
Roxy Software Inc.

**Using the Roxy Software
Database Download Service**

Table of Contents

About the Database Download Service	1
Getting Started Step 1 - Generate a private and public key pair using GNU Privacy Guard	2
Getting Started Step 2 – Send Us Your Public Key.....	8
Configure an SFTP Client.....	9
Decrypting Your Backup	10

About the Database Download Service

Organizations who use our hosting services often wish to regularly download a copy of the data to their location. Please note that you must register with us for this service and bandwidth fees may apply if you have a large dataset. Check our website for pricing.

The steps that follow are fairly technically involved. We suggest you consult with your technical support department or consultant.

To ensure that your data is as secure as possible, you must use an SFTP client to connect to our server. The backup file is encrypted using a public/private key pair that only you can decrypt.

In order to register for the database download service you must generate a private/public key pair using GNU privacy guard (a free, open-source encryption tool) and e-mail us the public key. See the following 'Getting Started' sections for instructions.

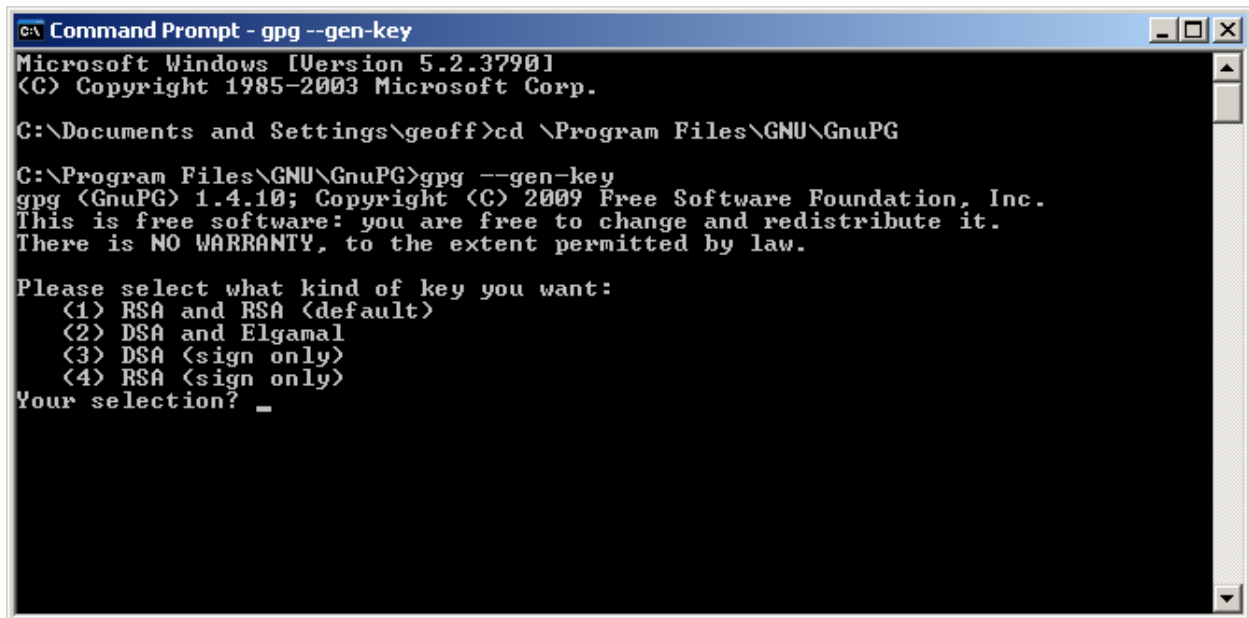
Getting Started Step 1 - Generate a private and public key pair using GNU Privacy Guard

You can download GNU Privacy Guard from <http://www.gnupg.org> or the Windows binary version from our website:

<http://www.roxysoftware.com/Downloads/gnupg.exe>

To generate a key pair, open a command prompt, change to the GPG install directory (typically C:\Program Files\GNU\GnuPG) and type:

```
gpg --gen-key
```

A screenshot of a Windows Command Prompt window titled "c:\ Command Prompt - gpg --gen-key". The window shows the following text:

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\geoff>cd \Program Files\GNU\GnuPG

C:\Program Files\GNU\GnuPG>gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2009 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? _
```

Use the default selections. In this case, simply press enter to select 'RSA and RSA'.

```
ca\ Command Prompt - gpg --gen-key
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\geoff>cd \Program Files\GNU\GnuPG

C:\Program Files\GNU\GnuPG>gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2009 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
```

Once again, select the default of 2048 by pressing enter.

```

C:\ Command Prompt - gpg --gen-key
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\geoff>cd \Program Files\GNU\GnuPG

C:\Program Files\GNU\GnuPG>gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2009 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0)

```

Press enter to indicate that the key does not expire, and then type 'y' and press enter to confirm.

```

C:\ Command Prompt - gpg --gen-key

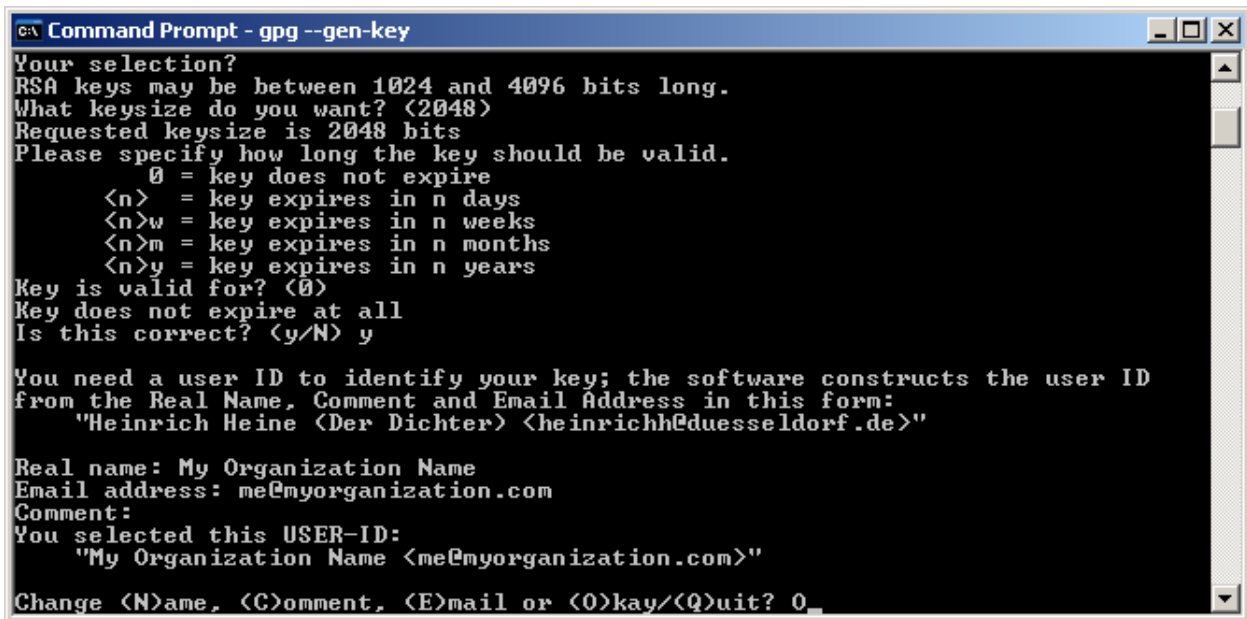
Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name:

```

Enter the name of your organization, and a contact e-mail address. You can enter a comment, or leave it blank. Confirm by typing 'O' (for 'Okay') and press enter.



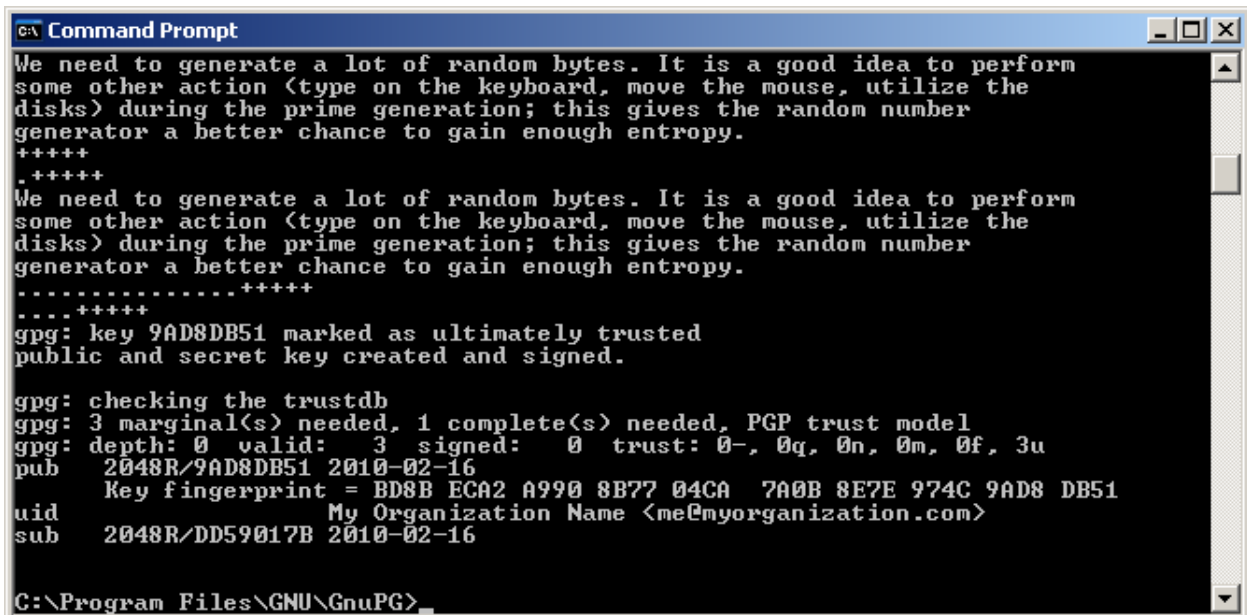
```
c:\ Command Prompt - gpg --gen-key
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? <2048>
Requested keysize is 2048 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? <0>
Key does not expire at all
Is this correct? <y/N> y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
  "Heinrich Heine <Der Dichter> <heinrichh@duesseldorf.de>"

Real name: My Organization Name
Email address: me@myorganization.com
Comment:
You selected this USER-ID:
  "My Organization Name <me@myorganization.com>"

Change <N>ame, <C>omment, <E>mail or <O>kay/<Q>uit? 0
```

Enter a passphrase. You can use spaces, so a phrase is preferable to a simple password. Type the passphrase again to confirm.



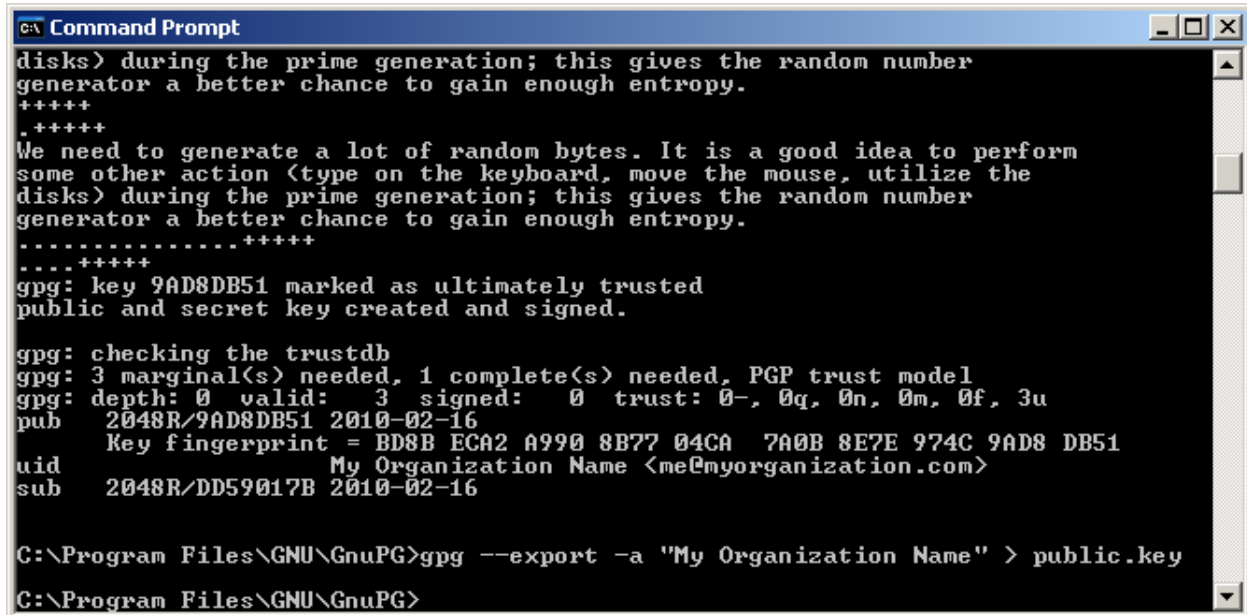
```
c:\ Command Prompt
We need to generate a lot of random bytes. It is a good idea to perform
some other action <type on the keyboard, move the mouse, utilize the
disks> during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++
.+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action <type on the keyboard, move the mouse, utilize the
disks> during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.....+++++
....+++++
gpg: key 9AD8DB51 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed. PGP trust model
gpg: depth: 0 valid: 3 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 3u
pub 2048R/9AD8DB51 2010-02-16
   Key fingerprint = BD8B ECA2 A990 8B77 04CA 7A0B 8E7E 974C 9AD8 DB51
uid  My Organization Name <me@myorganization.com>
sub 2048R/DD59017B 2010-02-16

C:\Program Files\GNU\GnuPG>
```

Your key has now been generated. You now need to export the public key so you can send it to us. Type:

```
gpg --export -a "My Organization Name" > public.key
```



```
C:\ Command Prompt
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
++++
.++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.....++++
....++++
gpg: key 9AD8DB51 marked as ultimately trusted
public and secret key created and signed.

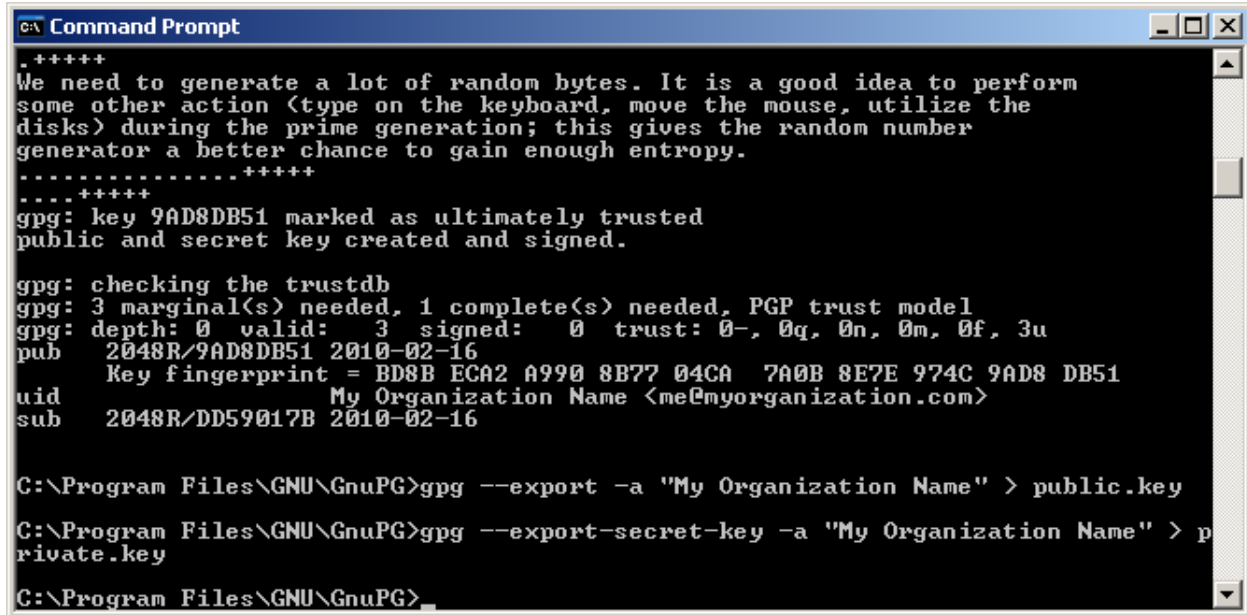
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 3 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 3u
pub 2048R/9AD8DB51 2010-02-16
    Key fingerprint = BD8B ECA2 A990 8B77 04CA 7A0B 8E7E 974C 9AD8 DB51
uid                               My Organization Name <me@myorganization.com>
sub 2048R/DD59017B 2010-02-16

C:\Program Files\GNU\GnuPG>gpg --export -a "My Organization Name" > public.key
C:\Program Files\GNU\GnuPG>
```

You now have a file called 'public.key' that you can send to us. It's okay to send this file by e-mail – it's possible to create an encrypted file with the public key, but it's not possible to decrypt the encrypted file without the private key.

You should also export your private key, and save copies of both the public and private keys somewhere safe. Type:

```
gpg --export-secret-key -a "My Organization Name" > private.key
```



```
C:\ Command Prompt
.,+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.....+++++
....+++++
gpg: key 9AD8DB51 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 3 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 3u
pub 2048R/9AD8DB51 2010-02-16
    Key fingerprint = BD8B ECA2 A990 8B77 04CA 7A0B 8E7E 974C 9AD8 DB51
uid          My Organization Name <me@myorganization.com>
sub 2048R/DD59017B 2010-02-16

C:\Program Files\GNU\GnuPG>gpg --export -a "My Organization Name" > public.key
C:\Program Files\GNU\GnuPG>gpg --export-secret-key -a "My Organization Name" > p
rivate.key
C:\Program Files\GNU\GnuPG>_
```

Getting Started Step 2 – Send Us Your Public Key

Send us your public key file (public.key) by e-mail to support@roxysoftware.com. Do not send us your private key – that's for your use only. The backup we will create can only be decrypted using the private key.

Configure an SFTP Client

To download your backup, you must use an SFTP (Secure File Transfer Protocol) client. Filezilla is a free, open-source file transfer client that supports SFTP:

<http://filezilla-project.org/>

If you wish to script a regular download of your backup, we suggest using putty SFTP (PSFTP):

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

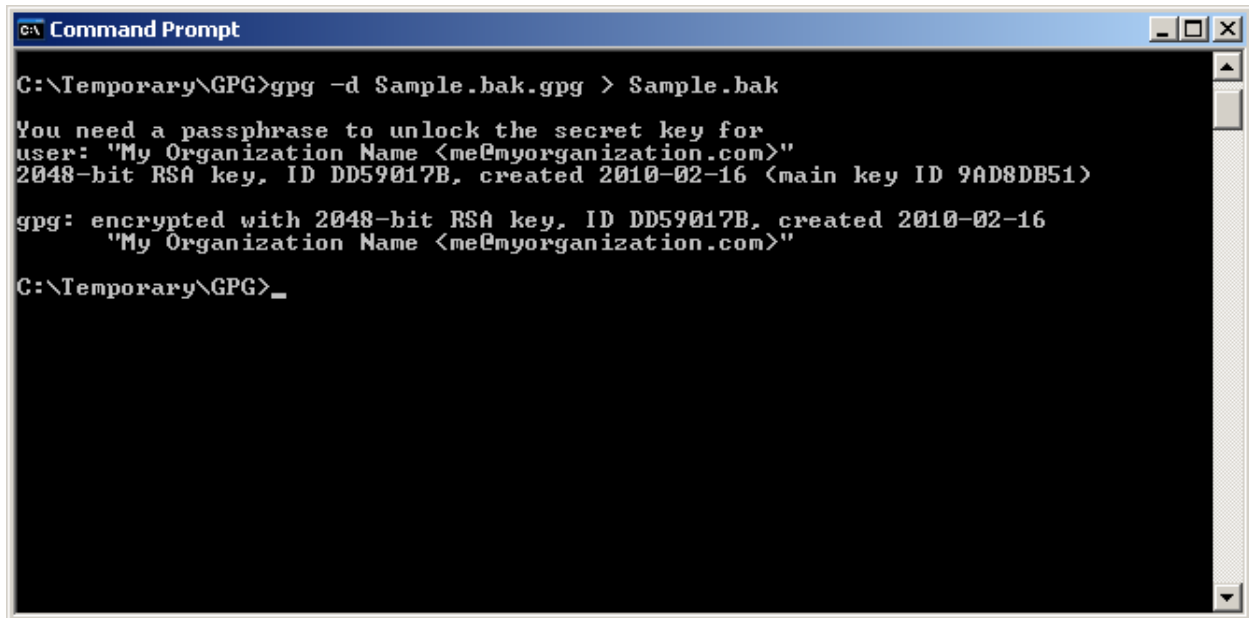
Once you have registered for the service, we will provide you with the SFTP site address, username and password.

Decrypting Your Backup

Once you have downloaded your backup, you will need to decrypt it before you can use it. To decrypt your backup, enter the command:

```
gpg -d Sample.bak.gpg > Sample.bak
```

Where Sample.bak.gpg is the encrypted filename, and Sample.bak is the filename you'd like to use for the unencrypted backup. Enter your passphrase when prompted.



```
c:\ Command Prompt
C:\Temporary\GPG>gpg -d Sample.bak.gpg > Sample.bak
You need a passphrase to unlock the secret key for
user: "My Organization Name <me@myorganization.com>"
2048-bit RSA key, ID DD59017B, created 2010-02-16 (main key ID 9AD8DB51)
gpg: encrypted with 2048-bit RSA key, ID DD59017B, created 2010-02-16
      "My Organization Name <me@myorganization.com>"
C:\Temporary\GPG>_
```