The following document provides a series of notes and examples which are designed to help the PGP novice user to properly maintain and care for public keys in a secure environment using the PGP utility software.

Item No.	Activity	Operative Command	Results/Disposition
1	Install System		Set DOS PATH command in AUTOEXEC.BAT so that DOS always find PGP; Set the DOS ENV variable TZ=-3 (EST). Set the DOS Env. Variable PGPPAT to the drive and sub-directory where you have your keyrings. This will make PGP available all the time.
2	REBOOT	Ctrl-Alt-Del	Required to make DOS Changes (Item 1) work.
3	Generate Secret Key	PGP -kg	System will create public and private keyrings in subdirectory specified by PGPPATH as specified in (1)
4	Create Public Key	PGP -kxa <user id> <keyfile>	This command will extract a "Public Key" from your keyring and put it in <keyfile>. Specify the <user id> to be extracted. To get ready to send out you public key: give your own user id. Save <keyfile>.

5Note: At this point you can send a message to someone and include your Public Key. After you have done that, then THEY will be able to send you a PGP crypted message.

::

6 Received Message containing Public Key for a remote correspondent.	Ah Ha!	Save this message. You will need to process this using PGP, shortly.
7 Add Public Key(s) to your keyring	PGP <filename>	PGP will add any key(s) found in <filename> to your Keyring
	New Key, without authenticating signature(s)	PGP will ask if you want to Authenticate these keys. You would only do this if you have personnally received the key directly from a trusted person.
	New Key, with Known Authenticating Signatures	?? Does PGP Authenticate the ke
	New Key, with a bad signature	??
	New key with 1 good and 1 bad signature	??
	Existing key, with no signature	PGP will check the new key to be sure it matches the old key
	New key matches existing key	No action
	New key not same as old key	??

can

'H

ey