the plus-sign icon and choose the public keys of the desired recipients.

– **Encrypt with passphrase only**. Lets you encrypt this PGP Zip archive to a passphrase you specify when saving the archive. Only those persons who know the passphrase will be able to open the archive.

Enter the passphrase in the **Passphrase** field and then again in the **Confirm** field. If you wish to see the passphrase as you type it, select **Show Keystrokes**.

Remember that you will need to communicate this passphrase to the person(s) you want to open the PGP Zip archive.

– **Do not encrypt**. Lets you create an unencrypted PGP Zip archive. However, because you are not encrypting the PGP Zip archive, you must specify a signing key using the **Signature** field.

8 If you have only one file in your PGP Zip archive and you are signing the file but not encrypting it, you can create a detached signature file by selecting the **Save Detached Signature File** checkbox.

If you want to create a detached signature file, you can put one file **only** in the archive, you must choose a signing key, and you cannot encrypt the archive.

9 Click **Save**.

10 Specify a filename and a location for the PGP Zip archive, then click **Save**.

If you specified a signing key in the **Signature** field, you are prompted for the passphrase to the signing key (if it is not already cached).

11 Enter the appropriate passphrase, then click **OK**.

The PGP Zip archive is created in the location you specified.

Opening a PGP Zip Archive

To open a PGP Zip archive:

1 Double click the archive file.

If the archive was encrypted to your public key, you are prompted for the passphrase to your private key, which will be used to decrypt the archive (if the passphrase is cached, you do not need to enter it). Enter the appropriate passphrase and click **OK**.

If the archive was encrypted to a passphrase, you are prompted for the passphrase. Enter the appropriate passphrase and click **OK**.

If the archive was also signed, PGP Desktop attempts to verify the signature; when verification is complete, a verification screen appears, displaying the results of the verification process.

2 If two or more files/folders were in the archive, a new folder is created that includes the files and/or folders that were in the PGP Zip archive.

If only one file was in the archive, just that file is created at the location of the PGP Zip archive.

Verifying Signed PGP Zip Archives

If you received a **signed** PGP Zip archive, you should verify it so that you know who it came from and that the archive was not tampered with before you got it. Files that are not signed cannot be verified.

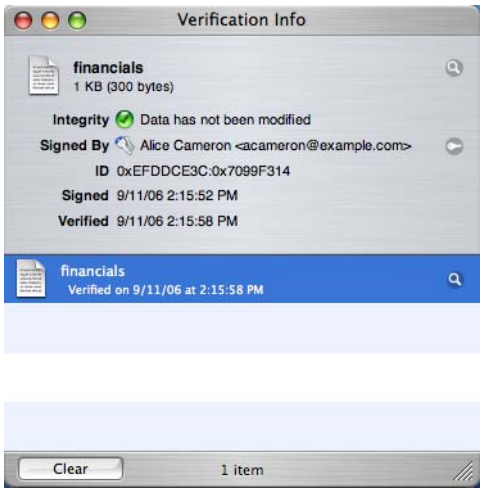
To verify a signed PGP Zip archive:

1 In PGP Desktop, from the **View** menu select **Verification Info**.

The Verification Info screen appears.

2 Drag the signed PGP Zip (.pgp) file you want verified onto the **Drag Signed Files Here** box.

PGP Desktop verifies the signature and displays the verification information.



3 To clear the list of verified archives, click **Clear**.

All listings on the Verification Info screen are removed.

9 PGP Desktop and the Finder

How PGP Desktop works with Mac OS X

This chapter tells you how you can access certain PGP Desktop functions using context menus in the Finder. These topics are available:

Overview

You can access PGP Desktop functions via context menus in the Finder. You can get the same PGP Desktop functionality via the Mac OS X Services menu.

Depending on what you select, you can:

- Encrypt, Sign, or Encrypt and Sign
- Shred
- Decrypt/verify
- Mount, edit, or unmount a PGP Virtual Disk volume
- Import a PGP key
- Add PGP keys to your keyring
- View the contents of a PGP Zip archive

You can access context menus in the Finder by:

- Ctrl-clicking: On a one-button mouse, hold down the Control (ctrl) key on the keyboard and click the item.
- Right-clicking: On a two-button mouse, click the item with the right mouse button held down.

In this chapter, the Ctrl-click method is used. If you right-click or use a different method for accessing context menus in the Finder, substitute that method where it says to Ctrl-click.

Files "in the Finder" also include files on the Mac OS X Desktop.

Encrypt, Sign, or Encrypt and Sign

PGP Desktop lets you encrypt, sign, or encrypt and sign unencrypted files, folders, and even entire drives from the Finder.

Encrypting and/or signing files and folders is a good way to protect just a few important files and/or folders in a situation where a PGP Virtual Disk volume isn't justified.

If you are considering encrypting and/or signing a drive in the Finder, a PGP Virtual Disk volume might be a better solution; refer to Chapter 7, Using PGP Virtual Disks for more information.

To encrypt and/or sign files and/or folders in the Finder:

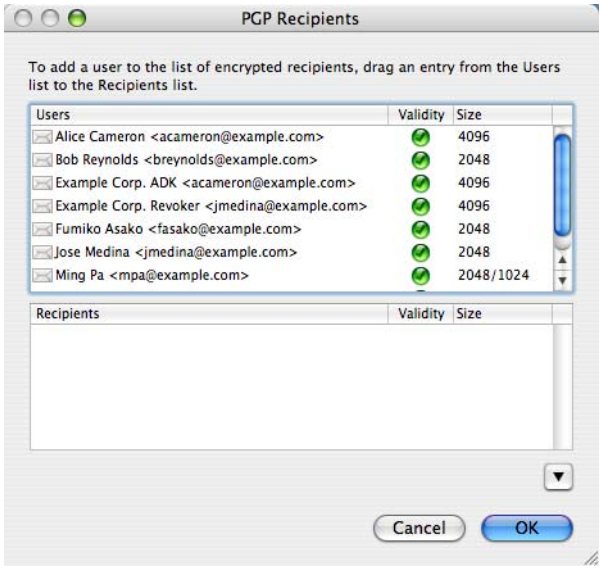
1 In the Finder, select the files and/or folders you want to encrypt and/or sign.

You can use the Shift or Command keys to select any combination of files and folders.

2 Ctrl-click the selected files and/or folders, or right-click if you have a two-button mouse. From the context menu that appears, choose **Encrypt & Sign** from the **PGP** menu.

(If you select just **Encrypt**, you will *not* be prompted for a signing key; if you select just **Sign**, you will *not* be prompted to select a public key to encrypt to.)

The PGP Recipients dialog appears.



3 Drag the public keys of the persons you want to be able to decrypt the items you are encrypting into the **Recipients** box.

4 Click the down-facing triangle above the **OK** button to specify the appropriate options:

- **Conventional Encrypt.** Select this checkbox 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 you specify.

  If you are using PGP Desktop in a PGP Universal-managed environment, conventional encryption may be disabled.

- **Text Output.** When sending files as attachments with some email applications, you may need to select the **Text Output** checkbox 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.

- **Shred Original.** Select this checkbox to overwrite the original document that you are encrypting, so that your sensitive information is not readable by anyone who can access your system.

- **MacBinary**. MacBinary is the standard method by which a Mac OS X file is converted into a single file so that it can be transferred to another Macintosh or PC without losing either its Data or Resource segment. Options are Yes, No, or Smart.

  Yes means the whole file is included, including the Mac OS X specific information. **No** means only the data segment is included. **Smart** means the file type determines if the Mac OS X specific information is included.

5 Click **OK**.

If you selected the Conventional Encryption option, you are prompted for a passphrase to protect the encrypted items.

6 Enter a passphrase, enter it again, then click **OK**.

The Confirm Passphrase dialog appears.

7 Using the Signing Key drop-down list, specify a private key to be used to sign the items you are encrypting and signing, then enter the passphrase of the signing key.

If the passphrase is cached, you do not have to enter it.

8 Click **OK**.

A PGP Zip archive (<filename>.pgp) file is created at the same location as the encrypted and signed items.

Shred

For those situations where you want to be absolutely certain that specific files and/or folders are securely deleted from your system, you can Shred them from the Finder.

Putting a file or folder into the Mac OS X Trash just allows new files to overwrite the file or folder you think you are "deleting." In fact, there could be days, weeks, or even months when just about anyone with physical access your system could retrieve these files.

The PGP Desktop Shred feature, in comparison, overwrites your files multiple times as soon as you ask them to be shredded. Refer to Chapter 12, Shredding for more information about how thoroughly the Shred feature erases your files.

To Shred files and/or folders in the Finder:

1 In the Finder, select the files and/or folders you want to Shred.

You can use the Shift or Command keys to select any combination of files and folders.

2 Ctrl-click the selected files and/or folders, or right-click if you are using a two-button mouse.

3 Choose **PGP**, then **Shred** from the context menu that appears.

A PGP screen appears, asking if you are sure you want to Shred the listed files.

4 Click **OK**.

The file(s) are Shredded (secure deleted) from your system; they do not appear in the Trash.

Decrypt/Verify

If you have a PGP Zip (.pgp) file on your system, you can decrypt and verify it in the Finder. Decrypt/verify will always decrypt an encrypted (.pgp) file. However, if the encrypted file wasn't signed, then the file will not be verified (as there's no signature to verify).

You can also decrypt/verify a PGP key (.asc) file, but this is just for importing the keys, not for decrypting or verifying the file. Refer to "Import a PGP Key" on page 101 for more information about importing PGP keys from an ASC file in the Finder.

To decrypt/verify a PGP Zip file in the Finder:

1 In the Finder, select the PGP Zip (.pgp) file you want to decrypt/verify.

2 Ctrl-click the selected files and/or folders, or right-click if you are using a two-button mouse. Choose **PGP**, then **Decrypt & Verify** from the context menu that appears.

The Confirm Passphrase dialog appears.

3 Enter the appropriate passphrase for the private key.

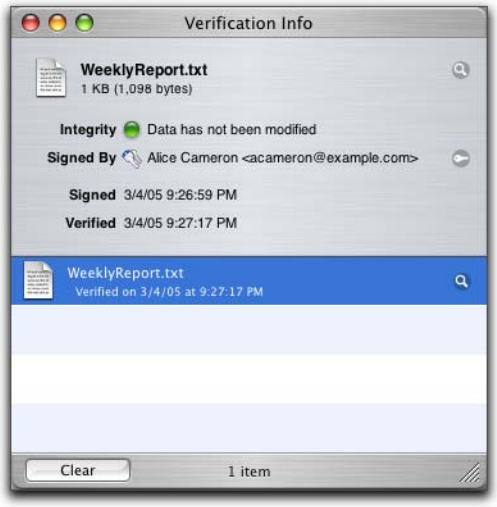
If the passphrase is cached, you aren't prompted for it.

Normally, as an added level of security, the characters you enter for the passphrase are not visible on the screen. However, if you are sure that no one is watching (either physically or over the network) and you would like to see the characters of your passphrase as you type, deselect the **Hide Typing** checkbox.

4 Click **OK**.

The file is decrypted at the location of the .pgp file.

If the file was signed, PGP Desktop opens the Verification Info screen and displays the results of the verification of the file.



Mount or Unmount a PGP Disk Volume

If you have an unmounted PGP Disk (.pgd) file, you can mount the corresponding PGP Disk volume from the Finder.

Refer to Chapter 7, Using PGP Virtual Disks for more information about PGP Disk volumes.

To mount a PGP Disk volume from the Finder:

1 In the Finder select the PGP Disk (.pgd) file whose volume you wish to mount.

2 Ctrl-click the selected .pgd file, or right-click if you are using a two button mouse. From the **PGP** menu, select **Mount**.

The **Enter Passphrase** dialog appears.

3 Enter the passphrase that protects the PGP Disk volume you want to mount.

Normally, as an added level of security, the characters you enter for the passphrase are not visible on the screen. However, if you are sure that no one is watching (either physically or over the network) and you would like to see the characters of your passphrase as you type, click the **Typing Hidden** button.

4 Click **OK**.

The PGP Disk volume is mounted.

To unmount a PGP Disk volume in the Finder:

1 Select the *mounted* PGP Disk (.pgd) file whose volume you wish to unmount.

2 Ctrl-click the .pgd file, or right-click if you are using a two-button mouse. From the context menu, choose **Unmount** from the **PGP** menu.

If the menu says *Mount*, then the volume is already unmounted.

The selected PGP Disk volume is unmounted.

Import a PGP Key

PGP keys can be exported from PGP Desktop as .asc files. This is a good way to back up your keys or exchange your public keys with others. If you have an .asc file on your system that includes a PGP key that you want on your keyring, you can import it from the Finder.

To import keys from an .asc file in the Finder:

1. In the Finder, select the PGP key (.asc) file with the PGP keys you want to import.
2. Ctrl-click the selected .asc file.
3. Ctrl-click the .pgd file, or right-click if you are using a two-button mouse. From the context menu, choose **Decrypt & Verify** from the **PGP** menu.

   The Select Keys dialog appears.
4. Select the PGP key(s) you want to import, then click **OK**.

   If you selected a private key, a dialog appears that tells you that trust values on the private key must be set manually using the key properties for the key.

   The selected key(s) are added to your keyring.

Add PGP Public Keys to Your Keyring

PGP Desktop stores your PGP keys on keyrings; you always have one private keyring (.skr) file that holds private keys and one public keyring (.pkr) file that holds public keys.

If you have a public keyring file (not your active public keyring file) on your system that holds keys you would like to add to your active keyring, you can add them from the Finder.

To add PGP public keys from a keyring file in the Finder:

1. In the Finder, select the PGP public keyring (pubring.pkr) file with the keys you would like to add to your keyring.
2. Ctrl-click the selected .pkr file.
3. Ctrl-click the .pkr file, or right-click if you are using a two-button mouse. From the context menu, choose **Decrypt & Verify** from the **PGP** menu.

   The Select Keys dialog opens and displays the public keys on the selected public keyring file.
4. Select the keys you want to add to your active keyring, then click **OK**.

You can use the Select All or Select None buttons and the Shift and Command keys to select the desired keys.

The Select Keys dialog disappears and the selected keys are added to your active keyring.

Extract the Contents of a PGP Zip Archive

If you have a PGP Zip archive on your system whose contents you want to extract, you can do that in the Finder.

To extract the contents of a PGP Zip archive in the Finder:

1. In the Finder, select the PGP Zip archive (.pgp) file whose contents you wish to extract.
2. Ctrl-click the .pgp file, or right-click if you are using a two-button mouse. From the context menu, choose **Decrypt & Verify** from the **PGP** menu.

   The Enter Passphrase dialog appears.
3. Enter the passphrase that protects the PGP Zip archive from which you are extracting files, then click **OK**.

   The file(s) are extracted from the archive to the same location in the Finder as the archive.

   If the archive was signed, the Verification Info dialog appears.

10 PGP Keys

Creating PGP Keys

This chapter tells you how to create and manage PGP keys. These chapters are available:

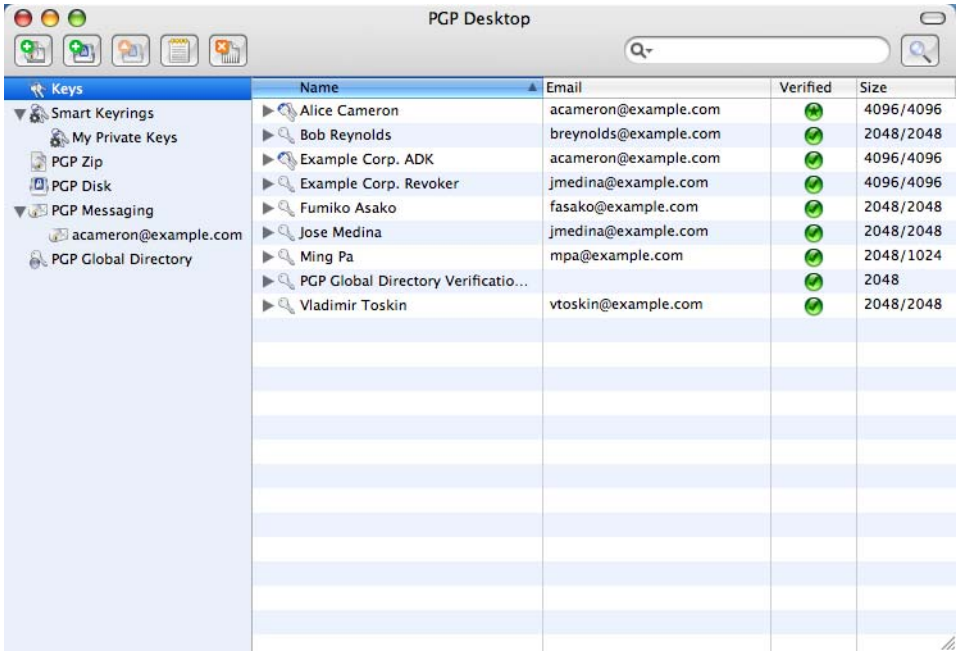
Overview

PGP Keys is the feature of PGP Desktop you use to create and maintain your keypair(s) and the public keys of other PGP Desktop users.

This chapter covers: viewing keys, creating a keypair, distributing your public key, getting the public keys of others, and working with keyservers.

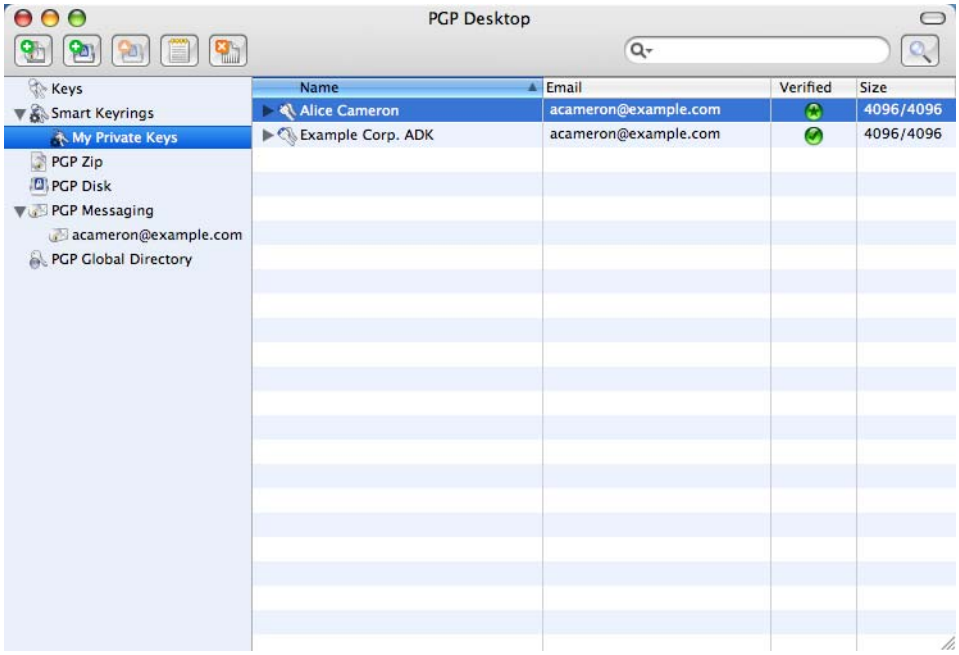
Viewing Keys

To view all of the keys on the local keyring, open PGP Desktop and click on the **Keys** item.



You can also use the *Smart Keyrings* feature. A Smart Keyring is a set of keys that fits the criteria you establish. For example, if you frequently send messages to PGP Desktop users from a particular email domain, you could create a Smart Keying that shows just the users from that email domain.

The default Smart Keyring is *My Private Keys*.



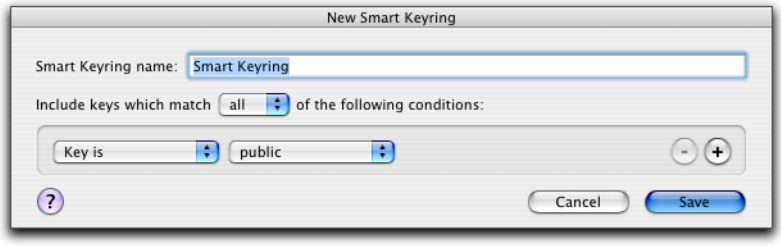
To create a Smart Keyring:

1 Open PGP Desktop.

2 Click the **Keys** item.

3 From the **File** menu, select **New > Smart Keyring**.

The New Smart Keyring screen appears.



4 In the **Smart Keyring name** field, enter a descriptive name for the Smart Keyring you are creating.

5 In the **Include keys which match the following conditions** menu, select either:

- **Any**. Displays keys that match any of the specified criteria (logical "OR").
- **All**. Only displays keys that match all of the specified criteria (logical "AND").

6 In the first matching column, select one of the following:

- **Key is**. Displays keys that meet the criteria.
- **Key is not**. Displays keys that do not meet the criteria.
- **Name**. Displays keys with the specified criteria in the Name.
- **Email**. Displays keys with the specified criteria in the Email address.
- **Key ID**. Displays keys with the specified criteria in the Key ID.
- **Key Size**. Displays keys of the specified Key Size.
- **Creation Date**. Displays keys created on the specified Creation Date.
- **Expiration Date**. Displays keys that expire on the specified Expiration Date.

7 The options in the second matching column change based on what you selected in the first matching column; select between:

- **Public**. Matches on public keys only.
- **Private**. Matches on private keys only.
- **Revoked**. Matches on revoked keys only.
- **Enabled**. Matches on enabled keys only.
- **Expired**. Matches on expired keys only.

- **Signed by**. Matches on keys signed by the specified person.
- **Contains**. Matches when key contains specified criteria.
- **Does not contain**. Matches when key does not contain specified criteria.
- **Is**. Matches when specified criteria is met.
- **Is not**. Matches when specified criteria is not met.
- **Is**. Matches when specified date is met.
- **Is on or before**. Matches when specified date is on or before the listed date.
- **Is on or after**. Matches when specified data is on or after the listed date.

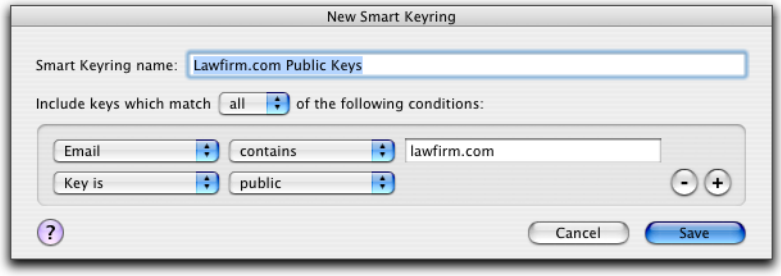
8 In the text box that is available for some matching items, you can type text (like an email address or a domain; wildcards are allowed), numbers, or dates.

9 To add extra rows for matching or excluding, click the plus-sign icon. Click the minus-sign item to remove rows.

10 Click **Save**.

The Smart Keyring appears in the Items list.

The following Smart Keyring, for example, matches the public keys of PGP Desktop users at your company's law firm.



When you select this Smart Keyring, only those keys that match these criteria appear.

Creating a Keypair

You probably already created a PGP keypair for yourself using the PGP Desktop Setup Assistant or with a previous version of PGP Desktop — but if you haven't, you need to now. Most of the things you do with PGP Desktop require a keypair.

It is bad practice to keep creating new keys for yourself. A PGP keypair is like a digital driver's license or passport; if you create lots of them, you're going to end up confusing yourself and those people who want to send you encrypted messages. It is best to have only one key that contains all the email addresses that you use. The PGP Global Directory will publish only one key per email address.

If you are using PGP Desktop in a PGP Universal-managed environment, keypair creation may be disabled.

To create a PGP keypair:

1 Open PGP Desktop.

2 From the **File** menu, select **New > PGP Key**.

The **Create a key to secure your communications** screen appears.

3 Read the information on this screen.

4 Select the Expert Mode checkbox if you want to specify advanced properties for your new key. For more information on these settings, see "Expert Mode Key Settings" on page 109.

5 Click **Continue**.

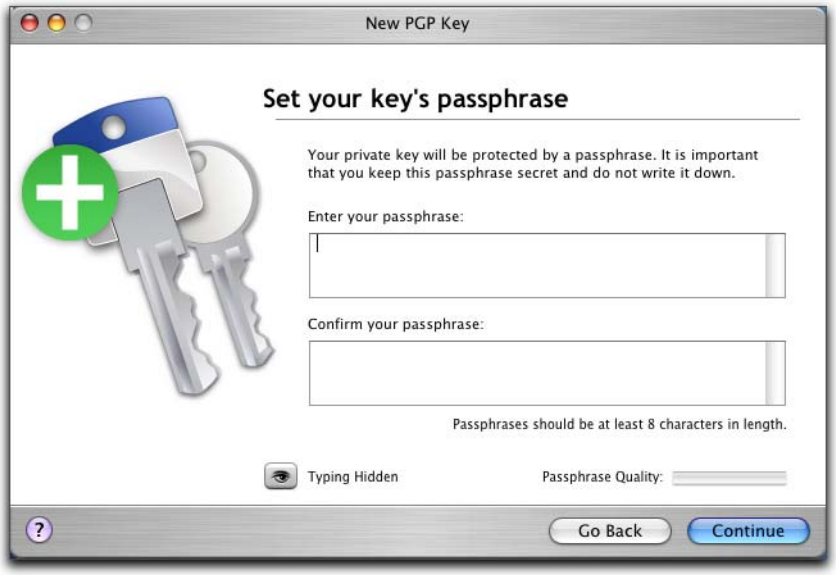
The **Set your key's contact information** screen appears.

6 Enter your real name in the **Full Name** field and your correct email address in the **Email Address** field.

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, when you upload your public key to the PGP Global Directory (which makes it easily available to other PGP Desktop users), your real email address is required.

7 Click **Continue**.

The **Set your key's passphrase** screen appears.



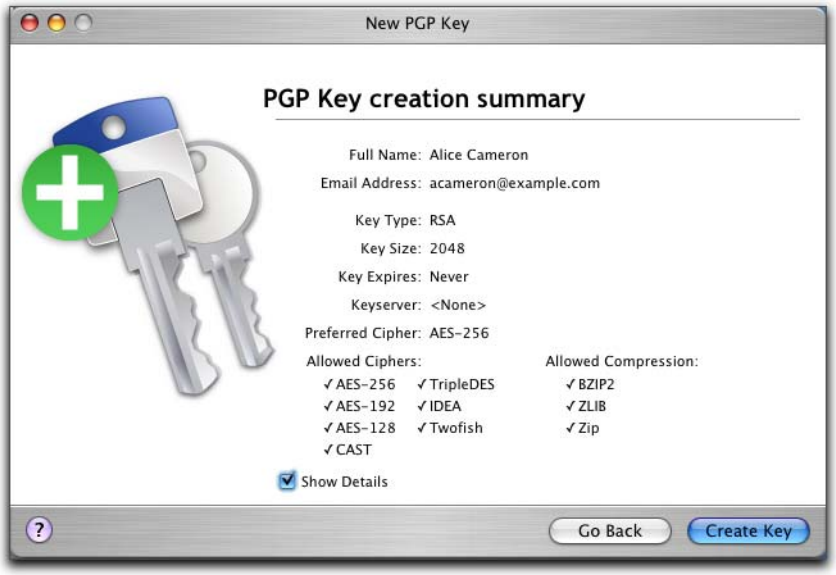
8 Enter a passphrase for the key you are creating, then enter it again to confirm it.

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, check the **Typing Hidden** icon.

Make sure that your passphrase is one that you can easily remember (without writing it down). Unless your PGP administrator has implemented a PGP key reconstruction policy for your company, no one, including PGP Corporation, can salvage a key with a forgotten passphrase.

9 Click **Continue**.

The PGP Key creation summary screen appears.



10 Click **Show Details** to show details about the key.

11 Click **Create Key**.

PGP Desktop generates your new keypair.

This process can take several minutes.

12 When the key generation process indicates that it is done, click **Finish**.

Expert Mode Key Settings

When you select **Export Mode** on the **Create a key to secure your communications** screen, in addition to specifying your name and email address, you also specify:

- **Key Type**. Choose between **Diffie-Hellman/DSS** and **RSA**.

Beginning with PGP Desktop 9.0, the older RSA Legacy key format from the early 1990s is no longer fully supported. You cannot create **new** PGP keypairs using the RSA Legacy key format; however, **existing** RSA Legacy keypairs continue to be supported in PGP Desktop.

- **Keyserver**. Specify a trusted keyserver or **<None>**.
- **Allowed Compression**. Deselect any compression type you do not want the key you are creating to support.
- **Allowed Ciphers**. Deselect any cipher you do not want the key you are creating to support.
- **Allowed Hashes**. Deselect any hash you do not want the keypair you are creating to support.
- **Preferred Cipher**. Select the cipher you want to be used in those cases where no cipher is specified. Only a cipher that is allowed can be selected as preferred.
- **Preferred Hash**. Select the hash you want to be used in those cases where no hash is specified. Only a hash that is allowed can be selected as preferred.
- **Key size**. Enter from 1024 bits to 4096 bits. The larger the key, the more secure it is, but the longer it will take to generate.
- **Key Expires.** Select **Never** or specify a date on which the key you are creating will expire.

13 Click **Continue**

The **Set Your Key's Passphrase** dialog box appears.

14 Enter the passphrase that you would like to use with this key, then type it again in the **Confirm your passphrase** box. It is critical that you keep this passphrase secret.

Click **Continue.**

15 Review the summary information, then click **Create Key** to begin the key generation process.

PGP Desktop generates your new keypair. This process can take several minutes.

16 When the key generation process indicates that it is done, click **Next**.

You are prompted to add the public key portion of the key you just created to the PGP Global Directory.

17 Read the text on the screen and click **Next**.

Click **Skip** to prevent the public key from being posted to the PGP Global Directory.

The **Completing the PGP Global Directory Assistant** screen appears.

18 Click **Finish**.

Your new PGP keypair has been generated. It should be visible in the PGP Keys Work area. If you don't see it listed, make sure **All Keys** or **My Private Keys** is selected in the **PGP Keys** item.

Passwords and Passphrases

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 password between three and eight letters. Using a single-word passphrase is generally a bad practice, and is discouraged. 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. You can imagine simple enhancements to dictionary attacks that manage to find broad arrays of passwords even when slightly modified from dictionary terms.

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.

Refer to Appendix B, Passwords and Passphrases for more information about passwords and passphrases.

Protecting Your Private Key

PGP Corporation recommends that you take these actions immediately after you create your keypair:

Failure to take these actions could result in a devastating loss of data some time in the future.

- Back up a copy of your private key file to another, safe location, in case your primary copy is ever damaged or lost. See "Backing up Your Private Key".

- Reflect on your chosen passphrase to ensure that you chose something that you will not forget. If you are concerned that you chose a passphrase during the key creation process that you will not remember, change it RIGHT NOW to something you will not forget. For information on changing your passphrase, see "Changing Your Passphrase" on page 127.

Your private key file is very important because once you have encrypted data to your public key, only the corresponding private key can be used to decrypt the data. This holds true for your passphrase as well; losing your private key or the passphrase means that you will not be able to decrypt data encrypted to the corresponding public key. When you encrypt information, it is encrypted to both your passphrase and your private key. You need both to decrypt the encrypted data. Once the data is encrypted, no one—not even PGP Corporation—can decrypt the data without your private key file and your passphrase.

Consider a situation where you have important encrypted data, and then either forget your passphrase or lose your private key. The encrypted data would be inaccessible, unusable, and unrecoverable.

Backing up Your Private Key

To back up your private key:

1. In the Smart Keyrings item, click **My Private Keys**.
2. Select the icon representing your keypair.
3. From the **File** menu, select **Export**.
4. Type a name for the file in the **Save As** field and specify a location in the **Where** field.
5. Select the **Include Private Key(s)** checkbox.

   This is important, because if you do not do this, only your *public* key will be exported.
6. Click **Save**.
7. Copy the file to a secure location.

   This may be a CD which you carefully archive, another personal computer, or a USB flash drive that you keep in a safe location. Please remember not to distribute this file to others, as it contains both your private key and your public key.

Distributing Your Public Key

After you create your PGP Desktop keypair, you need to get your public key to those with whom you intend to exchange encrypted messages.

You make your public key available to others so they can send you encrypted information and verify your digital signature; you need their public key to send encrypted messages to them.

You can distribute your public key in various ways:

- Publish your key on the PGP Global Directory. Generally, none of the other methods are necessary once your key is published to this directory.
- 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 Keyserver

The best method for making your public key available is to place it on a public keyserver, 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 keyservers, including the PGP Global Directory, where you can make your key available for anyone to access. If you are using PGP Desktop in a domain protected by a PGP Universal Server, your PGP administrator will have pre-configured PGP Desktop with appropriate settings.

When you're working with a public keyserver, 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 you only put keys on a keyserver 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?
- Other than the PGP Global Directory, once a key is posted, there is little chance that it can be removed. In fact, some public keyservers have a policy against deleting keys. Others have replication features that replicate keys between keyservers, so even if you are able to delete your key on one server, it could reappear later.

Most people post their public key to the PGP Global Directory right after they create their keypair. If you have already posted your key to the PGP Global Directory, you do not need to do it again. Under most circumstances, there is no need to publish your key to any other keyserver. Note also that other keyservers may not verify keys, and thus keys found on other keyservers may require significantly more work on your part to contact the key owner for fingerprint verification.

To manually send your public key to a keyserver:

1. Open PGP Desktop.
2. Ctrl-click the keypair whose public key you want to send to the keyserver.
3. Select **Send Key To Server**, then select the keyserver you want to send the public key to from the list.

   Refer to "Working with Keyservers" on page 116 if the keyserver you want to send your public key to is not on the list.

Once you place a copy of your public key on a keyserver, 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 keyserver 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.

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 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 PGP Desktop.
2. Open your email client, create a new message, address it to the person to whom you are sending your public key.
3. From PGP Desktop, drag your keypair onto the body of the email message and drop it.
4. Send the message.

If this method doesn't work for you, you can open PGP Desktop, select your keypair, then from the **Edit** menu select **Copy.** Open an email message, then paste the public key into the body of the message. With some email applications you can simply drag your key from PGP Desktop into the text of your email message to transfer the public key information.

Exporting Your Public Key to a File

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

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

- Select your keypair, then from the **File** menu select **Export**. Enter a name and a location for the file, then click **Save**. Be sure **not** to include your private key along with your public key if you plan on giving this file to others.
- Ctrl-click the key you want to save to a file, select **Export** from the list, enter a name and a location for the file, then click **Save**. Be sure **not** to include your private key along with your public key if you plan on giving this file to others.

- Select your keypair, then from the **Edit** menu select **Copy.** Open a text editor and select **Paste** to insert the key information into the text file. Save the file and send it to anyone you like. The recipient needs to use PGP Desktop on their system to retrieve the public key portion.

Getting the Public Keys of Others

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

There are multiple ways to obtain someone's public key:

- Automatically retrieve the verified key from the PGP Global Directory
- Find the key manually on a public keyserver
- Automatically add the public key to your keyring directly from an email message
- Import the public key from an exported file
- Get the key from your organization's PGP Universal Server

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 PGP Desktop.

Getting Public Keys from a Keyserver

If the person to whom you want to send encrypted mail is an experienced PGP Desktop user, it is likely that a copy of his or her public key is on the PGP Global Directory or another public keyserver. 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 domain protected by a PGP Universal Server, then your PGP administrator may direct you to use the keyserver built into the PGP Universal Server. In this case, your PGP Desktop software is probably already configured to access the appropriate PGP Universal Server. Similarly, the PGP Universal Server is configured by default to communicate with the PGP Global Directory. Thus, the PGP ecosystem distributes the load of key lookup and verification.

There are a number of public keyservers, such as the PGP Global Directory hosted by PGP Corporation, 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 keyserver and do a search for the user's name or email address. This may or may not work, as not all public keyservers are regularly updated to include the keys stored on all the other servers.

To get someone's public key from a keyserver:

1 Open PGP Desktop.

2 Click the PGP Global Directory item or the item of another keyserver you wish to search.

The Search for Keys screen appears in the Work area.

3 Specify your search criteria, then click **Search**.

If the keyserver you want to search isn't shown, from the Keys menu, select **Add Keyserver**, and configure it.

You can search for keys on a keyserver by specifying values for multiple key characteristics. The inverse of most operations is also available. For example, you may search using "User ID is not Charles" as your criteria.

The results of the search appear.

4 If the search found a public key you want to add to your keyring, Ctrl-click it and select **Add To Default Keying**.

The selected key is added to your keyring.

Getting Public Keys from Email Messages

A convenient way to get a copy of someone's public key is to have that person attach it to an email message.

To add a public key attached to an email message:

1 Open the email message.

2 Double-click the **.asc** file that includes the public key.

PGP Desktop recognizes the file format and opens the **Select keys** dialog.

3 Select the public key(s) you want to add to your keyring and click **OK**.

Working with Keyservers

PGP Desktop understands three kinds of keyservers:

- **PGP Universal keyservers**. If you are using PGP Desktop in a domain protected by a PGP Universal Server, PGP Desktop is pre-configured to only communicate with the keyserver built into the PGP Universal Server with which it has a relationship. To PGP Desktop, this is a trusted keyserver, and PGP Desktop will automatically trust any key it finds on this keyserver unless the PGP Universal Server tells PGP Desktop that the key is not trusted—this can happen, for instance, when verifying signatures from remote keys.

- **The PGP Global Directory**. If you are using PGP Desktop outside of a domain protected by a PGP Universal Server, PGP Desktop is pre-configured to communicate with the PGP Global Directory.

  The PGP Global Directory is a free, public keyserver hosted by PGP Corporation. It provides quick and easy access to the universe of PGP keys. It uses next-generation keyserver technology that verifies the key associated with each email address (so that the keyserver doesn't get clogged with unused keys, multiple keys per email address, forged keys, and other problems that plagued older keyservers) and it lets you manage your own keys, including replacing your key, deleting your key, and adding email addresses to your key. Using the PGP Global Directory significantly enhances your chances of finding the public key of someone with whom you want to send secured messages.

  To PGP Desktop, the PGP Global Directory is a trusted keyserver, and PGP Desktop will automatically trust any key it finds there. During the initial connection to the PGP Global Directory, the PGP Global Directory Verification Key is downloaded, signed, and trusted by the key you publish to the directory. All of the keys verified by the PGP Global Directory are thus considered valid by your PGP Desktop.

- **Other keyservers**. In most cases, other keyservers are other public keyservers. However, you may have access, through your company or some other means, to a private keyserver.

Refer to "Keys Preferences" on page 153 for more information about working with keyservers.

11 Managing PGP Keys

Working with PGP Keys to secure your computer

This chapter tells you how to manage keys with the PGP Desktop application. These topics are available:

Examining and Setting Key Properties

The **Key Info** dialog shows everything there is to know about a key.

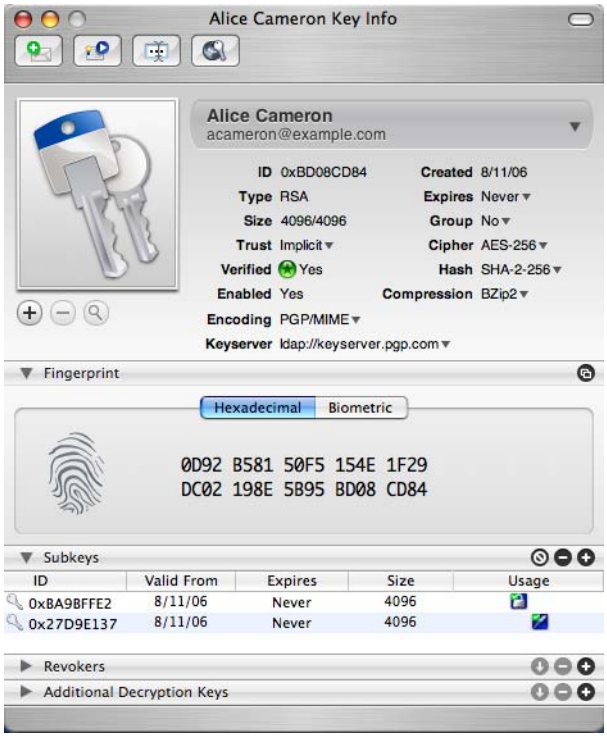
To view the properties of a key:

1. Open **PGP Desktop**, then click the **Keys** item.

   All of the keys on your keyring appear.

2. Double-click a key to see its properties.

The **Key Info** dialog for that key appears.



The **Key Info** dialog shows the following information about a key:

- **Key Info Toolbar** (only available for private keys):
  - Click **Add Email Address** to add an email address to this key.
  - Click **Request Certificate** to create a certificate request to add a certificate to this key.
  - Click **Change Passphrase** to change the key's passphrase.
  - Click **Publish** to publish your key to the PGP Global Directory.

  The **Key Info Toolbar** is only available for private keys because you cannot make any of these changes to public keys other than your own.
- **Photo ID**. If a photograph has been added to the key, it displays in the upper-left corner of the **Key Info** dialog. If no photograph has been added, an icon appears instead: a single key icon for public keys, a double key icon for private keys.

  See "Adding and Removing Photographs" on page 125 for instructions how to add a photo ID to a key.
- **Name** and **Email address**. The user name typed when the key was created displays at the top of the screen. This should be the real name of the key owner, as this helps others find the correct key. However, this is not a requirement, so the name you see is **not necessarily** the real name of the key owner.

Clicking the user name shows the name/email address combinations currently associated with the key. To make another name/email address combination display, click the current name and select the desired name from the list.

- **ID**. The 32-bit key ID of this key. To copy the key ID to the Clipboard, right-click it and select **Copy KeyID** from the context menu. If you have a one-button mouse, you can press and hold the Ctrl key as you click the ID field.
- **Type**. The key type of this key. RSA and Diffie-Hellman are the most common. You may see older RSA Legacy keys that have been imported, but you cannot use PGP Desktop to create keys in this format.
- **Size**. The size of the key, in bits. The larger the size, the more secure, but it can also take longer to create the key and to use it. The first shown is the number of bits of the encryption subkey, the second is the number of bits of the signing key.
- **Trust**. Indicates how much you trust the owner of this key to act as an introducer for others, whose keys you may get in the future.

  Refer to *An Introduction to Cryptography* for more information about trust.

  Public keys can be **None**, **Marginal**, or **Full**. Your private keys can be **None** or **Implicit** (meaning it's your own key and thus you trust it completely). The None setting only occurs if you import your key from a file; Implicit is set automatically when you create a keypair.

  If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change the trust setting of keypairs you import to Implicit.

  If you import a key from a file into PGP Desktop, it will be imported in an unverified state; PGP Desktop knows it's a PGP key, but it doesn't know whether to trust it or not. If you import your own keypair that you saved to a file, set the **Trust** setting to **Implicit**. If you import someone else's public key, set the **Trust** setting to **Marginal** (if you are not certain of how responsible that person is when signing keys) or **Trusted** (you trust that the person signs keys only after they are sure the key can be trusted), then **Sign** the key **if you are certain that it belongs to the claimed owner.**
- **Verified**. A measure of the level to which you can be certain that this key really belongs to the claimed owner (it is a value calculated by PGP Desktop). If you obtained a key from a trustworthy source, such as a PGP Universal Server or the PGP Global Directory, PGP Desktop shows the key as verified.

  If the Verified status of a public key that you put onto your keyring is **Unknown**, you can verify the key by signing it, indicating that you believe the claimed key owner is the actual key owner. If for some reason you import your own key into PGP Desktop—perhaps because you are restoring from a backup or moving to another computer—you can verify your key by setting the Trust field to **Implicit**. In effect, by setting the field to **Implicit,** you are saying that you trust yourself to be the actual key owner.
- **Enabled**. Status of this key. **Yes** means the key is enabled, **No** means the key is disabled. An enabled key can be used for encrypting, signing, decrypting, and verifying. A disabled key cannot be used.

You can change the enabled/disabled status for a public key. Your private keys are always enabled.

- **Encoding**. The preferred message encoding format for this key. Select **PGP/MIME** or **Partitioned**. You can only modify this setting for your private keys. You can see the setting for a public key on your keyring, but you cannot modify the setting.

  PGP/MIME is able to encrypt and sign the entire message including attachments in one pass and is usually therefore faster and better able to reproduce the full message fidelity. **Partitioned** is the most backwards compatible with older PGP and OpenPGP products

- **Keyserver**. The preferred keyserver for this key, if specified. If a key has a preferred keyserver, that keyserver will be checked first when PGP Desktop synchronizes the key.

  To specify a preferred keyserver for a key, click a listed keyserver or **None**, enter the information for the keyserver, click **OK**, enter the passphrase for the key, then click **OK**.

  You can only set a preferred keyserver for your private keys. A key can have only one preferred keyserver, but it can have multiple trusted keyservers.

- **Created**. The date the key was created.

- **Expires**. The date the key will expire or **Never**. To change the expiration date for a private key, click on the current setting and select **Never** or specify an expiration date by selecting **Select Date**.

  You can only change the expiration date for a private key.

- **Group**. Group status of this key, **Yes** or **No**. Yes means that more than one person or entity (such as a PGP Universal Server) has a copy of the private key together with the passphrase.

  If your PGP Universal administrator has required that some keys are generated by the server, you may encounter keys with this set to **Yes**. When PGP Desktop is managed by a PGP Universal Server, it is not possible for this to occur. However, PGP Universal Satellite users may be provided with such keys if the administrator configures the server as such.

  You can only change the Group status for your private keys.

- **Cipher**. Shows the preferred cipher for this key. Click the Cipher field to see the allowed ciphers.

  If you think a cipher doesn't meet your needs, you can disable it for this key. To do this, click the current cipher, select **Edit**, deselect the ciphers you don't want supported by this key, click **OK**, enter the passphrase for the key, then click **OK** again. The selected ciphers are disabled for this key. Disabled ciphers display grayed out in the list.

  If you deselect all ciphers, TripleDES is used.

  You can only disable a cipher for your private keys.

- **Hash**. Shows the type of hash being used for this key. Click the Hash field to see the allowed hashes. Hashes are used by PGP Desktop to detect changes in a signed document.

  The Digital Signature Standard requires the use of the SHA-1 hash when calculating signatures. Thus, any hash preference set on DSS/DH keys may not be observed.

  If you prefer a particular hash algorithm not be used, you can prevent PGP Desktop from using it for this key by clicking on **Hash**, selecting **Edit**, and deselecting any hash algorithm you do not want PGP Desktop to use.

  If you deselect all hash algorithms, SHA-1 will be used for version 4 keys and MD5 will be used for version 3 (older) keys.

  You can only disable a hash for your private keys.

- **Compression**. The preferred compression type for this key. Options are BZip2, ZLIB, and Zip. To see all supported compression types, click the name of the preferred compression type.

  If you don't care for a particular compression type, you can disable it on this key. To do this, click the current compression type, select **Edit**, deselect the compression types you don't want supported by this key, click **OK**, enter the passphrase for the key, then click **OK** again. The selected compression types are disabled for this key.

- **Fingerprint**. A unique identifying string of numbers and characters used to identify a specific public key. No two PGP Desktop keys ever created have the same fingerprint. You cannot change a key's fingerprint.

  Fingerprints can be displayed in either hexadecimal format (10 sets of four characters per set) or word list format (four columns with five unique words per column). Click the fingerprint to switch from one format to the other.

  What is a biometric word list? PGP Desktop 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. The list contains 256 phonetically distinct words to represent the 256 possible byte values of 0 to 255.

  This list enables users to read PGP public key fingerprints over the phone to authenticate the public key. The fingerprint is 20 bytes long, thus 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, thus PGP Corporation has provided the word list as well to represent each byte using a word.

- **Subkeys list**. Shows the subkeys currently configured on this key. The master key on a PGP key is for signing only; you can add subkeys for encrypting or for signing. Creating additional encryption subkeys, with specific expiration dates, can help keep your data secure (because the encryption subkey changes regularly). Creating

additional signing subkeys for specific uses is helpful for file verification (and is required in some areas). Subkeys can be revoked, removed, or added to a PGP key without affecting the master key and the signatures on it.

To revoke a subkey, select the subkey to be revoked, click the backslash circle icon, click **Yes** on the confirmation dialog, enter the passphrase for the key, then click **OK** again. The subkey is revoked.

To remove a subkey, select the subkey to be removed, click the minus sign icon, then click **Yes** on the confirmation dialog. The subkey is removed.

If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change your Subkey settings.

To add a subkey, click the plus sign icon, configure the new subkey, click **Create**, enter the passphrase for the key, then click **OK** again. The subkey is added.

You can only modify subkeys on your private keys.

- **Revoker list**. Shows the Revoker keys currently configured on this key. A Revoker key can be used to revoke a key if the key itself or the passphrase to the key is ever lost.

  To update a Revoker key, select the Revoker key to be updated and then click the down-facing arrow icon. The Revoker key is updated.

  To remove a Revoker key, select the Revoker key to be removed, click the minus sign icon, click **Yes** on the confirmation dialog, enter the passphrase for the key, then click **OK** again. The Revoker key is removed.

  If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change your Revoker settings.

  To add a Revoker key, click the plus-sign icon, select the key to use as the Revoker key, click **OK**, click **Yes** on the confirmation dialog, enter the passphrase for the key, click **OK** again, then click **OK** on the information dialog. The Revoker key is added.

  You can only modify Revoker keys on your private keys.

- **ADK (Additional Decryption Key) list**. Shows the ADKs currently configured on this key. Messages encrypted by a key with an ADK are encrypted to the public key of the recipient and to the ADK, which means the holder of the ADK can also decrypt the message. Generally, ADKs are used as a corporate security measure if an employee is unable or unwilling to decrypt a message.

  To update an ADK, select the ADK to be updated and then click the down-facing arrow icon. The ADK is updated.

  To remove an ADK, select the ADK to be removed, click the minus sign icon, then click **Yes** on the confirmation dialog. The ADK is removed.

  If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change your ADK settings.

To add an ADK, click the plus-sign icon **[+]**, select the key to use as the ADK, click **OK**, click **Yes** on the confirmation dialog, enter the passphrase for the key, click **OK** again, then click **OK** on the information dialog. The ADK is added.

You can only modify ADKs on your private keys.

Adding and Removing Photographs

You can include a photograph to your Diffie-Hellman/DSS and RSA keys.

Although you can view for verification the photograph accompanied with someone's key, the digital fingerprint is the final word. Always check and compare it.

To add your photograph to your key:

1 Open PGP Desktop, then click **My Private Keys**.

2 Double-click the private key to which you are adding the photo.

The **Key Info** dialog for the selected key appears.

3 Click the plus-sign icon under the current photo for the key.

The **Add Photo** screen appears.

4 Drag and drop, or paste, your photograph onto the **Add Photo** screen.

The photograph can be from the Clipboard, a JPG, or BMP file. For maximum picture quality, crop the picture to 120 x 144 pixels before adding it. If you do not do this, PGP Desktop scales it for you.

5 Click **OK**.

The **Enter Passphrase** screen appears, unless the passphrase for the key you are modifying is cached.

6 Enter your passphrase for the key you are modifying, then click **OK**.

Your photo ID is added to your private key.

When you add or change key information, be sure to update it on the keyserver so that your most current key is always available.

To delete a photo ID:

1 Click the minus-sign icon under the existing photo.

A confirmation dialog box appears.

2 Confirm that this is your choice.

The photo is removed from the key.

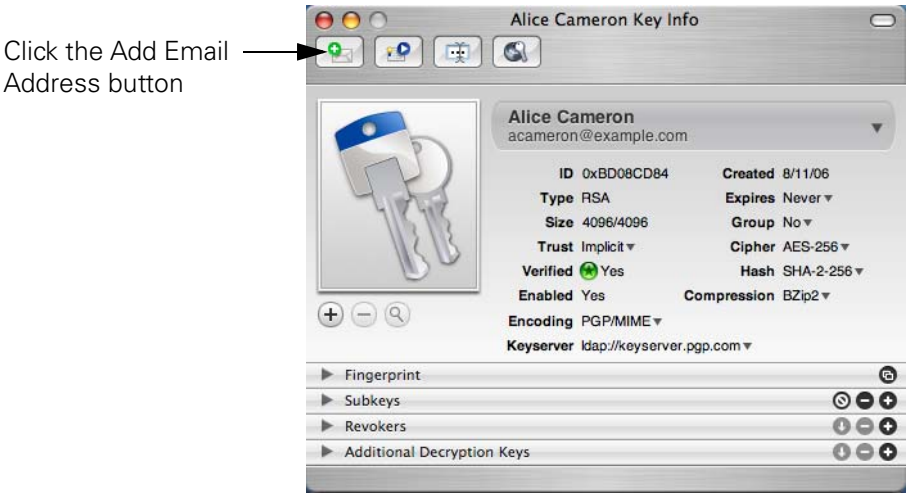
Managing User Names and Email Addresses on a Key

PGP Desktop supports multiple user names and email addresses on your keypair. These names and email addresses help others find your key so that they can send you encrypted messages.

To add a new user name/address to your keypair:

1 Open PGP Desktop, then double-click the appropriate key.

The **Key Info** dialog for the key you double-clicked appears.



2 Click the **Add Email Address** button.

The **Add Name** screen appears.

3 Enter the new **Full Name** and **Email Address** in the appropriate fields, then click **OK**.

The **Enter Passphrase** screen appears, unless the passphrase for the key you are modifying is cached.

4 Enter the private key passphrase of the key you are modifying, then click **OK**.

The new name is added to the end of the user name list associated with the key.

When you add or change information in your keypair, always synchronize it with your keyserver so that your most current key is always available.

To delete a name/email address from your keypair:

1 From the list of keys, click the triangle left of the key name.

2 Select the user ID you want to delete.

3 Press the Delete key on your keyboard. Alternatively, from the **Edit** menu, select **Clear**.

A confirmation dialog box appears.

4 Click **Delete**.

The user ID is deleted.

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 at the keyboard as you typed it in.

To change the passphrase for a split key, you must rejoin it first.

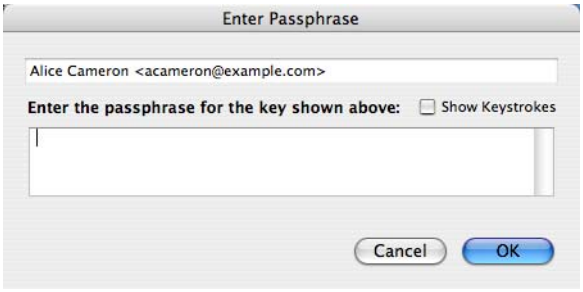
To change your private key passphrase:

1 Open PGP Desktop, then double-click the appropriate key.

The **Key Info** dialog for the key you double clicked appears.

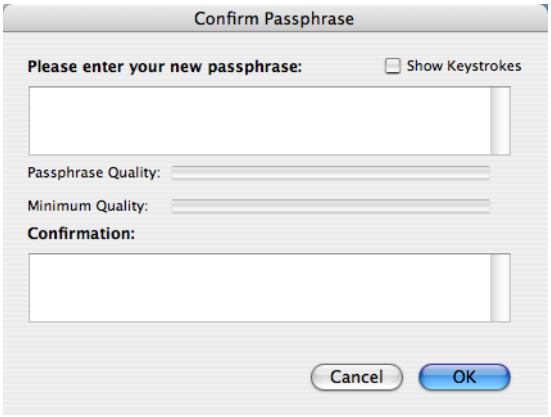
2 Click the Change Passphrase icon, then select **Change Passphrase** from the list of commands that appears.

The **Enter Passphrase** dialog appears.



3 Enter the **current** passphrase for the private key, then click **OK**.

The **Confirm Passphrase** dialog appears.



4 Enter your new passphrase in the first text box.

5 Press **Tab** to advance to the **Confirmation** box.

6 Confirm the new passphrase by entering it again.

The **Passphrase Quality** bar provides a basic guideline for the strength of the passphrase you are creating by comparing the amount of entropy in the passphrase you enter against a true 128-bit random string (the same amount of entropy in an AES128 key). Filling the Passphrase Quality bar gives you a strong passphrase that could take in the billions (billions with a 'b') of years to brute-force decrypt. Refer to "The Passphrase Quality Bar" on page 166 for more information.

7 Click **OK.**

An information dialog appears, telling you the passphrase has been changed.

8 Click **OK**.

The passphrase is changed.

If you are changing your passphrase because you feel that it has been compromised, it is recommended that you shred all backup keyrings, then make a backup copy of the key with the new passphrase.

Deleting Keys, User IDs, and Signatures

PGP Desktop gives you control over the keys on your keyrings, as well as the user IDs and signatures on those keys.

With public keys on your keyrings, you can delete:

- Entire keys.
- Any or all user IDs on a key.
- Any or all signatures on a key.

With your own keypairs, you can delete:

- Entire keypairs.
- Any or all signatures

To delete a key from your PGP keyring:

1. Open PGP Desktop, then click the **Keys** item.

   All keys on your keyring appear.

2. Select the key you want to delete.
3. From the **Edit** menu, select **Clear.**

   A confirmation dialog appears.

4. Click **OK.**

   The key is deleted from your keyring.

To delete a user ID or signature from a key:

1. Open PGP Desktop, then click the **Keys** item.

   All keys on your keyring appear.

2. Click the triangle to the left of the key with the User ID or Signature that you want to delete.

   The user IDs and signatures appear.

3. Click the user ID or signature that you wish to delete.
4. From the **Edit** menu, select **Clear.**

   A confirmation dialog appears.

5. Click **OK**.

   The user ID or signature is deleted.

Remember that you cannot delete a user ID from a keypair.

Disabling and Enabling Public Keys

Sometimes you may want to disable a public key on your keyring temporarily, which can be 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.

You cannot disable your keypairs.

To disable a public key:

1 Open PGP Desktop, then click the **Keys** item.

All keys on your keyring appear.

2 Double-click the public key you want to disable.

The **Key Info** dialog box for that key appears.

3 If the **Enabled** setting is **No**, then the key is already disabled.

4 If the **Enabled** setting is **Yes**, click that **Yes** setting.

A pop-up menu appears.

5 Select **No**.

The key is disabled.

A disabled key cannot be used for encrypting, signing, decrypting, or verifying.

To enable a disabled public key:

1 Open PGP Desktop, then click the **Keys** item.

All keys on your keyring appear.

2 Double-click the public key you want to enable.

The **Key Info** dialog box for that key appears.

3 If the **Enabled** setting is **Yes**, then the key is already enabled.

4 If the **Enabled** setting is **No**, click that **No** setting.

A pop-up menu appears.

5 Select **Yes**.

The key is enabled.

Verifying a Public Key

Being certain that a public key is genuine can be difficult. If the key owner physically hands the key to you on removable media you can be certain—but this is not usually practical, especially for users who are far apart. You could also be certain a key is genuine by getting it from the PGP Global Directory—but you may need to use a key that resides only on another keyserver.

For this reason, key verification—checking the key's digital fingerprint—is the best way to make sure that the key is genuine. Every key has a unique fingerprint. It can be found in the Key Info box, and it consists of a unique series of hexadecimal numbers or a corresponding list of words.

You can use the fingerprint to verify a key's authenticity in several ways, but the safest is to call the person and have them read the fingerprint to you over the phone. It is highly unlikely that someone would try to intercept the call, and you can quickly and easily verify the key.

To check the digital fingerprint of a public key:

1 Open PGP Desktop, then click the **Keys** item.

All keys on your keyring appear.

2 Double-click the public key with the fingerprint that you want to check.

The **Key Info** dialog appears.

3 Locate the **Digital Fingerprint** in the second section of the **Key Info** dialog.

If necessary, click the triangle to face downward and display the fingerprint, which is shown either in hexadecimal format (10 sets of four characters per set) or word list format (four columns with five unique words per column).

4 Compare the fingerprint on the key with the original fingerprint.

If the two are the same, then you have the real key—otherwise, you likely do not.

The word list is made up of special authentication words that PGP Desktop 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.

5 If you have a forged key, delete it.

If you have not yet already searched the PGP Global Directory for the real public key, look for it there: https://keyserver.pgp.com.

Signing a Public Key

When you create a keypair, the keys are automatically signed. Similarly, once you are sure a key belongs to the correct person, you can sign that person's public key, indicating that you have verified the key. When you sign someone's public key, a signature icon along with your user name is shown attached to that key.

If you are using PGP Desktop in a PGP Universal-managed environment, key signing may be disabled.

If you import a keypair from a backup or from a different computer, that keypair needs to be signed.

To sign a key:

1 Open PGP Desktop, then click the **Keys** item.

All keys on your keyring appear.

2 Select the key you want to sign, then from the **Keys** menu, select **Sign.**

You can also Ctrl-click the key (or right-click it if you have a two-button mouse). When the contextual menu appears, select **Sign.**

The **Sign Key** dialog appears with the user name/email address and hexadecimal fingerprint displayed in the text box.

3 From the **Sign With Key** menu, select which of your keys you want to sign with.

4 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. The checkbox indicates your approval that your signature be exported.

5 In the **Select Items to Sign** box, verify that you are signing the right key.

6 If you would like to configure additional options, such as such as signature type and signature expiration, click the **Options** button.

7 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.
- **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.

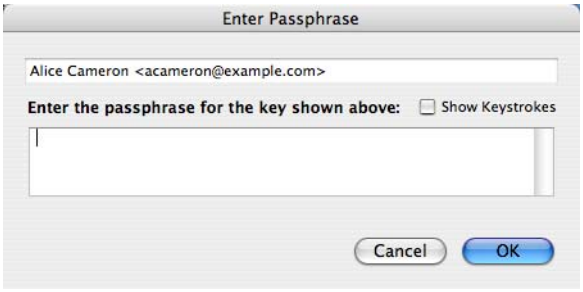
8 In the **Expires** field, select **Never** if you do not want this signature to expire. Otherwise, select a date for it to expire.

9 In the **Advanced** field, specify a maximum depth for trust and a domain restriction:

- The **Maximum 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.
- 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.

10 Click **Sign**.

The **Enter Passphrase** dialog appears.



11 Type the passphrase of the signing key, if required. PGP Desktop does not ask you to type your passphrase if it is cached.

12 Click **OK**.

The key is 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 (those whose keys you may get in the future).

For example, if you get a key from someone who you have designated as trustworthy, and they have signed the key, that key is considered valid—even though you have not done the check yourself.

You must sign a key before you can set a trust level for it.

Public keys can have trust levels of:

- **None:** You do not trust the owner to act as an introducer.
- **Marginal:** You partially trust the owner to act as an introducer.
- **Full:** You fully trust the owner to act as an introducer.

Your keypairs can have trust levels of:

- **None:** You do not trust the owner to act as an introducer
- **Implicit:** It is your own key, so therefore you trust it.

For more information about trusting keys, see *An Introduction to Cryptography*.

To grant trust to a key:

1 Open PGP Desktop, then click the **Keys** item.

All keys on your keyring appear.

2 Double-click the key for which you are granting trust.

The **Key Info** dialog appears.

3 In the **General Information** section, click the current **Trust** field setting.

A menu of trust settings appears.

4 Select the desired setting.

Selecting a Trust setting of None or Marginal is not intended to indicate that a owner of a key is untrustworthy or dishonest. It means that **you do not have enough information** to be sure that a key's owner or source is genuine.

Working with Subkeys

A PGP Desktop keypair consists of these elements:

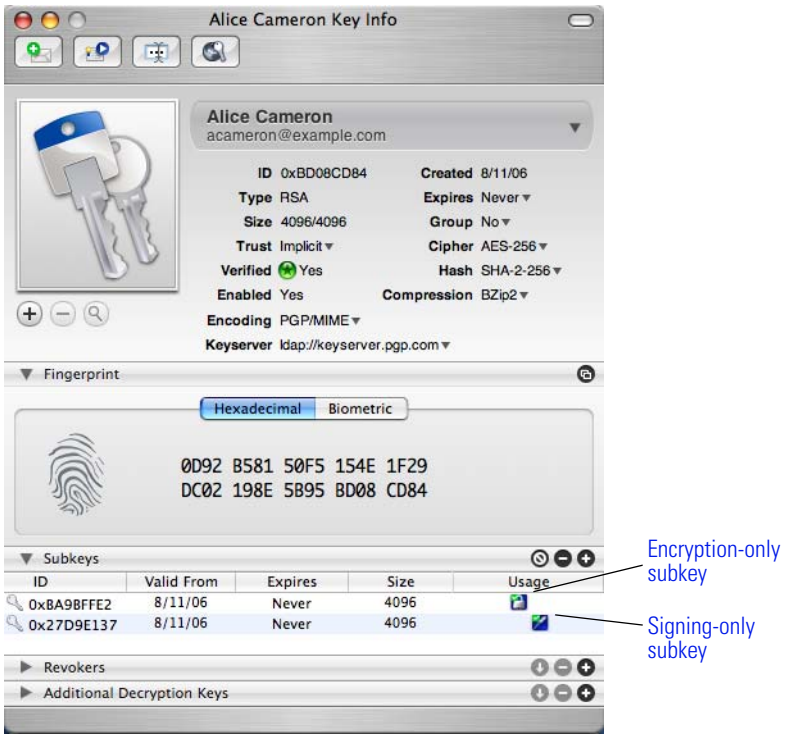
- the **Master Key**, for signing only;
- one mandatory **Subkey** for encryption;
- one or more *optional* **Separate Subkey(s)** for signing, encryption, or signing/encryption.

The Master Key is used by default for signing, while a subkey is always used for encryption. This can improve the security of a PGP Desktop keypair, as a separate encryption subkey can be revoked, removed, or added to the PGP Desktop keypair without affecting the Master Key or the signatures on it.

In addition to the Master Key and the mandatory encryption subkey, you have the option of creating one or more additional subkeys for your PGP Desktop keypair. You can create any combination of subkeys that can be used for encryption only, for signing only, or for both encryption and signing.

You can view the subkeys of a keypair from the Key Properties dialog. The Usage column indicates the function that a subkey performs:

- Encryption subkeys display a blue padlock symbol.
- Signing subkeys display a blue pen symbol.
- Subkeys used for both encryption and signing display both symbols.



PGP Desktop uses the last valid Encryption Subkey that is listed in the Subkeys section of the Key Properties dialog. The same is true for Signing Subkeys. If the bottommost subkey of either type is not valid, PGP Desktop checks the key above it, and keeps repeating that pattern until it finds valid subkeys for both encryption and signing functions (it uses the Master key for signing if there is no separate Signing Subkey). PGP Desktop continues using a subkey as long as it remains valid.

Subkeys that both encrypt and sign are treated as separate subkeys. In some cases, PGP Desktop might use only the encryption portion of an encryption/signing subkey, or only the signing portion.

The symbols for the subkeys that are in use have a small overlay of a white checkmark against a green background.

Using Separate Subkeys

Here are some examples of how additional separate subkeys can be useful:

- **Multiple encryption subkeys** that are valid during different portions of the keypair's lifetime can increase security. You can create encryption subkeys that have the Start and Expiration dates set so that only one encryption subkey at a time is valid. For example, you could create several encryption subkeys that are valid only during one future year (make sure you specify correct dates). The Encryption Subkey in use then changes with the new year. This can be a useful security measure, as it provides an automatic way to switch to a new encryption key periodically without having to recreate and distribute a new public key. Expired subkeys display a key icon with a red clock.
- **Separate signing subkeys** are needed in regions where separate subkeys for signing are required for legally-binding digital signatures.

The separate subkeys that you can create depend on the type of keypair that you are working with:

- For RSA keypairs, you can create subkeys for encryption, signing, and encryption/signing.
- For Diffie-Hellman/DSS keypairs, you can create subkeys for encryption or signing, but you cannot create subkeys that both encrypt and sign.
- For older PGP Legacy keypairs, subkeys are not supported.

Viewing Subkeys

You can view and change the subkey information on your keypairs. However, you can only view subkey information on the public keys on your keyring.

To see what subkeys are on a key:

1. Open PGP Desktop, then click the **Keys** item.

   All keys on your keyring appear.

2. Double-click the key with the properties you want to view.

The **Key Properties** dialog for the key you selected appears.

3 Click the triangle to the left of **Subkeys**.

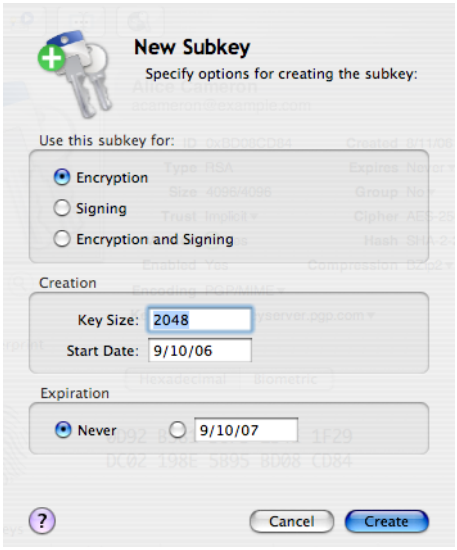
The Subkeys information for this key appears.

Creating New Subkeys

To create new subkeys for a keypair:

1 In the **Subkeys** section of the **Key Properties** dialog, click the plus-sign icon.

The **New Subkey** dialog appears.



2 In the **Use this subkey for** area, select **Encryption, Signing,** or **Encryption and Signing,** depending on how you want to use the new subkey.

3 In the **Key Size** field, type a key size from 1024 to 4096 bits.

4 In the **Start Date** field, enter a date on which the subkey you are creating becomes effective.

5 In the **Expiration Date** field, select **Never,** or specify a date. This information controls when the subkey expires.

To avoid confusion when maintaining more than one subkey on your keypair, try not to overlap the start and expiration dates of your subkeys.

6 Click **Create**.

The **Passphrase** dialog appears.

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

The subkey is created.

When you add or change information in your keypair, update it on the keyserver so that your most current key is always available. With the key selected in the Keys list, from the **Keys** menu select **Update Selection.**

Revoking Subkeys

To revoke a subkey:

1. In the **Subkeys** section of the **Key** Properties dialog, select the subkey you want to revoke.
2. Click **Revoke** (backslash-circle icon above the subkey list).

   A confirmation dialog box appears.
3. Click **OK** to revoke the subkey.

   The **Passphrase** screen appears.
4. Type your passphrase, then click **OK**.

   The subkey is revoked and the icon changes to a key with a red circle/slash.

Removing Subkeys

To remove a subkey:

1. In the **Subkeys** section of the **Key Properties** dialog, select the subkey you want to remove.
2. Click **Remove** (a minus-sign icon above the subkey list).

   A confirmation dialog appears.
3. Click **OK** to remove the subkey.

   The subkey is removed.

Working with ADKs

An additional decryption key (ADK) is a key generally used by security officers of an organization to decrypt messages that have been sent to or from employees within the organization.

Messages encrypted by a key with an ADK are encrypted to the public key of the recipient and to the ADK, which means the holder of the ADK can also decrypt the message.

Although your PGP administrator should not ordinarily need to 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.

You can only modify ADKs on your personal keypairs.

To Add an ADK to a Keypair

1. Open PGP Desktop, then click the **Keys** item.

   All keys on your keyring appear.

2. Double-click the keypair to which you are adding the ADK.

   The **Key Info** dialog for the key you double-clicked appears.

3. If necessary, click the triangle icon, on the left side of the **Additional Decryption Keys** section, so that it is pointing downward.

   The ADK information for this key appears, if it has been configured.

4. Click the plus-sign icon on the right side of the **Additional Decryption Keys** section.

5. From the list that appears, select the key you want to use as the ADK.

6. Click **OK.**

   The **PGP Enter Passphrase for Key** dialog appears.

7. Enter the passphrase for the key to which you are adding the ADK, then click **OK**.

   The ADK is added.

To Update an ADK

1. Select the ADK you want to update from the list of ADKs.

   The selected ADK highlights.

2. Click the down-facing arrow icon.

   The ADK is updated.

To Remove an ADK

1. Select the ADK you want to remove from the list of ADKs.

   The selected ADK highlights.

2. Click the minus-sign icon.

   A **PGP Warning** dialog appears, asking if you are sure you want to remove the ADK.

3. Click **OK** to remove the ADK.

   The ADK is removed.

Working with Revokers

It is possible that one day you might forget your passphrase or lose your keypair (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.

For a key to appear revoked to another user, both the revoked key and the Designated Revoker key must be on their 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 revoker's key is not present on a person's keyring, then the revoked key does not appear revoked to that user and they may continue to encrypt to it.

This feature is available for both Diffie-Hellman/DSS and RSA keys.

You can only change revoker information on your keypairs. If a public key on your keyring has a revoker, you can see that information but you cannot change it.

Appointing a Designated Revoker

To add a designated revoker to your key:

1 Open PGP Desktop, then select **My Private Keys,** under the Keys item.

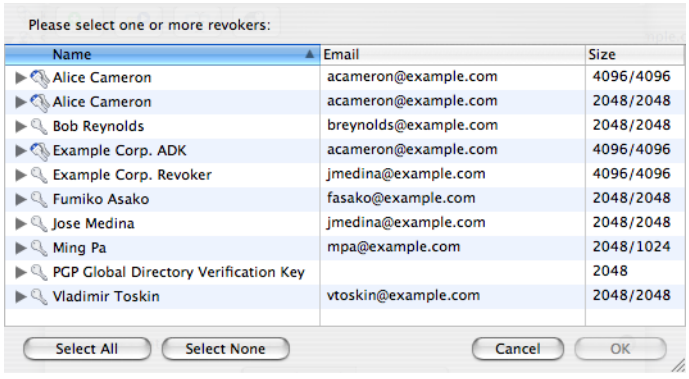
All of the keys on your keyring appear.

2 Double-click the key to which you are adding a revoker.

The **Key Info** screen for the key you selected appears.

3 Click the plus-sign icon on the right side of the **Revokers** section.

The **Select key(s)** dialog appears.



4 Select the key you want to use as the revoker key, then click **OK.**

A **PGP Warning** dialog appears, asking if you are certain that you want to grant revoker privileges to the selected key(s).

5 Click **Yes** to continue or **No** to cancel.

The **PGP Enter Passphrase for Key** screen appears.

6 Enter the passphrase for the keypair to which you are adding the revoker, then click **OK**.

A **PGP Information** dialog appears.

7 Click **OK**.

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 keyserver.

Revoking a Key

If the situation ever arises that you no longer trust your personal keypair, you can revoke your key, which tells everyone to stop using your public key.

The best way to circulate a revoked key is to place it on a public keyserver.

To revoke a key:

1 Open PGP Desktop, then select **My Private Keys** under the Keys item.

All of the keys on your keyring appear.

2 Ctrl-click the key you want to revoke (or right-click if you are using a two-button mouse).

A contextual menu appears.

3 Select **Revoke**.

A Confirm Revocation dialog appears, asking if you are sure you want to revoke this key.

4 Click **OK** to confirm your intent to revoke the selected key or **Cancel** to cancel.

5 Enter the passphrase for the keypair you are revoking, then click **OK**.

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

6 Synchronize the revoked key so everyone will know not to use the now revoked public key.

Splitting and Rejoining Keys

Any private key can be divided up, or *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.

A typical use would be an organization that keeps a key that is split between multiple individuals. Whenever the need to sign with that key arises, the shares of the key are rejoined temporarily.

Split keys are **not** compatible with versions of PGP Desktop previous to 6.0.

Creating a Split Key

When you split a key, the shares are saved as files, either encrypted to the public key of a shareholder, or encrypted conventionally (using a passphrase) 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.

To create a split key:

1 Open PGP Desktop, then click the **PGP Keys** item.

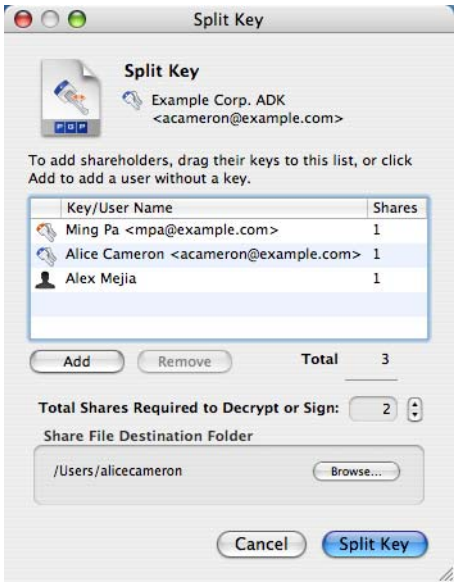
All of the keys on your keyring appear.

2 Select the keypair you want to split.

The selected keypair highlights.

3 Select **Keys > Share Key > Make Shared.**

The **Split Key** dialog appears.



4 Add shareholders for the split key by dragging and dropping their keys in the **Key/ User Name** list.

5 To add a shareholder who does not have a public key, **that person must be physically present to enter their own passphrase.** Click **Add**.

6 Allow the shareholder to type in their passphrase twice, then click **OK**.

Unnamed User appears in the list.

7 Double-click Unnamed User and enter a descriptive name for the person or organization holding the shares.

8 To specify a location for the split shares, click **Browse** in the Share File Destination Folder, then select the desired location.

9 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.

By default, each shareholder is responsible for one share. To increase the number of shares a shareholder possesses, double-click the number in the Shares column and enter the number of shares they control.

10 Click **Split Key**.

The **Confirm Key Split** dialog appears.

11 Click **OK** to continue splitting the key.

The Passphrase screen appears.

12 Enter the passphrase for the key being split, then click **OK**.

A confirmation dialog box opens.

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 and a .shf extension.

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

Rejoining Split Keys

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

Rejoining key shares locally requires the shareholder's 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. The PGP Desktop Transport Layer Security (TLS) feature provides a secure link to transmit key shares, allowing multiple individuals in distant locations to securely sign or decrypt with their key share.

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 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, make sure the remote shareholders have PGP Desktop installed and are prepared to send their key share file. Remote shareholders must have:

- Their key share files and passwords.
- A keypair (for authentication to the computer that is collecting the key shares).
- A network connection.
- The IP address or Fully Qualified Domain Name of the computer that is collecting the key shares.

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

3 Ctrl-click the file(s) and select **Sign or Decrypt** from the PGP context menu.

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

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

The **Key Share Collection** screen appears.

5 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 removable drive, or a mounted drive. Continue with Step 6
- **If you are collecting key shares over the network,** click **Start Network**.

  The **Passphrase** dialog box opens. In the **Signing Key** box, select the keypair 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.

  When a share is received, the **Remote Authentication** screen appears. 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.

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

7 Continue collecting key shares until the value for Total Shares Collected matches the value for Total Shares Needed on the Key Shares Collection screen.

8 Click **OK**.

The file is signed or decrypted with the split key.

Protecting 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 flash drive, 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.

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 removable disk. By default, the private keyring (secring.skr) and the public keyring (pubring.pkr) 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 Desktop to back up your keyrings automatically after you close PGP Desktop. Your keyring backup options can be set in the Keys tab of the Preferences panel.

12 Shredding

Secure file deletion

This chapter describes shredding (securely deleting) files or folders using the PGP Shredder feature in PGP Desktop. These topics are available:

About PGP Shredder

If you want to destroy sensitive files or folders completely, use the PGP Shredder feature. When you delete files or folders using PGP Shredder, all traces of the item are removed.

The PGP Shredder feature works by overwriting your data with random text. It repeats this multiple times, or *passes*. You can set the number of passes that the PGP Shredder feature makes whenever it deletes a file—do that by opening the Disk panel of the Preferences screen. See "Disk Preferences" on page 159 for more information about setting preferences.

When set for three passes, PGP Shredder exceeds the media sanitization requirements specified in the Department of Defense 5220.22-M standard. Security continues to increase up to approximately 28 passes. The PGP Shredder feature is capable of up to 49 passes, but remember that more passes means more time needed for secure deletion.

There are multiple ways to use PGP Shredder:

- **Via the PGP Shredder icon**. When PGP Desktop was installed, the PGP Shredder feature was installed into the same directory as the PGP Desktop application. Creating an Alias to the PGP Shredder icon, then moving the Alias to the Dock or Desktop makes the PGP Shredder convenient and easy to use.
- **Via the PGP Shredder icon on the PGP Toolbar**. Click the PGP Shredder icon in the Toolbar, then browse to the file/folder you want to shred.
- **Via the Shred command under the File menu**. Select the Shred command (from the File menu), then browse to the file/folder you want to shred.
- **From the Finder**. The PGP Shredder is available in the Finder by Ctrl-clicking or (right-clicking if you are using a two-button mouse) the file or folder that you want to delete securely.

Some filesystems use a feature called Journaling. Apple has introduced this feature for Mac OS Extended (HFS+) filesystems in Mac OS X 10.2.2. Journaling causes a copy of everything written to disk to be written a second time in a private area of the filesystem. Thus, wiping the original file causes the original file to be wiped while the original file data is written to another part of the disk. To avoid this problem, do not use the Journaling feature. Journaling can be disabled using Apple's Disk Utility. For more information, from the Apple Support website, refer to Technical Article ID 107249.

Deleting Items Permanently Using PGP Shredder

With the PGP Shredder feature, erasing sensitive files and folders permanently is as easy as deleting them the usual way.

Many programs automatically save files in progress, so backup copies of the file you deleted may exist. After you delete the primary copy of a file, it is recommended that you then use the PGP Shredder feature to delete any backup copies securely.

The shred session can be lengthy, depending on such factors as the number of passes you specified, the speed of the processor, and how many other applications are running.

Shredding Files using the PGP Shredder icon

To shred a file or folder using the PGP Shredder icon:

1 Locate the file or folder you want to delete securely.

2 Drag the file or folder onto the PGP Shredder icon.

A confirmation dialog appears.

3 Click **OK**.

The file or folder is deleted from your system securely. You can also use an Alias of the PGP Shredder icon the same way.

Shredding Files using the Shred Files Icon in the PGP Desktop Toolbar

To shred a file or folder using the PGP Desktop Toolbar:

1 Click the **Shred Files** icon in the Toolbar.

2 Locate the file or folder you want to Shred, then click **Shred**.

A confirmation dialog appears.

3 Click **OK**.

The file or folder is securely deleted from your system.

Shredding Files using the Shred Command from the File menu

To shred a file or folder using the Shred command:

1. From the **File** menu, select **Shred.**
2. Navigate to the file or folder you want to Shred, then click **Shred**.

   A confirmation dialog appears.
3. Click **OK**.

   The file or folder is securely deleted from your system.

Shredding Files in the Finder

To shred a file or folder in the Finder:

1. Open a Finder window.
2. In the Finder, locate the file or folder that you want to shred.
3. Ctrl-click the file or folder (or right-click it if you are using a two-button mouse).

   A contextual menu appears.
4. From the **PGP** menu, select **Shred.**

   A confirmation dialog appears.
5. Click **OK**.

   The file or folder is securely deleted from your system.

A Setting PGP Desktop Preferences

Adjusting settings to suit your needs

PGP Desktop is configured to accommodate the needs of most users, but you can adjust some settings to suit your requirements. You specify these settings on the **Preferences** screen.

Accessing PGP Desktop Preferences

To access the **Preferences** screen:

1 Open PGP Desktop.

2 From the **PGP** menu, select **Preferences**.

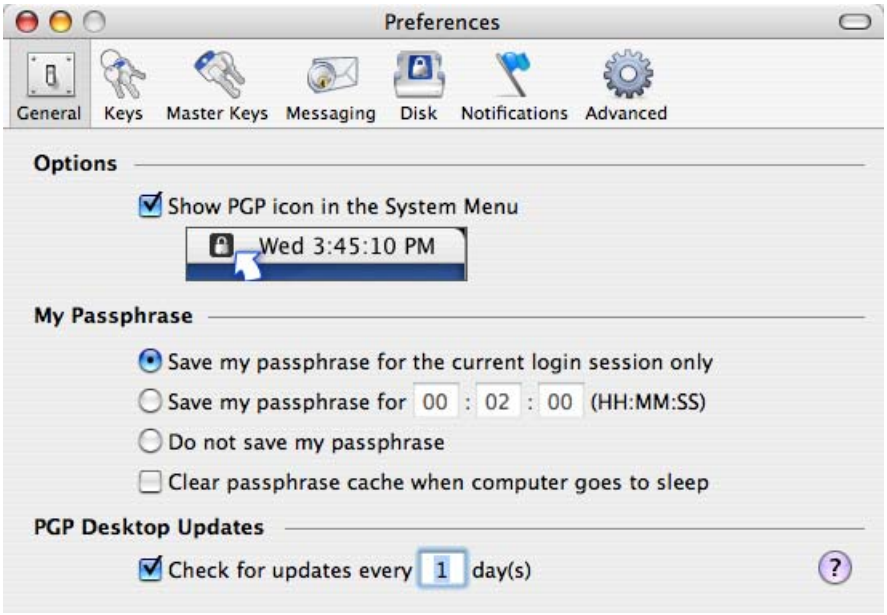
You can move between different kinds of preferences by clicking the icons at the top of the **Preferences** screen.

When you are done setting preferences, click the close button (the red circle in the upper left corner of the screen).

To get help for the fields on any Preferences screen, click the **Help** question-mark icon.

General Preferences

The **General** Preferences panel covers a variety of PGP Desktop settings.



The **General** preferences are:

- **Show PGP icon in the System Menu.** When enabled, the PGP Desktop icon appears in the Mac OS X Menu Bar while PGP Desktop is active on the system. The PGP Menu Bar icon provides easy access to PGP Desktop functions.

  To remove the PGP Desktop icon from the Menu Bar, deselect the checkbox.

  To restore the PGP Desktop icon to the Menu Bar, navigate to the General preferences screen and select the **Show PGP icon in the System Menu** checkbox.

If you are using PGP Desktop in a PGP Universal-managed environment, this option may be required.

Removing the PGP Desktop icon from the Menu Bar does *not* shut down PGP Desktop services; they continue running.

To stop PGP Desktop services:

a Press the **Option** key.

b In the Menu Bar, click the PGP Desktop icon, then select **Quit**.

PGP Corporation suggests you do not stop PGP Desktop services unless required to do so.

- **Save my passphrase for the current login session only**. Automatically saves your passphrase in memory until you log off your computer. This is called **caching** your passphrase. If you enable this option, you are prompted for your passphrase once per private key. You are not prompted to enter it again for the same key until you log off your computer.

When this option is enabled, it is very important that you log off your computer before leaving it unattended. (You can log out by selecting **Log out [your name]** from the Apple menu.) If you never log off, your passphrase can remain cached for weeks, allowing anyone to read your encrypted messages, or encrypt messages with your key while you are away from your computer. If you normally remain logged on to your computer for long periods of time, consider choosing one of the other passphrase caching options.

- **Save my passphrase for X**. Automatically saves your passphrase in memory for the specified duration of time. If you enable 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 specified time has elapsed. The three number fields are for **hours, minutes, seconds,** respectively. The default setting is two minutes.
- **Do not save my passphrase**. Prevents your passphrase from being stored in memory. If you enable this option, you must enter your passphrase each time it is needed.
- **Clear passphrase cache when computer goes to sleep**. Enable this preference to have PGP Desktop clear any saved passphrases from memory when your computer goes into Sleep mode. (Not all computers have a Sleep mode.)
- **Check for updates every X day(s).** When enabled, PGP Desktop checks for software updates automatically at the specified interval. The default interval is one day. If a newer version of PGP Desktop is available for download, a notification screen is displayed to notify you of the new version and help you download it.

This option requires an available Internet connection to work correctly.

When this option is disabled, PGP Desktop does not automatically check for software updates. If you are using PGP Desktop in a PGP Universal-managed environment, PGP Desktop searches for updates on its associated PGP Universal Server.

If you are using PGP Desktop in a PGP Universal-managed environment, this option may be required.

Keys Preferences

The **Keys** Preference panel covers settings that apply to PGP Desktop keys.

The **Keys** preferences are:

- **Synchronize with keyservers daily**. When selected, PGP Desktop performs a daily synchronization of the public keys on your keyring with your list of keyservers. This list includes the PGP Global Directory.

If you are using PGP Desktop in a PGP Universal-managed environment, this option may be required.

If changed versions of the keys are available, they are downloaded automatically. If the keyserver notifies PGP Desktop that a key is removed from the keyserver, PGP Desktop disables that key on the local keyring.

If you use PGP Desktop to make a change to a public key on your Keyring, that change is not automatically uploaded from your computer to any keyserver. You must manually upload the changed key to the desired keyserver. PGP Desktop prompts you to upload changed keys when you quit. Otherwise, to send the key to the keyserver, right-click the changed key, select **Send To** from the shortcut menu that appears, and then select the desired keyserver from the list.

- **Automatically lookup keys on keyservers when verifying signatures.** When this option is enabled, you can specify that PGP Desktop should search the configured keyservers for the necessary public key if you receive an email message signed by a private key and you do **not** have the corresponding public key on your local keyring.

If you are using PGP Desktop in a PGP Universal-managed environment, this option is not used. Your PGP Universal Server defines whether keys are looked up and, if found, if they are cached. Keys found in a PGP Universal-managed environment are never saved to your keyring.

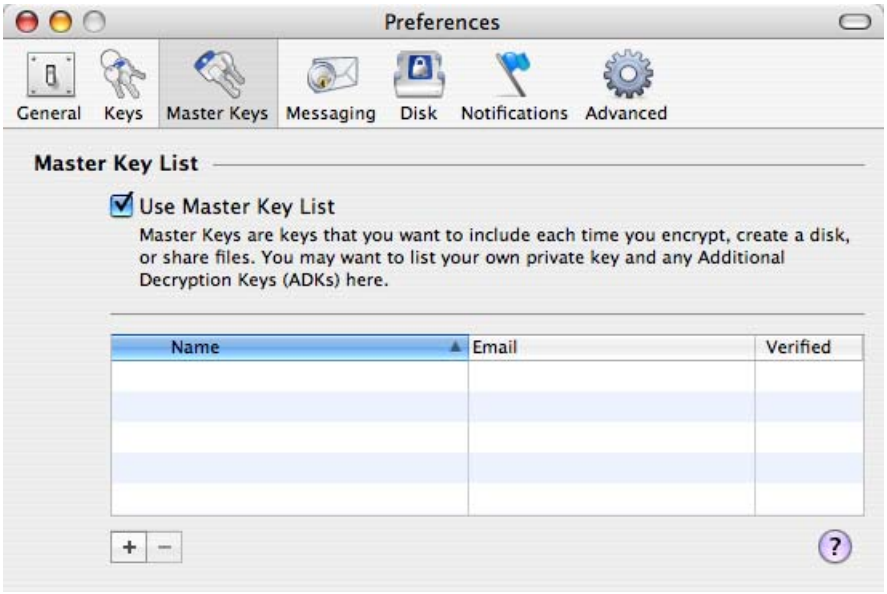
If the public key *is* found on the keyserver, there are three options:

  - **Do not save to my keyring.** Any key(s) found on the configured keyservers are used only once, to verify the signature with which you are currently working. The key is not saved to your keyring.
  - **Ask to save to my keyring.** Specifies that PGP Desktop should ask if you want to save found keys to your local keyring.
  - **Save keys to my keyring**. Specifies that found keys are automatically be saved to your local keyring.

- **Backup keys upon exiting PGP Desktop.** When enabled, PGP Desktop automatically backs up your keys to the location you specify:
  - **to my keyring folder (default).** When selected, your keys are backed up to the default keyring folder on your system.
  - **to this location.** When selected, your keys are backed up to the location on your computer that you specify. Click **Browse** to set a location.

Master Keys Preferences

The **Master Keys** Preferences panel is a set of keys that you want added by default any time you are selecting keys for messaging or disk encryption. This saves you the step of dragging the keys that you regularly use into the **Recipients** box.



The **Master Keys** preferences are:

- **Use Master Key List**. Select if you wish to use the Master Key List. You cannot add or remove keys from the Master Key List unless this checkbox is selected.

To add keys to the Master Key List:

1 Click the plus-sign icon (**+**) beneath the key list.

The **Select Master Keys** box appears.

2 From the **Name** list on the left, select the key(s) that you want to use. You can Shift-click or Cmd-click to select multiple keys.

3 After selecting the keys you want, click **OK.**

The keys you have selected appear in the Master Key List.

To remove keys from the Master Key List:

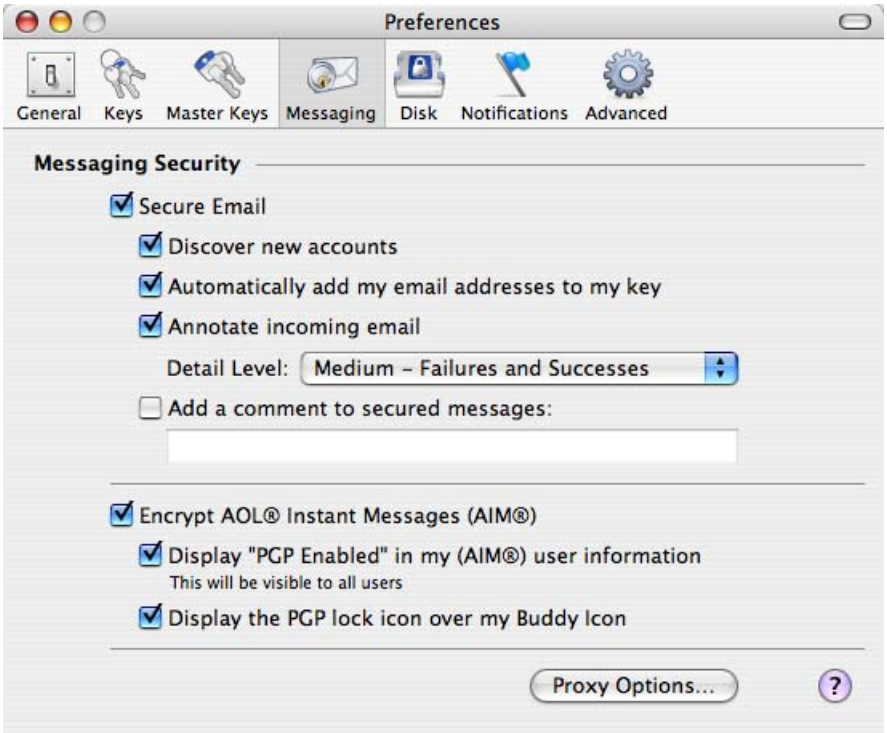
1 Select the key(s) that you want to remove. You can Shift-click or Cmd-click to select multiple keys.

2 Click the minus-sign icon (–) beneath the key list.

The key(s) are removed.

Messaging Preferences

The **Messaging** Preferences panel contains settings that apply to your messaging security. It also provides access to email and IM settings.



The **Messaging** preferences are:

- **Secure Email.** Select the **Secure Email** checkbox if you want PGP Desktop to automatically secure all your email accounts. When enabled, PGP Desktop intercepts both incoming and outgoing email messages, and secures them based on the appropriate policies.

  Deselect the **Secure Email** checkbox to stop PGP Desktop from securing your email accounts.

  If you select the **Secure Email** checkbox, you can choose these additional options:

  – **Discover new accounts.** Select this checkbox if you want PGP Desktop to monitor your email activity and automatically discover new email accounts that you are using. It then secures messages sent using those accounts.

  – **Automatically add my email addresses to my key.** If you select this checkbox, PGP Desktop automatically adds to your key the email addresses that you use to send messages. This option is enabled by default.

    Deselect this checkbox to prevent email addresses from being automatically added to your key. This has privacy value; for example, if you wish to prevent someone from finding your email address.

  – **Annotate incoming email.** Select this checkbox if you want incoming email messages to be annotated with explanatory text detailing the actions that PGP Desktop took when processing your incoming messages. You can choose from three annotation levels:

    Maximum: Verbose Annotation. Adds annotations to your incoming email detailing every action that PGP Desktop has taken during message processing.

    Medium: Failures and Successes [**this option is the default**]. Provides annotations when there has been a processing failure, such as an unknown key, or unknown signer. The Medium setting adds annotation when incoming email has been successfully decrypted and/or signed.

    Minimum: Failures Only. Only provides annotations when there has been a processing failure.

  – **Add a comment to secured messages.** When enabled, the text you enter here is always included in messages you encrypt or sign. Comments entered in this field appear below the `--BEGIN PGP MESSAGE BLOCK--` text header and PGP Desktop version number of each secured message. These comments are not visible in decrypted email.

If you are using PGP Desktop in a PGP Universal-managed environment, there may already be text in this field.

- **Encrypt AOL® Instant Messages (AIM®).** Enable if you want PGP Desktop to encrypt instant message sessions with supported instant messaging clients. The other participant in the IM session must also be using PGP Desktop.

  AOL® Instant Messenger™ and iChat software applications are supported.

- **Display "PGP Enabled" in my AIM user information**. When selected, **PGP Enabled** is added to your screen name in such places as the AIM Buddy List and the Get Buddy Info command. When disabled, your screen name appears without **PGP Enabled**. The appearance of this text may vary depending on your instant messaging client.
- **Display the PGP lock icon over my buddy icon**. When selected, the PGP stylized lock icon appears with your buddy icon, so others can see that the IM session is protected. When disabled, your icon appears normally.

- Click **Proxy Options** to access advanced messaging settings.

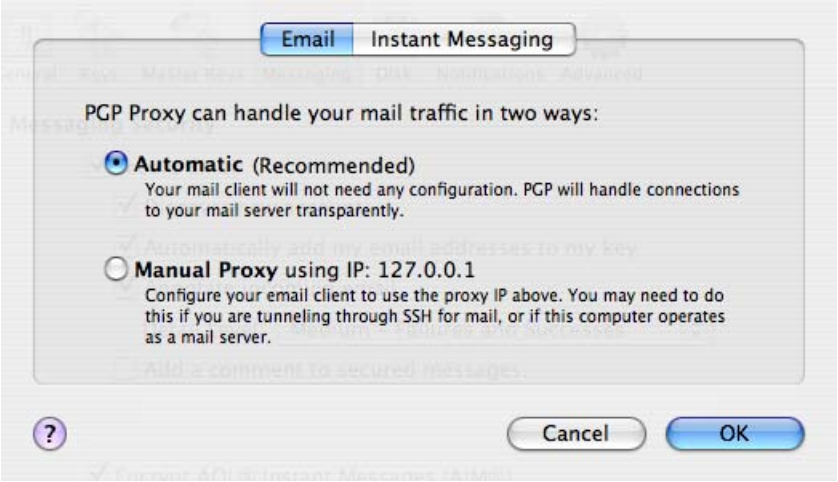
Proxy Options

The **Proxy Options** button gives you access to advanced email and IM preferences.

Email Preferences

If your computer needs to have a proxy manually configured so that you can send and receive email, you would use this feature.

PGP Desktop works between your email application and the mail server that provides your mail. This configuration enables PGP Desktop to filter, or *proxy,* your email traffic for you automatically. PGP Desktop can protect your messages, based on the applicable policy, without interrupting your work.

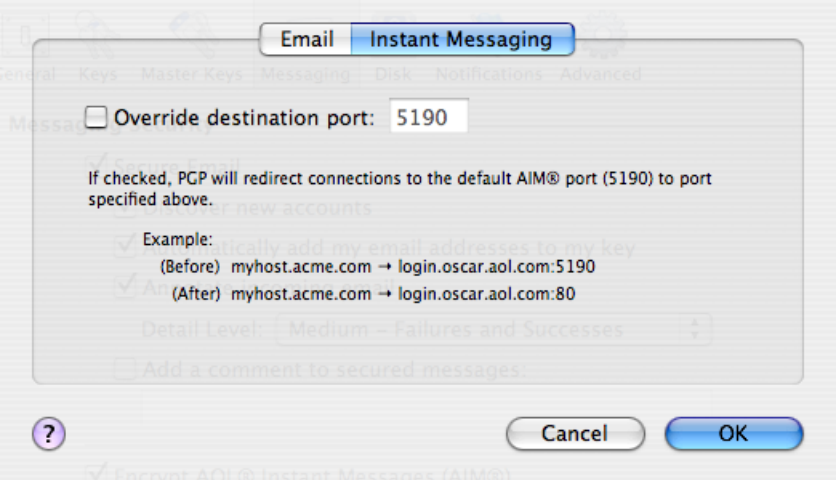


Normally, you do not need to change the PGP Proxy settings. However, some users must specify proxy settings manually. Choose the setting that your network administrator recommends:

- **Automatic:** The default, recommended setting. Your email is protected automatically and transparently. PGP Corporation recommends that you leave this option selected unless you are instructed to use the manual proxy setting.
- **Manual Proxy.** This option is needed if your computer is "tunneling" through SSH to your mail server, or if the computer on which you are running PGP Desktop also functions as a mail server.

Instant Messaging Preferences

If your computer is behind a network firewall, you may need to change the network port that AIM uses for your IM chat sessions. Most users do not need to change this setting.



- **Override destination port.** Select this checkbox to change the port that AIM uses for your IM sessions. Change the value to one other than the default (5190). Your network administrator can tell you if you need to change this setting and, if so, what port number to use.

Disk Preferences

The **Disk** Preferences panel contains settings that apply to volumes protected using the PGP Virtual Disk and the PGP Shredder features.

If you are using PGP Desktop in a PGP Universal-managed environment, these preferences may already be configured.

The **Disk** preferences are:

- **Allow PGP Disks to unmount even while files are open.** Normally, you cannot automatically unmount a PGP Virtual Disk if any of the files in that volume are open. Enabling this option allows unmounting even with open files, a practice known as a forcible unmount.

  You may lose data if you forcibly unmount a PGP Virtual Disk volume with open files.

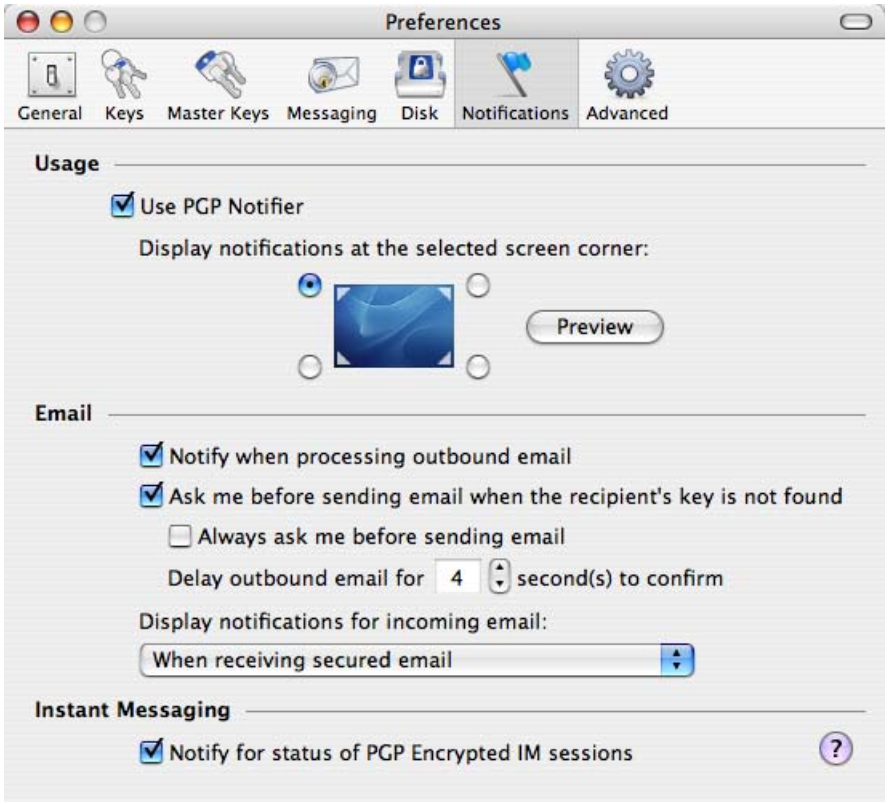
- **Unmount when computer goes to sleep.** When enabled, PGP Desktop automatically unmounts any mounted PGP Virtual Disk volumes when your computer goes into Sleep mode.
  - **Prevent sleep if disk(s) cannot be unmounted.** This setting is inactive until you select the **Unmount when computer goes to sleep** checkbox. This setting prevents your computer from sleeping if a PGP Virtual Disk volume cannot be unmounted.
- **Number of passes.** The PGP Shredder feature removes your file(s) securely by deleting them normally, then using numerous "0" characters to overwrite the disk space that had been occupied by the files you just deleted.

  Using this method, your files can be deleted very securely with only a few overwriting "passes." For this reason, a setting of **3** is the default, and offers an extremely high level of security, but you can adjust this setting to reflect the level of security that you desire.

  Be aware that the cost of added security is increased time needed to shred your file(s), depending on several factors, particularly the speed of your computer's processor.
- **Always warn me before shredding.** Select this checkbox if you would like a confirmation dialog box to appear before any shredding takes place. This gives you a chance to double-check that only the files you intended are the ones that are to be shredded. This option is selected by default.

Notifications Preferences

The **Notifications** Preferences panel contains settings that apply to the PGP Desktop Notifier feature, which displays status messages in a corner of your screen when you send or receive email messages. It also displays status messages when you use PGP Desktop disk features.



The **Notifications** preferences are:

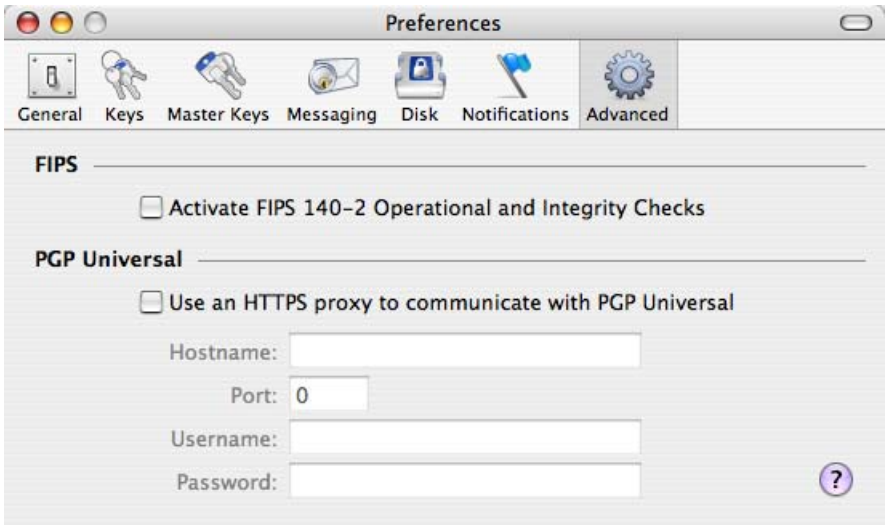
- **Use PGP Notifier:** PGP Desktop Notifications can appear at any of the four corners of your screen. Select a button to indicate the corner that you would like PGP Desktop Notifications to appear. Click **Preview** to see how the PGP Desktop Notification alert box looks in the specified corner.
- **Notify when processing outbound email:** Select this checkbox if you want PGP Desktop Notifiers to appear, informing you of encryption and/or signing status when you send mail. Deselect this checkbox to stop PGP Desktop Notifications from appearing when you send mail.
- **Ask me before sending email when the recipient's key is not found:** PGP Desktop looks for a public key for every recipient of the email messages that you send. By default, if it cannot find a public key for a recipient, it sends that email in the clear (without encryption). If you select this PGP Desktop Notification option, you are notified that this is the case, and given a chance to block the email so that it is not sent.

(For more information on the PGP Desktop default policy settings, see "Services and Policies" on page 25.)

- **Always ask me before sending email:** You can select this checkbox if you would prefer approving every email that you send. You can review the encryption status in the PGP Desktop Notification, and either send or block the email.
- **Delay outbound email for n second(s) to confirm** (where *n* is a number from 1-30). If you would like a PGP Desktop Notification for every message that you send—but you would prefer that they did not wait for your explicit approval—you can select this option. Outbound email is delayed, and a PGP Desktop Notifier displays, for the time period that you choose. If you want the email to be sent, do nothing: the email is sent once the time interval elapses. If you would like a closer look at the PGP Desktop Notification, move your cursor over it. The PGP Desktop Notification changes from translucent to opaque in appearance, and the outbound email is delayed while you review the PGP Desktop Notification information. You can then allow the email to be sent, or block it.
- **Display notifications for incoming mail:** For incoming email, you can choose the extent to which you are notified of its status upon arrival. Your choices are:
  - **When receiving secured email**—A PGP Desktop Notification box appears whenever you receive secured email. The box displays who the email is from, its subject, its encryption and verification status, and the email address of the person sending it.
  - **Only when message verification fails**—For incoming email, you see a PGP Desktop Notification box only when PGP Desktop is unable to verify the signature of the incoming email.
  - **Never**—If you do not need or want to see a PGP Desktop Notification box as you receive email, select this option. This option does not affect PGP Desktop Notifications for outgoing mail.
- **Notify for status of PGP Encrypted IM sessions**: Select this checkbox if you would like a PGP Desktop Notifier box to appear briefly when you begin a secure instant message chat, and appear briefly again when the chat ends.

Advanced Preferences

The **Advanced** Preferences panel provides settings that most users will not need to change.



The **Advanced** preferences are:

- **Activate FIPS 140-2 Operational and Integrity Checks.** Select this option if you or your organization require FIPS 140-2 checks, but be aware that it slows down your computer's performance. You must reboot your computer for this setting to take effect.
- **Use an HTTPS proxy to communicate with PGP Universal.** Do not change these settings unless you are instructed to by your network administrator.

  If your PGP Universal installation requires a secure client/server connection via a proxy, you can use these option settings to specify that. Your administrator can supply you with the server name, the correct communications port, your user ID, and your password, so you can configure this section correctly.

B Passwords and Passphrases

Creating effective passphrases

This appendix describes the differences between passwords and passphrases, tells you about the **Passphrase Quality Bar** in PGP Desktop, and provides some guidelines for creating strong passphrases.

Passwords and Passphrases

Passwords and passphrases are used to protect things. In general, passphrases are longer and use a wider variety of characters than do passwords.

For example, a simple password might be four-letter two words concatenated: "whenjobs" without the quotes. A stronger password could use uppercase characters as well: WhenJobs. A stronger yet password could add numbers: When9Jobs4.

Passphrases, in comparison, are longer and use a wider variety of characters. For example, a simple passphrase might be: "Mb&1a>ttA." without the quotes, but including the period. This passphrase might seem difficult to remember easily, but in fact it's based on a simple phrase that is much easier to remember.

Passphrases can also be simple phrases, perhaps from a familiar book, that include the punctuation and capitalization: "Because that's not golf, I replied" including the quotes. Although this may not seem like a strong passphrase, it is in fact at least twice as strong as any of the other examples.

Choosing whether to use a password or passphrase

So how do you know whether to choose a password or a passphrase? It depends on what you are trying to protect. The more valuable the information you are protecting, the stronger the protection should be.

Most Word documents are not protected at all; the content is not valuable enough to justify the effort. When you access your bank account online, some banks require only a four-letter PIN; depending on the amount of money in that account, this very well may be very poor security. You may use a free Hotmail email account for unimportant correspondence; a simple password is adequate security. With your corporate email account you send and receive proprietary product, customer, or financial information.

With PGP Desktop, for example, you create passphrases for both your PGP keypair and for your PGP Virtual Disk volumes. If you create a weak passphrase for your PGP keypair, and an attacker managed to get physical control of your private key file, all they would need to do to be able to read your messages and send messages that appear to be coming from you would be to figure out that passphrase.

The Passphrase Quality Bar

When you create passphrases in PGP Desktop, the Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating. Nevertheless, it is a much better guideline than just number of characters.

In general, the longer the bar, the stronger the passphrase. But what does the length of the Passphrase Quality bar actually mean?

The Passphrase Quality bar compares the amount of randomness (entropy) in the passphrase you enter against a true 128-bit random string (the same amount of entropy in an AES128 key). This is called 128 bits of entropy.

(Entropy is a measure of the difficulty in determining a password or key.)

So if the passphrase you create fills up approximately half the Passphrase Quality bar, then that passphrase has approximately 64 bits of entropy. And if your passphrase fills the Passphrase Quality bar, then that passphrase has approximately 128 bits of entropy.

So how strong is 128 bits of entropy? In the late 1990s, specialized "DES cracker" computers were built that could recover a DES key in a few hours by trying all possible key values.

Assuming you could build a computer that could recover a DES key in one second (the computer would have to be able to try 2^{55} keys per second), then it would take that computer approximately 149 trillion (thousand billion) years to crack one 128-bit AES key. In comparison, the universe is believed to be less than 20 billion years old.

How is the entropy of a particular character measured? The answer is, the bigger the pool of characters there is to choose from when picking a particular character, the more entropy is assigned to the chosen character.

For example, if you are told to choose a numeric PIN, you are restricted to the numbers zero through nine; a total of 10 characters. This is a rather small pool, so the entropy for a chosen character is relatively low.

When you are choosing a passphrase using the English version of PGP Desktop, however, things are different. You have three pools of characters to choose from: uppercase and lowercase letters (52 characters), numbers zero through nine (10 characters), and the punctuation characters on a standard keyboard (32 characters).

When you enter a character, PGP Desktop determines the entropy value for that character based on the pool it is in and applies that value to the Passphrase Quality bar.

The same concept applies to the character sets of other languages; the larger the pool, the more entropy per character. So if you were using an Asian or Arabic character set, for example, some of which have hundreds of characters in the set, the amount of entropy for a selected character would be correspondingly higher, and thus fill up the Passphrase Quality bar that much faster.

Creating Strong Passphrases

Creating a good passphrase is a trade-off between ease of use and strength of the passphrase. Longer passphrases, with a mixture of uppercase and lowercase letters, numbers, and punctuation characters, are stronger, but they are also harder to remember.

Studies have shown that passphrases that are harder to remember are more frequently written down, which defeats the purpose of having a strong passphrase. It's better to have a somewhat shorter strong passphrase that you will remember than a longer strong passphrase that you will write down or forget.

One common system for generating strong passphrases takes a phrase and reduce it to individual characters. For example, the phrase:

My brother and I are greater together than apart.

becomes the passphrase:

Mb&1a>ttA.

This passphrase has 10 characters, and is a mix of uppercase and lowercase letters, numbers, and punctuation characters. At 10 characters, this is a relatively short passphrase. If you think 10 characters is not enough, consider either creating another passphrase using the same method and then use both together or simply use a longer phrase to start with.

Another approach is to use simple phrases that include punctuation and capitalization. For example:

"Edited by John Doe (not John Doe, Editor)"

While not overly long or complicated, this is a strong passphrase. If you decide to use a phrase from a familiar book, make sure not to lose the book.

When creating a passphrase in PGP Desktop, you can use up to 255 characters, including spaces.

Another approach is to concatenate many short, common words. A method called Diceware™ uses dice to select words at random from a special list called the Diceware Word List, which contains 7776 short English words, abbreviations, and easy-to-remember character strings. If you put together enough of these, you can create a strong passphrase. The Diceware FAQ states you may achieve 128 bits of entropy using a 10-word Diceware passphrase.

Refer to **http://world.std.com/~reinhold/diceware.html** for more information about Diceware.

When it comes to creating passphrases, here are some things you should do:

- Use a phrase that is in your long-term memory. You are less likely to forget it that way.
- Make your passphrase at least eight characters long. Length is not the best indicator of strength, but it's still better than shorter.

- Use a mixture of uppercase and lowercase letters, numbers, and punctuation characters.

Try to use only ASCII characters, if possible. This is particularly important when using international keyboards, as some special characters are not supported (for example, "§") in passphrases.

-
- Change your passphrase on a regular basis; every three months is a good rule of thumb. The longer you use the same passphrase, the more time there is for someone to figure it out.

Here are some things you should **not** do when creating passphrases:

- Don't write down your passphrase.
- Don't give your passphrase to anyone.
- Don't let anyone see you entering your passphrase.
- Don't use "password" or "passphrase."
- Don't use patterns. Not "abcdefgh" or "12345678" or "qwertyui" or "88888888" or "AAAAAAAA."
- Don't use common words. Almost any skilled attacker is using a password-cracking dictionary that tries regular words. Don't put two common words together, don't use the plural of a common word, don't use a common word with the first letter capitalized.
- Don't use numbers that pertain to you. If anyone knows these numbers, then an attacker could find out. Don't use your birthday, your phone number, your social security number, or your street address.
- Don't use names. Not the names of people, not the names of fictional characters, not your pet's name. Not where you vacationed last winter, not your login name, not your company's name. Not your favorite team's name, not a body part, not a name from any book, especially the Bible.
- Don't use any of the above backwards, or with a preceding or following single digit.

C PGP Desktop and PGP Universal

Using PGP Desktop in a PGP-Universal Managed Environment

This appendix describes how using PGP Desktop is different in a PGP Universal-managed email domain.

If you are using PGP Desktop outside of a PGP Universal-managed email domain, this appendix does not apply to you.

PGP Universal allows enterprises to automatically and transparently (to end users) protect email messages based on configurable policies the PGP administrator establishes to enforce the organization's security policies. PGP Universal also lets PGP administrators manage PGP Desktop deployments to users in their organization. Refer to http://www.pgp.com/products/universal/index.html for more information about PGP Universal.

Using PGP Desktop in a PGP Universal-managed environment gives you proven PGP encryption technology all the way to your desktop, plus the other security features in PGP Desktop: PGP Whole Disk Encryption, PGP Virtual Disk volumes, PGP Zip archives, and PGP Shredding, among others.

Overview

To use PGP Desktop in a PGP Universal-managed environment, you must install PGP Desktop using an installer application you receive from your PGP administrator.

If you obtained your PGP Desktop installer from a different source, you should check with your PGP administrator *before* installing or using that version of PGP Desktop.

Your PGP Desktop installer will have been configured by your PGP administrator in one of the following ways:

- **No policy settings**. Your copy of PGP Desktop will not have any built-in settings; you can use any feature your license supports.
- **Auto-detect policy settings**. Your copy of PGP Desktop will contact the PGP Universal Server that created the installer and download the appropriate settings. The settings it receives may require you to use PGP Desktop features in specific ways.
- **Preset policy settings**. Your copy of PGP Desktop will have the appropriate settings built in. These settings may require you to use PGP Desktop features in specific ways.

The result of your copy of PGP Desktop receiving settings from a PGP Universal Server means you may have to use PGP Desktop features in specific ways. This includes:

- You may have to take certain actions when you install PGP Desktop: you may have to whole disk encrypt your boot drive or create a PGP Virtual Disk volume, for example.
- You may be allowed or required to use PGP Desktop features in certain ways: you may be required to encrypt your AIM instant messaging sessions or you may be allowed to automatically shred files when deleting them, for example.
- You may be prevented from using certain PGP Desktop features: for example, you may be prevented from using conventional encryption (passphrases instead of keys).
- You may be required to adhere to certain messaging policies: you may be required to encrypt and sign messages to certain email domains, for example.

Those features of PGP Desktop that can be managed by a PGP administrator in a PGP Universal-managed environment are noted in their descriptions throughout this User's Guide.

Contact your PGP administrator for more information about how using PGP Desktop in a PGP Universal-managed environment affects your usage of PGP Desktop.

For PGP Administrators

If you are a PGP administrator managing the rollout of PGP Desktop to some or all users in your organization, PGP Corporation recommends you allow your PGP Desktop users to manage their own keys, called Client Key Mode.

When you are preparing to create the PGP Desktop installers on your PGP Universal Server, you can control whether your PGP Desktop users are able to manage their own keys, Client Key Mode, or whether the PGP Universal Server will manage their keys, called Server Key Mode.

These settings are established in the Key Management section of the Key Setup: Default screen, which is part of the configuration of the default user group policy for internal users (User Group –> Policy Options --> Key Setup: Default in the PGP Universal Server's administrative interface).

For PGP Desktop users, Client Key Mode is the better choice because:

- Many PGP Desktop features require the user to have control of their private key. If the PGP Universal Server is managing that private key, those features will be unavailable to your PGP Desktop users.
- If you specify Server Key Mode, certain options you pre-configure for your PGP Desktop users will not be available. For example, the automatic creation of PGP Virtual Disks is not possible.

Glossary

AES (Advanced Encryption Standard)	The NIST-approved encryption standard. The underlying cipher is Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen. The AES replaces the previous standard, the Data Encryption Standard (DES).
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.
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.
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.

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) 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).

common access cards (CACs) Read-only smartcards used by the U.S. Department of Defense. CACs include two separate certificates, one for signing and one for encrypting. PGP Desktop filters the two certificates based on intended usage; for example, only the signing certificate is presented on the file signing dialog.

compression function A compression function takes a fixed-sized input and returns a shorter, fixed sized output.

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 you will be asked to choose.

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.

cryptanalysis The art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

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.

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.

direct trust An establishment of peer-to-peer confidence.

digital signature See signature.

encryption A method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt it to read it.

entropy In cryptography, a measure of randomness. It specifically relates to the difficulty in determining a passphrase or key. The greater the amount of entropy, the more difficult something is to determine. For example, if you were to pick a number from zero to 9, you would have a one in 10 chance, which works out to certain amount of entropy. If you were to pick a letter in the English alphabet, from A to Z, then you would have a one in 26 chance, a far greater amount of entropy.

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.

implicit trust Implicit trust is reserved for keypairs located on your local keyring. If the private portion of a keypair is found on your keyring, PGP Desktop assumes that you are the owner of the keypair 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.

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 keypairs 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 keypair. Two keypairs 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.

keypair A public key and its complimentary private key. In public-key cryptosystems, like the PGP program, each user has at least one keypair.

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.

MD5 (128 bits) A legacy hash algorithm provided only for backwards compatibility. Deprecated.

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.

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. A passphrase can generally use non-alphanumeric characters such as *, +, or ~. Because passphrases are generally longer than passwords and use a wider variety of characters, they are more secure than passwords.

password A sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification. Passwords are generally restricted to letters and numbers.

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.

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.

private key The secret portion of a keypair; 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 keypair-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 keypair 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.

RIPEMD-160 (160 bits) An independent hash algorithm; it provides up to 80 bits of brute force resistance.

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.

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.

SHA-1 A second-generation hash algorithm; it provides up to 80 bits of brute force resistance. Partially deprecated.

SHA-2 (256 bits) A third-generation hash algorithm; it provides up to 128 bits of brute force resistance.

SHA-2 (384 bits) A third-generation hash algorithm; it provides up to 192 bits of brute force resistance.

SHA-2 (512 bits) A third-generation hash algorithm; it provides up to 256 bits of brute force resistance.

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 Also known as 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.

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 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the Advanced Encryption Standard (AES).

user ID A text phrase that identifies a keypair. 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 keypair.

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.

web of trust A distributed trust model used by PGP technology 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

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Y