

How to use PGP Encryption with iScribe

iScribe e-mail supports seamlessly e-mail encryption and digital signatures.

This bulletin describes how to setup iScribe so that you can send and receive encrypted e-mails and/or digitally sign your e-mails using the GnuPG encryption package.

Lets start...

What is PGP encryption anyway?

Before we start you might want to look at the concepts section of the GnuPG mini howto document. You can read this now by [clicking here](#). Don't worry if the document doesn't make much sense to you. Read the rest of this and then go back to it. It should make more sense once you read the explanation below.

PGP stands for Pretty Good Protection. It's an encryption standard developed to facilitate the sending and receiving of digital documents securely. It's a very good standard and you are pretty much assured that if you send a message to Joe and it's encrypted with Joe's "public key" (more on this later) only Joe will be able to read the message.

iScribe makes the sending and receiving of PGP encrypted messages a synch. With a click of a button you can encrypt a message. When you receive an encrypted message simply pressing a button causes iScribe to prompt for your "private pass key" (more on this later) and if you enter it correctly decrypt the message that was addressed to you.

What are digital signatures?

Digital signatures are a way of encoding documents so that the recipient knows that the document was created by you and that it has not been tampered with. A digitally signed document or e-mail does not have to be encrypted. If for example you have a favorite recipe that you want to mail to an Internet news group (say the island packet news group) but you want to make sure no one modifies it and then passes it on to friends as their creation then you would simply digitally sign the plain text (or clear text) e-mail. People receiving your message could then verify that the recipe you signed came from you and has not been modified.

Note that the recipient of your encrypted e-mail and/or digital signatures does not need to be running iScribe to view the messages. As long as they have some PGP standard e-mail program (there are many) they can read and verify your messages. Similarly, users sending you encrypted e-mails do not need to be using iScribe. Any PGP encoding program will do.

What is a key pair?

A key pair is what is required to encrypt/decrypt a document. When you install the PGP software on your computer you will be prompted to create a key pair. The installation software will prompt you for a "Pass Key" and generate two keys from it, the "Public Key", and the "Private Key". These keys are big long horrible sequences of letters and numbers which are used to encode your message. Fortunately iScribe manages these keys for you in a simple way so that you don't actually need to know what they are. The only really important thing to keep secure and not forget is your "Pass Key". This is a simple string of text that you will need to decode megs addressed to you. If you forget your "Pass Key" you will not be able to open messages sent to you. The "Pass Key" can be any free text you want as long as it's longer than 8 characters. "Honey I am home" is a perfectly good pass key. The pass key is case sensitive so keep this in mind when you commit it to memory.

How it works...

Let's say you want to receive encrypted messages from Joe@somewhere.net. Before Joe can send you an encrypted e-mail he needs to know your "public key". So in a plain e-mail you mail him your public key. Any one in the world can see the key, but it doesn't matter. The public key can only be used to encrypt a message to you. It can not be used to read a message addressed to you. Only you can do that.

Once Joe receives your public key he can use PGP software to generate an encrypted message to you. If he is using iScribe the process is simple. When you receive the encrypted e-mail from Joe and try to read it with iScribe, iScribe will prompt you for your "pass key" (The Honey I am home thing...). iScribe will then generate the "private key" from the pass key and decrypt and display the message for you.

For you to send an encrypted message to Joe, you need to have his public key. So, Joe first sends you an e-mail with his public key. Once you receive the public key with iScribe, you push a button and Joe's public key is automatically added to an address book. To send an encrypted message to Joe you then create the messages as usual, push a button and send the encrypted message to Joe. Very, Very simple and secure...

We will see later on how to actually carry out a send/receive operation.

What you need

1. iScribe e-mail
2. A free copy of WinPT which incorporates GnuPG for Windows. This program can be downloaded the WinPT website or by clicking here.
3. A Windows machine running Win95-WinXP.

Installing the software

Here are the steps.

1. Download WinPT from http://winpt.gnupt.de/int/?page_id=10 and save it on your computer and run it.
2. The installation program will ask you a pile of questions. Simply accept all the defaults until you reach the final screen and then hit finish.
3. The WinPT installation script will then run the WinPT program. You should then see a message box popup on the screen with the following. "Something seems to be wrong with your GPG keyrings". This message pops the very first time you run the program and occurs because you have no public or private keys. Hit yes to create your keys.
4. Next select "Have WinPT generate a key pair" and hit OK.
5. Now enter your name (Luis Soltero in my case), your e-mail address (lsoltero@globalmarinenet.net in my case) and your pass key (Honey I am home). Use the default key type and never have the key expire. Hit Start to generate the keys.
6. After the key generation completes WinPT will ask you if you want to save your keys. Answer yes and store the files in a safe place.
7. You are now done with the WinPT installation. You will see a "Key" shaped icon in the system tray. Double clicking on the icon will bring up WinPT. Clicking on the X on the top right will minimize WinPT to the system tray. We will discuss the usage of WinPT a little later.
8. Now install iScribe if you haven't done so. XGate/OCENS.Mail users can do this by running the appropriate installation program. Follow the XGate/OCENS.Mail installation instructions to complete the installation. Test iScribe, XGate/OCENS.Mail to make sure all is working.
9. Next run iScribe and go to the File->Plugins. If you see GnuPG then select it and hit remove. Now click on Add and select the gnupg plugin. iScribe should tell you that it has been loaded correctly.

10. Finally click on the GnuPG plugin and select configure. You should see your name in User.

Once you startup iScribe you will see a new PGP menu and new Icons on the tool bar when creating a new e-mail or reading a pre-existing one. These icons are used to manage PGP and are described below.

You are now ready to encrypt/decrypt and sign e-mails...

Note that most of the following is in the iScribe Help file under the help menu. Menu->iScribe Guide. Click on Index and type PGP. This will get you to the PGP documentation.

Step one

Sending your public key to a user you want to correspond with. As I mentioned before you must publish a public key before you can receive an encrypted message. Here are the steps (BTW This is the most complex procedure in the whole thing).

1. Run iScribe.

2. Compose a "regular" e-mail to joe@somewhere.com. While in the compose window move the mouse down to the windows application tray and double click on the "key". This should 3. Scroll down until you find your Name and e-mail address. Then right click on your name and select copy.

4. Now exit PGPkeys.

5. Back in the iScribe compose window click the screen where you want to place your public key and then right mouse click and select paste. You should see some thing like

```
-----BEGIN PGP PUBLIC KEY BLOCK-----Version:  
GnuPG v1.2.3 (GNU/Linux)
```

```
  mQGibEBCR6DwRBAD0/+7qtgiMqITxr974yzw1YRZfVi+xVHsi8V5QvPcVG9Ja50Nw  
J/vDShbByv7ZQRY2CsODxVxomX3Xm+I58WTrVwAYWUIRuaFxBGRa61MhklzdAcPV  
Am1VOrul99gr9TTBG51I8KsrVehA7h2yizFCPJ7gOE1AKjsrkDefzGLVewCgtwZh  
JVAMgH2NxuaUJfT1LMp3WvKALbVTb3r8Ci2mTtuhLg+Pn2FKKMio3ijSRUgzBWD  
LgIxLkZ5pSH0Sk3nxOb6b7gXM3zjSZOeuHNZvcGW0kYaPgkvKUtZYDUA/G3HuIxC  
/TxT0Tgo1A29hNYhe3tjBeimmjeJf+VetkvatESVfkcVGw6Ns0WpO2IrAq0YRLco  
+/FSA/wOeD2rDj/5zusj3YF60Crun9OpfFRDMDjoLNUiIAT88lKwSMzUEZwgP+ap  
AZUoZjh3T/lMP6+0Y7s1FP6Ux1hq/GmAlbGFfskYTY4meymNOe3FzpJgLUovwZ1+  
I83nMdc6cqEFscuFwViUMDUL0Ar/Afam+8kjWplhGXj61iXkr7QrTHVpcyBTb2x0  
ZXJvIDxsc29sdGVyb0BnbG9iYWxtYXJpbmVuZXQubmV0PoheBBMRAGAeBQJAKEg8  
AhsDBgsJCACDAgMVAqMDFgIBAh4BAheAAAoJEId/BV9J6V4zm8MAn38jevUyM2nh  
7VKVIE/QpVSHVYahAJ9ilTiYSrNN408ABE1BPIKwuK57rbkBDQRAkeg/EAQA1p5d  
6n+Je6GHZCBKA0lyTtAosrjf6c/m/wHi4A2vUGpBKPq8x/ZhG79/OwVw/MO3Uk28  
xBLpK/tiCj7FOkbBP/3UsVfNmHmXFdG19xSaAAYFoIEDRo6lmw0xRNnz7kY0Bkvj  
c+Fita1Wk1vE+ddIXmT8zMWT6eVGHJCJg0UN76MAAwUD/0BwfK1lUKw8yx2I9z72  
4e9HLrVbLR+z2zMzH4nOuwYpH4lMd2jf618IOon3P0w1CXR6tg1LQTLZHUKhsfA01  
y8HrKRYhnh1dFkHY+MsbIjp+iwcJv3r1/nBmJnFgAz/SPXnZAumuH7HBXmwDRiWk  
fYpuA3WXc6cAFhU/HLE8IOZuiEKEGBECAAKFAkCR6D8CGwwACgkQh38FX0npXjOr  
3gCdElVUftrEtKjcvfB57OPjuLVuiWsAnj23p6/Et3Rak75H9sOvpf77hApk  
=V7sh  
-----END PGP PUBLIC KEY BLOCK-----
```

Which is a copy of my public key. Note that in the next step you will be able to save this key to your address book and send me encrypted messages in the future.

6. now send the message.

7. You are now done... Now we wait...

Step 2

Receiving and recording a public key... While we wait for joe@somewhere.com to send us an encrypted message some one else doe@somewhereelse.com sends us an e-mail with his public key. doe wants us to send him encrypted messages from now on...

To record his public key we do the following... You might actually try this on this messages.

1. Open the message as you normally would in iScribe.
2. Push the "Add Key" button. It's the one on the very right of the tool bar. iScribe should tell you that it found 1 or more keys and that the key has been added to your keyring.
3. Now double click on the "Key Icon" in the system tray to bring up WinPT and find doe@somewhereelse.com in the list.
*** This is very Important ***

now right click on doe@somewhereelse.com and select sign. By signing Doe's public key you are confirming to the software that the key does indeed belong to Doe. You might actually call Doe on the phone or contact him via some other means to confirm hat he indeed sent you his public key. iScribe will not encrypt a message unless the key that is being used has been signed. Please see the section of the "Web of trust" in the GnuPG howto for more info. Here is the link.

4. Back in iScribe create or edit the contact information for Doe and make sure that the e-mail address and name appears in the contact information exactly like it does in the WinPT entry. Note that iScribe will report an empty key ring error when ecrypting an e-mail if the UserName and E-Mail address in the key does not exactly match the entry in the contacts list.
You can now send me or doe@somewhereelse.com encrypted messages.

Step 3

Sending an encrypted message...

1. Compose a message to doe@somewhereelse.com in iScribe as you normally would.
2. Before you send it click on the "Encrypt" button on the tool bar.
3. If you want to digitally sign an e-mail click on the "Sign" button. As I mentioned before messages do not need to be encrypted to be signed. See discussion above on signing vs. encryption.
4. Send the message...
That is all there is to it..

Step 4

Decoding encrypted messages...

You have finally received an encrypted message from joe@somewhere.com. when you try to read it it looks like.

-----B_EGIN P_GP MESSAGE-----Version:
GnuPG v 1.2.3 (Gnu/Linux)

qANQR1DBwU4DZqz+jDG31EcQB/9AwVMqHsNGCvumYk4CYE0RNTSGxIX6uAAHk3UL
7mFzD0lE5Dc8qfswwedf9urZx1F+rUZ6//XRDR9bqPrh/5S2D0gdYZGpx3my5X0U
kr39Vc1drit780Vvh+k5d9HwiDpe5xZ6MeDBknWyzD1BK4UnkFFdxBeLAxtNLMLA
+7j8R/wWzeK0MnhejE2CFq14jR5azdT7JbFbiOzPgoXxvVBVbRBGEEc8x6H/LpJ0
01nJrvaTQXhVRIKV0UMS3DVzadfQFQgbV1kf6mbj0fCD2rZUfnHJayY5kpOd6REi
c7RqqQZlKfHE6euQH84ek+U6nPn+P7nV1lP5DX0dafdX+rv6B/95GcebViVpBH/6
uoAwz9pXAKb7BOzbePuYQBzyAtZEv6B9MTMYOVP+A0E81xRFbn20bNkmcsEB/z5O
rLooPKbFnqYXQvEuOnOMW+dDB1P+5NRY4pnKghwZX4HP1t/YJjo5d4axwBcSyOf2
rBKMf1XK+453ugsoyKIIChr2GpbegH5dxWLgqLXkrroQFeePVrT8YwXkL8SH43Tj
iIVvZTroYEw7Ai6bMplLjusNhLhVIHtgcbSzQrw4mvZTvrxFs6PFYwL/RQTP6DVM
NLamyy/xQ0mbJOaWREMcrlVWyHtMfSin/cJEilAFGjSN65bMDcsG1ULDMgKBRrtk
iBqXAJXSybFvt892NacNlxNGqSoe2CznEkeZWU6SSez5mtbvKd0h9KpJqe13GcnY
FQkCymNLdCLKzQz9ZGzNtCNYRGE5mmwX7pjBYAiJpy0ve10zgU9GU6nZFjWmudoa
WaVqDJ8UpPLbQq+Bm1DeeYO5H2jA5yhmVNLt4GfRi+g4KSqmV6BvKCT/YZaS4cBP
ONJ6fij0Kk355mFecqMhNqPN3YJTUGUfHkJGBGGZuLFNQaMzgFzPrCU=
=T7Ge

-----END PGP MESSAGE-----

Note: that I have altered this message by adding "_" to the PGP header so that it would not interfere with these instructions. Had I not done this iScribe would ask you for a pass code when you hit the "Decrypt" button in Step 2.

To decode PGP encrypted messages do the following.

1. Display the message as you would a normal e-mail.
2. Click on the "Decrypt" button on the tool bar
3. A window pops up requesting your "Pass Key". Enter the pass key.
4. The clear text message replaces the encrypted message.

That is it...

Simple as pie.

Luis Soltero, Ph.D., MCS
Director of Software Development
Global Marine Networks, LLC
Tel: 865-379-8723
Fax: 615-985-0403
E-Mail: lsoltero@globalmarinenet.net