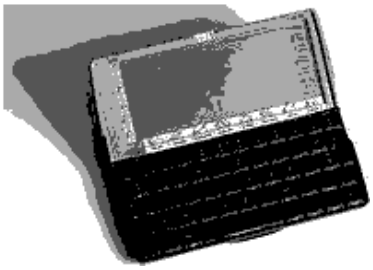


# PSION Program

# REVIEW

Paper No 2 Date 23rd November 2009

AS WITH ALL ENCRYPTION SOFTWARE IF YOU LOSE YOUR KEYS OR YOUR PASSWORDS YOUR DATA IS NOT RECOVERABLE. USE AT YOUR OWN RISK.

PGP (Pretty Good Privacy) is a program originally written by Phil Zimmerman for encrypting and digitally signing data.

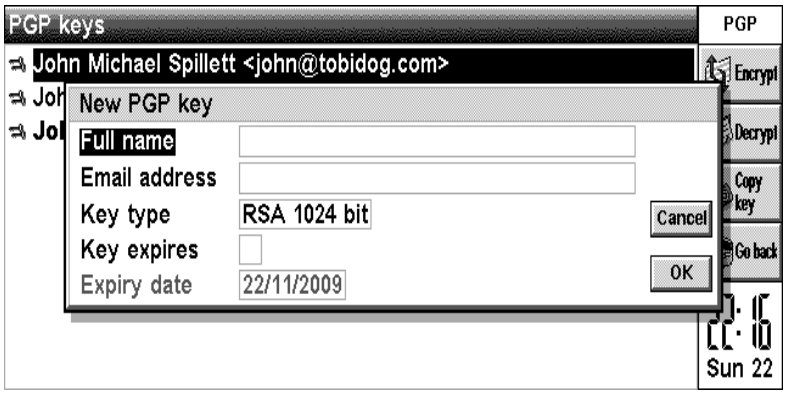
Version 2.6.3a has been ported to EPOC 32. The current version for MS systems is around version 8 but the version available for the Psion will do a good job of encrypting documents and messages.


There are potential compatibility issues with later versions of PGP but these seem only to relate to importing / creating private keys using DH/DSS.

Many users have remained with version 2.6.x which has no weaknesses other than those caused by poor password security procedures for private keys by users.

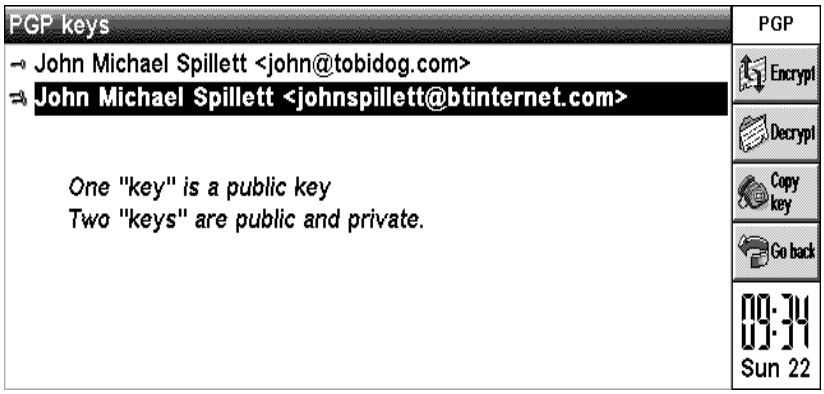
In the following paragraphs I have tried to set out the various actions needed to set up and use the program.

PGP makes use of two keys, a private key used by the owner to decipher messages sent to him/her and a public key provided by the owner to the world to enable messages to him/her to be encrypted.



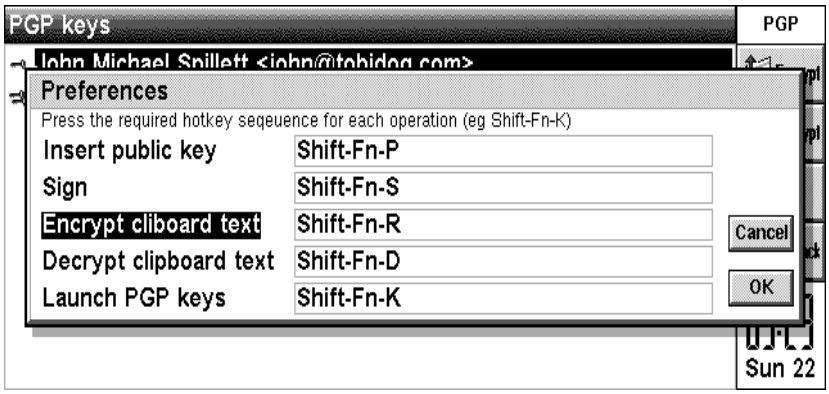

After this screen the user has to enter a long random string after which the keys are generated. This takes a few minutes.

While PGP for EPOC is running any data copied to the clipboard may be encrypted or decrypted using a hotkey .




To see and change your hotkey settings look at the Preferences option in the Tools menu of the PGP for EPOC application. When changing the hotkey you need to actually key in the required key combination e.g. hold down shift fn r for example.

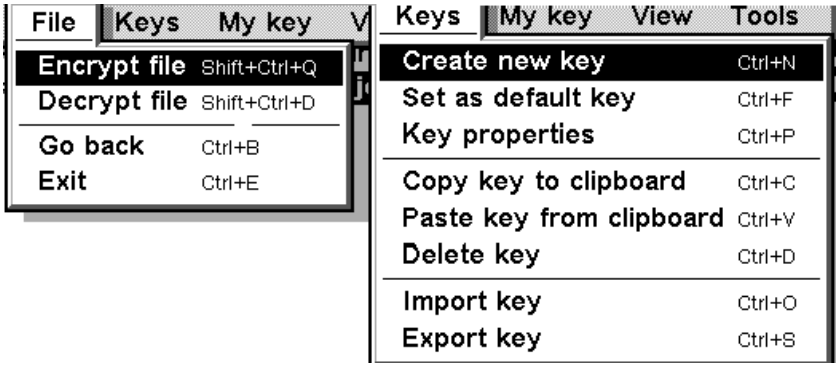
Trouble with hotkeys: Depending on your locale certain hotkeys will not work. For example, pressing Shift-Fn-P on an English Series 5 should copy your public key to the clipboard, but it does not. Similarly for German Series 5s Shift-Fn-E will not encrypt the clipboard. This is easily fixed by selecting a different combination of keys for the function. Use the Preferences option of the Tools menu to customise hotkey settings.




The problem seems to arise if a key already has a fn operation assigned to it. e.g. P has =, E has € on a UK 5MX.

Encrypting files

Entire files may be encrypted or decrypted directly from the PGP for EPOC application either using the File Menu or the side toolbar. Th is will bring up a file find dialog. The application will go dead for up to a few minutes during encryption and decryption .




Export Key will only export public keys

DH/DSS keys are supported, but only public ones , you cannot create a DH/DSS key or import a private DH/DSS key

Importing other peoples Public Keys.

The easiest way of doing so is viewing the text of the key in another app (such as Email, if that's how you received the key), selecting it and copying it (ctrl-c). If the key is on your PC, ensure PsiWin's "Copy Anywhere" function is enabled and your EPOC device and PC are connected, copy the text of the key on the PC. Then open PGP and press ctrl-v. Alternatively, save the key as a file on your EPOC device, enter PGP and press ctrl-o. This will bring up a select file dialogue with which you can find the saved key. Once you've found the key, press enter and the key will be imported.

Importing Private Keys

You can import private keys generated with PGP v2.x. However the EPOC port does not support the import of private keys generated with PGP v6.x. To import a private key, save it on your EPOC device, open PGP and press ctrl-o. Select the key file with the dialogue and press enter.

Signing messages

Ensure PGP is open. Move your cursor into the body of your finished message and press ctrl-a to select all the text. Press ctrl-x to cut the text into the clipboard. Press the hotkey combination to sign the clipboard, which is shift-fn-s by default. Press ctrl-v to paste your signed message.

Encrypting a message

Ensure PGP is open. Move your cursor into the body of your finished message and press ctrl-a to select all the text. Press ctrl-x to cut the text into the clipboard. Press the hotkey combination to encrypt the clipboard, which is shift-fn-r by default.(change this to suit your Psion) Press ctrl-v to paste your encrypted message.

To decrypt a message

Ensure PGP is open. Move your cursor into the body of the encrypted message and press ctrl-a to select all the text. Press ctrl-c to copy the te xt into the clipboard. Press the hotkey combination to decrypt the clipboard, which is shift-fn-d by default. Open Word or other text editor and press ctrl-v to paste the decrypted message.

Files PGPdoc1 and PGPdoc2 set out a detailed analysis of the encry ption process by the programs author.

A copy can be downloaded from the Pscience5 site and for convenience from this site also.( see links on the Review page )

It can also be downloaded from:

http://www.symbiangear.com/en/usd/device:Psion_Serie+5/freedownload.html?pid=103409

Conclusions

The main signs of this not being a fully developed program are the lack of export of private keys and the lack of any feedback during encryption and decryption.

The set-up process for keys uses a lot of CPU power but is a one off process.

The hot keys need fine tuning to your individual keyboard.

The public key / private key concept means that an encrypting key can be freely shared without compromising the decrypting key.

The password for the private key is the keystone to this working and should follow the normal rules for passwords:

- use random characters, not words in a dictionary
- include special characters such as #,€ etc.
- make it as long as possible

Keep the data and the private key apart as far as is feasible e.g. data on a compact flash card.

Prepared on a Psion 5mx using Epoc Word and PDFWriter