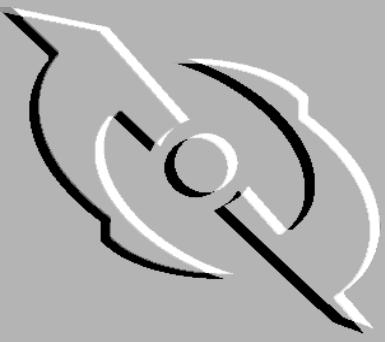

PGP

Administrator’s Guide

Version 6.5

PGP*, Version 6.5.1

06-99. Printed in the United States of America.

Network Associates, Inc. (408) 988-3832 main
3965 Freedom Circle
Santa Clara, CA 95054
http://www.nai.com

info@nai.com

***** is sometimes used instead of the ® for registered trademarks to protect marks registered

LIMITED WARRANTY

Limited Warranty. Network Associates warrants that for sixty (60) days from the date of original purchase the media (for example diskettes) on which the Software is contained will be free from defects in materials and workmanship.

Customer Remedies. Network Associates' and its suppliers' entire liability and your exclusive remedy shall be, at Network Associates' option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained with a copy on nondefective media. You must return the defective media to Network Associates at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent Network Associates is subject to restrictions under United States export control laws and regulations.

Warranty Disclaimer. To the maximum extent permitted by applicable law, and except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, NETWORK ASSOCIATES MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

Table of Contents

Preface

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

Entire books have been written on the subject of implementing network security. The focus of this guide is on implementing PGP as a tool within your overall network security structure. PGP is only one piece of an overall security system, but it is an extremely important one. PGP provides encryption, which protects data from the eyes of anyone for whom it was not intended, even those who can see the encrypted data. This protects information from both internal and external "outsiders."

This guide explains how to implement PGP in an enterprise environment. For information on encryption and cryptographical concepts and terminology, see *An Introduction to Cryptography*.

Who should read this guide

This guide is geared toward anyone making security decisions in an organization. You may be a system administrator, designated corporate security officer, part of a corporate security group, or part of an information services organization. You may be deciding which encryption software to buy.

Regardless of your title, if you are responsible for ensuring that your organization's information is secure and that messages and files are viewed only by their intended recipients, you should read this guide.

How to use this guide

This guide describes how to use PGP to securely manage your organization's messages and data storage.

Chapter 1, "Introducing PGP." describes the pieces of an overall PGP implementation and how they interact.

Chapter 2, "The Implementation Process." describes the implementation process and suggests the order in which to install PGP products.

Chapter 3, “Setting up a Network Security Policy.” is a brief overview of the issues you must consider as you create a security policy for your organization.

Chapter 4, “Implementing a PGP Public Key Infrastructure.” discusses how to use public keys effectively in a widespread organization with a large user population.

Chapter 5, “Creating a Corporate Signing Key.” is an overview of the process you use to create a master signing key for your corporation.

Chapter 6, “Creating Additional Decryption Keys.” is an overview of the process of creating keys that allow you to decrypt information encrypted to your employees’ keys.

Chapter 7, “Running the PGPAdmin Wizard.” describes how to set preferences in PGP that your users cannot change once they install PGP.

Chapter 8, “Distributing PGP to Users.” discusses the PGP distribution process.

Related Documentation

The following documentation is available to help you install, configure, and get up to speed on the entire PGP product line.

- **An Introduction to Cryptography.** This guide is for anyone new to the science of cryptography. It is a high-level overview of the terminology, concepts, and processes used by PGP. It includes a section on security by PGP’s creator, Phil Zimmermann.
- **PGP Installation Guide.** The Installation Guide describes how to install the following products:
  - **PGP Desktop Security.** Configuration techniques for PGP Desktop Security, including instructions on how to create a PGP Client installer with pre-configured settings, are included in the PGP Administrator’s Guide (this guide).
  - **PGP Certificate Server.** Describes how to install the Certificate Server for Windows NT and UNIX software.
  - **PGP Policy Management Agent.** Describes how to install the PGP Policy Management Agent for SMTP software.
- **PGP Desktop Security User’s Guide.** The User’s Guide describes how to use the email, file, and disk encryption utilities of PGP and PGPdisk. This guide also describes how to make your applications and data securely available to all corporate users and branches using PGPnet.

For more information

There are several ways to find out more about Network Associates and its products.

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department.

You can contact Customer Care Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

Phone	(408) 988-3832

Or write to:

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

Technical support

Network Associates is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for access to Network Associates news and encryption information.

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

Technical Support for your PGP product is also available through these channels:

Phone	(408) 988-3832
Fax	(408) 970-9727
Email	PGPSupport@pgp.com

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 have this information ready before you call:

- PGP product name

- PGP product version number
- Computer platform and CPU type
- Amount of available memory (RAM)
- Operating system and version and type of network
- Content of any status or error message displayed on screen, or appearing in a log file (not all products produce log files)
- Email application and version (if the problem involves using PGP with an email product, for example, the Eudora plug-in)

Year 2000 compliance

Information regarding NAI products that are Year 2000 compliant and its Year 2000 standards and testing models may be obtained from NAI's website at http://www.nai.com/y2k.

For further information, email y2k@nai.com.

Related reading

Here are some documents that you may find helpful in understanding cryptography:

Non-Technical and beginning technical books

- "*Cryptography for the Internet*," by Philip R. Zimmermann. Scientific American, October 1998. This article, written by PGP's creator, is a tutorial on various cryptographic protocols and algorithms, many of which happen to be used by PGP.
- "*Privacy on the Line*," by Whitfield Diffie and Susan Eva Landau. MIT Press; ISBN: 0262041677. 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, and contains information that even a lot of experts don't know.
- "*The Codebreakers*," by David Kahn. Scribner; ISBN: 0684831309. 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, and published a revised edition in 1996. This book won't teach you anything about how cryptography is accomplished, but it has been the inspiration of the whole modern generation of cryptographers.

- *"Network Security: Private Communication in a Public World,"* by Charlie Kaufman, Radia Perlman, and Mike Spencer. Prentice Hall; ISBN: 0-13-061466-1. This is a good description of network security systems and protocols, including descriptions of what works, what doesn't work, and why. Published in 1995, it doesn't have many of the latest technological advances, but is still a good book. It also contains one of the most clear descriptions of how DES works of any book written.

Intermediate books

- *"Applied Cryptography: Protocols, Algorithms, and Source Code in C,"* by Bruce Schneier, John Wiley & Sons; ISBN: 0-471-12845-7. This is a good beginning technical book on how a lot of cryptography works. If you want to become an expert, this is the place to start.
- "*Handbook of Applied Cryptography*," by Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone. CRC Press; ISBN: 0-8493-8523-7. This is the technical book you should read after Schneier's book. There is a lot of heavy-duty math in this book, but it is nonetheless usable for those who do not understand the math.
- "*Internet Cryptography*," by Richard E. Smith. Addison-Wesley Pub Co; ISBN: 0201924803. This book describes how many Internet security protocols work. Most importantly, it describes how systems that are designed well nonetheless end up with flaws through careless operation. This book is light on math, and heavy on practical information.
- "*Firewalls and Internet Security: Repelling the Wily Hacker*," by William R. Cheswick and Steven M. Bellovin. Addison-Wesley Pub Co; ISBN: 0201633574. This book is written by two senior researchers at AT&T Bell Labs and is about their experiences maintaining and redesigning AT&T's Internet connection. Very readable.

Advanced books

- "*A Course in Number Theory and Cryptography*," by Neal Koblitz. Springer-Verlag; ISBN: 0-387-94293-9. An excellent graduate-level mathematics textbook on number theory and cryptography.
- "*Differential Cryptanalysis of the Data Encryption Standard*," by Eli Biham and Adi Shamir. Springer-Verlag; ISBN: 0-387-97930-1. This book describes the technique of differential cryptanalysis as applied to DES. It is an excellent book for learning about this technique.

Introducing PGP 1

Why encryption is necessary

Your company relies on your internal and external networks every day as a way to send critical information back and forth between your customers, vendors and personnel. However, there are many points along the network where your data and messages can be intercepted, copied and re-routed. Monitoring network traffic is now relatively easy and commonplace, which makes eavesdroppers a potential danger. (Ironically, Network Associates sells sophisticated network analysis tools that can be misused for this very purpose.) And, even if you deploy strong security mechanisms to keep attackers out of your networks, it is likely that some will get through.

How do you protect your data from a security breach? Most businesses eventually turn to encryption to prevent information from getting into the wrong hands. Encryption hides your sensitive information from those who should not read it, even if they can see or take the encrypted files. Encryption keeps your information private.

What is PGP?

PGP is a *cryptosystem*. PGP provides your company with complete email, file, folder, and disk volume security and integrity. PGP includes encryption, digital signing, and key management utilities which provide *privacy*, *integrity*, *non-repudiation*, and *authenticity* of information, whether it is stored or exchanged over networks.

- **Privacy.** Privacy is confidentiality gained by rendering information unreadable through encryption.
- **Integrity.** Integrity provides confidence to all parties that information was unchanged from the time it was created to the time it was read.
- **Non-repudiation.** Non-repudiation provides assurance that a document was originated by a specific individual even if that person denies it.
- **Authentication.** Authentication provides two services. The first is to identify the origin of the information and some certainty that it is authentic. The other is to verify the identity of an individual.

What does a full, enterprise-wide implementation of PGP provide my company?

PGP is one piece of an overall network security system. You can deploy PGP throughout your organization, or you can provide it only to those individuals who exchange data you want to protect—for example, your research and development organizations, your executives, and your personnel departments. You decide who should use PGP and the manner in which they should use it. You can use PGP for secure local data storage, or for securing data in transit— such as email or web communication—or for some combination of the two.

You can use PGP straight out of the box, or you can configure it to adhere to your security policies. PGP enforces your encryption policies at two levels: client and server. You can configure PGP for the desktop and then enforce your policies on the server. You can then be sure that employees are exchanging and saving sensitive data in a manner that adheres to your corporate policy.

What are the pieces of an overall PGP implementation?

The following products comprise the PGP product suite:

- **PGP Desktop Security** includes email plugins, key generation and management tools, disk utilities, and Virtual Private Networking (VPN) utilities that enable users to securely exchange and store data. You can distribute PGP to your users straight from the box, or pre-configure PGP with settings that enforce your security policy:
  - **PGPAdmin Wizard.** The PGPAdmin Wizard generates a client installer, which you distribute to your users. The preferences you set when creating the installer cannot be changed by the user, and can include: permission to generate a key pair, key size and type, selection of installed components, the path to the default Certificate Server, interaction with a Corporate Signing Key or Additional Decryption Key, designated key revokers, password length and strength, and so on.
  - **PGP Client.** The PGP Client is the Installer that results from running the PGPAdmin Wizard.

- **PGP Certificate Server.** The Certificate (Cert) Server, also called a *key server*, stores employees' *digital certificates*. A digital certificate consists of a PGP user's public key, name and user ID, digital signature, and the digital signatures of others verifying the authenticity of the user's key. In a typical implementation of PGP, employees in a company store their public key certificates on the corporate Cert Server. When any PGP user wants to exchange information with others via email, PGP retrieves the recipients' key from the server. Users can also search the Cert Server for particular keys, which they can then download to their personal keyrings.

- **Policy Management Agent.** The Policy Management Agent for Simple Mail Transfer Protocol (SMTP) works in conjunction with a standard SMTP mail server to ensure that incoming and outgoing email adheres to the security policies of a given site. It intercepts email normally bound for the SMTP server and checks to make sure that it conforms with policies configured for your organization. If the email adheres to the policies, it is forwarded to the SMTP server, where it is routed to the intended recipient. If the email does not adhere to the policies specified, a message of your choosing is sent to the client indicating that the email was rejected.

The Implementation Process 2

Checklist for installing and configuring PGP

This chapter describes how to plan for your organization's use of PGP. Planning has two parts:

- You need to make sure your network and the machines on it meet PGP's system requirements, and
- You need to make sure you have a comprehensive, organization-wide network security policy.

Your network security policy is the single most important part of your planning, because ultimately any security tool—even a world-class tool like PGP—can only be as valuable to you as the policy it supports.

A high-level description of how to set up and network security policy is provided in Chapter 3, "Setting up a Network Security Policy."

Implementing PGP in your organization

The following instructions describe the process of installing and implementing PGP in your organization at a high level.

1. Determine your PGP security policies

First establish how you will use PGP in your environment. This involves answers to some hard questions, which might include:

- **Who needs to use PGP?** What information do you need to protect? You may need to deploy PGP to every employee in your company, or only to those with certain titles or within specific departments, such as Human Resources, Finance, and / or Legal. Or perhaps you need to institute policies that every employee use PGP when communicating on specific matters, with particular departments, or when creating certain types of information.
- **Do you have different physical office locations to protect?** You can deploy Certificate Servers at different physical sites and then replicate their information to each other to provide seamless key updates and retrieval.
- **Do you have remote users?** You can deploy PGPnet to enable remote users secure, authenticated access to internal networks.

- **Do you have different types of users with a variety of needs within your company?** For example, do you trust your executives to use PGP in an unrestricted fashion because they are your executives, or do you need to hand-hold your executives because they are some of your most naive computer users? (Don't laugh—both types are out there.)

As you can see, some planning is in order before you begin to deploy PGP. For general information on security policies, see Chapter 3, "Setting up a Network Security Policy."

2. Determine your PGP and key distribution process.

Next, determine how you will distribute PGP and keys to your users. This is an important step, because you may need to increase the security of the systems on which you will install PGP and on which you will generate and distribute keys.

Most corporate environments configure PGP in some way. This enables them to implement and enforce a public-key infrastructure that facilitates key management.

You have two choices of method for distributing keys to users:

- Allow users to create their own keys. If you want to allow users to create their own keys, you can have each user run the PGP Key Generation Wizard constrained by the settings you configured using the PGPAdmin Wizard. This allows you to ensure keys are created in a manner that adheres to your policies.

  or

- Create keys yourself. If you want to create keys for all users in your organization, you must create and distribute the keys to all who need them. Bear in mind, though, that distributing keys to many users can take a long time and may create a potential security threat. You also lose non-repudiation as a feature of your cryptosystem.

3. Install PGP on your machine

Install PGP on your machine (or some other secure machine). For detailed installation instructions, see the *PGP Desktop Security User's Guide.*

4. Use the PGP Key Generation Wizard to create a Corporate Signing Key

The first key you create should be the Corporate Signing Key. A Corporate Signing Key (usually a split key) is the root key used to authenticate all your users' keys (or to set up trusted introducers who will then authenticate keys).

Create a key of the type and size that fits your security requirements. Later, when you run the PGPAdmin Wizard, you will designate this key as the Corporate Signing Key. You will also need to supply the key ID information from this key when you set up the Certificate Server.

For more information on Corporate Signing Keys, see Chapter 5, "Creating a Corporate Signing Key."

5. If needed, create Incoming and Outgoing Additional Decryption Keys

Additional Decryption Keys are a means by which you can retrieve information encrypted to an employee who is unable to recover the information.

Create a key (or keys) of the type and size that fits your security requirements. As with the Corporate Signing Key, you will later designate these keys as Additional Decryption Keys.

For more information on Additional Decryption Keys, see Chapter 6, "Creating Additional Decryption Keys."

6. Install and configure the PGP Certificate Server

The Certificate Server (also called a *key server* or *cert server*) stores your company's digital certificates. Digital certificates are more than just keys; they include identification and authentication information so your users can determine whether a particular key actually belongs to the purported owner.

You can specify the Corporate Signing Key as a certification key when you set up the Certificate Server. Any key not validated by the Corporate Signing Key will not be added to the server, but instead be held in a pending area until it is signed by the Corporate Signing Key. This will prevent invalid keys from being added to the server.

The computer on which you install the Cert Server should be physically and electronically secure—that is, in a locked room and behind your organization's firewall.

For detailed installation instructions, see the *PGP Installation Guide.* For complete configuration instructions, see the *PGP Certificate Server Administrator's Guide.*

7. Install and configure the Policy Management Agent

The Policy Management Agent for SMTP resides on your mail server and prevents email that does not adhere to your security policies from being distributed. You can set email preferences on your users' desktops; for extra security, you can enforce the settings on the server using the PMA.

For detailed installation instructions, see the *PGP Installation Guide.* For complete configuration instructions, see the *PGP Policy Management Agent for SMTP Administrator's Guide*.

8. If you are installing PGPnet, ensure that your users can authenticate to your gateway.

There are several ways that your users can authenticate to a gateway. Your users can authenticate to a gateway by using their PGP keypair, their X.509 certificate, or a shared secret.

If you are using Gauntlet VPN (GVPN), install the NetTools PKI (Public Key Infrastructure) Server or VeriSign CA so that your users can create X.509 certificates.

Note that to use shared secret, the gateway must include an entry for each user that connects to it, and each of those users must have a static IP address. As a result, using shared secrets is only practical in small, controlled installations.

9. Add your gateway and machines to PGPnet's hosts list.

On a Windows computer, you can run PGPnet's Add Host/Gateway wizard to identify your corporate network. On a Macintosh computer, use PGPnet's **Host/Gateway** dialog box to setup your hosts lists. For detailed instructions, see "Adding a host, subnet, or gateway" in the *PGP User's Guide.*

10. Create your CA certificate and import it to your keyring.

For detailed instructions, consult your Certification Authority's documentation and the *PGP User's Guide*.

11. Make selections for your Certificate Authority on the CA Options panel, available from the PGPKeys Edit menu.

Use PGP's **CA Options** panel, available from PGP Options, to set the URLs for your Certification Authority, CA type, and your root certificate. For detailed instructions, see the *PGP User's Guide*.

12. Set your PGPnet user preferences.

Use PGPnet's **General** panel to set user preferences. For details, see "Viewing the General Panel" in the PGP User's Guide.

13. Run the PGPAdmin Wizard

PGP is very flexible when installed straight from the box. If your security policy requires a specific configuration, you can set preferences in PGP and then create a version of PGP configured with your settings. Your users then install the pre-configured version. The tool for configuring PGP is called the PGPAdmin Wizard. The pre-configured version that you create is called the PGP Client.

You must create any Corporate Signing Keys and Additional Decryption Keys before you run the PGPAdmin Wizard. You designate each key's functionality in the Wizard; the keys must be present on your local keyring before you start the Wizard.

For detailed instructions, see Chapter 7, "Running the PGPAdmin Wizard."

14. Export the Corporate Signing Key and Additional Decryption Keys to the Certificate Server

For detailed instructions, see the *PGP Desktop Security User's Guide.*

15. Test your PGP Client installer on a client computer

Install the PGP Client you created in Step 13, preferably a different machine than the one on which you ran the PGPAdmin Wizard. Check to ensure that you configured the PGP Client to suit your organization's needs.

For detailed instructions, see the *PGP Desktop Security User's Guide.*

16. Use the PGP Key Generation Wizard to create your own key pair

As you use the Key Generation Wizard, check to ensure that the key settings you chose in PGPAdmin are correct.

For instructions on generating a key, see the *PGP Desktop Security User's Guide*.

17. Sign your own key pair with the Corporate Signing Key

Test your key-signing process. If you are using split keys, determine how you will reconstitute the key to sign all of your users' keys.

18. Export your own public key to the Certificate Server

For detailed instructions on exporting your key, see the *PGP Desktop Security User's Guide.*

19. Distribute PGP to your users.

Distribute the PGP Client to users either by posting it on a server or by creating and distributing disks.

For PGP Client installation instructions, see the *PGP Desktop Security User's Guide.*

Installing PGPnet on a server or stand-alone system

If you are installing PGPnet on a server or stand-alone system, please refer to "Installing and configuring PGPnet on a server or stand-alone system" on page 62.

Setting up a Network Security Policy 3

Because policy is so fundamental, this chapter offers an introduction to developing a network security policy. As you read, please remember that developing such a policy can be a major undertaking, and that you should only consider this chapter's policy discussion as a first introduction, not a full course in the subject.

WARNING: Using network security tools without a clear policy can lull you into a dangerous false sense of security. The true source of good network security is a good network security policy.

For detailed information, consult a professional security analyst. Network Associates, Inc. offers consulting in this area. For more information, see the Network Associates Website at http://www.nai.com.

Your organization's network security policy

A company's most important security tool is its *network security policy*.

A network security policy is a corporate statement concerning every aspect of security for your company's assets, including its information. When you are connected to the Internet, you put your network at risk from many types of attackers: Internet vandals, disgruntled employees or contractors, or industrial spies. Your company's network security policy can help reduce the risk by instituting specific security guidelines and procedures.

The goals of network security differ between companies, but generally include the following:

- control of access to the network
- **control of access to specific resources (for example, files and applications)**
- **protection of information while in transit**
- **protection of information in archives**
- detection of breaches in security
- actions to take in event of a network breach

- prevention of accidental damage
- recovery from system failure
- **theft and tamper protection**
- disaster planning

PGP products provide the security features listed in boldface type.

Network Associates' Website contains links to other sites that provide information on developing a security policy.

Creating a Security Policy

We cannot overstress the importance of developing a good, written security policy. In fact, deploying a security product without a security policy can actually be worse because it can encourage a false sense of security that can lead to complacency. Without a policy, you cannot effectively protect your network. That's so important, we're going to repeat it in bold:

Without a security policy, you cannot effectively protect your network.

And yet, studies show that 92% of all corporations have no security policy at all. So, the single most important part of any PGP deployment is the effort you put into defining your network security objectives, and then translating those objectives into a concrete set of specific policies. Configuring PGP is nothing more than instructing the PGP Admin Wizard in how to implement each of those concrete policies.

You should plan to spend some time developing and implementing your network security policies. PGP can't write your policies for you. All it can do is enforce the policies you set.

How to develop a network security policy

NOTE: To have real value, a network security policy must be developed as an integrated component of an organization's master security policy. The network security policy should harmonize with security policies in other areas such as physical plant integrity, employee background checks, electronic eavesdropping detection, and so forth.
Because of this— and because so many organizations have no security policy at all— in this section we discuss how to develop a master security policy. But keep in mind that only a portion of your master security policy will affect the way you use PGP.

An organization-wide security policy isn't something you can buy in a store, because every organization has its own unique priorities and its own unique way of doing business. Every organization needs to develop the unique set of security policies that will work for them. And so every organization needs to do the challenging work of developing its own security policy.

Before you start

Before you can create a policy, you need to determine what to cover. For example:

- **What do you need to protect?** A security policy should be based on an inventory of your company's assets. Determine and define what you will protect and then prioritize which system or information is most crucial to protect. This includes everything: information, desktop computers, servers, wires, your furniture, and so on. Talking to your users could be very effective during this process. If you do not determine what is important to protect, you may sacrifice performance or incur costs protecting information that is not valuable. Alternatively, you may develop a false sense of security about a system in which your most sensitive information is left exposed.
- **From whom will you protect it?** Do you envision corporate spies when you imagine someone attempting to breach your network? It's very possible that your biggest threat might be a determined internal or external infiltrator. And what about the user with too many administrative privileges who wreaks havoc inadvertently? (We all have one of those.) Unintentional harm can be just as damaging as a concerted attack.
- **Against what threats will you protect yourself?** Determine what might befall your network and to what level of damage. Theft, viruses, physical attacks, eavesdroppers and sniffers over the net, system failure, and so on. This list will help you determine where to focus your attention when planning how to prevent problems. It will also help you determine your security budget and where to ensure your security is most effective.
- **What will you do in the event of a network crisis?** What actions will you take should your fears come to pass? Who will be notified in the event of a security breach? How will you get your systems back online after the fire / earthquake / tornado? What will you do when your secret formula falls into the wrong hands?

After establishing baseline rules, and ranking your information assets, you are ready to tackle possible security holes in a prioritized fashion, and identify ways to address them. After you consider points like those above, you will find it easier to sit down and create a policy.

Include your users in the process

Don't forget to include the people who will be following the policy during the planning phase. You probably won't know the operating needs of all of your users until you talk to them. While it will be the responsibility of your group to implement the policy, it is those who will follow the policy who can help determine what is necessary and reasonable from an operational standpoint. Include individuals from all areas of the company. You may also uncover employees in your company who are security experts with advice and experience to share.

Aside from the valuable information and insight they can provide, many users find policy more palatable if they help to create it. "Ramming it down their throats" could create the sort of resentment that leads to security breaches.

Write it down

The most important single thing you can do is to publish your company policy. For example, if your organization reserves the right to monitor users' email, then your corporate email policy should clearly spell that out.

To protect itself, your company should have a written security policy, and every user should receive and understand it.

Like any safety tool, network security policies are only effective when understood and used. Every time a change to your Internet configuration is considered, you should first consult your network security policy and, if necessary, modify it and then communicate the changes to your users. You must effectively communicate to anyone with network access—employees, contractors, third-party vendors, and so on. These users need to know what, why, and how they can protect the network and for what breaches they will be held responsible, because most reported intrusions are the result of an internal security failure. (In fact, tricking someone into disclosing password information is one of the easiest and most successful attacks on a network.)

Whatever choices you make with respect to your organization's security policy, make sure that your users understand that policy fully before they use PGP or any other security software.

Policy and privacy

Some companies conclude that they can and should reserve the right to access employees' files at any time, because they provide the hardware and software that employees use. But the boundaries between company property and the property of others, between employees and independent contractors, and even between the company's computer systems and those of others, are blurring.

Consider the following points:

- Many employees work at home and use equipment not owned by the company.
- Company-owned databases, bulletin boards, and Web pages may contain links to materials that are not owned or authored by the company.
- Many of those who use the company systems may be independent contractors rather than employees. They may even be entirely independent suppliers or customers.
- Your company may or may not own the system used to provide email for employees. Many companies contract with third-party networks for this service.
- Email originating on your company system may be sent over private links or the public Internet to third parties. Some messages in employee mailboxes may have come in through such routes—and the senders of such messages may have no notice of, and may not have consented to, any company policies regarding privacy, access, or disclosure.
- Your company also owns and provides to employees many other types of property, such as pencils and telephones, that are regularly used by employees to send personal and private messages.

Your company probably considers some of the spaces inside its buildings, such as drawers in an employee's desk, to be entitled to special privacy protections.

Because privacy is an important aspect of any healthy culture, corporate or not, finding an appropriate line of division between personal privacy and corporate property is essential; but it is a challenge.

Corporate liability for employees' acts

If an employee uses the corporate network in the performance of a criminal act, your corporation may be implicated. Make sure that your employees understand that they are not to use company equipment, including email, for illegal purposes.

Security issues

This section covers, at a very high level, some issues to take into account when developing a security policy.

Encryption

If you want to protect data from eavesdroppers as it travels from your network to other companies over an unsecured network like the Internet, you will need encryption. Encryption is recommended for any sensitive data, such as private email, data exchanged between business partners, or customer information collected on a Web site. In addition, PGPdisk protects your current and archival files from unauthorized users.

PGP provides encryption as well as authentication, which ensures the integrity of your data.

Passwords and passphrases

Because passwords generally establish access to your network, it is wise to institute policies that dictate how and when they should be used or discarded.

Password policies that require users to change their passphrase often or insert non-alphabetic characters make it difficult for employees to remember their passwords. Many employees end up writing down their passwords and taping them to the inside of a desk drawer.

If your users must write down their passwords, consider having them create a text file on their computer desktop listing their passwords and then encrypting the file with PGP's strong encryption. This method does not prevent employees from accidentally deleting the file, but the file should be more secure against an attacker than a Post-It adhered to the employee's monitor.

Residual data

Residual data refers to the data remaining on the physical hard disk of a computer after an employee has deleted it. Applications generally delete the name of the file but leave the actual data intact, waiting to be overwritten by another application. Some applications also create automatic backups of file to memory, which are stored in locations a user might not expect or remember to purge.

This data is available to any attacker with a disk recovery toolkit, particularly if your company discards the old computer. *Dumpster diving* is a legal method for attackers to retrieve confidential information from discarded systems.

PGP's disk wiping utilities permanently deletes any residual data. If you consider theft of data a threat, then your security policy may need to require users to purge their systems of discarded data on a routine basis.

Physical security

Physical security implies the protection of the actual computer systems in your company. It refers to locking doors and limiting access. Do you know who has access to your server facilities and who has access to your wiring closets? Many network disasters are caused by angry employees seeking retribution.

For example, if your company uses the PGP Certificate Server, it might be a good idea to ensure that the system on which it is installed is kept behind a locked door.

Corporate Signing Keys

A *Corporate Signing Key* is a key pair used to prove that digital certificates, information, products, and so on have been validated by an authority acting on behalf of the company. The Corporate Signing Key is primarily used for signing, but can also be used for encryption. It is typically held by the Corporate Security Officer alone, or split into multiple shares (see Key splitting, below).

Some examples of uses for a Corporate Signing Key are:

- signing employees' digital certs or keys
- signing softcopies of legal documents
- signing software produced by your company

Because the Corporate Signing Key is used to validate all keys in your organization as well as provide authentication for other data as well, it is vital that this key is never compromised, lest someone else pretend to act in the company's name.

Additional Decryption Keys

An *Additional Decryption Key* (ADK) enables a company to access information encrypted by its employees in the event of an emergency. ADKs are useful in situations where the user to whose key information is encrypted is somehow unable to decrypt the information, either because the key or passphrase is lost or because the user is unavailable due to an accident or other absence. For an environment employing strong encryption with no available "back door," an ADK is a prudent data recovery tool.

In environments that enforce the use of ADKs, any information encrypted to the user's key is also encrypted to the ADK. When someone inside or outside the organization encrypts information to a user, the information is also encrypted to the ADK. This allows the holder of the ADK to decrypt any information sent to the user. This operation happens automatically, and is fully integrated into the encryption process.

Consider your ADK usage policy carefully, paying attention to striking the correct balance between employee privacy and data recovery. If your policy is too strict, your users may view it as a lack of trust and choose not to use any encryption, which could leave you with vulnerabilities in your system. Recovery of stored data, such as that on a PGPdisk volume, is generally viewed more favorably than recovery of communications, such as private email.

Key validation

Every user in a public key system is vulnerable to mistaking a phony key (digital certificate) for a real one. *Validity* is confidence that a public key certificate belongs to its purported owner. Validity is essential in a public key environment where users must constantly establish whether or not a particular certificate is authentic.

When a user is assured that a certificate belonging to someone else is valid, the user can sign the copy on her local keyring to attest to the fact that she has checked the certificate and that it's a good one. If that person wants others to know that she gave the certificate her stamp of approval, she can export the signature to a certificate server so that others can see it.

Some companies designate one or more *Certification Authorities (CA)*, to check the validity of all the certificates in the organization and sign the authenticated ones. The CA is responsible for validation in an organization, and is an entity whom everyone trusts; in some public key environments, no certificate is considered valid unless it has been attested to by a CA. For information on how a CA validates keys, see "Validating keys with a Corporate Signing Key" on page 40.

Key splitting

Key splitting, also called “secret sharing” is the ability to split a private key into multiple pieces or *shares*, and share those pieces among a group of people. To use the key, a designated number of the keyholders must bring their shares of the key together to reconstitute the key.

Splitting or sharing the private key used for signing ensures that any one person cannot compromise the key and greatly reduces the possibility of abuse.

PGP uses a secure TLS connection during key reconstitution, which allows the process to be completed securely over an untrusted network without requiring any shareholders to be physically present.

Designated revokers

When a private key or its passphrase is lost, the key’s security is compromised. The safest action to take in such a situation is to prevent others from encrypting information to the key by revoking it. The difficulty in a scenario such as this is that the passphrase and private key are required to revoke a key.

A *designated revoker* is another key pair that has been authorized to revoke the key on behalf of the owner. You can configure the PGP Client to add a designated revoker key for all keys generated with the PGP Key Generation Wizard.

Determining your email policy

Because PGP is widely used for privacy of email, we’ll use email examples in demonstrating what to consider when creating a network security policy.

Employee email privacy

PGP software makes possible an unprecedented increase in privacy for personal and corporate email. Within the confines of the work environment, employees must understand that they must reconcile their personal privacy with corporate security, but employers should consider that there is a legitimate need for personal privacy in the workplace. Businesses operate on trust, trust that employees know their jobs and trust that they do their work in the best interests of the organization. However, there may be occasions when a compelling reason for monitoring, accessing, or reading employees’ email arises, for example, death or other unavailability of an employee, forgotten passwords, or unethical and/or illegal activity by an employee.

If your company reserves the right to monitor, read, intercept, or access employees' email messages, it is imperative to have a clear, definitive policy statement and to make sure that everyone reads and understands it.

Creating a written email policy

Here are some things to consider when creating your organization's email policy. (Adapted with permission of the Cyberspace Law Institute.)

Purposes for which company email may be used

- Email may be used only for company business.
- Email may be used for incidental personal purposes.
- Email may be used for personal purposes without restriction.

Encryption and labeling

- Encryption of any kind is permitted.
- Only specified forms of encryption are permitted.
- Personal email must be labeled as such.
- Signature files or message text must disclose limitations of the employee's authority.

Systemic monitoring

- No systemic monitoring.
- Monitoring allowed for any business purpose.
- Monitoring allowed only with good-cause legal obligations.

Access and disclosure without consent in specific cases

- No access without consent unless required by law or other duty.
- Access or disclosure with good cause and appropriate measures.
- Access or disclosure for any business by those with authority.
- Notification after the fact of any access or disclosure.

Substantive rules

- Company email may not be used for illegal or wrongful purposes.
- Company email may not be used to download software without checking for viruses.

- Electronic snooping prohibited.
- Electronic mail may not be used for sexual harassment, chain mail messages, or other purposes that are against organizational rules of conduct.

Protection of proprietary information

Policies and safeguards should be put into place requiring that proprietary information transmitted via email be encrypted. You should specify which types of information must be encrypted and which types may be sent in clear text.

Regular destruction of email archives

Are there legal timebombs in your email archives? Keeping email archives forever is an unnecessary exposure to the risk of litigants subpoenaing your archives and investigators sifting through the contents of employees' email.

Your company should take the following actions:

- Have a policy that says how long email is to be kept or how often the archive must be purged.
- Have a procedure or process in place to guarantee that the destruction or purging actually happens.
- Communicate your email archive policies to users.
- Decide whether the email of certain classes of users is archived longer than others. You may choose to only archive the email of special classes of users, such as corporate officer's or key technical contributors, after a given period of time.

Any email message that pertains to any kind of legal case can be subpoenaed as evidence. If you don't have an email destruction policy and procedure in place, you could find yourself accused of intentionally destroying evidence years after the actual destruction took place.

This is particularly important if your organization uses additional decryption keys associated with users' keys. See Chapter 6, "Creating Additional Decryption Keys" for more information. Consider carefully how to achieve a balance between your potential exposure to litigation and the need to have information available—for example, consider making policy the regular destruction of your ADKs.

Implementing a PGP Public Key Infrastructure 4

Many companies are composed of various and highly diverse organizations and departments that need to work together in complex ways. Users trying to communicate with others in a public key environment need to understand how to find and validate a complete certification path from the public keys of people they have never met to completely trusted Certification Authorities. Alert and knowledgeable users are less likely to encrypt information to counterfeit keys.

A *public key infrastructure* is necessary if public-key-based technologies are to support a large or diverse user population. It provides a framework of relationships between certification authorities, ways to validate keys, digital certificate management and so on.

What is a Public Key Infrastructure?

A PKI contains the certificate storage facilities of a certificate server (also called a key server), but also provides certificate management facilities (the ability to issue, revoke, store, retrieve, and trust certificates). The main feature of a PKI is the introduction of what is known as a *Certification Authority*, or *CA*, which is a human entity—a person, group, department, company, or other association—that an organization has authorized to issue certificates to its computer users. (A CA's role is analogous to a country's government's Passport Office.) A CA creates certificates and digitally signs them using the CA's private key. Because of its role in creating certificates, the CA is the central component of a PKI. Using the CA's public key, anyone wanting to verify a certificate's authenticity verifies the issuing CA's digital signature, and hence, the integrity of the contents of the certificate (most importantly, the public key and the identity of the certificate holder).

Validating users' keys

Every user in a public key system is vulnerable to mistaking a phony key (certificate) for a real one. *Validity* is confidence that a public key certificate belongs to its purported owner. Validity is essential in a public key environment where you must constantly establish whether or not a particular certificate is authentic.

Some companies designate one or more Certification Authorities (CAs) to indicate certificate validity. In an organization using a PKI with X.509 certificates, it is the job of the CA to *issue* certificates to users—a process which generally entails responding to a user's request for a certificate. In an organization using PGP certificates without a PKI, it is the job of the CA to check the authenticity of all PGP certificates and then sign the good ones. Basically, the main purpose of a CA is to bind a public key to the identification information contained in the certificate and thus assure third parties that some measure of care was taken to ensure that this binding of the identification information and key is valid.

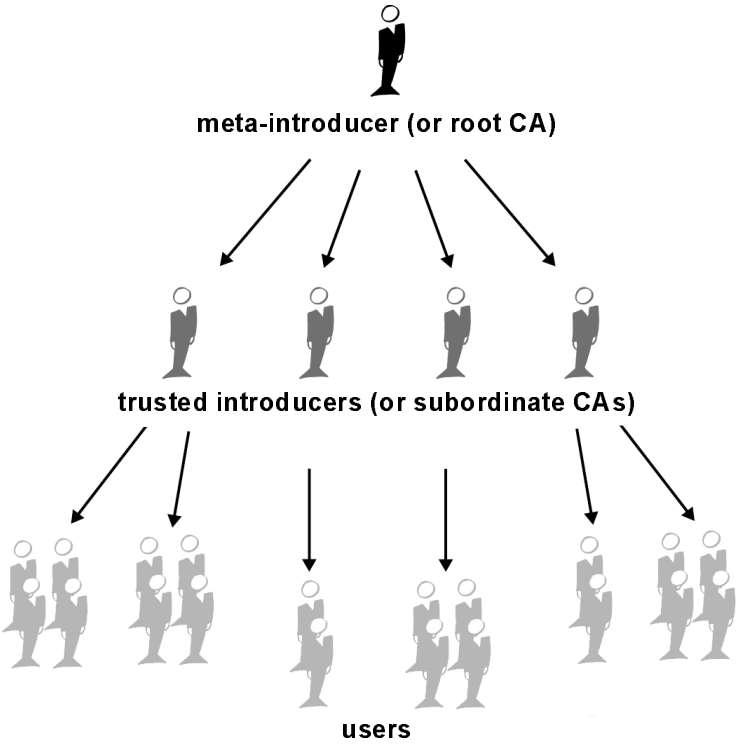

Figure 4-1. Meta and Trusted Introducers

Trust models

A *trust model* is a convention that governs how validation works in a public-key environment. In relatively closed systems, such as within a company, it is easy to trace a certification path back to the root CA. However, users must often communicate with people outside of their corporate environment, including some whom they have never met, such as vendors, customers, clients, associates, and so on.

There are three different trust models:

- Direct Trust
- Hierarchical Trust
- A Web of Trust

Direct Trust

Direct trust is the simplest trust model. In this model, a user trusts that a key is valid because he or she knows where it came from. All cryptosystems use this form of trust in some way. For example, in web browsers, the root CA keys are directly trusted because they were shipped by the manufacturer. If there is any form of hierarchy, it extends from these directly trusted certificates. In PGP, a user who validates keys herself and never sets another certificate to be a trusted introducer is using direct trust.

Small organizations with no central certification authority would probably use direct trust as their trust model.

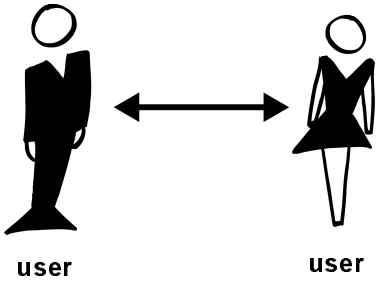

Figure 4-2. Direct trust

Hierarchical Trust

In a hierarchical system, there are a number of “root” certificates from which trust extends. These certificates may trust certificates themselves, or they may trust certificates that trust still other certificates down some chain. Consider it as a big trust “tree.” The “leaf” certificate's validity is verified by tracing backward from its certifier, to other certifiers, until a directly trusted root certificate is found.

This model is the one most commonly used in corporations. See Figure 4-1 for an illustration of hierarchical trust.

Web of Trust

A web of trust encompasses both of the other models, but also adds the notion that trust is in the eye of the beholder (which is the real-world view) and the idea that more information is better. It is thus a cumulative trust model. A certificate might be trusted directly, or trusted in some chain going back to a directly trusted root certificate (the meta-introducer), or by some group of introducers.

PGP uses digital signatures as its form of introduction. When any user signs another's key, he or she becomes an introducer of that key. As this process goes on, it establishes a *web of trust*.

In a PGP environment, *any* user can act as a certifying authority. Any PGP user can validate another PGP user's public key certificate. However, such a certificate is only valid to another user if the relying party recognizes the validator as a trusted introducer. (That is, you trust my opinion that others' keys are valid only if you consider me to be a trusted introducer. Otherwise, my opinion on other keys' validity is moot.)

Stored with each key on a user's public keyring file are indicators of:

- whether or not the user considers a particular key to be valid
- the level of trust the user places on the key that the key's owner can serve as a certifier of others' keys

You indicate, on your copy of my key, whether you think my judgement counts. It's really a reputation system: certain people are reputed to give good signatures, and people trust them to attest to other keys' validity.

Validating keys with a Corporate Signing Key

Manually validating all keys in an organization can be a daunting task. More importantly, it is a task that must be accomplished methodically so that invalid keys are not accidentally mingled with valid keys. PGP provides a mechanism to prevent accidental posting of invalid keys on the server.

This mechanism is a holding, or *pending*, area for any keys sent to the server that do not meet security policy requirements.

(See the *PGP Certificate Server Administrator's Guide* for more information on setting up a key acceptance policy on the server.)

A commonly enforced practice is to require only those certificates which have been signed by the Corporate Signing Key (or authorized trusted introducers) to be accepted by the Certificate Server. The PGP Certificate Server automatically redirects any keys that do not adhere to corporate policy to the "Pending Area." You can search this pending area periodically and validate any keys in there. You can then send them to the server.

The typical process for validating corporate keys is as follows:

1. The user generates a new key.
2. The key is automatically sent to the Certificate Server.
3. Any keys that do not adhere to policy are held in the Pending Area of the Certificate Server.
4. Periodically, the CA checks the Pending Area for new keys. Upon finding a new key, the CA manually authenticates the key—that is, checks its fingerprint against the one on the user's private key (either by phone or in person).
5. The CA signs the key to validate it.
6. The CA moves the key to the Certificate Server where it is available to other PGP users.

By holding keys in a pending area and allowing only valid keys to be moved to the Certificate Server, you can ensure that only valid keys are available to your user community.

Creating a Corporate Signing Key 5

What is a Corporate Signing Key?

A *Corporate Signing Key* is a key pair used to prove that digital certificates, information, products, and so on have been validated by an authority acting on behalf of the company. The holder(s) of the Corporate Signing Key acts as a root *Certification Authority (CA).*

Typically held by the corporate security officer alone or split into multiple shares and held by an entire security team, the Corporate Signing Key is used primarily for validating employees' keys. To ensure that all keys in an organization are valid, many companies institute a policy dictating that digital certificates signed by the Corporate Signing Key are valid and that employees should be cautious of keys or documents not signed by the Corporate Signing Key (or trusted introducers created by the key) because they have not been authenticated by a known certifying authority. The Corporate Signing Key can be the meta-introducer for an organization.

Some examples of uses for the Corporate Signing Key are:

- signing employees' digital certs or keys
- creating trusted introducer signatures on trusted keys
- signing softcopy of legal documents
- signing software produced by your company
- signing official corporate email and announcements

A Corporate Signing Key is typically used for signing only. Some companies use a Corporate Signing Key for encryption as well, but it is a less common practice to encrypt with the corporate key. If you use a Diffie-Hellman/DSS key as a Corporate Signing Key, you can remove the encryption portion of the key (the encryption *subkey*) and designate the key as a *signing-only* key. For more information on creating and deleting encryption subkeys for a Corporate Signing Key, see the section on creating new subkeys in the *PGP Desktop Security User's Guide*.

Protecting a Corporate Signing Key

Because it is used to validate all keys in your organization as well as provide authentication for other data as well (files, personnel information, legal documents, your products), it is vital that this key is never compromised. Thus it is a good idea to implement key splitting for the Corporate Signing Key so no one individual can use it alone.

It is important to add some measure of physical security to the storage of a Corporate Signing Key or its share files, however. For example, the machine used for reconstituting the Corporate Signing Key should be secure, possibly behind a locked door. You may wish to lock the key share files or the key itself in a safe.

Creating a Corporate Signing Key

Use the Key Generation Wizard to create a Corporate Signing Key that meets your security needs. This key pair will appear on your local keyring. You designate it as the Corporate Signing Key when you configure the PGP Client using the PGPAdmin Wizard; not during Key Generation. For information on how to designate the key you create as the Corporate Signing Key, see Chapter 7, “Running the PGPAdmin Wizard.”

After you designate a key as the Corporate Signing Key, you can use it to sign all the other keys in your organization, including your own personal key. You can also configure the PGP Client so that any key generated by a user automatically signs the Corporate Signing Key.

The sections below provides some additional information you may find useful as you generate your key.

Key type

The Corporate Signing Key is generally used for signing, not encryption. If you use a Diffie-Hellman / DSS key, you can ensure that the Corporate Signing Key is used only for that purpose by making it a signing-only key. This is only possible with a Diffie-Hellman / DSS key. See the section on Subkeys, later in this chapter.

Key size

The Corporate Signing Key should be at least 1024-bit.

Splitting

Most companies split the Corporate Signing Key and distribute the shares among multiple individuals. PGP implements a secure network connection so that shareholders of a split key do not need to be physically present throughout the reconstitution process. For more information, see the section on key splitting in the *PGP Desktop Security User's Guide.*

Subkeys

After you have created the key, you may wish to prevent the key from being used for encryption. To do so, you can delete any encryption subkeys associated with the key. For more information on creating and deleting encryption subkeys for a Corporate Signing Key, see the section on creating new subkeys in the *PGP Desktop Security User's Guide.*

Using the Corporate Signing Key

The following suggestions will help you establish trust in the Corporate Signing Key throughout your company.

- **Distribute the key with the PGP Client.** Add the key to the default keyring installed with the PGP Client so that every PGP user receives a copy of the Corporate Signing Key on his or her local keyring. (You specify the default keyring in one of the panes of the PGPAdmin Wizard. For more information see Chapter 7, "Running the PGPAdmin Wizard.")
- **Publish the key's fingerprint.** Once you have created the Corporate Signing Key, you should publish the key's fingerprint in a non-electronic format so that users can verify its validity or distribute it through another trusted means.
- **Utilize the Certificate Server's validation features.** You can configure the Certificate Server to send any keys not signed by the Corporate Signing Key to a Pending Area, where the keys will remain until you can validate them. For more information, see the *PGP Certificate Server Administrator's Guide.*
- **Make the key available to the public.** If you plan to use the Corporate Signing Key to sign information distributed or sold outside the company, you may want to post the key on a public keyserver so that recipients of the signed information can verify the signature.

Creating Additional Decryption Keys 6

What are Additional Decryption Keys?

Suppose your chief scientist is hit by a bus and is hospitalized for months. Or that your lead engineer, in a rage, encrypts his entire hard drive and leaves the company. Or your office manager forgets his password, or loses his key. What happens to all that data, which is so securely encrypted? Can you retrieve it, or is it gone forever?

An Additional Decryption Key (ADK) is a data recovery tool. In an environment that enforces use of an ADK, any information encrypted to a user's key is also encrypted to the Additional Decryption Key. When someone inside or outside the organization encrypts information to a user, the information is also encrypted to the Additional Decryption Key. This allows the owner of the Additional Decryption Key to decrypt any information sent to the user. This process happens automatically, and is fully integrated into the encryption process.

Recover data in an emergency

An ADK is a powerful security tool in situations where an employee is injured, incapacitated, or terminated, leaving valuable information encrypted. Because PGP has no "back door," recovery of this information would be otherwise infeasible.

While you may not ordinarily use the ADKs, there may be circumstances when it is necessary to recover someone's email, for example, if someone is out of work for some time or if you are subpoenaed by a law enforcement agency and must decrypt messages or files for a court case.

PGP offers an Incoming ADK and an Outgoing ADK. These keys can also interact with policies that you configure using the Policy Management Agent for SMTP.

Data recovery versus key recovery

Do not confuse data recovery with key recovery. An Additional Decryption Key enables you to recover information that has been encrypted to a particular key, not the key itself. The difference is crucial. If a mechanism exists to obtain a copy of a user's key, one major feature of a public-key cryptosystem—non-repudiation—is lost. If more than one copy of a key exists, then a user can deny having signed information with the key.

Retaining copies of users' keys has an added security risk: the machine storing the keys is an obvious target for attack, as is the administrator of the machine.

An Additional Decryption Key is far easier to protect, and it enables you to retain non-repudiation, which is a major advantage inherent to public-key cryptography.

Incoming Additional Decryption Keys

An Incoming ADK causes encrypted mail sent to people in your organization to be encrypted to the Incoming ADK as well as to the intended recipient.

When users generate Diffie-Hellman / DSS keys, their keys contain a pointer to the Incoming ADK.

You can select Enforce Incoming Additional Decryption Key as an option in the PGPAdmin Wizard; this causes the PGP Client to list the Incoming ADK as another recipient of the encrypted information in the sender's PGP Recipients List. The user is unable to remove the Incoming ADK from the list.

Incoming ADKs must be Diffie-Hellman keys.

Outgoing Additional Decryption Keys

The Outgoing ADK causes encrypted mail sent from people in your organization to also be encrypted to the Outgoing ADK.

If you check Enforce Additional Decryption when running the PGPAdmin Wizard, all outgoing encrypted mail must be encrypted to the Outgoing ADK.

Outgoing ADKs can be either RSA or Diffie-Hellman keys. One Diffie-Hellman key can serve as both an Incoming and Outgoing ADK.

TIP: Consider whether you want to have multiple Additional Decryption Keys to minimize the risk of having one key become the object of a single point of attack. If you have multiple Additional Decryption Keys, if one is compromised, the rest of your encrypted data that is encrypted to other Additional Decryption Keys is not in danger of being decrypted.

Additional Decryption Key policy

As security officer, you decide whether your company enforces the use of ADKs. You should have a policy that governs how and when they will be used and should communicate this policy to everyone who will be affected by it. Obviously, this policy should consider employee privacy.

Protecting Your Additional Decryption Key

Additional Decryption Keys must be secured both physically and electronically in order to prevent a security breach. If either the Incoming or Outgoing ADK is ever compromised, all encrypted messages sent to users with additional decryption enabled could be decrypted by the attacker.

To prevent unauthorized additional decryption and problems with liability, your organization should enforce a policy that the key should be shared by at least two individuals.

Do *not* use ADKs unless you can ensure their security. In an environment that enforces use of an ADK, security of these keys determines the security of all encrypted messages in your entire organization.

Creating Additional Decryption Keys

The ADKs should be the next sets of keys you create after you create the Corporate Signing Key.

If you want separate keys for the Incoming ADK and the Outgoing ADK, you must go through the Key Generation Wizard twice, once for each key.

Key type

Select a key type, either Diffie-Hellman / DSS or RSA. (RSA is an option only if the version of PGP you are using provides RSA support.)

NOTE: Only Diffie-Hellman keys can be used as Incoming ADKs. Outgoing Additional Decryption Keys can be either Diffie-Hellman or RSA. If users have RSA keys, only another RSA key can be used as the ADK. If users have Diffie-Hellman keys, then you must use another Diffie-Hellman key as the Additional Decryption Keys. If users have both RSA and Diffie-Hellman keys, you will need both types of Additional Decryption Keys.

Diffie-Hellman/DSS

Diffie-Hellman / DSS keys have the advantage that they can be used as both Incoming and Outgoing ADKs.

- If your users correspond with people who have PGP Version 5.0 or later, you can take advantage of the new technology and generate a pair of Diffie-Hellman / DSS keys.
- If your users want to be able to exchange email with all PGP users, you should make a pair of RSA keys and a pair of Diffie-Hellman / DSS keys and then use the appropriate pair depending on the version of PGP used by the recipient with whom you are communicating.

RSA

For RSA keys, Outgoing ADKs work by specifying the ADK in a read-only setting on the users' machine. This means that the ADK is enabled only within the organization. When someone inside the organization encrypts a message to the user, the message will also be encrypted to the ADK. However, encrypted messages from outside users to an internal user are not encrypted to the ADK.

NOTE: If your users correspond with people who are using RSA keys, you will probably want to generate an RSA key pair that is compatible with older versions of the program.

Key size

Your Additional Decryption Keys should be as large as possible.

Select a key size that is 2048 bits or higher. The key size corresponds to the number of bits used to construct your digital key. The larger the key, the less chance that someone will ever be able to crack it, but the longer it takes to perform the decryption and encryption process. Note that RSA keys are limited to 2048 bits in order to maintain compatibility with older versions of PGP.

NOTE: A custom-sized key may take a few minutes to generate, depending on the computer that you are using.

Expiration

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

Splitting

Most companies split the Additional Decryption Key and distribute the shares among multiple individuals. PGP implements a secure network connection so that shareholders of a split key do not need to be physically present throughout the reconstitution process. For more information, see the section on key splitting in the *PGP Desktop Security User's Guide.*

Passphrase

Additional Decryption Keys' passphrases should have a security score of at least 50.

Running the PGPAdmin Wizard 7

The PGPAdmin Wizard allows you to specify security options for your site.

When you run the PGPAdmin Wizard, you create a PGP Client installer, which installs a version of PGP pre-configured with options that users cannot change. These options are stored in a binary file which is part of the PGP Client installer and include the user's ability to generate their own key, the type of key generated, use of Additional Decryption Keys, whether to automatically sign the Corporate Key, designated key revokers, and password length and strength.

NOTE: In addition to setting preferences on the desktop, consider taking the security measure of enforcing your policies on the server using the Policy Management Agent.

What you need to know before you start

You run the PGPAdmin Wizard only once, to preconfigure PGP with corporate defaults for your users before they use it themselves.

Before you run the wizard, you must complete the following tasks.

- Install PGP on your machine.
- If you plan to use a Corporate Signing Key, create it and make sure it is on your keyring.
- If you plan to use Incoming or Outgoing Additional Decryption Keys, create them and make sure they are on your keyring.
- If you plan to specify a Designated Certificate Revoker other than the Corporate Signing Key (CSK), create the designated revoker key and make sure it is on your keyring.
- If you are installing PGPnet, perform the following tasks:
  - Ensure that your users can authenticate to your gateway via PGPkeys, X.509 certificates, or shared secret.
  - Run PGPnet's Add Host/Gateway wizard to identify your gateway and create other host entries (see the User's Guide for instructions).

- If you are using a Certification Authority, create your Certification Authority certificate and import it to your keyring.
- Make selections for your Certification Authority on the PGPKeys CA Options panel.
- Set your PGPnet user preferences.

To run the PGPAdmin Wizard

The steps below describe how to run the PGPAdmin Wizard and provide information on the options available.

The wizard leads you through the steps of creating the PGP Client installer. For each window, either enter the requested information or accept the defaults provided on each screen. Click **Next** or **Back** to move between the panes of the Wizard.

1. Start the PGPAdmin Wizard.
   - On a Windows machine, select **Start—>Programs—>PGP—>PGPadmin**.
   - On a Macintosh, double-click the **PGPadmin** icon.

   The PGPadmin screen appears.
2. Enter your company name in the space provided.

   The PGPadmin Introduction screen appears. Click **Next**.

Specifying Additional Decryption Keys

3. If you want to designate an ADK on your key ring to include with each user's public key for incoming email messages, check the **Use an Incoming Additional Decryption Key** checkbox.

   IMPORTANT: This key must be present on the keyring before you can continue. If it is not, you must create it: open PGPkeys, select New Key to start the Key Generation Wizard, generate a Diffie-Hellman / DSS key, and then continue running the PGPAdmin Wizard.

   An Incoming ADK causes encrypted mail sent to people in your organization to be encrypted to the Incoming ADK as well as to the intended recipient. **The ADK enables the administrator to unlock files in an emergency without archiving a copy of the user's private key.**

4. Choose the key to use as the Incoming ADK from the **Incoming Additional Decryption Key Selection** dialog box, then click **Next**.

5. If you want to designate an Outgoing ADK to include with each user's public key for outgoing email messages, check the **Use an Outgoing Additional Decryption Key** checkbox.

   An Outgoing ADK automatically encrypts all outgoing messages to both the specified user and the Outgoing ADK. This key can be either an RSA or Diffie-Hellman/DSS key. If you wish to combine the use of the Incoming and Outgoing ADKs, both keys must be Diffie-Hellman/DSS.

6. Choose the key to use as the outgoing ADK from the **Outgoing Additional Decryption Key Selection** dialog box, then click **Next**.

7. Enforce the use of ADKs.

   At this point you can enforce the use of additional decryption. You can enforce the use of any or all of the following:

   - **Enforce Incoming Additional Decryption Key.** Select this checkbox if you want to enforce the use of the Incoming ADK. This option is available only if you chose to use an incoming ADK. If you choose not to enforce the use of the Incoming ADK, the user can bypass the use of the ADK.
   - **Enforce Outgoing Additional Decryption Key.** Select this checkbox to enforce the use of the Outgoing ADK. This option is available only if you chose to use an outgoing ADK. If you choose not to enforce the use of the Outgoing ADK, the user can bypass the use of the ADK.
   - **Enforce remote Additional Decryption Key strictness.** Select this checkbox to force your users to respect an external organization's use of Incoming ADKs. That is, if a user in another company sends one of your users a public key that is associated with the sender's company's Incoming ADK, the recipient will be forced to use the other company's ADK.

   WARNING: If you choose not to enforce use of ADKs, users attempting to encrypt information can remove an associated ADK from the recipient list and encrypt the information without encrypting to the ADK.

   ---

8. If you want to include an ADK with each user's public key for PGPdisk volumes, check the **Use a PGPdisk Additional Decryption Key** checkbox.

A PGPdisk ADK causes any PGPdisk volumes created by the user also to be accessible to the holder of the ADK; this aids recovery of information encrypted within a PGPdisk volume.

9. Choose the key to use as the PGPdisk ADK from the **PGPdisk Additional Decryption Key Selection** dialog box, then click **Next**.

Specifying Passphrase Security

10. Specify the passphrase length and quality required for your users. Your options are:

    - **Enforce minimum number of characters.** There are trade-offs between security and ease of use. A long passphrase may be harder for an attacker to guess but also harder for the user to type successfully and remember.
    - **Enforce minimum amount of quality.** Quality must be at least 20 out of 100 (default value for a user's key). You should use a value of at least 50 when creating Corporate Keys and ADKs.

Specifying a Corporate Signing Key

11. If you plan to use a Corporate Signing Key, select the **Automatically sign Corporate Key** checkbox. This option causes all keys generated using the PGP Client installer to sign the Corporate Key automatically. If you plan to use a CSK, you can choose from these options:

    - **Designate Corporate Key as a Meta-introducer**. If you select this option, the PGP Client installer will automatically sign the Corporate Key as a *meta-introducer*. All keys validated by the meta-introducer appear as valid on a user's local keyring.

      The Key Generation Wizard notifies users that their new key pair will sign the Corporate Key automatically.

    - **Warn if encrypting to keys not signed by Corporate Key.** If you select this option, users are warned if they encrypt to keys that are not signed by the Corporate Key.

      If your company's policy is to prevent users from encrypting to keys not signed by the Corporate Key, select this option, and then enforce the policy using the Policy Management Agent.

12. Choose the Corporate Key from the **Corporate Signing Key Selection** dialog box, then click **Next**.

Specifying a Designated Revoker

13. If you want assign a designated revoker to keys generated by this install, select the **Enable Designated Revoker Key** checkbox.

    A designated revoker can revoke a user's key at any time. Situations where a revoker key might be useful include those in which the key's owner has lost the private key, forgotten the password, or been terminated.

14. Choose a Designated Revoker Key from the **Designated Revoker Key Selection** dialog box, then click **Next**.

    IMPORTANT: A Designated Revoker Key must be a Diffie-Hellman / DSS key.

X.509 Certificate Settings

15. If your organization uses X.509 certificates, choose settings for the following three options:

    - **Key Generation Performs Certificate Request.** Select this checkbox if you want an X.509 certificate request automatically generated for the user upon creating their PGP key.
    - **Allow Manual Certificate Request.** Select this checkbox to allow users to request X.509 certificates manually.
    - **Automatically Update Certificate Revocation Lists.** Select this checkbox if you want to update the certificate revocation lists (CRLs) automatically.

    Choose the Default Certificate Type for your organization and enter the Certificate Attributes required by your CA (for example, Organization Name and Organizational Unit Name).

Allowing Key Generation

16. If users will generate their own keys, select the **Allow Key Generation** checkbox.

    Normally, PGP users generate their own keys. This allows all users to choose their own passphrase and be responsible for their own keys.

You may optionally choose to disable key generation for users. This means that someone must be responsible for generating all users' keys and handing them out. In a large organization, this sort of operation can be very time consuming.

We discourage administrators from disabling key generation because it forces key generation for a large group of users to occur on one machine, making the machine and its administrator prime targets for attack.

If you allow key generation, you can also select these options:

- **Minimum key size.** You can specify the smallest key that your users are allowed to generate. Larger keys are more secure, but they take longer to generate.
- **Allow RSA key generation.** Selecting this option allows users to generate RSA keys. This is an older style of encryption key that was used in previous versions of PGP. (This option is only available if your version of PGP supports RSA.)

Specify Default Keys

17. Select the keys that you want to include with the PGP Client installer.

    This option lets you choose which keys appear on your users' public keyring when they first use PGP.

    IMPORTANT: If you designated a Corporate Signing Key, Additional Decryption Keys, and / or Designated Revoker Key, you must select them at this time.

Specify Server Updates

18. To schedule automatic key updates for your users, choose from these options:
    - **Automatically update all keys every X days.** Select this checkbox to automatically update users' copy of the key with the copy on the server. Use the text box to specify how often the keys should be updated.
    - **Automatically update all Trusted Introducers every X days.** Select this checkbox to update the list of trusted introducer signatures on users' keyrings with those on the server. Use the text box to specify how often the signatures should be updated.

Miscellaneous Options

19. To allow your users to use conventional encryption and to create self decrypting archives, select the **Allow conventional encryption and Self Decrypting Archives** checkbox.

    If you select this option, your users can use secret-key encryption instead of public-key encryption—that is, information is encrypted to a passphrase, not a person's public key.

    Also, your users can create self-decrypting archives (SDAs). An SDA is an executable file. If you select this option, your users can encrypt using a session key, which encrypts (and decrypts) using a passphrase that they are asked to choose. The resulting executable file can be decrypted by simply double-clicking on it and entering the appropriate passphrase.

    WARNING: Consider this option carefully—it poses a potential security risk, because users must communicate this passphrase to one another, **and** conventional encryption is not recoverable via the Additional Decryption Keys.

    ---

20. To add comments such as a URL or other helpful information that you want all PGP users to read with their PGP messages, enter the text in the **Message Header Comment** field.

    The text of the comment appears under the "BEGIN PGP MESSAGE" header and version number in any message encrypted or signed with PGP. The text of the comment appears read-only to users in PGP's **General Preferences** window.

Options Review

The options you selected are listed for your review. If you chose to include special function keys (Corporate Signing Key, Additional Decryption Keys, and so on), they are listed by name. Review this list to be sure all the options you want are included.

User Options

21. Select the **Copy client options to installer** checkbox to copy the settings from your current PGP Options, or PGP Preferences on Macintosh computers, to the PGP Client installer.

    This is useful for specifying a default certificate server, for example. While users can change these settings, it ensures that all users start using PGP with the Options or Preferences configured in the same manner.

    - To check and / or edit your PGP Options or Preferences, start PGPkeys and select **Options** or **Preferences** from the **Edit** menu.
    - To check and / or edit your PGPnet options, start PGPnet and review the settings on the three **Options** or **Preferences** panels, available from the **View** menu (**General**, **Authentication**, and **Advanced**).

Installation Options (for Windows systems only)

22. Select the **Pre-select installation options for the user** checkbox to specify the installation options and components that you want to include in the PGP Client installer.

    You can pre-select installation options for the PGP Client to use when installing on your users' machines. Pre-selecting these options causes the PGP Client to install without prompting the user for the information (a so-called *silent install*).

    The installation options are:

    - **Directory to install user's copy of PGP.** If you select this option, enter the drive letter and installation path.

      NOTE: Ensure that the drive letter of the file installation path you select is available on your users' systems.

    - **PGP Key Management (required).** This item installs the PGP program. You must install the Key Management utilities.
    - **PGP CommandLine.** Select this option if you want to install the command line version of PGP for Windows NT systems.
    - **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.

- **PGPnet Virtual Private Networking.** Select this option to install the PGPnet program. 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.
- **PGP Eudora Plug-in.** Select this option if you want to integrate PGP functionality with your Qualcomm Eudora email program. PGP version 6.5.1 supports Eudora versions 3.05 and later.
- **PGP Microsoft Exchange/Outlook Plug-in.** Select this option if you want to integrate PGP functionality with your Microsoft Exchange / Outlook email program. PGP version 6.5.1 supports Outlook 97 and 98.
- **PGP Microsoft Outlook Express Plug-in.** Select this option if you want to integrate PGP functionality with your Microsoft Outlook Express email program. PGP version 6.5.1 supports the version that is included with Internet Explorer versions 4.x.
- **PGP User's Manual (Adobe Acrobat format).** Select this option to install the PGP User's Guide.
- **Uninstall old versions of PGP.** Select this option to first run the PGP uninstaller to remove older versions of PGP before installing the new version.

NOTE: The PGP Lotus Notes plug-in is installed separately. For information about the Lotus Notes plug-in, please refer to the LotusNotesReadme.txt file located on your PGP CD.

Create Non-Admin PGP Installer

23. On a Windows computer, enter the path to the original installer or browse to the location. Next, specify the name and directory to which you want to save the PGP Client installer.

    On a Macintosh computer, click **Choose** to browse to the original installer, then click **Next**. Click **Save** and specify the name and directory to which you want to save the PGP Client installer.

Installing and configuring PGPnet on a server or stand-alone system

If you have a server running services and you want users to be able to access those services securely, follow these instructions to install and configure PGPnet on that server.

To install and configure PGPnet on a server

1. Install PGP on the server. When the PGP install wizard displays the component screen, select the PGPnet component. If the server has multiple network adapters, you must identify the network adapter that you want to secure. To communicate securely over a modem, select the server's WAN or dialup adapter. To communicate securely over a LAN, select the server's LAN adapter. Note that you can change the adapter that you secure at any time (use the **Set Adapter** feature, available from the **Start** menu).
2. Generate a key for the server. The key type can be either PGP or an X.509 certificate, depending on whether the users connecting to the server will be using—OpenPGP-compatible IPSEC implementations such as PGPnet, X.509-based implementations.
3. Have a trusted introducer sign the server's certificate and then distribute the certificate.

   TIP: One way you can distribute the certificate is by uploading it to a certificate server.

4. Start PGPnet from the Start menu or system tray. The Add Host/Gateway wizard displays. Click **Cancel**.

   Select **Options** from the **View** menu on the PGPnet main window. Click the **Authentication** tab.

   Select the server's key or certificate. Click **OK**.

   Enter the passphrase for the key. Click **OK**.

5. Select **Options** from the **View** menu on the PGPnet main window. Click the **General** tab.

   Click the **Allow communications with unconfigured hosts** checkbox. This setting lets anyone connect to the server. Do not enable the **Require secure communications with all hosts** checkbox unless all hosts that connect to this server are running an IPSEC product.

6. Create keys for the users who will access the server, and have the keys signed by the same trusted introducer who signed the server's key. Everyone who accesses the server should have all the trusted introducer's keys on their keyring. This eliminates the need to keep each user's key on the server. The key that the remote user uses to authenticate must be considered valid on the server.

   Note that you do not need to add any hosts, gateways, or subnets to your hosts list. As a server, the machine does not initiate connections, therefore you do not need to identify hosts that the server want s to connect to securely.

7. PGPnet is ready for use.

Example

The following example describes how you might configure a Windows NT server with a static IP address, running various services (for example, ftp, web site, and file server). Assume that the installation has no gateway and no IT department.

1. Install PGPnet on the server.
2. Create a key for the server.
3. Have the key signed by a trusted introducer and then distribute the certificate.
4. Start PGPnet. PGPnet displays the Add Host/Gateway wizard. Click **Cancel**.
5. Select **Options** from the **View** menu on PGPnet's main window. Click the **Authentication** tab.

   Select the server's key and click **OK**.

   Enter the key's passphrase, and click **OK**.

6. Select **Options** from the **View** menu on the PGPnet main window.

   Click the **General** tab.

   Click the **Allow communications with unconfigured hosts** checkbox. This setting lets anyone connect to the server.

   If you would like the server to communicate only with users who can authenticate to the server as valid, check the **Require secure communications with all hosts** checkbox as well.

7. Create keys for the users who will access the server, and have the keys signed by the same trusted introducer who signed the server's key.
8. Do not add any entries to PGPnet's hosts list.

In this case, if the server was a mail server, and it received mail that it must forward to another secure mail server outside the installation, you could create an Insecure host entry for the destination mail server. You could also cross-sign certificates using PGPkeys. In general, mail servers are not secure.

9. PGPnet is ready for use.

Installing and configuring PGPnet on a stand-alone system

If you are a mobile user, follow these instructions to install and configure PGPnet.

To install and configure PGPnet on a stand-alone system

1. Install PGP on your machine.

   When the install wizard displays the component screen, select the PGPnet component. If your system has multiple network adapters, identify the network adapter you want to secure. To communicate securely over a modem, select your WAN or dialup adapter. To communicate securely over a LAN, select your LAN adapter. Note that you can use the **Set Adapter** option, available from the **Start** menu, to change the adapter that you secure.

2. Generate a key or certificate.

   What you use for authentication (a PGP key, an X.509 certificate, or a shared secret) depends on the authentication mode of others you want to communicate with. Note that if you are communicating with a server and you intend to use a shared secret for authentication, the server must have a entry for you in its PGPnet hosts list.

3. Start PGPnet.

   On a Windows system, use the Add Host/Gateway wizard to identify the hosts, subnets, and gateways that you want to communicate with securely. If you want to communicate with your company's server, make an entry for that machine as well.

   - A *secure host* is a machine running PGPnet or another IPSEC-compatible peer-to-peer capable client software (that is, software that allows hosts to communicate directly with each other).

- A *secure subnet* is one that has up to 254 machines behind it that are generally running PGPnet or a compatible client software. The secure subnet designation allows you or your administrator to identify a number of machines in the same IP address range that are known to be IPSEC compatible. Note that secure subnets do not have to be behind gateways.

- A *secure gateway* is a firewall or other gateway machine that tunnels packets through it for authorized parties. In this case, authorized means the certificate or shared passphrase of the client software is configured as acceptable on the gateway. (When you use PGPnet, you can elect to communicate with a host using either your PGP certificate or a shared passphrase.)

4. Select **Options** from the **View** menu on PGPnet's main window. Click the **Authentication** tab.

   Select the key or certificate that you will use for authentication and click **OK**.

   Enter the key's passphrase, and click **OK**.

5. Select **Options** from the **View** menu on the PGPnet main window.

   Click the **General** tab.

   To allow communications with unconfigured hosts, enable the **Allow communications with unconfigured hosts** checkbox.

   To communicate only with hosts who can authenticate themselves to you, enable the **Require secure communications with all hosts** checkbox.

6. PGPnet is ready for use.

NOTE: If you install PGPnet and there are no entries in the hosts list and there is no certificate selected on the **Authentication** panel, you cannot communicate securely with anyone. Shared secret is also inoperative, as there are no hosts in the hosts list. You must first set this up within the PGPnet application. Refer to the *PGP Desktop Security User's Guide* for instructions about using PGPnet.

Distributing PGP to Users 8

This chapter describes how you distribute PGP software and keys to users in your organization.

If you created a PGP Client installer as described in Chapter 7, you determined whether your users automatically interact with other keys, such as the Corporate Signing Key or Additional Decryption Keys.

NOTE: You must run the PGPAdmin Wizard to create the client installer before users can install and use PGP software.

Distributing PGP software

After you have installed PGP and used the PGPAdmin Wizard to configure PGP for your users, you can distribute PGP software using the following methods:

- Allow users to download the PGP Client software from a file server.
- Distribute the PGP Client software on disks to users.

If you have not already run the PGPAdmin Wizard, see Chapter 7 for information.

If you need to distribute PGP to many users, the most expedient way is to put PGP software on a file server after you have used the Admin software. Then users can download PGP, generate their own keys, and begin using PGP.

Allowing users to create their keys

The most efficient way to provide your users with keys is to allow them to generate their own keys. Once users have installed the PGP software, they can use the Key Generation Wizard to create their own keys.

Distributing administrator-created PGP keys

If you do not want to allow users to generate their own keys, carefully consider the security implications of your decision. First, the time involved in creating keys for many users is considerable. We strongly discourage disabling key generation because it forces key generation for a large group of users to occur on one machine making that machine or its administrator a prime target for attack. The administrator can keep copies of users' keys, which compromises non-repudiation of signed information, one of the major features of public-key cryptography.

There are several means of distributing keys to users:

- You can call each user into your office individually, go through the key generation procedure, and have him or her choose and enter a passphrase.
- You can generate keys for each user and provide them with a passphrase.

NOTE: If you create a passphrase for each user, you must ensure that you have a secure means of distributing the passphrase to the intended recipient. Do not send the passphrase by email; you could jeopardize your organization's security operation.

Glossary

A5	a trade-secret cryptographic algorithm used in European cellular telephones.
Access control	a method of restricting access to resources, allowing only privileged entities access.
Additional recipient request key	a special key whose presence indicates that all messages encrypted to its associated base key should also be automatically encrypted to it. Sometimes referred to by its marketing term, *additional decryption key.*
AES (Advanced Encryption Standard)	NIST approved standards, usually used for the next 20 - 30 years.
AKEP (Authentication Key Exchange Protocol)	key transport based on symmetric encryption allowing two parties to exchange a shared secret key, secure against passive adversaries.
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.
API (Application Programming Interface)	provides the means to take advantage of software features, allowing dissimilar software products to interact upon one another.

ASN.1 (Abstract Syntax Notation One)	ISO / IEC standard for encoding rules used in ANSI X.509 certificates, two types exist - DER (Distinguished Encoding Rules) and BER (Basic Encoding Rules).
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	to prove genuine by corroboration of the identity of an entity.
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.
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.
Blowfish	a 64-bit block symmetric cipher consisting of key expansion and data encryption. A fast, simple, and compact algorithm in the public domain written by Bruce Schneier.
CA (Certificate Authority)	a trusted third party (TTP) who creates certificates that consist of assertions on various attributes and binds them to an entity and / or to their public key.
CAPI (Crypto API)	Microsoft's crypto API for Windows-based operating systems and applications.
Capstone	an NSA-developed cryptographic chip that implements a US government Key Escrow capability.
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.

CBC (Cipher Block Chaining)
the process of having plain text XORed with the previous cipher text block before it is encrypted, thus adding a feedback mechanism to a block cipher.

CDK (Crypto Developer Kit)
a documented environment, including an API for third parties to write secure applications using a specific vendor's cryptographic library.

CERT (Computer Emergency Response Team)
security clearinghouse that promotes security awareness. CERT provides 24-hour technical assistance for computer and network security incidents. CERT is located at the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, PA.

Certificate (digital certificate)
an electronic document attached to a public key by a trusted third party, which provides proof that the public key belongs to a legitimate owner and has not been compromised.

CFM (Cipher Feedback Mode)
a block cipher that has been implemented as a self-synchronizing stream cipher.

CDSA (Common Data Security Architecture)
Intel Architecture Labs (IAL) developed this framework to address the data security problems inherent to Internet and Intranet for use in Intel and others' Internet products.

Certification
endorsement of information by a trusted entity.

CHAP (Challenge Authentication Protocol)
a session-based, two-way password authentication scheme.

Cipher text
the result of manipulating either characters or bits via substitution, transposition, or both.

Clear text
characters in a human readable form or bits in a machine-readable form (also called *plain text*).

Confidentiality
the act of keeping something private and secret from all but those who are authorized to see it.

Cookie

Persistent Client State HTTP Cookie - a file or token of sorts, that is passed from the web server to the web client (your browser) that is used to identify you and could record personal information such as ID and password, mailing address, credit card number, and other information.

A Corporate Signing Key (CSK)

a key pair used to prove that digital certificates, information, products, and so on have been validated by an authority acting on behalf of the company. The Corporate Signing Key is primarily used for signing, but can also be used for encryption. It is typically held by the Corporate Security Officer alone, or split into multiple shares.

Some examples of uses for a Corporate Signing Key are:

- signing employees' digital certs or keys
- signing softcopies of legal documents
- signing software produced by your company

Because the Corporate Signing Key is used to validate all keys in your organization as well as provide authentication for other data as well, it is vital that this key is never compromised, lest someone else pretend to act in the company's name.

CRAB

a 1024-byte block cipher (similar to MD5), using techniques from a one-way hash function, developed by Burt Kaliski and Matt Robshaw at RSA Laboratories.

Credentials

something that provides a basis for credit or confidence.

CRL (Certificate Revocation List)

an online, up-to-date list of previously issued certificates that are no longer valid.

Cross-certification

two or more organizations or Certificate Authorities that share some level of trust.

Cryptanalysis

the art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

CRYPTOKI

same as PKCS #11.

Cryptography	the art and science of creating messages that have some combination of being private, signed, unmodified with non-repudiation.
Cryptosystem	a system comprised of cryptographic algorithms, all possible plain text, cipher text, and keys.
Data integrity	a method of ensuring information has not been altered by unauthorized or unknown means.
Decryption	the process of turning cipher text back into plain text.
DES (Data Encryption Standard)	a 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for over 20 years, adopted in 1976 as FIPS 46.
Dictionary attack	a calculated brute force attack to reveal a password by trying obvious and logical combinations of words.
Diffie-Hellman	the first public key algorithm, invented in 1976, using discrete logarithms in a finite field.
Digital cash	electronic money that is stored and transferred through a variety of complex protocols.
Direct trust	an establishment of peer-to-peer confidence.
Discrete logarithm	the underlying mathematical problem used in/by asymmetric algorithms, like Diffie-Hellman and Elliptic Curve. It is the inverse problem of modular exponentiation, which is a one-way function.
DMS (Defense Messaging System)	standards designed by the U.S. Department of Defense to provide a secure and reliable enterprise-wide messaging infrastructure for government and military agencies.

DNSSEC (Domain Name System Security Working Group)	a proposed *IETF* draft that will specify enhancements to the DNS protocol to protect the DNS against unauthorized modification of data and against masquerading of data origin. It will add data integrity and authentication capabilities to the DNS via digital signatures.
DSA (Digital Signature Algorithm)	a public key digital signature algorithm proposed by NIST for use in DSS.
Digital signature	an electronic identification of a person or thing created by using a public key algorithm. Intended to verify to a recipient the integrity of data and identity of the sender of the data.
DSS (Digital Signature Standard)	a NIST proposed standard (FIPS) for digital signatures using DSA.
ECC (Elliptic Curve Cryptosystem)	a unique method for creating public key algorithms based on mathematical curves over finite fields or with large prime numbers.
EDI (Electronic Data Interchange)	the direct, standardized computer-to-computer exchange of business documents (purchase orders, invoices, payments, inventory analyses, and others) between your organization and your suppliers and customers.
EES (Escrowed Encryption Standard)	a proposed U.S. government standard for escrowing private keys.
Elgamal scheme	used for both digital signatures and encryption based on discrete logarithms in a finite field; can be used with the DSA function.
Encryption	the process of disguising a message in such a way as to hide its substance.
Entropy	a mathematical measurement of the amount of uncertainty or randomness.
FEAL	a block cipher using 64-bit block and 64-bit key, design by A. Shimizu and S. Miyaguchi at NTT Japan.

Filter

a function, set of functions, or combination of functions that applies some number of transforms to its input set, yielding an output set containing only those members of the input set that satisfy the transform criteria. The selected members may or may not be further transformed in the resultant output set. An example would be a search function that accepts multiple strings having a boolean relationship (`( like` *`a`* `or like` *`b`* `) but not containing` *`c`*), and optionally forces the case of the found strings in the resultant output.

Fingerprint

a unique identifier for a key that is obtained by hashing specific portions of the key data.

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.

GAK (Government Access to Keys)

a method for the government to escrow individual's private key.

Gost

a 64-bit symmetric block cipher using a 256-bit key, developed in the former Soviet Union.

GSS-API (Generic Security Services API)

a high-level security API based upon IETF RFC 1508, which isolates session-oriented application code from implementation details.

Hash function

a one-way hash function - a function that produces a message digest that cannot be reversed to produced the original.

HMAC

a key-dependent one-way hash function specifically intended for use with MAC (Message Authentication Code), and based upon IETF RFC 2104.

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.
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.
IETF (Internet Engineering Task Force)	a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.
Identity certificate	a signed statement that binds a key to the name of an individual and has the intended meaning of delegating authority from that named individual to the public key.
Initialization vector (IV)	a block of arbitrary data that serves as the starting point for a block cipher using a chaining feedback mode (see cipher block chaining).
Integrity	assurance that data is not modified (by unauthorized persons) during storage or transmittal.
IPSec	a TCP / IP layer encryption scheme under consideration within the IETF.
ISA/KMP (Internet Security Association, Key Mgt. Protocol)	defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation, for example, denial of service and replay attacks.
ISO (International Organization for Standardization)	responsible for a wide range of standards, like the OSI model and international relationship with ANSI on X.509.
ITU-T (International Telecommunication Union-Telecommunication)	formally the CCITT (Consultative Committee for International Telegraph and Telephone), a worldwide telecommunications technology standards organization.

Kerberos	a trusted third-party authentication protocol developed at MIT.
Key	a means of gaining or preventing access, possession, or control represented by any one of a large number of values.
Key escrow/recovery	a mechanism that allows a third party to retrieve the cryptographic keys used for data confidentiality, with the ultimate goal of recovery of encrypted data.
Key exchange	a scheme for two or more nodes to transfer a secret session key across an unsecured channel.
Key length	the number of bits representing the key size; the longer the key, the stronger it is.
Key management	the process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic key to authorized recipients in a secure manner.
Key splitting	a process for dividing portions of a single key between multiple parties, none having the ability to reconstruct the whole 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.
Lexical section	a distinct portion of a message that contains a specific class of data, for example, clear-signed data, encrypted data, and key data.
MAA (Message Authenticator Algorithm)	an ISO standard that produces a 32-bit hash, designed for IBM mainframes.
MAC (Message Authentication Code)	a key-dependent one-way hash function, requiring the use of the identical key to verify the hash.
MD2 (Message Digest 2)	128-bit one-way hash function designed by Ron Rivest, dependent on a random permutation of bytes.

MD4 (Message Digest 4)
128-bit one-way hash function designed by Ron Rivest, using a simple set of bit manipulations on 32-bit operands.

MD5 (Message Digest 5)
improved, more complex version of MD4, but still a 128-bit one-way hash function.

Message digest
a number that is derived from a message. Change a single character in the message and the message will have a different message digest.

meta-introducer
A trusted introducer of trusted introducers.

MIC (Message Integrity Check)
originally defined in PEM for authentication using MD2 or MD5. Micalg (message integrity calculation) is used in secure MIME implementations.

MIME (Multipurpose Internet Mail Extensions)
a freely available set of specifications that offers a way to interchange text in languages with different character sets, and multimedia email among many different computer systems that use Internet mail standards.

MMB (Modular Multiplication-based Block)
based on IDEA, Joan Daemen developed this 128-bit key /128-bit block size symmetric algorithm, not used because of its susceptibility to linear cryptanalysis.

MOSS (MIME Object Security Service)
defined in RFC 1848, it facilitates encryption and signature services for MIME, including key management based on asymmetric techniques (not widely used).

MSP (Message Security Protocol)
the military equivalent of PEM, an X.400-compatible application level protocol for securing e-mail, developed by the NSA in late 1980.

MTI
a one-pass key agreement protocol by Matsumoto, Takashima, and Imai that provides mutual key authentication without key confirmation or entity authentication.

NAT (Network Address Translator)

RFC 1631, a router connecting two networks together; one designated as inside, is addressed with either private or obsolete addresses that need to be converted into legal addresses before packets are forwarded onto the other network (designated as outside).

NIST (National Institute for Standards and Technology)

a division of the U.S. Dept. of Commerce that publishes open, interoperability standards called FIPS.

Non-repudiation

preventing the denial of previous commitments or actions.

Oakely

the “Oakley Session Key Exchange” provides a hybrid Diffie-Hellman session key exchange for use within the ISA / KMP framework. Oakley provides the important property of “Perfect Forward Secrecy.”

One-time pad

a large non-repeating set of truly random key letters used for encryption, considered the only perfect encryption scheme, invented by Major J. Mauborgne and G. Vernam in 1917.

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).

Orange Book

the National Computer Security Center book entitled *Department of Defense Trusted Computer Systems Evaluation Criteria* that defines security requirements.

PAP (Password Authentication Protocol)

an authentication protocol that allows PPP peers to authenticate one another, does not prevent unauthorized access but merely identifies the remote end.

Passphrase

an easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

Password

a sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification.

PCT (Private Communication Technology)

a protocol developed by Microsoft and Visa for secure communications on the Internet.

PEM (Privacy Enhanced Mail)

a protocol to provide secure internet mail, (RFC 1421-1424) including services for encryption, authentication, message integrity, and key management. PEM uses ANSI X.509 certificates.

Perfect forward secrecy

a cryptosystem in which the cipher text yields no possible information about the plain text, except possibly the length.

Primitive filter

a function that applies a single transform to its input set, yielding an output set containing only those members of the input set that satisfy the transform criteria. An example would be a search function that accepts only a single string and outputs a list of line numbers where the string was found.

Pretty Good Privacy (PGP)

an application and protocol (RFC 1991) for secure e-mail and file encryption developed by Phil R. Zimmermann. Originally published as Freeware, the source code has always been available for public scrutiny. PGP uses a variety of algorithms, like IDEA, RSA, DSA, MD5, SHA-1 for providing encryption, authentication, message integrity, and key management. PGP is based on the “Web-of-Trust” model and has worldwide deployment.

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.

Plain text (or clear text)

the human readable data or message before it is encrypted.

Pseudo-random number

a number that results from applying randomizing algorithms to input derived from the computing environment, for example, mouse coordinates. See *random number*.

Private key

the privately held "secret" component of an integrated asymmetric key pair, often referred to as the decryption key.

Public key

the publicly available component of an integrated asymmetric key pair often referred to as the encryption key.

RADIUS (Remote Authentication Dial-In User Service)

an IETF protocol (developed by Livingston, Enterprise), for distributed security that secures remote access to networks and network services against unauthorized access. RADIUS consists of two pieces - authentication server code and client protocols.

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.

RC2 (Rivest Cipher 2)

variable key size, 64-bit block symmetric cipher, a trade secret held by RSA, SDI.

RC4 (Rivest Cipher 4)

variable key size stream cipher, once a proprietary algorithm of RSA Data Security, Inc.

RC5 (Rivest Cipher 5)

a block cipher with a variety of arguments, block size, key size, and number of rounds.

RIPE-MD — an algorithm developed for the European Community's RIPE project, designed to resist known cryptanalysis attacks and produce a 128-bit hash value, a variation of MD4.

REDOC — a U.S.-patented block cipher algorithm developed by M. Wood, using a 160-bit key and an 80-bit block.

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).

ROT-13 (Rotation Cipher) — a simple substitution (Caesar) cipher, rotating each 26 letters 13 places.

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.

SAFER (Secure And Fast Encryption Routine) — a non-proprietary block cipher 64-bit key encryption algorithm. It is not patented, is available license free, and was developed by Massey, who also developed IDEA.

Salt — a random string that is concatenated with passwords (or random numbers) before being operated on by a one-way function. This concatenation effectively lengthens and obscures the password, making the cipher text less susceptible to dictionary attacks.

SDSI (Simple Distributed Security Infrastructure)

a new *PKI* proposal from Ronald L. Rivest (MIT), and Butler Lampson (Microsoft). It provides a means of defining groups and issuing group-membership, access-control lists, and security policies. SDSI's design emphasizes linked local name spaces rather than a hierarchical global name space.

SEAL (Software-optimized Encryption ALgorithm)

a fast stream cipher for 32-bit machines designed by Rogaway and Coppersmith.

Secret key

either the “private key” in public key (asymmetric) algorithms or the “session key” in symmetric algorithms.

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.

SEPP (Secure Electronic Payment Protocol)

an open specification for secure bankcard transactions over the Internet. Developed by IBM, Netscape, GTE, Cybercash, and MasterCard.

SESAME (Secure European System for Applications in a Multi-vendor Environment)

European research and development project that extended Kerbros by adding authorization and access services.

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.

SET (Secure Electronic Transaction)

provides for secure exchange of credit card numbers over the Internet.

SHA-1 (Secure Hash Algorithm)

the 1994 revision to SHA, developed by NIST, (FIPS 180-1) used with DSS produces a 160-bit hash, similar to MD4, which is very popular and is widely implemented.

Single sign-on — one log-on provides access to all resources of the network.

SKIP (Simple Key for IP) — simple key-management for Internet protocols, developed by Sun Microsystems, Inc.

Skipjack — the 80-bit key encryption algorithm contained in NSA's Clipper chip.

SKMP (Secure key Management Protocol) — an IBM proposed key-recovery architecture that uses a key encapsulation technique to provide the key and message recovery to a trusted third-party escrow agent.

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.

SNAPI (Secure Network API) — a Netscape driven API for security services that provide ways for resources to be protected against unauthorized users, for communication to be encrypted and authenticated, and for the integrity of information to be verified.

SPKI (Simple Public Key Infrastructure) — an IETF proposed draft standard, (by Ellison, Frantz, and Thomas) public key certificate format, associated signature and other formats, and key acquisition protocol. Recently merged with Ron Rivest's SDSI proposal.

SSH (Secure Shell) — an IETF proposed protocol for securing the transport layer by providing encryption, cryptographic host authentication, and integrity protection.

SSH (Site Security Handbook)

the Working Group (WG) of the Internet Engineering Task Force has been working since 1994 to produce a pair of documents designed to educate the Internet community in the area of security. The first document is a complete reworking of RFC 1244, and is targeted at system and network administrators, as well as decision makers (middle management).

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.

SST (Secure Transaction Technology)

a secure payment protocol developed by Microsoft and Visa as a companion to the PCT protocol.

Stream cipher

a class of symmetric key encryption where transformation can be changed for each symbol of plain text being encrypted, useful for equipment with little memory to buffer data.

STU-III (Secure Telephone Unit)

NSA designed telephone for secure voice and low-speed data communications for use by the U.S. Dept. of Defense and their contractors.

Substitution cipher

the characters of the plain text are substituted with other characters to form the cipher text.

S/WAN (Secure Wide Area Network)

RSA Data Security, Inc. driven specifications for implementing IPSec to ensure interoperability among firewall and TCP/IP products. S/WAN's goal is to use IPSec to allow companies to mix-and-match firewall and TCP/IP stack products to build Internet-based Virtual Private Networks (VPNs).

Symmetric algorithm

a.k.a., conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another. Two sub-categories exist - Block and Stream.

TACACS+ (Terminal Access Controller Access Control System)	a protocol that provides remote access authentication, authorization, and related accounting and logging services, used by Cisco Systems.
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.
Transposition cipher	the plain text remains the same but the order of the characters is transposed.
Triple DES	an encryption configuration in which the DES algorithm is used three times with three different keys.
Trust	a firm belief or confidence in the honesty, integrity, justice, and / or reliability of a person, company, or other entity.
TTP (Trust Third-Party)	a responsible party in which all participants involved agree upon in advance, to provide a service or function, such as certification, by binding a public key to an entity, time-stamping, or key-escrow.
UEPS (Universal Electronic Payment System)	a smart-card (secure debit card) -based banking application developed for South Africa where poor telephones make on-line verification impossible.
Validation	a means to provide timeliness of authorization to use or manipulate information or resources.
Verification	to authenticate, confirm, or establish accuracy.
VPN (Virtual Private Network)	allows private networks to span from the end-user, across a public network (Internet) directly to the Home Gateway of choice, such as your company's Intranet.

WAKE (Word Auto Key Encryption)	produces a stream of 32-bit words, which can be XORed with plain text stream to produce cipher text, invented by David Wheeler.
Web of Trust	a distributed trust model used by PGP to validate the ownership of a public key where the level of trust is cumulative based on the individual's knowledge of the "introducers."
W3C (World Wide Web Consortium)	an international industry consortium founded in 1994 to develop common protocols for the evolution of the World Wide Web.
XOR	exclusive-or operation; a mathematical way to represent differences.
X.509	an ITU-T digital certificate that is a 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 in version 3.
X9.17	an ANSI specification that details the methodology for generating random and pseudo-random numbers.

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W