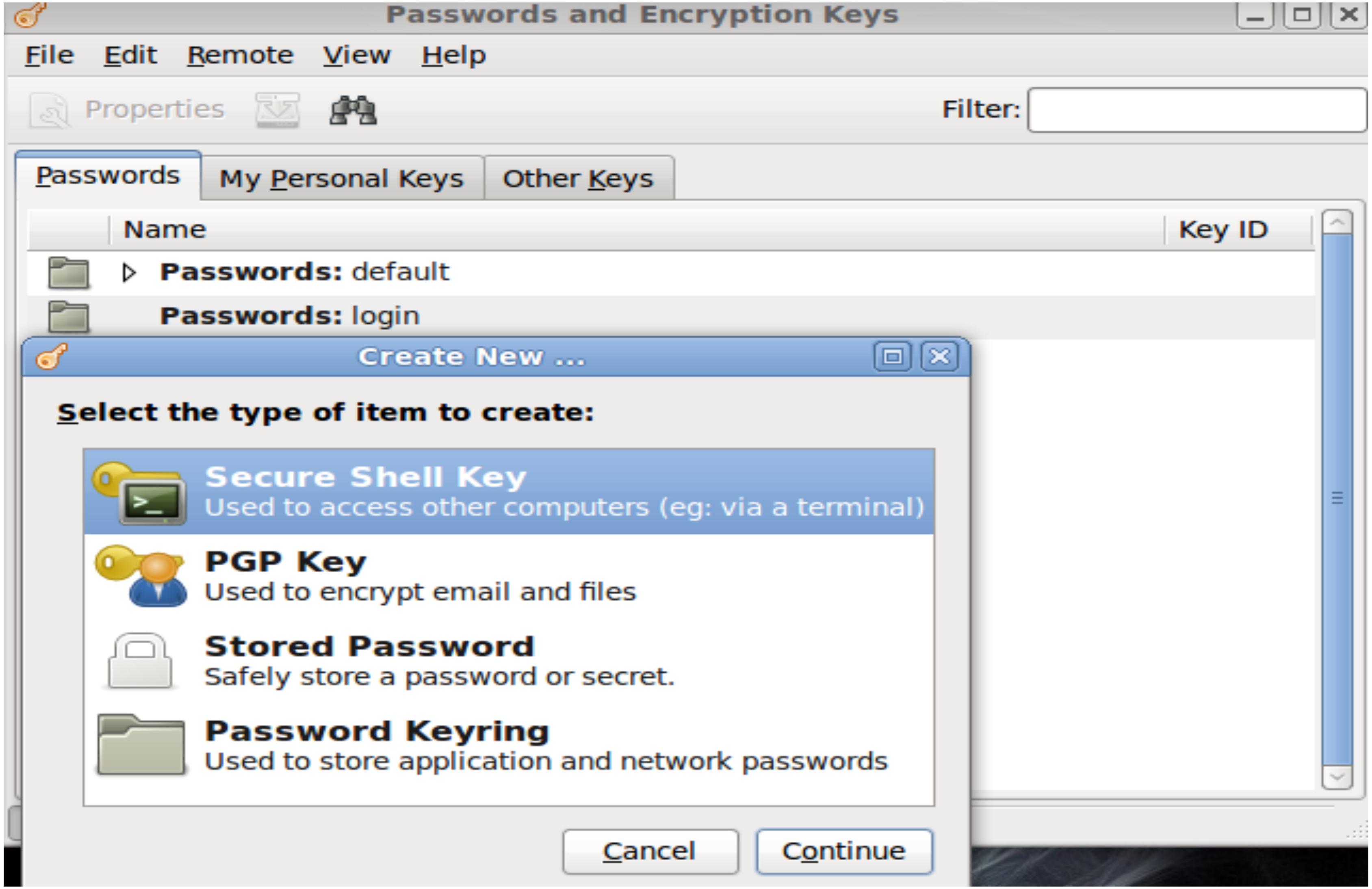
Launchpad GPG & SSH Key Basics

Class on making and importing your own GPG & SSH Key(s) into Launchpad

Making your GPG Key

Ok the things you'll need for this process.
1) Email Client such as Thunderbird.
2) A GPG/PGP Key Plugin for your email client. Enigmail is the one you'll need for Thunderbird.
3) An open Terminal and some patience!
Ok, so first thing you'll need to do is go to Applications -> Accessories -> Passwords & Encryption Keys. Open that up and choose, File -> New -> PGP Key. It should look something like this.



Passwords: default

Passwords: login

Select the type of item to create:

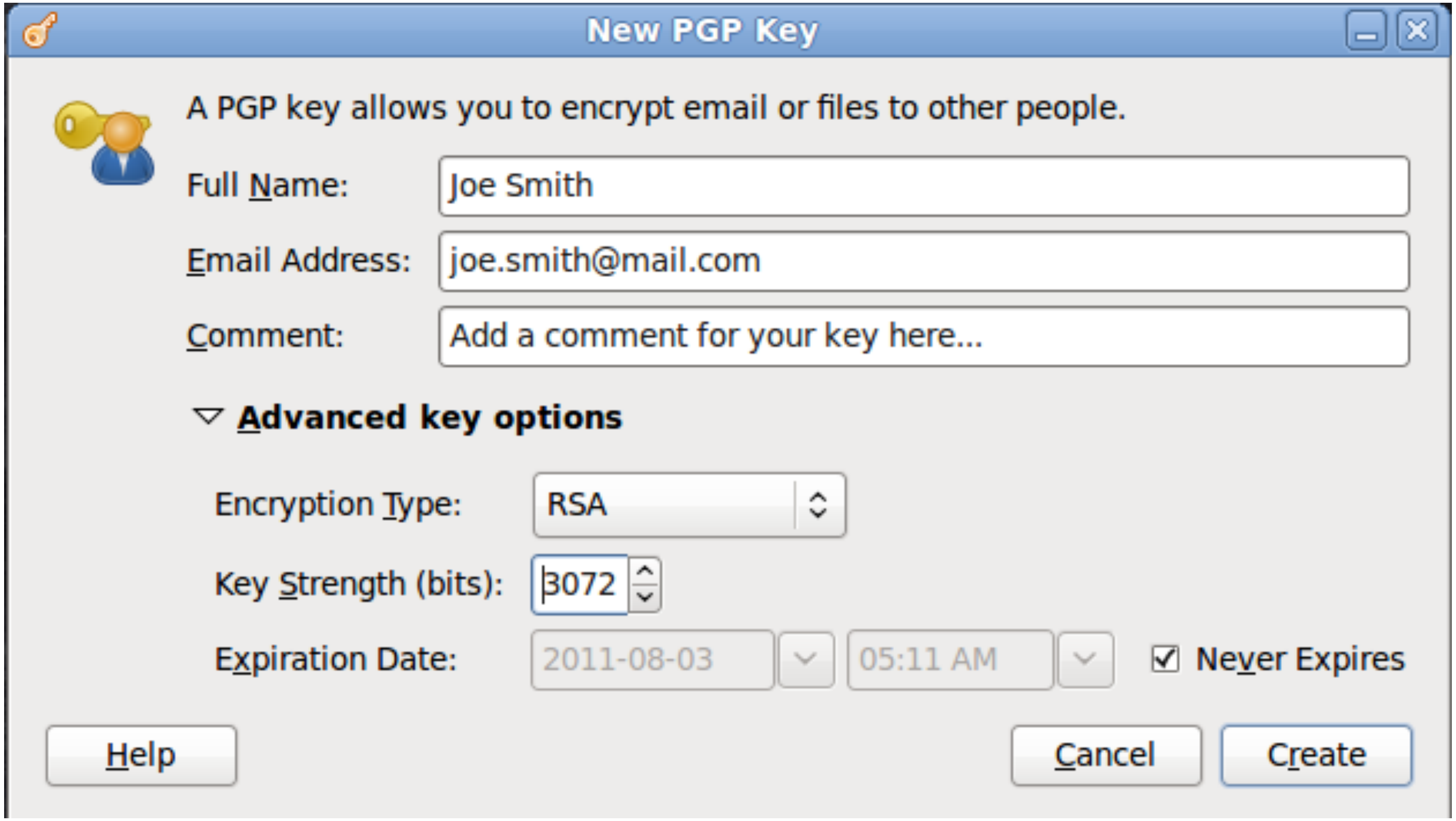
Secure Shell Key
Used to access other computers (eg: via a terminal)

PGP Key
Used to encrypt email and files

Stored Password
Safely store a password or secret.

Password Keyring
Used to store application and network passwords

After you click, "File -> New" and open that window, choose "PGP Key -> Continue" After that you should see a window similar to this: Enter in your info and then click "Create". Note, you can click the "Advanced key options" tab and then choose the key's encryption type, it's strength, and if and when it expires. Usually the defaults are ok to accept. After you click "Create" you'll have a window in which it will ask you to enter a "Passphrase". Choose one and then click "Ok". NOTE: Either save or write your chosen passphrase down as there is no way to recover it if lost thereby making the key useless/invalid. After you're done click create and it will generate the key. Now to push it to the keyserver and then to Launchpad!!!



New PGP Key

A PGP key allows you to encrypt email or files to other people.

Full Name: Joe Smith

Email Address: joe.smith@mail.com

Comment: Add a comment for your key here...

▽ Advanced key options

Encryption Type: RSA

Key Strength (bits): 3072

Expiration Date: 2011-08-03 05:11 AM ☑ Never Expires

Adding your GPG/PGP Key to the Ubuntu Keyserver

Ok so now that you've made your key what we need to do now is push it to the keyserver. To do that we're going to use the Terminal. The Terminal can be found by going to Applications -> Accessories -> Terminal. Open that and then type in the following without quotes. " gpg --list-keys " If it's successful it should display something similar to

```
"/home/zach/.gnupg/pubrin.gpg
----------------------------
pub 1024D/12345678 2010-08-25
uid   Zach Kriesse (My Test GPG Key) <test@zachkriessetest.com>
sub 2048/9ABCDEF1 2010-08-25"
```

Make a note of the public id which in this case is "1024D/12345678" Specifically the last part "12345678" Now because Launchpad doesn't automatically store your key(s) we have to add them to the keyserver. To do that we run the following in the Terminal " gpg --send-keys --keyserver keyserver.ubuntu.com 12345678 " The 12345678 being your own public key ID. If its successful it should display something similar to "gpg: sending key 12345678 to hkp server keyserver.ubuntu.com"

Importing your GPG/PGP Key into Launchpad

Ok so now that we've added our key(s) to the Ubuntu Keyserver we now need to import it into Launchpad. This part is pretty easy and fairly quick. Ok so for Launchpad to know that the key you just imported is actually yours and belongs to you it needs it's personal fingerprint. Much like your own fingerprint it's the unique identifier for that specific key and it alone. Ok so open up your terminal....yes again you gotta open just one more time! Come on you can do it! Ok, in your terminal type " `gpg --fingerprint` " It should output something akin to, "

```
pub   3584R/12345678 2010-08-06
      Key fingerprint = 3D5A 45BC D847 2509 59RT 29TQ 3214 1234 ABCD EFGH
uid                  Billy Bob (My test key for the session...it may be deleted after this is over.)
<email@mail.com>
sub   3584R/123456FG 2010-08-06
```

" What you'll need is the Key fingerprint. Copy that and then go to your Your GPG Key Page and paste your Key's fingerprint into the fingerprint text box and then click import. After that you'll get a message stating that an email has been sent. You'll have to decode this email with the Passphrase you gave for the key back in the first part of this session. NOTE: If the key fingerprint reports an error stating that the key is either invalid or not acceptable don't worry. All you'll have to do is type it in manually. Make sure to put only ONE space between each set of the letters/numbers. Now for the email part.

Decrypting the email

To decrypt the email copy the part of the email that starts with " -----BEGIN PGP MESSAGE----- " and ends with " -----END PGP MESSAGE----- " and save it to your desktop as a .txt file. You may call it whatever you wish. After that open up your terminal and type " cd ~/Desktop " as it's where you should have saved that file. Then type " gpg --decrypt file.txt " File being the name of the file itself. After typing that you will be required to type in your passkey for the PGP/GPG key and then hit enter. The message should now be decrypted and at the bottom of the message there will be a link. Click that, choose confirm on the Launchpad page which is displayed and your key is now imported!