PGP

Installation Guide

Version 7.0

LIMITED WARRANTY

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

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

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

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

Table of Contents

Introduction to PGP 1

Welcome to PGP security software! This Installation guide provides general information about PGP and describes the system requirements and installation instructions necessary to successfully run it.

PGP includes email plug-ins, key generation and management tools, disk utilities that enable users to securely exchange and store data, Personal Firewall and Personal IDS (Intrusion Detection System) which provides a dual-layer security perimeter around your PC to protect against common attacks, and VPN (Virtual Private Network) that allows PGP users to communicate securely over a network. You can distribute PGP to your users straight from the box, or pre-configure PGP with settings that enforce your security policy.

If you are new to cryptography and would like an overview of the terminology and concepts you will encounter while using PGP, see *An Introduction to Cryptography.*

How to contact PGP Security and Network Associates

Customer service

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

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

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

Other contact information for corporate-licensed customers:

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

Other contact information for retail-licensed customers:

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

Technical support

PGP Security and Network Associates are famous for their dedication to customer satisfaction. The companies have continued this tradition by making their sites on the World Wide Web valuable resources for answers to technical support issues. PGP Security encourages you to make this your first stop for answers to frequently asked questions, for updates to PGP Security and Network Associates software, and for access to news and virus information**.**

World Wide Web:	http://support.nai.com

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers between 8 A.M. and 8 P.M. Central time, Monday through Friday, to find out about Network Associates technical support plans.

For corporate-licensed customers:

Phone:	(972) 308-9960

For retail-licensed customers:

Phone:	(972) 855-7044

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please include this information in your correspondence:

- Program name and version number

- Computer brand and model

- Any additional hardware or peripherals connected to your computer

- Operating system type and version numbers

- Network name, operating system, and version

- Network card installed, where applicable

- Modem manufacturer, model, and bits-per-second rate, where applicable

- Relevant browsers or applications and their version numbers, where applicable

- How to reproduce your problem: when it occurs, whether you can reproduce it regularly, and under what conditions

- Information needed to contact you by voice, fax, or email

Download support

To get help with navigating or downloading files from the Network Associates Web sites or FTP sites, call:

Corporate customers:	(801) 492-2650
Retail customers:	(801) 492-2600

Network Associates training

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

Comments and feedback

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

Recommended readings

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

The history of cryptography

- *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., 1999, ISBN 0-385-49531-5.

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

Technical aspects of cryptography

Web sites

- www.iacr.org—International Association for Cryptologic Research (IACR). The IACR holds cryptographic conferences and publishes journals.

- www.pgpi.org—An international PGP Web site, which is not maintained by PGP Security, Inc. or Network Associates, Inc., is an unofficial yet comprehensive resource for PGP.

- www.nist.gov/aes—The National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) Development Effort, perhaps the most interesting project going on in cryptography today.

- www.ietf.org/rfc/rfc2440.txt—The specification for the IETF OpenPGP standard.

Books and periodicals

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edition, Bruce Schneier, John Wiley & Sons, 1996; ISBN 0-471-12845-7. If you can only buy one book to get started in cryptography, this is the one to buy.

- *Handbook of Applied Cryptography*, Alfred Menezes, Paul van Oorschot and Scott Vanstone, CRC Press, 1996; ISBN 0-8493-8523-7. This is the technical book you should get after Schneier. There is a lot of heavy-duty math in this book, but it is nonetheless usable for those who do not understand the math.

- *Journal of Cryptology*, International Association for Cryptologic Research (IACR). See www.iacr.org.

- *Advances in Cryptology*, conference proceedings of the IACR CRYPTO conferences, published yearly by Springer-Verlag. See www.iacr.org.

- *Cryptography for the Internet*, Philip Zimmermann, Scientific American, October 1998 (introductory tutorial article).

- *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*, Bruce Schneier, et al, John Wiley & Sons, Inc., 1999; ISBN: 0471353817. Contains details about the Twofish cipher ranging from design criteria to cryptanalysis of the algorithm.

Politics of cryptography

Web sites

- www.epic.org—Electronic Privacy Information Center.

- www.crypto.org—Internet Privacy Coalition.

- www.eff.org—Electronic Frontier Foundation.

- www.privacy.org—The Privacy Page. Great information resource about privacy issues.

- www.cdt.org—Center for Democracy and Technology.

- www.pgp.com/phil—Phil Zimmermann's home page, his Senate testimony, and so on.

Books

- *Privacy on the Line: The Politics of Wiretapping and Encryption*, Whitfield Diffie and Susan Landau, The MIT Press, 1998, ISBN 0-262-04167-7. This book is a discussion of the history and policy surrounding cryptography and communications security. It is an excellent read, even for beginners and non-technical people. Includes information that even a lot of experts don't know.

- *Technology and Privacy: The New Landscape*, Philip Agre and Marc Rotenberg, The MIT Press, 1997;ISBN 0-262-01162-x.

- *Building in Big Brother, The Cryptographic Policy Debate*, edited by Lance Hoffman, Springer-Verlag, 1995; ISBN 0-387-94441-9.

- *The Official PGP User's Guide*, Philip Zimmermann, The MIT Press, 1995; ISBN 0-262-74017-6. How to use PGP, written in Phil's own words.

- *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. This book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography.

Network security

Books

- *Building Internet Firewalls*, Elizabeth D. Zwicky, D. Brent Chapman, Simon Cooper, and Deborah Russell (Editor), O'Reilly & Associates, Inc., 2000; ISBN: 1565928717. This book is a practical guide to designing, building, and maintaining firewalls.

- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick, Steven M. Bellovin, Addison Wesley Longman, Inc., 1994; ISBN: 0201633574. This book is a practical guide to protecting networks from hacker attacks through the Internet.

- *Hacking Exposed: Network Security Secrets and Solutions*, Stuart McClure, Joel Scambray, and George Kurtz, The McGraw-Hill Companies, 1999; ISBN: 0072121270. The state of the art in breaking into computers and networks, as viewed from the vantage point of the attacker and the defender.

Upgrading from a previous version of PGP

2

This chapter describes how to upgrade from a previous version of PGP.

Compatibility with previous versions of PGP

PGP has gone through many revisions since it was released by Phil Zimmermann as a freeware product in 1991. Although this version of PGP represents a significant rewrite of the original program and incorporates a completely new user interface, it has been designed to be compatible with previous versions of PGP. This means that you can exchange secure email with people who are still using these older versions of the product:

- PGP 2.6 (Distributed by MIT)
- PGP 2.7.1 for the Macintosh (Released by ViaCrypt)
- PGP 4.0 (Released by ViaCrypt)
- PGP 4.5 (Released by PGP, Inc.)
- PGP for Personal Privacy, Version 5.0 - 5.5
- PGP for Business Security or PGP for Email and Files Version 5.5
- PGP for Desktop Security or PGP for Personal Privacy Version 6.0.x
- PGP for Desktop Security or PGP for Personal Privacy Version 6.5.x
- PGP for Desktop Security Version 7.0

Upgrading from a previous version of PGP

If you are upgrading from a previous version of PGP (from PGP, Inc., Network Associates, Inc. or ViaCrypt), you may want to remove the old program files before installing PGP to free up some disk space. However, you should be careful not to delete the private and public keyring files used to store any keys you have created or collected while using the previous version. When you install PGP, you are given the option of retaining your existing private and public keyrings, so you don't have to go to the trouble of importing all of your old keys. To upgrade from a previous version, follow the appropriate steps listed next.

To upgrade from PGP Version 2.6.2 or 2.7.1:

1. Exit all programs or open applications.

2. Make backups of your old PGP keyrings on another volume. In PGP for Windows versions 2.6.2 and 2.7.1, your public keys are stored in "pubring.pgp" and your private keys are stored in "secring.pgp". In versions 5.x - 7.0, your public keys are stored in "pubring.pkr" and your private keys are stored in "secring.skr".

    > **TIP:** Make two separate backups of your keyrings onto two different floppy disks just to be safe. Be especially careful not to lose your private keyring; otherwise you will never be able to decrypt any email messages or file attachments encrypted with the lost keys. Store the keyrings in a secure place where only you have access to them.

3. When you have successfully backed up your old keyrings, remove or archive the (old) PGP software. You have two options here:

    - Manually delete the entire old PGP folder and all of its contents; or

    - Manually delete the old PGP program and archive the remaining files, especially the configuration and keyring files.

    > **NOTE:** If you obtain a copy of the patched PGP 2.6.4 version, your old software will be able to read the RSA keys on the new 7.0.1 keyrings and will not fail when it encounters the new Diffie-Hellman/DSS format keys. You can download this patch from the Network Associates web-site.

4. Install PGP Version 7.0.1 using the provided Installer.

5. Restart your computer.

To upgrade from PGP Versions 4.x - 7.0:

If you are upgrading from PGP Versions 4.x - 7.0, follow the installation instructions outlined in Chapter 3, "Installing PGP on a Windows system" or Chapter 4, "Installing PGP on a Macintosh system".

Installing PGP on a Windows system

3

This chapter describes how to install PGP for Windows software. Before you begin installing PGP, however, be sure to review the system requirements outlined below.

System requirements

To install PGP on a Windows system, you must have at least:

- Pentium 166 or compatible processor

- Windows 95 OSR 2, Windows 98, Windows 2000, Windows NT 4.0 (Service Pack 4 or later), or Windows Millennium Edition (ME)

  On Windows 2000 and Windows NT systems, you must have Administrator privileges for the workstation on which you plan to install the program, and you must have logged on to that system correctly.

- 32 MB RAM

- 32 MB Hard Disk Space

If you plan to run PGPnet on the system, you must also have:

- Microsoft TCP/IP

- Compatible LAN/WAN network adapter

Installing PGP Version 7.0.1

You can install the PGP software from a CD-ROM or from a file server. The self-extracting file, Setup.exe, automatically extracts and steps you through the installation process. After you install the software, you can create your private and public keypair and begin using PGP. Refer to the PGPWinUsersGuide.pdf file included with the program for instructions on using PGP.

To install PGP for Windows 95, Windows 98, Windows 2000, Windows NT, and Windows ME systems, carefully follow the steps outlined below.

To install PGP on a Windows system:

1. Exit all programs currently running on your computer, then do one of the following:

   - **To install from a CD-ROM,** insert it into the CD-ROM drive.

     The Setup program automatically starts. If, however, the Setup program does not initiate, double-click **Setup.exe** in the PGP folder on the CD-ROM.

   - **To install from your company file server,** contact your security officer for information about the server from which to download PGP. Log on to the server.

2. Double-click **Setup.exe** in the PGP folder to start the Setup program.

3. The Setup program searches for open programs and prompts you to close them.

   If you have PGP version 5.x - 7.0 currently installed, the PGP setup program prompts you to uninstall the old PGP files. Click **Yes** to automatically uninstall the old version. Your keyring files are saved in a file named **Old keyrings**.

   You must reboot your computer after uninstalling the files. Once your computer reboots, the installer continues.

   The **PGP Installation** screen appears.

4. Review the instructions in the **PGP Welcome** dialog box, then click **Next**.

   The Network Associates license agreement appears.

5. Review the license agreement information, then click **Yes** to accept the licensing terms.

   The **Readme.txt** file appears listing the new features and other important information regarding PGP version 7.0.1.

6. Review the Readme.txt file, then click **Next**.

   The **User Type** dialog box appears.

7. Select the appropriate button:

- Click **Yes** to use your existing PGP keyrings.

   The installation wizard asks you to locate your PGP keyrings later in the installation process.

- Click **No** if you are a New User and do not have existing PGP keyrings.

   The key generation wizard assists you in creating a PGP keypair at the end of the installation process.

8. Click **Next**.

9. Click **Browse** to navigate to a destination folder for your PGP files or accept the default folder. Click **Next** to continue.

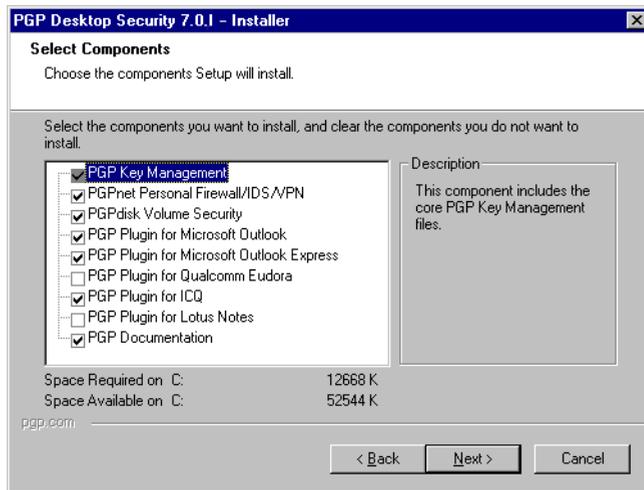   The **Select Components** dialog box appears, as shown in Figure 3-1.

Figure 3-1. PGP Select Components dialog box

10. Select the components you want to install. Your installation options are:

- **PGP Key Management.** This item is required. Select this option to install the PGP program and Key Management utilities.

- **PGPnet Personal Firewall/IDS/VPN.** Select this option to install the PGPnet program. The PGPnet program includes a Personal Firewall and Intrusion Detection System (IDS) to identify and protect against common attacks, and a Virtual Private Network (VPN) to enable you to communicate securely and economically with other PGPnet users on your own corporate intranet and with users throughout the world.

- **PGPdisk Volume Security.** Select this option to install the PGPdisk program. PGPdisk is an easy-to-use encryption application that enables you to set aside an area of disk space for storing your sensitive data.

- **PGP Plug-in for Microsoft Outlook.** Select this option if you want to integrate PGP functionality with your Microsoft Exchange/Outlook email program. PGP supports Outlook 97, Outlook 98, and Outlook 2000.

- **PGP Plug-in for Microsoft Outlook Express.** Select this option if you want to integrate PGP functionality with your Microsoft Outlook Express email program. PGP supports the version that is included with Internet Explorer versions 4.x and above.

- **PGP Plug-in for Qualcomm Eudora.** Select this option if you want to integrate PGP functionality with your Qualcomm Eudora email program. PGP supports Eudora versions 4.0.x and above.

- **PGP Plug-in for ICQ.** Select this option if you want to integrate PGP functionality with your ICQ instant messaging program. PGP supports ICQ versions 99b, 2000a, and 2000b.

- **PGP Plug-in for Lotus Notes.** Select this option if you want to integrate PGP functionality with your Lotus Notes email program. PGP supports Lotus Notes versions 4.5x, 4.6x, and R5.

> **IMPORTANT:** To successfully use the PGP plug-in for Lotus Notes, your System Administrator must configure the Domino server after the PGP program is installed.

- **PGP Documentation (PDF format).** Select this option to install the PGP User's Guide in PDF format.

> **TIP:** You can run the PGP Setup Maintenance Utility at any time to add or remove PGP components or plug-ins. See "Modifying your PGP Installation" on page 20 for more information.

11. Click **Next**.

    A dialog box appears, alerting you that the installer is ready to copy files.

12. Review the installation settings, then click **Next**.

    The PGP files are copied to the computer.

13. If you chose to install the PGPnet application, the **PGPnet Set Adapter List** appears listing the network adapters found on your system, as shown in Figure 3-2.

Figure 3-2. PGPnet Set Adapter List

If you want to communicate securely over a modem, select your Dial-up or WAN adapter (for example, Remote Access WAN Wrapper). If you want to communicate securely over an Ethernet connection, select your LAN adapter (for example, 3COM Fast Etherlink). When you have made your selection(s), click **OK**.

> **NOTE:** You can secure all adapters, WAN and LAN, on your system at this time.
>
> On Windows 2000, Set Adapter displays, "All Network and Dial-up Adapters." Select this checkbox to secure all network interfaces.

> **TIP:** You can change the selected network adapter(s) at any time after installation. Go to **Start—>Programs—>PGP—>SetAdapter** and select the network adapter(s) you want PGP to bind to, or deselect the network adapter(s) you no longer want PGP to bind to.

The installation program binds the PGPnet driver to the adapter(s) you selected and configures your computer to use the PGPnet application.

14. If you have keyrings on your computer from a previous version of PGP, and selected **Yes** in step seven, a browse dialog box appears.

    Browse to locate your public keyring, Pubring.pkr, and your private keyring, Secring.skr.

    If you do not have keyrings on your computer from a previous version of PGP, and selected **No** in step seven, you are prompted to create a keypair after completing the PGP installation. The key generation wizard will guide you through the necessary steps to create a new PGP keypair.

15. To start using PGP immediately, select **Yes, I want to restart my computer now**.

16. Click **Finish** to complete the PGP installation and reboot your computer.

Modifying your PGP Installation

You can run the PGP Setup Maintenance utility at any time to modify your current PGP installation.

The PGP Setup Maintenance utility allows you to:

- add or remove PGP components,

- re-install all program components installed by a previous setup, or

- remove all installed components.

To modify your PGP installation:

1. Exit all programs currently running on your computer.

2. Double-click **Setup.exe** in the PGP folder to start the Setup program.

3. The Setup program searches for open programs and prompts you to close them.

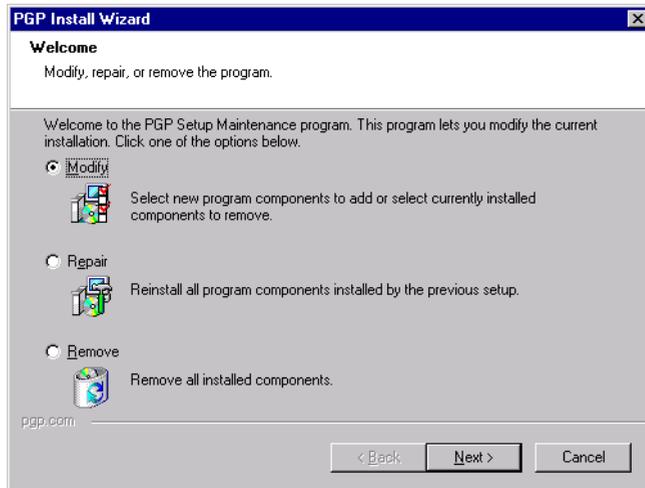   The **PGP Install Wizard Welcome** screen appears. (See Figure 3-3.)

Figure 3-3. PGP Install Wizard Welcome screen

4. Select **Modify** to add new PGP components or remove currently installed PGP components.

   The **Select Components** dialog box appears, as shown in Figure 3-1 on page 17.

5. Select the components you want to install, or deselect the components you want to remove from your current installation. (For a detailed description of each component, refer to Step 10 on page 18.)

6. Click **Next**.

7. To start using PGP immediately, select **Yes, I want to restart my computer now**.

8. Click **Finish** to complete the PGP maintenance and reboot your computer.

To repair your PGP installation:

1. Exit all programs currently running on your computer.

2. Double-click **Setup.exe** in the PGP folder to start the Setup program.

3. The Setup program searches for open programs and prompts you to close them.

   The **PGP Install Wizard Welcome** screen appears. (See Figure 3-3 on page 21.)

4. Select **Repair** to re-install all program components installed by a previous setup. This may be necessary if you modified your installation, and now want to return to your original setup.

    PGP re-installs all program components from the original installation.

5. To start using PGP immediately, select **Yes, I want to restart my computer now**.

6. Click **Finish** to complete the PGP maintenance and reboot your computer.

To remove your PGP installation:

1. Exit all programs currently running on your computer.

2. Double-click **Setup.exe** in the PGP folder to start the Setup program.

3. The Setup program searches for open programs and prompts you to close them.

    The **PGP Install Wizard Welcome** screen appears. (See Figure 3-3 on page 21.)

4. Select **Remove** to uninstall all PGP program components.

    PGP asks you to confirm your request to remove the PGP application and all of its components.

5. Click **OK** if you want to remove PGP, or click **Cancel** if you do not want to remove PGP.

6. Select **Yes, I want to restart my computer now**.

7. Click **Finish** to complete the uninstall of PGP and reboot your computer.

Installing PGP on a Macintosh system

4

This chapter describes how to install PGP for Macintosh software. Before you begin installing PGP, however, be sure to review the system requirements outlined below.

System requirements

To install PGP on a Macintosh system, you must have:

- Power Macintosh (PowerPC processor required)

- Mac OS 8.6.1

- 16 MB RAM

- 10 MB hard disk space

If you plan to run PGPnet on the system, you must also have:

- Compatible LAN/WAN hardware and software (refer to the PGP Readme file for more information about PGPnet compatible software and hardware)

Installing PGP Version 7.0.1

You can install the PGP software from a CD-ROM or from a your company file server. The Installer program () automatically extracts and steps you through the installation. After you install the software, you can create your private and public keypair and begin using PGP. Refer to the PGPMacUsersGuide.pdf file included with the program for instructions on using PGP.

To install PGP for Macintosh systems, carefully follow the steps outlined below.

To install PGP on a Macintosh system:

1. Exit all programs currently running on your computer, then do one of the following:

    • **To install from a CD-ROM,** insert it into the CD-ROM drive.

      The Installer program automatically starts. If, however, the Installer program does not initiate, double-click the PGP Desktop Security 7.0.1 program file on the CD-ROM.

    • **To install from your company file server,** contact your security officer for information about the server from which to download PGP. Log on to the server.

2. Double-click the installation icon ( ) to start the Installer program.

    The Network Associates license agreement appears.

3. Review the license agreement information, then click **Accept** to continue the installation.

    The PGP Readme file appears.

4. Review the Readme file for new features and known issues, then click **Continue**.

    The installation screen appears, as shown in Figure 4-1.
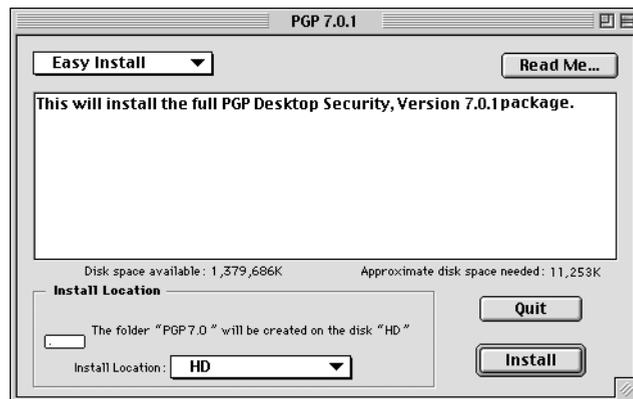
Figure 4-1. PGP Installation screen

5. Choose **Easy Install** to perform a full installation of PGP. The following components are included in the full installation.

   - **PGPkeys.** This item installs the PGP program.

   - **PGPtools.** PGPtools is a toolbar that allows you to perform PGP functions from within other applications. You can encrypt and sign, decrypt and verify, and securely wipe messages and files directly from PGPtools.

   - **PGPdisk Volume Security.** PGPdisk is an easy-to-use encryption application that enables you to set aside an area of disk space for storing your sensitive data.

   - **PGPnet Virtual Private Networking.** PGPnet, a *Virtual Private Network (VPN)*, is an easy-to-use encryption application that allows you to communicate securely and economically with other PGPnet users on your own corporate intranet and with users throughout the world.

   - **PGPmenu.** PGPmenu allows you to performs most PGP functions from the Finder or from within most applications.

   - **PGPcontextmenu**. PGPcontextmenu allows you to perform encryption task by holding down the CONTROL KEY and clicking on a file or volume in a window or on your desktop.

   - **PGP Qualcomm Eudora Plug-in.** PGP Qualcomm Eudora plug-in integrates PGP functionality with your Qualcomm Eudora email program. PGP now supports Eudora versions 3.05 and later.

   - **PGP Screen Locking.** When your screen is locked, all cached passphrases are automatically cleared. The screen locking is immune to debuggers and other system utilities.

   > **IMPORTANT:** The only ways to bypass the screen locking are to enter your passphrase (after hitting **Escape**), or reboot – in which case your PGPdisks are of course no longer mounted.

   - **PGP Documentation/AppleGuide.** The PGP Documentation includes a PGP User's Guide and Apple Guide help.

6. Select a location for your PGP files, then click **Install**.

   A warning screen appears advising you to close all open applications.

7. Close all open applications, then click **Continue**.

   The PGP files are copied to the computer.

8. Click **Restart** to reboot the computer.

   The computer restarts. PGP is now installed on the computer.

Index