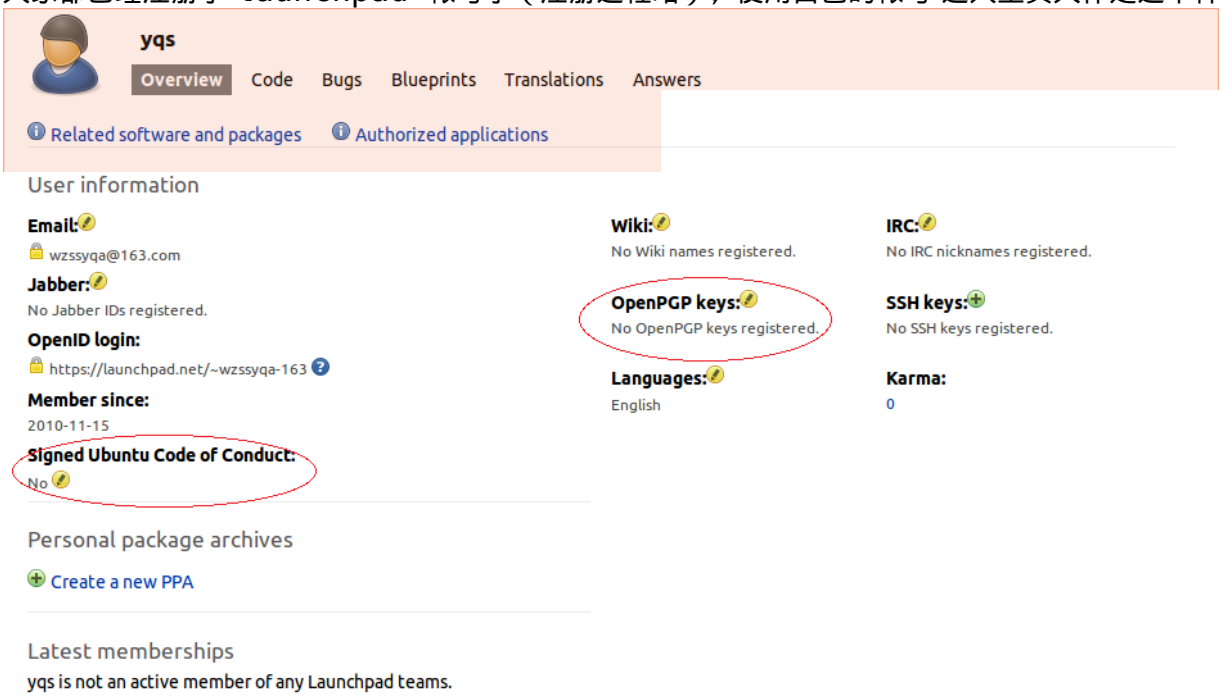
生成 OpenPGP 密钥和签署 Code of Conduct

Wzssyqa

(11-15-2010)

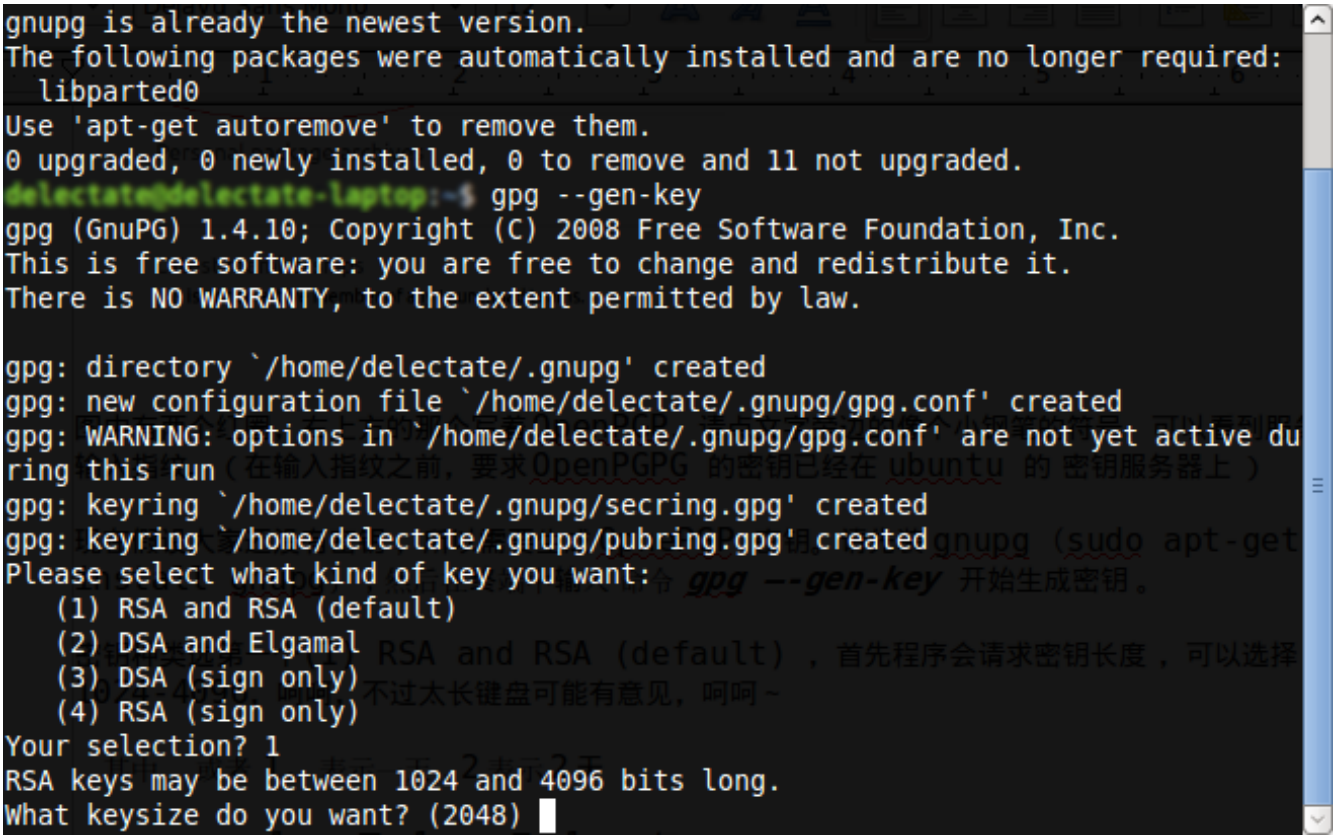
相信大家都已经注册了 launchpad 帐号了（注册过程略），使用自己的帐号 进入主页大体是这个样子



图中有两个红圈，右上方的那个写着 OpenPGP，请点文字旁边的像个小钢笔的符号，可以看到服务器要求输入指纹。（在输入指纹之前，要求你的 OpenPGP 密钥已经在 ubuntu 的 密钥服务器上 ）

现在假设大家还没有密钥，所以需要生成 OpnePGP 密钥。请先装 gnupg （sudo apt-get install gnupg），然后在终端中输入 命令 ***gpg --gen-key*** 开始生成密钥。

密钥种类选第一个(1) RSA and RSA (default) ，首先程序会请求密钥长度，可以选择 从 1024-4096，建议选择 4096，如果需要可以再生成短点的子密钥。呵呵，不过太长键盘可能有意见，呵呵~




```
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)
```

其中， 或者 1， 表示一天；2 表示 2 天； 1w 一周；1m，一月；1y 一年。

然后会问 以上正确吗？(y/n) ，确定正确之后，输入 y 回车

然后会问真实姓名，看自己爱好，最好还是像个名字 lol

```
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? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 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) 1
Key expires at Sat 20 Nov 2010 12:55:22 PM CST
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:
```

然后，会请求输电子邮件地址
随后，输入注释，比如 I am not a donkey.

```
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 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) 1
Key expires at Sat 20 Nov 2010 12:55:22 PM CST
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: 1412
Name may not start with a digit
Real name: addition
Email address: addition@eyou.cn
Comment: i'm not a donkey~
```

这时候，会给个总结，问 是否正确，看看，正确否

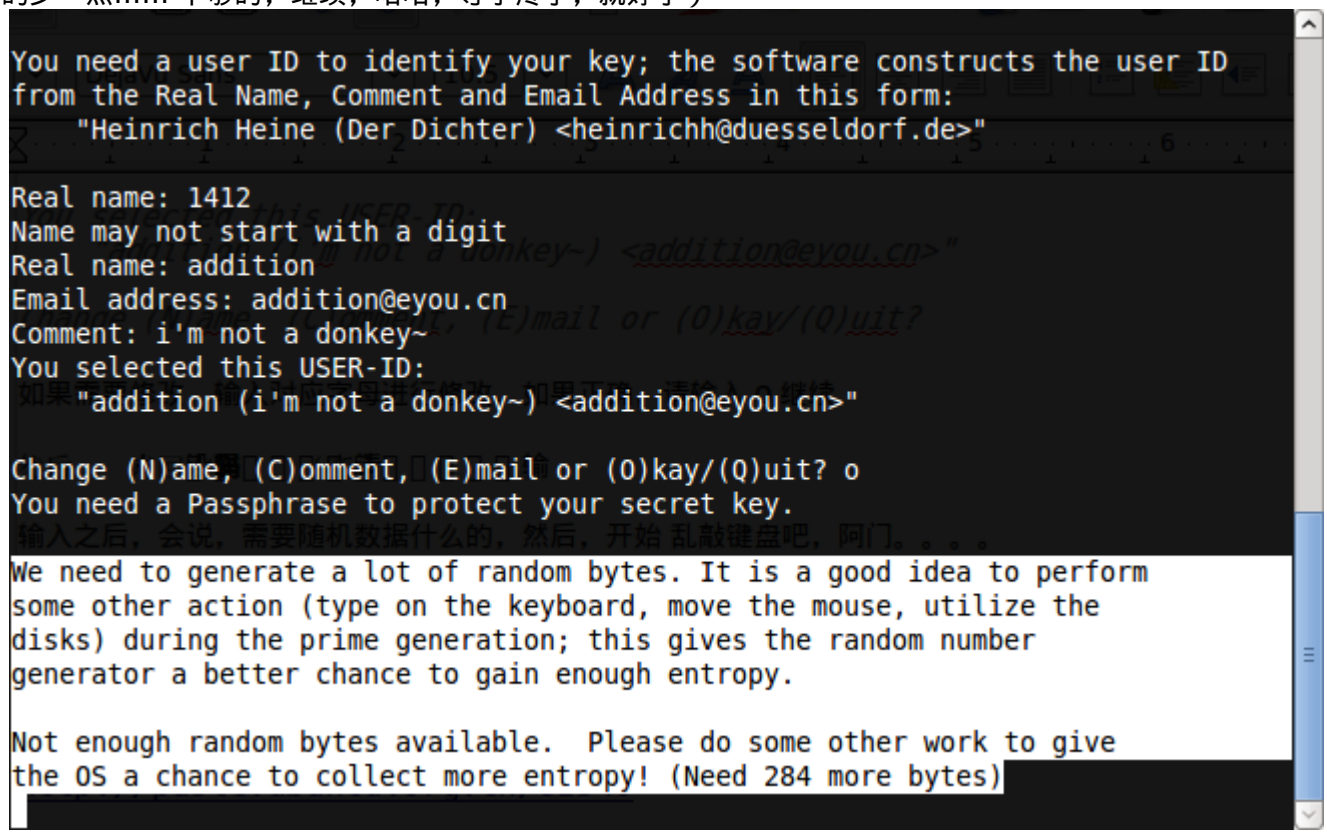
```
You selected this USER-ID:
  "addition (i'm not a donkey~) <addition@eyou.cn>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
```

如果需要修改，输入对应字母进行修改。如果正确，请输入 o 继续

然后，请求输入密码。（密码没有回显）

输入之后，会提示需要随机数据，然后，开始乱敲键盘吧，阿门。。。。（如果刚才选 1024 的话，就输入的少一点..... 不够的，继续，哈哈，等手疼了，就好了）



生成之后的密钥大约会是这个样子

```
gpg: 正在检查信任度数据库
gpg: 需要 3 份勉强信任和 1 份完全信任，PGP 信任模型
gpg: 深度：0 有效性： 1 已签名： 0 信任度：0-，0q，0n，0m，0f，1u
pub   1024R/61574D78 2010-11-15
    密钥指纹 = 9163 4415 C66E E247 25D2  4556 3B67 0BB9 6157 4D78
uid                  YunQiang Su (I am not a donkey.) <wzssyqa@163.com>
sub   1024R/BBF9DC40 2010-11-15
```

其中 密钥指纹 = 9163 4415 C66E E247 25D2 4556 3B67 0BB9 6157 4D78

后边的数字，就是要往刚才的网页里填的（如果已经生成成功了，但是没有看到类似内容，可以使用 ***gpg —-fingerprint*** 看密钥的指纹）

经常使用的密钥服务器，有很多，这里使用 keyserver.ubuntu.com 作为演示。

使用 gpg --fingerprint 查看密钥的简单情况: sub 1024R/BBF9DC40 2010-11-15

gpg --keyserver keyserver.ubuntu.com --send-keys BBF9DC40

其中 BBF9DC40 就是新加了源之后，提示的字符串。

将密钥‘xxxxxxxx 上传到 hkp 服务器 keyserver.ubuntu.com，现在可以试试去 刚才的页面填指纹了。打开页面，然后点 import key 成功后会收到一封邮件，邮件正文中有一部分是一个加密的。（生成证书已经设置邮箱）加密的内容是，一个网址 ，需要点下那个网址，来确认导入。可以使用带有 PGP 功能的邮件客户端，也可以将加密部分复制到一个文本文件中:
比如将如下部分复制并保存到一个文件 a.txt:

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.10 (GNU/Linux)

hIwDPzuU2Lv53EABA/0VlDK8FlDz6u5yaxzcHOowP0V5HZBzRG6WLmtVdS4oEOcp
n9QuSZhKOVciGtE8aiCSIJV6xB7MxPzfpskx8KOb/5HYsKtpeXYOaq0jWKfkWFNx
BGVBhu/MarK8Var83uphEVKceoberoShMfqhBSWJfMnvGJ8+42+pL5X3FNXPYtLA
tAFAqrHAYVuu0O0JinDdqIEOH0qVXEG/LzAa9pAJY1e0bbRgxNgkhyGSy8BDcYkx
xbYhB+zKKvs5YGUcwB7IozVsjwLl2c2yYjX+ULHaSSuk6WBipVYUftyNLqPTFmNw
QacgfzKZ4QQsh0QAaSahKAyYDkLpTSxeB01r7VGUUeufiE/jIOwaXGtLlmA35f11
zBrJ7xhD7+xs3wrjaVpLBO8U40QLPKqspNqT0mZMNrDO382mS6w9tqi91ukPeTTm
Ue6UJa5K3VLawtcTLa1u712yMizLJxN08w7SCS1qidKhb/sgYPzA2gp8GI7sxFxE
1K+iZUw0rzAOZBbDFecb+R/jgDoI9kc0WBnYFROu3ycCG5MIrxnDMZLWp/L4uzFG
xvpm93Fi7rG+7f8e/IOp3kQjqUWnPFXQ8BvxbfOFMWuFc2PKozlbn3HUSsrRyHNM
44uf3cwxg0QncLPEoPfwbhNcR0LAV7YJATV7XeNH1I6GwqY0AQ==
=pkRl
-----END PGP MESSAGE-----
```

然后运行命令: gpg -d a.txt 来解密文件。

解密完成，之后，点那个网址，就可以确认导入密钥了。

看其中的第二步，登录 https://launchpad.net/codeofconduct 下载， 会下载得到一个文本文件。然后对其进行签名
gpg --clearsign UbuntuCodeofConduct-1.1.txt
得到一个 UbuntuCodeofConduct-1.1.txt.sig 文件，将这个文件的内容复制到签署 Ubuntu Code of Conduct 页面中的文本框中。

http://logs.ubuntu-eu.org/free/2010/11/15/%23ubuntu-cn.html（50% start）