How to use PGP Encryption with iScribe

iScribe e-mail seamlessly supports 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.

If you are familiar with PGP encryption, simply follow the steps below. If you are new to PGP encryption you might want to read the Basic PGP Information section before you begin.

What you need

1. iScribe e-mail
2. A free copy of GNU Privacy Guard for Windows.
3. A personal computer running Win7, Vista, or WinXP operating system.

Installing the software…

1. Download GNU Privacy Guard for Windows from http://www.gnupt.de and Save the file to your computer. Then run the file.
2. The installation program will ask you numerous questions. Simply accept all the defaults until you reach the final screen and then click finish.
3. The installation script will then run the program. You should see a message box with the following. "Something seems to be wrong with your GPG keyrings". This message appears the very first time you run the program and occurs because you have no public or private keys. Select <Yes> to create your keys.
4. Next select "Have GnuPG 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 private pass key (mine is, Honey I am home). Use the default key type and never have the key expire. Select <Start> to generate the keys.
6. After the key generation completes you will be asked if you want to save your keys. Answer <Yes> and store the files in a safe place.
7. You are now done with the GnuPG installation. You will see a "Key" shaped icon in the system tray. Double clicking on the icon will bring up GnuPG. Clicking on the X on the top right will minimize GnuPG to the system tray. We will discuss the usage of GnuPG 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.

Now when 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 an existing one. These icons are used to manage PGP and are described below.

How 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 – Send your public key

You must publish a public key before you can receive an encrypted message.

1. Run iScribe.
2. Compose an 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 icon>. This should bring up the PGPkeys application.
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 this:

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

   mQGiBECR6DwRBAD0/+7qtgiMqITxr974yzw1YRZFVi+xVHsi8V5QvPcVG9Ja50Nw
   J/vDShbByv7ZQRY2CsODxVxomX3Xm+I58WTrVwAYWUIRuaFxBGRa6lMhklzdAcPV
   Am1VOrul99gr9TTBG51I8KsrvEhA7h2yizFCPJ7gOElAKjsrkDefzGLVewCgtwZh
   JVAMgH2NxuaUJFt1LMp3WvkEALbVTb3r8Ci2mTtuhLg+Pn2FKKMio3ijSRUgzBWD
   LgIxLkZ5pSH0Sk3nxOb6b7gXM3zjSZOeuHNZvcGW0kYaPgkvKUtZYDUA/G3HuIxC
   /TxT0TgolA29hNYhe3tjBeimmjeJf+VetkvatESVfkcVGw6Ns0WpO2IrAq0YRLco
   +/FSA/wOeD2rDj/5zusj3YF6OCrun9OpfFRDMDjoLNuIiAT88lKwSMzUEZwgP+ap
   AZUoZhj3T/lMP6+0Y7s1FP6Ux1hq/GmAlbGFfskYTY4meymNOe3FzpJgLUovwZ1+
   I83nMdc6cqEFscuFwViUMDUL0Ar/Afam+8kjWplhGXj61iXkR7QrTHVpcyBTb2x0
   ZXJvIDxsc29sdGVyb0BnbG9iYWxtYXJpbmVuZXQubmV0PoheBBMRAgAeBQJAkeg8
   AhsDBgsJCAcDAgMVAgMDFgIBAh4BAheAAAoJEId/BV9J6V4zm8MAn38jevUyM2nh
   7VKVIE/QpVSHVYahAJ9ilTiYSrNN4O8ABE1BPIKwuK57rbkBDQRAkeg/EAQA1p5d
   6n+Je6GHZCBKAO1yTtAosrjf6c/m/wHi4A2vUGpBKPq8x/ZhG79/OwVw/MO3Uk28
   xBLpK/tiCj7FOkbBP/3UsVfnmHmXFdG19xSaAAYFoIEDRo6lmw0xRNnz7kY0Bkvj
   c+Fita1Wk1vE+ddIXmT8zMWT6eVGHJCJg0UN76MAAwUD/0BwfK1lUKw8yx2l9z72
   4e9HLrvbLR+z2zMzH4nOuwYpH4lMd2jf6l8lOn3P0wlCXR6tg1LQTLZHUkhsfA01
   y8HrKRyhnh1dFkHY+MsbIjp+iwcJv3rl/nBmJnFgAz/SPXnZAumuH7HBXmwDRiwk
   fYpuA3WXc6cAFhU/HLE8I0ZuiEkEGBECAAkFAkCR6D8CGwwACgkQh38FX0npXjOr
   3gCdElVUftrEtkjcVfB57OPjuLVuiWsAnj23p6/Et3Rak75H9sOvpf77hApk
   =V7sh
   -----END PGP PUBLIC KEY BLOCK-----

   This sample above is a copy of my public key. In Step 2 you can save this key to your address book and send me encrypted messages in the future.
6. Now <Send> the email message.
7. You are done... Now we wait...

Step 2 – Receive and record a public key

While we wait for joe@somewhere.com to reply to us with an encrypted message someone 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:

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 one 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 ***

   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 that 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 Basic PGP Information below for more info.
4. Back in iScribe, create or edit the contact information for Doe and make sure that the email address and name appears in the contact information **exactly** like it does in the GnuPG entry. Note that iScribe will report an empty key ring error when ecrypting an email 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 email

1. In iScribe, compose a message to doe@somewhereelse.com .
2. Before you send it click on the <Encrypt> button on the tool bar.
3. If you want to digitally sign this email as well, click on the <Sign> button. You can “sign” a message without encrypting it.
4. <Send> the message.

Step 4 – Decoding encrypted email

You have finally received an encrypted message from joe@somewhere.com. When you try to read it, it looks something like this:

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

qANQR1DBwU4DZqz+jDG31EcQB/9AwVMqHsNGCvumYk4CYE0RNTSGxIX6uAAHk3UL
7mFzDOlE5Dc8qfswwedf9urZx1F+rUZ6//XRDR9bqPrh/5S2D0gdYZGpx3my5X0U
kr39Vc1drit780Vvh+k5d9HwiDpe5xZ6MeDBknWYzD1BK4UnkFFdxBeLAxtNLMLA
+7j8R/wWzeKoMnhejE2CFq14jR5azdT7JbFbiOzPgoXxvVBVbRBGEEc8x6H/LpJ0
01nJrvaTQXhVRIKV0UMS3DVzadfQFQgbV1kf6mbj0fCD2rZUfnHJayY5kpOd6REi
c7RqqQZlKFhE6euQH84ek+U6nPn+P7nVlIP5DX0dafdX+rv6B/95GcebViVpBH/6
uoAwz9pXAkB7BOzbePuYQBzyAtZEv6B9MTMYOVP+A0E81xRFbn20bNkmcsEB/z5O
rLooPKbFnqYXQvEuOnOMW+dDB1P+5NRY4pnKghwZX4HPlt/YJjo5d4axwBcSyOf2
rBKMflXK+453ugsoyKIIChr2GpbegH5dxWLgqLXkrroQFeePVrT8YwXkL8SH43Tj

iIVvZTroYEw7Ai6bMplLjusNhLhVIHtgcbSzQrw4mvZTvrxFS6PFYwL/RQTP6DVM
NLaMyy/xQ0mbJOaWREMcr1VWyHtMfSin/cJEi1AFGjSN65bMDcsGlULDMgKBRrtk
iBqXAJXSybFVt892NAcNlxNGqSOe2CznEkeZWU6SSez5mtbvKd0h9KpJqel3GcnY
FQkCymNLDCLKzQz9ZGzNtCNYRGE5mmwX7pjBYAijpy0vel0zgU9GU6nZFjWmudoa
WaVqDJ8UpPLbQq+BmlDeeYO5H2jA5yhmVNLt4GfRi+g4KSqmV6BvKCT/YZaS4cBP
ONJ6fij0Kk355mFecqMhNqPN3YJTUGUfHkJGBGGZuLFNQaMzgFzPrCU=
=T7Ge
-----END PGP MESSAGE-----

1. Click on the <Decrypt> button on the tool bar
2. A window pops up requesting your "Pass Key". Enter the pass key.
3. The clear text message replaces the encrypted message.

That's all there is to it.

If you are unfamiliar with PGP Encryption you may find the following information helpful.

BASIC PGP INFORMATION

What is PGP encryption?

PGP stands for Pretty Good Protection. It's an encryption standard developed to facilitate the sending and receiving of digital documents securely.

Classic methods for encryption use only one "key" for encryption. The sender encrypts the message with this key. The receiver of the message must have the very same key. This key must be passed to the receiver in such a way that others do not have access to it. If somebody else does have the key, then this method of encryption is useless.

Using private keys with public keys strengthens security. The public key can be shared with others and can be distributed via email or the internet. The private key, however, is kept secret and should never be shared by any method. When implemented correctly, the private key cannot be decoded from the public key. With this two-key method the sender will encrypt the message with the public key that belongs to the receiver. The receiver will decrypt the message with his/her private key.

It is a very good standard and you are pretty much assured that if you send a message to Joe and it is encrypted with Joe's "public key" only Joe will be able to read the message.

iScribe makes it easy to send and receive PGP encrypted messages. 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 key" 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 has not been modified by anyone else. 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 (i.e. the island packet news group) but you want to make sure no one modifies the recipe and then passes it on to friends as their creation; 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: The recipient of your encrypted email and/or digital signatures does not need to be running iScribe to view the messages. As long as they have some PGP standard email program (there are many) they can read and verify your messages. Similarly, anyone sending you encrypted emails 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 that 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. They 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 messages 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 is 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 email he needs to know your "public key". So in a plain email you mail him your public key. Anyone 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 cannot 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 email 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 email with his public key. Once you receive Joe's 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 create the messages as usual, push a button and send the encrypted message to Joe. Very, Very simple and secure...

If there is a weak point in this method, it is in the spreading of the public keys. Please use caution when distributing your public key and when accepting the public key of others. You may consider a public key as trustworthy when you trust the sender of the key.

Thank you!
Global Marine Networks, LLC
www.globalmarinenet.com
email: support@globalmarinenet.com