

Date: 12/24/02 1:43 AM
From: Luis Soltero
To: Bulletins@marinenet.net
Copy:
Subject: How to Encrypt your Mail With Calypso

Return-Path: <lsoltero@globalmarinenet.net>
Delivered-To: bulletins@marinenet.net
Message-ID: <200212240143280258.004E82BE@gmn.mارينet.net>
References: <200212240112390850.00324E66@gmn.mارينet.net>
<200212240127360700.003FFDB8@gmn.mارينet.net>
<200212240128580618.00413DB6@gmn.mارينet.net>
X-Mailer: Calypso Version 3.20.02.00 (1)
Date: Tue, 24 Dec 2002 01:43:28 -0500
Reply-To: lsoltero@globalmarinenet.net
From: "Luis Soltero" <lsoltero@globalmarinenet.net>
To: Bulletins@marinenet.net
Subject: How to Encrypt your Mail With Calypso
Content-Type: text/plain; charset="us-ascii"
X-Virus-Scanned: by AMaViS perl-11

Hello All,

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

This bulletin describes how to setup calypso so that you can send and receive encrypted e-mails and/or digitally sign your e-mails.

So lets start...

What is PGP encryption anyway?

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 mesg to joe and it's encrypted with joe's "public key" (more on this later) only joe will be able to read the mesg.

Calypso makes the sending and receiving of PGP encrypted mesgs a synch. With a click of a button you can encrypt a mesg. When you receive an encrypted mesg simply pressing a button causes calypso to prompt for your "private key" (more on this later) and if you enter it correctly decrypt the mesg 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 your creation then you would simply digitally sign the plain text (or clear text) e-mail. People receiving your mesg 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 calypso to view the mesgs. As long as they have some PGP standard e-mail program (there are many) they can read and verify your mesgs. Similarly, users sending you encrypted e-mails do not need to be using calypso. 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 mesg... Fortunately Calypso 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 mesgs addressed to you. If you forget your "Pass Key" you will not be able to open mesgs 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 mesgs 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 mesg to you. It can not be used to read a mesg addressed to you. Only you can do that.

Once Joe receives your public key he can use PGP software to generate an encrypted

mesg to you. If he is using Calypso the process is simple. When you receive the

encrypted e-mail from joe and try to read it with calypso, calypso will prompt you

for your "pass key" (The Honey I am home thing...). Calypso will then generate

the "private key" from the pass key and decrypt and display the mesg for you.

For you to send an encrypted mesg 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 calypso, you push a button and joe's public key is automatically added to an address book. To send an encrypted mesg to joe you then create the mesgs as usual, push a button and send the encrypted mesg to joe. Very, Very simple and secure...

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

What you need

- a) Calypso e-mail
- b) A free copy of the Network Associates PGP program PGPFW658Win32.exe. This program can be downloaded from support page at my website at www.globalmarinenet.net.
- c) A Windows machine running Win95-WinXP.

Next you need to install the software

Here are the steps.

- a) Download the PGP software from www.globalmarinenet.net
- b) Double click on PGPFW56832.exe
- c) Accept the defaults until you get to "Select Components". Unselect all components except "PGP Key Management". Then hit next...
- d) Continue to accept defaults until you are asked: "Do you have Key Rings you wish to use?" The answer is NO unless you know what you are doing. Answering NO causes the software to create a key pair for you.
- d) Make sure the "Launch PGPKeys" check box is marked and hit Finish.

The installation program now runs PGPKeys to create the key pair required.

- a) Accept the defaults until you reach the name/e-mail dialog. Enter your full name and your e-mail address. For me that would be
Full Name: Luis Soltero
EMail Address: lsoltero@globalmarinenet.net

For you it will be "you@marinenet.net" or "you@mailmarinenet.net".

Continue accepting defaults until you reach the "Pass Phrase" dialog.

- b) Enter your "Pass Phrase". Commit it to memory. Do not forget it or you will be in trouble... You will need to move the mouse around until the process completes. The wizard uses your mouse movements to generate randomness in the keypair.
- c) When promoted to "send key to root server" say NO. Unless you are connected to the internet. Most of you will not use this feature. Even if you are connected to the internet you may not want to publish your public key to the world...

Or
maybe you do...

so check
"Do not send key to root server"

d) you are done. Exit PGPKeys and Save Backup... Choose a safe location to save your keys to... Like a floppy or CD or Desktop...

You are now done with the installation.

***** REBOOT YOUR COMPUTER *****

The PGP software will not work unless you restart your computer. This goes for Windows XP users as well. Once the computer reboots you will know the software installed correctly by observing a small pad lock in the application tray (bottom right of screen).

Once you startup calypso you will see a new PGP menu and new Icons on the tool bar. 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 Calypso Help file under the help menu. Menu->Calypso 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 mesg. Here are the steps (BTW This is the most complex procedure in the whole thing).

- a) Run calypso.
- b) Compose a "regular" e-mail to joe@somewhere.com. While in the compose window move the mouse down to the windows application tray and right click on the lock and select "PGPKeys". This should bring up the PGPkeys application.
- c) Scroll down until you find your Name and e-mail address. Then right click on your name and select copy.
- d) Now exit PGPkeys.
- e) Back in the calypso 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: PGPfreeware 6.5.8 for non-commercial use <<http://www.pgp.com>>

```
mQGIBD4H7WoRBADx4xKAjeCpj6N+A+8Jd+5jhG74BKAt6JR03owbBjjaoWNZDtP5
xFy8suJvOzclZY3C88EPj73D3/+bYY5Z3q4RCpHwAUDli2S0R77BX4BFYKj0XQ9I
ZMlVlvhuHqkCNVnFBDqm+Kd2vWJC9+NLHPTJe61c2ztw9rPtAVbQ+r8mNwCg/5OG
eYvNvodAY01aH3SEMiMoc4cD/RqQn9B1LtVLyRhG5ObtpD5E0vrDUgPt/tqgCO78
0g3eOw4EvWvjczRkJN1PImZ0KCLRhChx7kjRIfrCBBGPDb8Xa6wd+oIS5aSK0H7x
sr/ZlyhFUf+aFh18ymz3y/oLUcg7pwfPegZwY7PpnnrngSSioa4dnj1Y75kidR5o
TwmaBACJXDTIWRP97MHCURcQ/ti2yASRGGUqz/zZYRR3kn1Iqs7srs2cFX7c1DrH
qqd0JLYeX6Vr1goyTKXpLYVLH0Blz2bPkhhX2MqePQc8SmvwBOVtNBmphWlucQQZK
tqOF3POwKs6GEMmu43Y0mvNtYhAm8bkjhF2RBYrK/2NEoWvPdbQrTHVpcyBTh2x0
ZXJvIDxsc29sdGVyb0BnbG9iYWxtYXJpbmVuZXQubmV0PokATgQQEQIADgUCPgft
agQLAwIBAhkBAAoJEOydhT+ISaNdXmWaoIoUIfSjqlLbt37cgn+1C33ofxfVAKD7
```

```
gZCYirhJWpD5WvmJxtbl021qR7kCDQQ+B+1qEAgA9kJXtwh/CBdyorrWqULzBej5
UxE5T7bxbrr1LOCdaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1
WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq0lue
jaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy209vPJ
I8BD8KVbGI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaG
xAMZyAcpesqVDNmWn6vQC1CbAkbtCD1mpF1Bn5x8vY1LIhkmuquiXsNV6TILowAC
Agf/eIpxSNeDrCaE6fcNQ2FhUmbKJsnH7JVqKO9NJ8LvtMkMXdDEnV4kCpbP63Bm
0MU+7v/q+SdsSq0RnxEUof0PoCjveCwBURmg1qu1RYzpuhyBpNLJ3s7qkluto1sF
bgrtZzr35tx0igL5DS1+080mQZyc7SRfUy0EP3/byJ6qSOrGnEEltHtosD7tyh5B
Qs2WGgQhZQZX+0UjSj6C0TLX95oEJadQ2g90EWCZcNHR3ow7P19Kh1ZgFtOPYpji
eqDCK9uWy01neCdJGJXwA0GsH6fmMMSoGqWovCNeenbs7WG412TJImxON3edvVdc
2oZ4083WB02HW6V1k4Mk3WQXnYkARgQYEQIABgUCPgftagAKCRDsnR7fiEmjXQmf
AKCmjcvtzIDFYDobXN5RCAADMKLuoqgCfZKVGLfhks5/vxmhCNJeQhaCSzrE=
=bpYY
-----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 mesgs in the future.

- f) now send the mesg.
- g) 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 mesg some one else doe@somewhereelse.com sends us an e-mail with his public key. doe wants us to send him encrypted mesgs from now on... To record his public key we do the following... You might actually try this on this mesgs.

- a) Open the mesg as you normally would.
- b) Push the "Decrypt message" button. It's the one on the very right of the tool bar.
or select it Decrypt from the PGP menu. PGP->Decrypt Message
- c) A window will popup with one or more PGP keys in it depending on the number of keys in the mesg (usually one). Highlight the users e-mail address
(In this case mine) and hit import.

You can now send me or doe@somewhereelse.com encrypted mesgs.

Step 3. Sending an encrypted mesg...

- a) Compose a mesg to doe@somewhereelse.com as you normally would.
- b) before you send it click on the "Encrypt" button on the tool bar or select the PGP->Encrypt menu entry.
- c) If you want to digitally sign an e-mail click on the "Sign the messg" button
or select PGP->Sign mesg when sending. As I mentioned before mesgs do not need to be encrypted to be signed. See discussion above on signing vs. encryption.
- d) send the mesg...

That is all there is to it..

Step 4. Decoding encrypted mesgs...

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

-----BEGIN PGP MESSAGE-----

Version: Encrypted with PGP Plugin for Calypso

```
qANQR1DBwU4DZqz+jDG31EcQB/9AwVMqHsNGCvumYk4CYE0RNTSGxIX6uAAHk3UL
7mFzD0LE5Dc8qfswwedf9urZx1F+rUZ6//XRDR9bqPrh/5S2D0gdYZGpx3my5X0U
kr39Vcldrit780Vvh+k5d9HwiDpe5xZ6MeDBknWyzD1BK4UnkFFdxBeLAxtNLMLA
+7j8R/wWzeKoMnhejE2CFq14jR5azdT7JbFbiOzPgoXxvVBVbRBGEEc8x6H/LpJ0
0lnJrvaTQXhVRIKVOUMS3DVzadfQFQgbV1kf6mbj0fCD2rZUfnHJayY5kpOd6REi
c7RqqQZlKfHE6euQH84ek+U6nPn+P7nVllP5DX0dafdX+rv6B/95GcebViVpBH/6
uoAwz9pXAkB7BOzbePuYQBzyAtZEv6B9MTMYOVP+A0E81xRFbn20bNkmcsEB/z5O
rLooPKbFnqYXQvEuOnOMW+dDB1P+5NRY4pnKghwZX4HPlt/YJjo5d4axwBcSyOf2
rBKMfLXK+453ugsoyKIIChr2GpbegH5dxWLGqLXkrroQFeePVrT8YwXkL8SH43Tj
iIVvZTroYEw7Ai6bMplLjusNhLhVIHtgcbSzQrw4mvZTvrxFs6PFYwL/RQTP6DVM
NLAMyy/xQ0mbJoAWREMcrlVWyHtMfSin/cJEi1AFGjSN65bMDcsGLULDMgKBRrtk
iBqXAJXSybFvt892NacNlxNgqSOe2CznEkeZWU6SSez5mtbvKd0h9KpJqel3GcnY
FQkCymNLDCLkzQz9ZGzNtCNYRGE5mmwX7pjBYAiJpy0ve10zgU9GU6nZFjWmudoa
WaVqDJ8UpPLbQq+BmlDeeYO5H2jA5yhmVNLt4GfRi+g4KSqmV6BvKCT/YZaS4cBP
ONJ6fij0Kk355mFecqMhNqPN3YJTUGUfHkJGBGGZuLFNqAmzgFzPrCU=
=T7Ge
```

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

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

To decode PGP encrypted mesgs do the following.

- a) Display the mesg as you would a normal e-mail.
- b) Click on the "Decrypt" button on the tool bar or
select the PGP->Decrypt message menu entry.
- c) A window pops up requesting your "Pass Key".
Enter the pass key.
- d) the clear text mesg replaces the encrypted mesg.

That is it...

Simple as pie.

--luis

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