Installing PGP

Run PGP Installer

To install PGP you must have installed and run The Secure Mail System at least once on your system. If you do not have PGP, you can obtain it from the World Wide Web at : http://web.mit.edu/network/pgp.html.

NOTE: **Only the DOS versions of PGP are compatible with The Secure Mail System! PGP 5.0 will not function with The Secure Mail System and can not be installed with the PGP Installer. PGP 5.0 will be available for The Secure Mail System in the near future.**

Once you have the latest version of PGP, (2.62 as of this writing) you can easily install it by using The Secure Mail System's PGP Install Program. Follow the easy step by step installation procedures of the install program and you will be up and running in no time.

Be sure you completely setup PGP, if you fail to do so, you will not be able to access any PGP function except for PGP Setup.

The following topics will help you through the PGP setup procedure:

User Information Setup
Key Ring Information
PGP Options

PGP User Information

The information in this area is passed to PGP and must be correct. If you make a mistake, The Secure Mail System can not access the data in your PGP Key Rings.

E-Mail Address:

This is your address that all your e-mail is being sent to. This information is used when you use the public key server.

PGP User ID:

This is the User ID you will enter when you generate a Secret Key. This should be the same as the first name or characters that you put into your public key.

Pass Phrase:

This is your Pass Phrase required to access your Secret Key. If you enter your Pass Phrase here, be sure you enter it correctly. If you leave this area blank, you will be asked what your pass phrase is when needed. This is the same pass phrase that you use for your public key. This is used be The Secure Mail System to automatically enter in your pass phrase when PGP asks for it.

Your Time Zone:

You must select your Time Zone from the drop down list. This is to insure that the correct time stamp is placed on the encryption.
NOTE: You must restart your computer before the changes take effect.

PGP Path:

This is the path where the PGP.Exe file is located. This will be \PGP if you used the PGP Install program that comes with The Secure Mail System. Use the Browse Button to select the correct directory. The path is where The Secure Mail System looks to run PGP, so wherever PGP is residing permanently on your system is the path, for example C:\raft\banjos\PGP. the previous would be the path.

Related Topics:

PGP Key Ring Information
PGP Options
PGP Installation

Key Ring Path Information

The Secure Mail System needs to know where your key rings are. The Secure Mail System will know the path to these key rings at setup if you used the PGP Install Program that is provided with The Secure Mail System, so don't change the names or paths unless you are a advanced user of PGP.

Secret Ring:

What you put here is where (the path)The Secure Mail System looks for your Secret Key Ring. Your secret ring is what holds the important information such as pass phrase and such that allow you to encode and decode messages. It is encrypted and only PGP can read it. You may want to keep your secret key ring in a directory separate from your PGP directory specified by your PGP Path below. This comes in handy for putting your secret key ring in a directory or device that is more protected than your public key ring. You may specify the full path and filename for your secret key ring by setting the SECRING parameter in PGP setup on the main menu. At setup The Secure Mail System will set this up for you in the PGP directory, so you do not need to change anything. For those truly security conscious, one can carry the Secret Ring(SECRING) on a floppy disk around their necks, only to be used when running The Secure Mail System. In such a case the path for the SECRING would be something like A:\secring.pgp. Read the PGP DOC 1and 2 to get a thorough understanding of keys, vulnerabilities ect. Suffice to say. those that wish to compromise your e-mail can do it easier with a both a public and secret key in hand then with just either. Keep your computer, pass phrase, and secret ring secure and you should thwart all but the most sophisticated of hackers.

Public Ring:

What is entered here is where (the path)The Secure Mail System finds the public keyring that holds the public keys. A public key is what you give other people to encrypt messages to you and visa versa. Other people have public keys that they give to you so that you can encrypt messages to them.

Backup Ring:

All of the key certification that PGP does on your public key ring ultimately depends on your own ultimately-trusted public key (or keys). To detect any tampering of your public key ring, PGP must check that your own key has not been tampered with. To do this, PGP must compare your public key against a backup copy of your secret key on some tamper-resistant media, such as a write-protected floppy disk. A secret key contains all the information that your public key has, plus some secret components. This means PGP can check your public key against a backup copy of your secret key. The Backup Ring configuration parameter specifies what path name to use for PGP's trusted backup copy of your secret key ring. You could set it to "a:\secring.pgp" to point it at a write-protected
backup copy of your secret key ring on your floppy drive. This check is performed only when you select check your whole public key ring from the PGP Menu. If your Backup Ring not defined or found, PGP will not check your own key against any backup copy.

Public Key Server:

This is the name of the public key server where you can send request for public keys or post your public key to for others to retrieve. Then names of the most common public key servers are listed. Pick one as a default and when you go to retrieve or

send a public key this place will be the one emailed.

SMTP Server:

Server: This is the address to the server that you will be sending your mail to. You must obtain this address from your service provider. Address example: smtp.win.net

Port: This is the address that is used by your service provider to distinguish what type of service you are requesting. (don't worry about it) Your service provider will let you know if default number of 25 will be acceptable or not.

Network To Dial:

If you are using an Alternate Provider you must select the network from the drop down list you would like to connect to. If the list is empty, you have not setup Dialup Networking for your Service Provider. The Secure Mail System uses your Dialup networking to make the phone call and hook up to your Internet e-mail provider.

Other Related Topics:

PGP User Information
PGP Options
PGP Installation

PGP Options

This area is used to setup how PGP should handle your files and messages. Do not change the Advanced Option unless you have a thorough understanding on how PGP function. You can read the on-line documentation of PGP for more information on the exact functions.

Default Signatures:

A signature is a PGP file that accompanies your e-mail for the express purpose of validating who the sender is and the information for tampering. This is the area used to select what type of default Signature when you Sign & Send a message. The following is the definition of each type of signature.

Attached Signature:

Attaches a coded PGP signature to the end of the e-mail text body.

Detached Signature:

Creates a file attachment that is your coded PGP signature.

Default Encryption:

This is where you can select the default encryption when you select Encrypt and Send Message. It is strongly suggested that you leave the default setting at Sign & Encrypt as it gives you the best security. Following is a description of what each type does.

Sign & Encrypt:

Signs your e-mail message with the coded PGP signature, then encrypts it. Keep in mind that if you chose a detached or attached signature it will still add a PGP signature.

Encrypt Only:

Encrypts only and does not add a PGP signature any which way.

Advanced Options:

Only changes these settings if you have familiarized your self with all PGP function. You can do this by reading the on-line PGP help manual.

Character Set:

For PGP users that use non-English 8-bit character sets, when PGP converts text to canonical form, it may convert data from the local character set into the LATIN1 (ISO 8859-1 Latin Alphabet 1) character set, depending on the setting of the Character Set Option. LATIN1 is a superset of ASCII, with extra characters added for many European languages.

Marginals Needed:

The Marginals Needed parameter specifies the minimum number of marginally trusted introducers required to fully certify a public key on your public key ring. This gives you a way of tuning PGP's skepticism.

Completes Needed:

The Completes Needed parameter specifies the minimum number of completely trusted introducers required to fully certify a public key on your public key ring. This gives you a way of tuning PGP's skepticism.

Cert. Depth:

The Cert. Depth configuration parameter specifies how many levels deep you

may nest introducers to certify other introducers to certify public keys on your public key ring. For example, If Cert Depth is set to 1, there may only be one layer of introducers below your own ultimately-trusted key. If that were the case, you would be required to directly certify the public keys of all trusted introducers on
your key ring. If you set Cert Depth to 0, you could have no introducers at all, and you would have to directly certify each and every key on your public key ring in order to use it. The minimum Cert Depth is 0, the maximum is 8.

Keep Binary Files:

When PGP reads a cipher file, it recognizes that the file is in radix-64 format and will convert it back to binary before processing as it normally does, producing as a by-product a PGP cipher text file in binary form. After further processing to decrypt the ".pgp" file, the final output file will be in normal plain text form. You may want to delete the binary ".pgp" intermediate file, or you may want PGP to delete it for you automatically. You can still rerun PGP on the original ".asc" file.
The Keep Binary File configuration parameter enables or disables keeping the intermediate ".pgp" file during decryption.

Use Armor:

The Use Armor configuration parameter, if enabled, it causes PGP to emit cipher text or keys in ASCII Radix-64 format suitable for transporting through E-mail
channels. If you intend to use PGP primarily for E-mail purposes, you should turn ARMOR=ON. When not encrypting an e-mail message you can still use armor as a low tech means of encryption, this will work for those that have The Secure Mail System. Armor=ON will render the text unreadable and the user on the other end will have to decrypt to be able to read the armored message.

Use Compression:

The Use Compression configuration parameter enables or disables data compression before encryption. It is used mainly for debugging PGP. Normally, PGP attempts to compress the plain text before it encrypts it. Generally, you should leave this alone and let PGP attempt to compress the plain text. Using compression also helps make the encrypted text tougher to decrypt, making your information more secure.

Other Related Topics:

PGP User Information
PGP Key Ring Information
PGP Installation

PGP Key Management Overview

Since the time of Julius Caesar, key management has always been the hardest part of cryptography. One of the principal distinguishing features of PGP is its sophisticated key management. Key management is an important part of being able to use PGP correctly. The Secure Mail System has made this task as easy as possible. All the key management options are located on the Main Menu Bar under PGP Key Man.. This menu will only become available after PGP has been installed. Until you have generated your keys, Generate Keys will be your only option. The following menu items and sub menu items can be found in the PGP Key Man Menu.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Removing Keys
Viewing Keys
Certifying Keys
Backup Key
Key Servers
Generating New Keys

Adding Keys

The Adding Keys menu item allows you to easily add PGP Keys to your public key ring. You can add a Secret Key or a Public Key. Click on the type of key you wish to add, Public or Secret. Using the Add Key Dialog Box, Select the key file you wish to add. Adding a key may show a DOS window as verification of the key may need to be done.

Editing Keys
Extracting Keys
Removing Keys
Viewing Keys
Certifying Keys
Backup Key
Key Servers
Generating New Keys

Editing PGP Keys

You can edit your Secret Key's ID and Pass Phrase or Edit a Public Keys trust parameters. Click on Public Trust Param from the menu. Select the User ID you wish to edit. If you select your own key, you will be able to edit your ID and Pass Phrase. A DOS window will appear allowing you to edit the key you have selected.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Removing Keys
Viewing Keys
Certifying Keys
Backup Key
Key Servers
Generating New Keys

Extracting PGP Keys

This option allows you to extract (Copy) a Secret Or Public Key. Click on the type of key you wish to extract. Select the key you wish to extract from the list of User Id's. When the Save Key Dialog Box appears, select the location and name you wish to save the key as.

Related Topics:

Adding Keys
Editing Keys
Removing Keys
Viewing Keys
Backup Key
Certifying Keys
Key Servers
Generating New Keys

Removing PGP Keys

This option allows you to remove a Secret or Public key, Signature, or Revoke your key. The following four sub-menu option are available.

Key:

Selecting this option will allow you to remove the selected Secret or Public Key from your Ring. ***NOTE:*** Avoid this option unless you are removing extra keys from your Key Ring. If you remove your ONLY a Secret Key and you do not have a backup, you will loose the ability to decrypt your incoming mail.

Signature:

Selecting this option will display a list of Public Keys you have available, choos the key you wish to remove your signature from.

Revoke Your Key:

Use this option to generate a key revocation certificate. This is useful if your key or pass phrase somehow got compromised and you need to get the word out to the rest of the world and have the stop using your Public Key. This certificate bears your signature, made with the same keys you are revoking. You should widely disseminate this key revocation certificate as soon as possible. Other people who receive it can add it to their public key rings and their PGP software then automatically prevents them from accidentally using your old key ever again.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Viewing Keys
Certifying Keys
Backup Key
Key Servers
Generating New Keys

Viewing PGP Keys

This menu option allows you to view the information that is contained in your Public or Secret Key Ring. The following sub-menu items are available.

Public Key:

This will display a list of public keys you have available in your public key ring. Choose the key you wish to view. Select the key you wish to view the information on and a Key Information Dialog Box will appear. This dialog box shows the Key ID and the Bit size, how trusted the key is, when it was created and who signed it.

Finger Print:

The option will display a list of public keys you have available in your Public Key Ring. Select the key you wish to view the finger print for. This will display the Key Finger Print Dialog Box. The information that is displayed can be used to verify that you have the correct Public Key over the phone.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Removing Keys
Certifying Keys
Backup Key
Key Servers
Generating New Keys

Certifying PGP Keys

This option allows you to certify a public key. This means that you are verifying that selected key does infact belong to the that person. Select the key you wish to certify. This will drop you to a DOS window. Follow the instructions on the screen to complete the certification. If you have already signed the selected key, you will here a beep and the operation is canceled.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Removing Keys
Viewing Keys
Backup Key
Key Servers
Generating New Keys

Backup PGP Key

This allows you to copy (Backup) your secret key ring. You can also verify all your keys with your backup. To use this option you must have selected a destination to backup your key to in the PGP Configuration under the Key Ring Information Tab. Verifying your key will show a complete list of your public keys and there trust. This is to make sure that no one has tampered with you public key ring.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Removing Keys
Viewing Keys
Certifying Keys
Key Servers
Generating New Keys

Public Key Servers

There are PGP public key servers which allow you to exchange public keys through the Internet. Sending your key to ONE server is enough. After the key server process your key, it will forward your key add request to the rest. The following option are available from this menu.

Add your Key:
This will send a message to the key server you have selected in the in the PGP Configuration under the Key Ring Information Tab with instruction to add/update your public key.

Index Matched User ID's:
This option will retrieve a list of users that match the partial ID you have selected. e.g. If you select Steve, you will receive a list of user id's that contain the word Steve.

Get Users On Server:
This gets a list of all users on the server. This function may not work on all servers.

Get All Public Keys:
This will retrieve the entire public key ring from the server. This function may not work with all servers.

Get Users Key:
This will retrieve a single public key from the key server.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Removing Keys
Viewing Keys
Certifying Keys
Backup Key
Key Servers
Generating New Keys

Generating Keys

If you changed your key ring and they do not exist, you must generate a new key ring set. You may have more then one secret key but you ***MUST*** use the same Pass Phrase that you specified in your PGP Configuration. Select this option and follow the easy instruction.

Related Topics:

Adding Keys
Editing Keys
Extracting Keys
Removing Keys
Viewing Keys
Certifying Keys
Backup Key
Key Servers

Key Manager Icons

The Icon Bar contains quick access to commonly used function. The Icons that can be found on the Icon Bar are listed below from left to right.

Key Details:

The Key Details button will display detailed information about the selected key. This includes trust and users who have signed this key.

Key Fingerprint:

This will display the Key Finger Print Dialog Box for the selected key. The information that is displayed can be used to verify that you have the correct Public Key over the phone.

Certify Public Key:

This option allows you to certify a public key. This means that you are verifying that selected key does infact belong to the that person. Select the key you wish to certify. This will drop you to a DOS window. Follow the instructions on the screen to complete the certification. If you have already signed the selected key, you will here a beep and the operation is canceled.

Add Key:

The Adding Keys menu item allows you to easily add PGP Keys to your public key ring. You can add a Secret Key or a Public Key. Click on the type of key you wish to add, Public or Secret. Using the Add Key Dialog Box, Select the key file you wish to add. Adding a key may show a DOS window as verification of the key may need to be done.

Remove Key:

See Removing PGP Keys for more information on this topic.

Key Viewer

The key viewer displays information on your Public and Secret keys. The yellow keys are Secret Keys and the blue keys are Public Keys.

If you double click a public key, the detail information can be viewed.