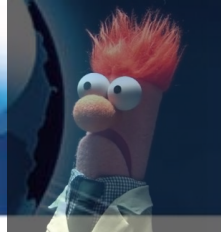
Exchanging Files with PGP



PGP by the PGP Corporation offers public key file encryption according to the RFC 4880 (Open PGP) standard using NIST standard algorithms, including AES-256, Diffie-Hellman/ DSS, and SHA-512. NSA has completed an evaluation of file encryption with PGP desktop version 9.6 and has the following recommendations for use.

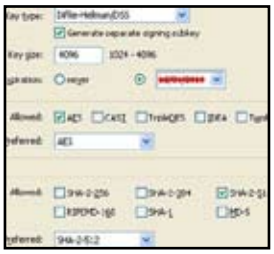
This guide provides guidance for sending encrypted files via e-mail and protecting them in transit. It is NOT appropriate to use these steps to protect data at rest. The steps described below are written for a computer using a Windows XP operating system although for other operating systems, the steps would be very similar. Note that the location of PGP Desktop in the start menu may be different from one installation of PGP to another.

1. Creating a Public/Private Key Pair

To enable the encryption of files between two users, both users must first generate a public/private key pair and exchange public keys with each other. To generate a key pair, use the PGP Key Generation Assistant. Follow these steps:

1. Start PGP Desktop (if it is not already started) by clicking **Start->All Programs->PGP->PGP Desktop.**

2. Select the **PGP Keys** tab on the left side of the window.
3. Select **File->New PGP Key**.
4. *PGP Key Generation Assistant:* Leave the **Generate Key on Token** box unchecked (it will most likely be grayed out anyway) and click **Next**.
5. *Name and E-mail Assignment*: Enter your name and an optional e-mail address. Click **Advanced**.
6. *Advanced Key Settings*: Select the following NSA recommended settings.
   - Key type: Diffie-Hellman/DSS
   - Generate separate signing subkey: Check this box
   - Key size: 4096
   - Expiration: Choose an expiration date of one year from the date of creation.
   - Ciphers: Check only AES
   - Hashes: Check only SHA-2-512



7. Click **OK**, then click **Next.**
8. *Passphrase Assignment*: Choose a strong passphrase and enter that same passphrase into both the Passphrase and Confirmation fields. Consult your organization's policy for appropriate passphrase strength. (NSA recommends at least 8 characters including upper-and lower-case letters, numbers, and symbols.) Click **Next**.
9. *Key Generation Progress*: Click **Next**.
10. *Completing the PGP Key Generation Assistant*: Click **Done**.
11. You should see the new key pair listed under **All Keys**.

2. Distributing Your Public Key

Next, you'll need to exchange public keys with anyone with whom you would like to exchange encrypted files. To send your key to someone, you can simply export your key to a file and include the file in an e-mail as follows:

1. Start PGP Desktop (if it is not already started) by clicking **Start->All Programs->PGP->PGP Desktop.**
2. On the left side of the application, click the **PGP Keys** tab.
3. Select your name from the keys listed under **All Keys**. (If the name is expanded and you see the name several times, choose the name at the top.)
4. Click **File->Export->Key**. Using the dialog, save the file to the desktop. This will result in the creation of a file containing your public key. Note: this file does not contain the private key, as only you are allowed access to your private key.
5. Compose an e-mail with your mail client and include this new file as an attachment. Address the e-mail to the person with whom you want to be able to exchange encrypted files.
6. Send the e-mail.
7. Delete the key file from your desktop.

3. Receiving a Public Key

In order for you to be able to send encrypted files to other users, they must send you their public key using the steps in Section 2. Once you have received their key, you must add that key to your collection. To do so, use the following steps:

1. Start PGP Desktop (if it is not already started) by clicking **Start->All Programs->PGP->PGP Desktop**.
2. Save the attached public key file to your desktop using your mail client.
3. Drag and drop the key file onto PGP Desktop.
4. Click **Import**.
5. Section 4 describes how to verify the sender's public key.

Exchanging Files with PGP
(continued)

4. Verifying a Public Key

When public keys are exchanged, it is important for the recipient of each key to verify that the key belongs to the sender. To do this, both the recipient and the sender should do the following:

1. Start PGP Desktop (if it is not already started) by clicking **Start->All Programs->PGP->PGP Desktop.**
2. Select the **PGP Keys** tab on the left side of the window.
3. Click on the name of the person that needs to be verified. (If the name is expanded and you see the name several times, choose the name at the top.)

4. Select **Keys->Key Properties** from the menu bar at the top of PGP Desktop.
5. If necessary, expand the section labeled **Fingerprint**.
6. In the **Fingerprint** section, select the **Biomeric** tab.
7. Have either the sender or the receiver read the 20 words aloud over the phone to ensure that the keys match. If they match, the key in question is verified. The biometric data should be checked for each key that is exchanged.

Assuming the words match, the user who received the public key should now mark the public key as valid by signing it. Do this using the following steps:

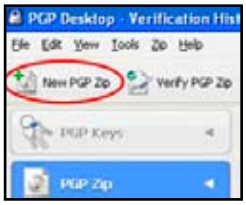
1. Close the key properties window.
2. In the PGP Desktop main window, click on the name of the person who sent the key. (If the name is expanded and you see the name several times, choose the name at the top.)
3. Select **Keys->Sign** from the menu bar at the top of PGP Desktop.
4. *PGP Sign Key*: Click **OK**.
5. *PGP Enter Passphrase for Selected Key*: Select your name from the drop-down menu. Enter your passphrase. Click **OK**. (Note: the passphrase may have been cached, in which case it does not need to be entered.)
6. The sender's public key should now have a green check mark next to it indicating that it is verified and trusted.

5. Sending an Encrypted File

Now that you have a key pair and some public keys of other users, you can encrypt files to send to those users. You can also sign the files so that others will know that the files were sent by you.

To do so, follow these steps:

1. Start PGP Desktop (if it is not already started) by clicking **Start->All Programs->PGP->PGP Desktop.**
2. Click the **New PGP Zip** button.



3. *New PGP Zip*: Drag and drop the file(s) to be encrypted into the box. Click **Next**.
4. *Encrypt:* Select **Recipient Keys**. Click **Next**.
5. *Add User Keys*: Choose the recipient username from the drop-down list. Click **Add**. Repeat if there are multiple recipients. Then click **Next**.
6. *Sign and Save*: Choose your name from the drop-down list. Enter your passphrase. (Note: the passphrase may have been cached, in which case it does not need to be entered.) Choose a place to save the encrypted file. Click **Next.** You will receive a message saying that your PGP Zip is secured.
7. *Finished*: Click **Finish**.
8. You should see a new PGP-encrypted version of the file in the location you chose. The original, unencrypted file will also still be there.
9. Attach the encrypted file to an e-mail using your mail client and send to the appropriate recipient(s).

6. Receiving an Encrypted File

When a user sends you an encrypted file, use the following steps to decrypt it and verify the identity of the sender:

1. Start PGP Desktop (if it is not already started) by clicking **Start->All Programs->PGP->PGP Desktop.**
2. Save the attached PGP Zip file to your desktop using your mail client.
3. In PGP Desktop, select **File->Open**.
4. Using the file dialog, select the file from the desktop and click **Open**.
5. The decrypted file should now be visible in the main PGP Desktop window. Note the **Status** section. Make sure that the file is not marked "invalid." If it is, the file may not have been sent by the person you think.
6. To save a copy of the decrypted file, right click the file, select **Extract** and choose a folder or location to extract the file to.

Systems and Network Analysis Center (SNAC)
410-854-6632
www.nsa.gov/snac *snac@radium.ncsc.mil*