PGP

**Decrypting:** The process of taking encrypted (scrambled) data and making it meaningful again. When you receive data that has been encrypted by someone using your public key, you use your private key to decrypt the data.

**Encrypting:** The process of scrambling data so that if an unauthorized person gets access to it, they cannot do anything with it. The data is so scrambled, it’s meaningless.

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

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

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

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

Caution: Do not give your private key, or its passphrase, to anyone! And keep your private key safe. **Public key:** The key you distribute to others so that they can send protected messages to you (messages that can only be decrypted by your private key) and so they can verify your digital signature. Public keys are meant to be widely distributed. Your public and private keys are mathematically related, but there’s no way to figure out your private key if someone has your public key.

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

**Smart cards and tokens:** Smart cards and tokens are portable devices on which you can create your PGP keypair or copy your PGP keypair. Creating your PGP keypair on a smart card or token adds security by requiring possession of the smart card or token in order to encrypt, sign, decrypt, or verify. So even if an unauthorized person gains access to your computer, your encrypted data is secure because your PGP keypair is with you on your smart card or token. Copying your PGP keypair to a smart card or token is a good way to use it away from your main system, back it up, and distribute your public key. Smart cards and tokens are not available for key storage when used with PGP Desktop for Mac OS X.

Conventional and Public Key Cryptography

**Conventional cryptography** uses the same passphrase to encrypt and decrypt data. Conventional cryptography is great for data that isn’t going anywhere (because it encrypts and decrypts quickly). However, conventional cryptography is not as well suited for situations where you need to send encrypted data to someone else, especially if you want to send encrypted data to someone you have never met.

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

Public-key cryptography works this way: let’s say you and your cousin in another city want to exchange private messages. Both of you have PGP Desktop. First, you both need to create your keypair: one private key and one public key. Your private key you keep secret, your public key you send to a public keyserver like the PGP Global Directory (keyserver.pgp.com), which is a public facility for distributing public keys. (Some companies have their own private keyservers.)

Viewing Keys

To view the keys on the local keyring, open PGP Desktop and click on the PGP Keys Control box**.** Then click:

**All Keys**. Shows all PGP keys on your keyrings.

**My Private Keys**. Shows only the private keys on your keyrings.

**Search for Keys**. Lets you search for keys on your keyrings based on criteria you specify.

**Smart Card Keys**. If you have a smart card on your system, you also have this option.

Some of the more common tasks you may want to perform are available from the PGP Keys Control box or work area. These are:

If a public key is selected in any view of the PGP Keys on your keyrings, the option to **Email this Recipient** is available in the PGP Keys Control box

If you perform a search, and you select a public key found in the search that is not on your local keyrings, the option **Add to my Keyring** is available in the PGP Keys Control box.

To see the properties of any key displayed in the work area, just double-click any part of the key listing to display the Key Properties dialog box for that key.

When you perform a search, the option **Save this Key Search** is available in the PGP Keys Control box, so you can save the results for later access.

To create a PGP keypair

1 Make sure the PGP Keys Control box is selected.

2 Select **File > New PGP Key** or press Ctrl+N. The first screen of the PGP Key Generation Assistant is displayed.

3 Read the information on this screen.

4 If you want to generate your new PGP keypair on a token or smart card, make sure the token or smart card is connected to the system and then select the box labeled **Generate Key on Token: [name of smart card or token on system]**. For more information about smart cards and tokens, see *Storing Keys on Smart Cards and Tokens* (on page 245).

5 Click **Next**. The Name and Email Assignment screen is displayed.

6 Type your real name in the **Full Name** field and your correct email address in the **Primary Email** field. It is not absolutely necessary to type your real name or even your email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, when you upload your public key to the PGP Global Directory (which makes it easily available to other PGP Desktop users), your real email address is required.

7 If you would like to add more email addresses to the key you are creating, click **More** and type them in the fields that appear.

8 To specify advanced settings for the key you are creating, click **Advanced**. The Advanced Key Settings dialog box is displayed. Use this dialog box to specify the key type and size, expiration, and other settings.