

PGP can encrypt and sign e-mails and documents.

If you run Windows it is recommended that you try both the 'commercial' implementation from pgp.com and the open source GnuPG

1a) install Seamonkey and/or Thunderbird mail client from www.mozilla.org Install the enigmail plugin - see enigmail.mozdev.org – you will also have to install GnuPG – see www.gnupg.org - You may also want to install GnuPG for Windows (www.gpg4win.org)

1b) generate a pair of keys (public and private)

1c) write an e-mail, encrypt and sign it and send it to yourself.

1d) receive an encrypted and signed e-mail from yourself and decrypt and verify the signature

1e) export your public key to a PGP server (can be tricky)

1f) import a friend's public key from a PGP server (can be tricky) 1g) send and receive e-mails to / from him (your friend from 1f)

- you can also export and send your public key to your friend by mail 1h) try to sign the keys from other PGP users you know

1j) look in PGP intro to crypto document (installed with the commercial PGP)

S/MIME

Seamonkey, Thunderbird and Outlook Express includes S/MIME features to encrypt and sign e-mails

Get an e-mail X509 certificate from one of the following sources

- http://www.globalsign.com/digital_certificate/personalsign/index.htm#1 30 day Demo ! – use this first ! – *They now require a lot of personal info so you may want to use these*
- <http://www.comodo.com/home/internet-security/free-email-certificate.php>
- <http://www.thawte.com/secure-email/personal-email-certificates/index.html?click=main-nav-products-email> free
- www.cacert.org free – recommended

2a) Use one of these applications to send and receive encrypted and signed emails - both to yourself and some friends.

2b) have a close look on the format of some of the S/MIME e-mails - that is all the S/MIME headers, the encrypted part and the signature part.

You can also try the commercial version of PGP for Windows For windows XP you will have to register and download the trial Version of PGP Desktop

(<http://www.pgp.com/downloads/desktoptrial/index.html>) – It will retain functionality comparable to the previous freeware version.

When installing DO NOT register or enter your serial number unless you have read and understands the documentation – doing so might mess up your e-mail settings. – Also do not let the program detect your e-mail accounts automatically.

Installing without entering the key will still give you basic functionality.

– Linux users can use GNU PG with a nice graphical frontend KGpg Hint! read PGP user's guide

PS PGP will also work with mail systems with WEB-interfaces