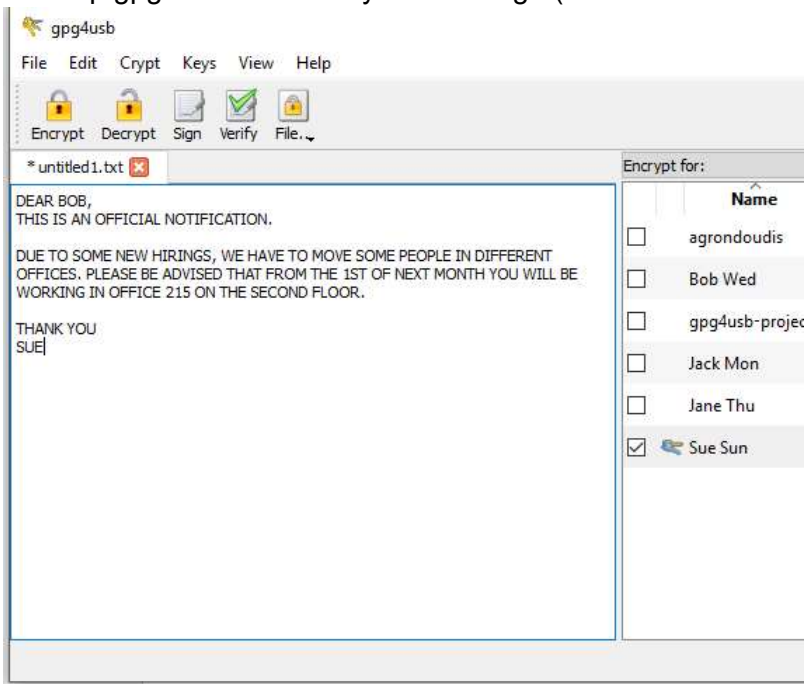
How to sign and authenticate a message

Most of time when we receive a message from somebody we take it for granted that the message is from who it claims to be. However, in certain instances, we might get a spoof (fake) email appearing to be from someone and actually being from somebody else.

In this how-to we'll show you how to sign and authenticate a message using asymmetric encryption and the free portable[1] piece of software called **gpg4usb**[2]. It is assumed that you have already used and configured the software as discussed in "how tp perform asymmetric encryption".

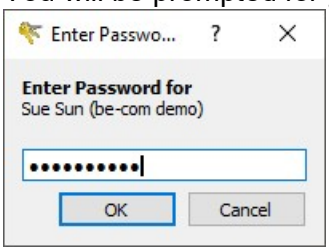
Here are the steps to follow:

1. Start up gpg4usb and write your message (to be authenticated) in the left area



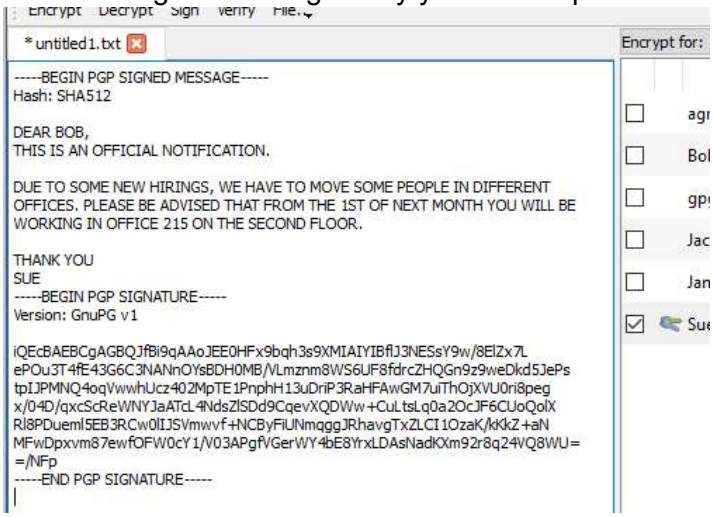
2. Next, if not already ticked, tick the box next to your key and then click the 'Sign' button from the toolbar.

3. You will be prompted for your password, enter it, and press enter or click OK.



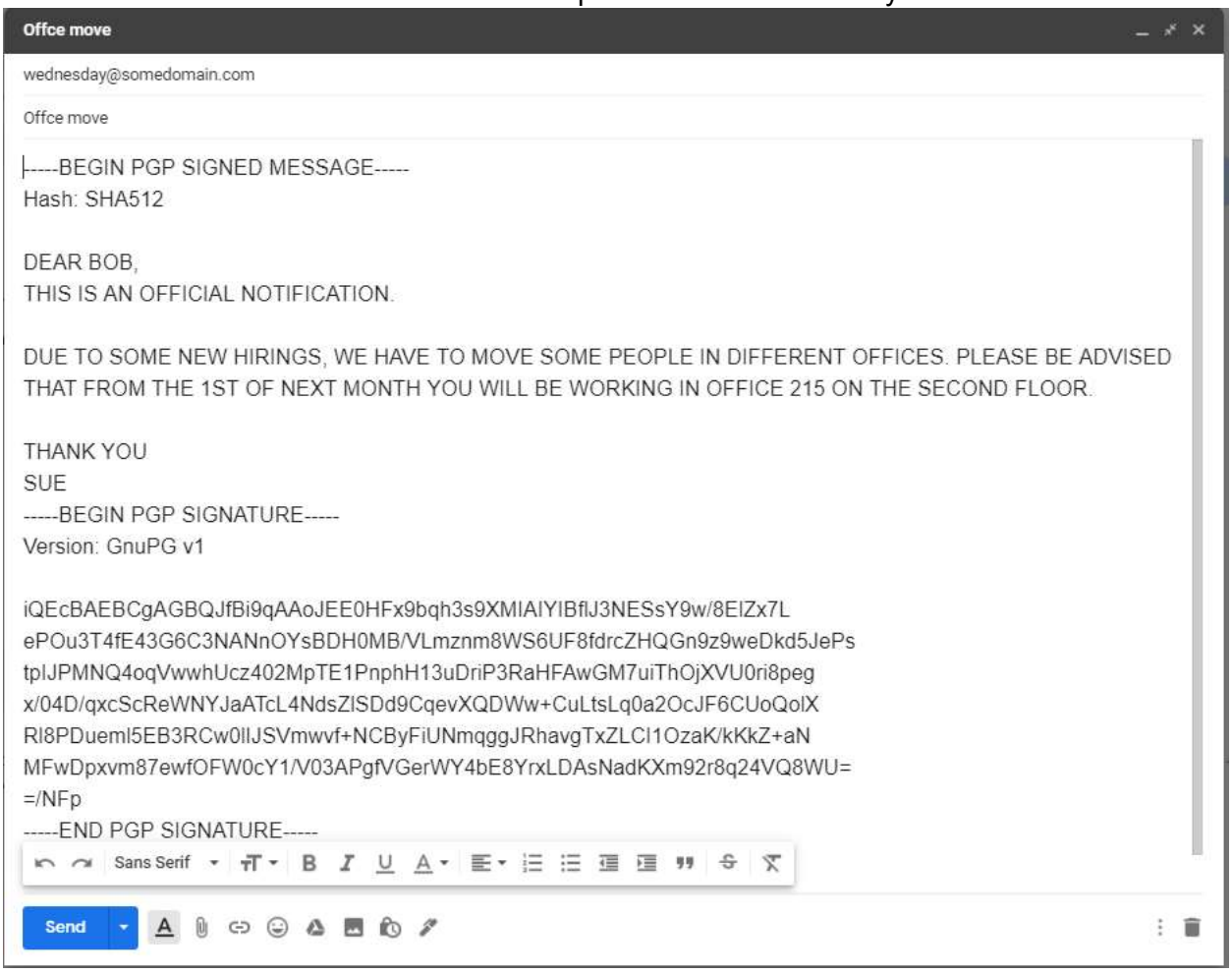
[1] A portable software does not require installation on your computer. Usually it comes in a .zip file and all you have to do is extract it at some place and run it from there. You can even run it form a USB stick.
[2] The version used for this how-to is gpg4usb 0.3.3, released on 2016. It is available for download at: https://www.gpg4usb.org/

4. This message is now signed by you. The capture below demonstrates



5. Notice how the message itself is NOT encrypted. This is not the point. The point is to ensure that the message is authentic and initiates from you. Select the whole text of the area (you can click Edit → Select All) and copy the text

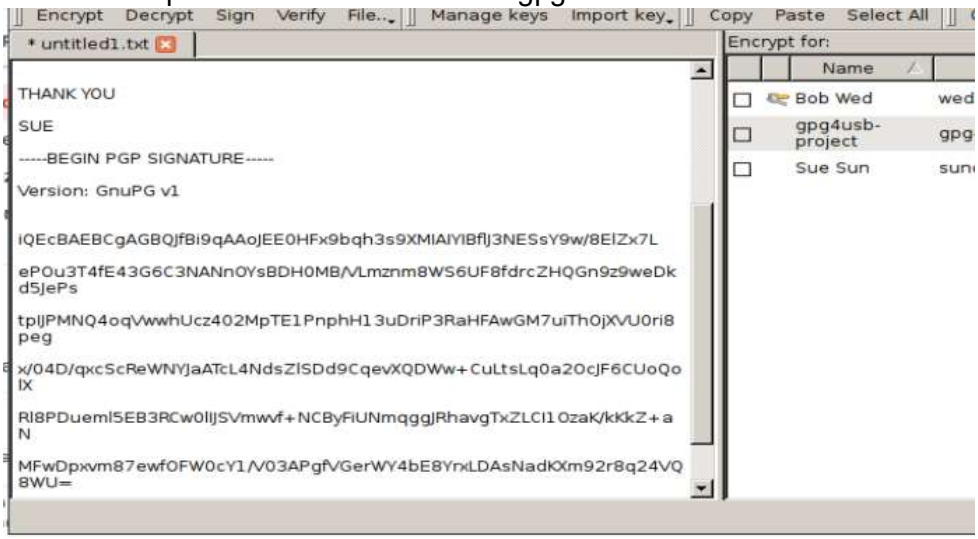
6. Now create a new e-mail to send to Bob and paste the text in the body of the email



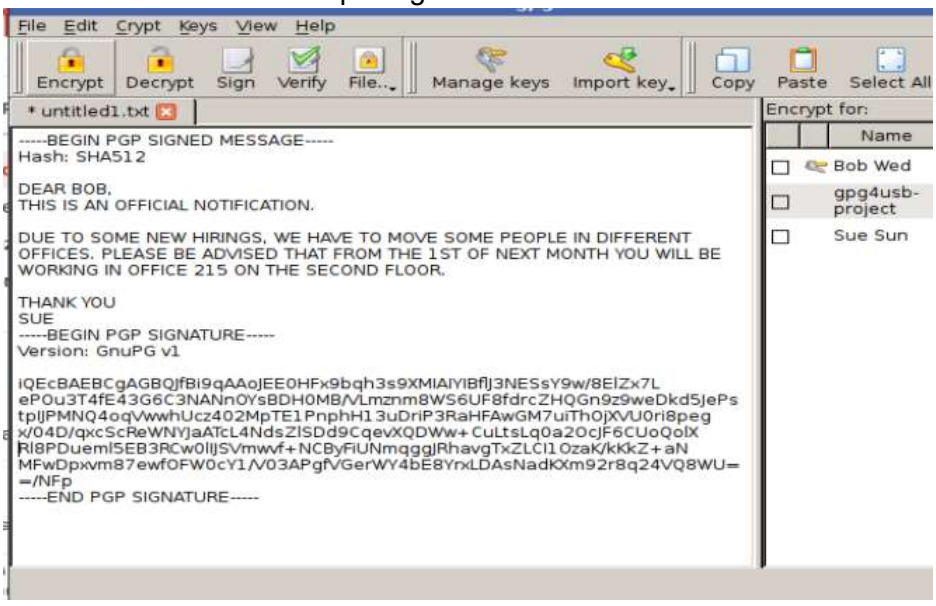
7. Click send to send the message.

On the other side when Bob receives this message he can perform the following steps to authenticate

1. Open up the email
2. Select the entire contents and copy them
3. Paste the copied text in the text area in gpg4usb



4. Use the Edit → Remove spacing command



5. And now click the Verify button from the tool bar. Given that Bob has Sue's public key, the message will be authenticated and the result confirmed to the user

6. So now Bob can rest assured that the message is authentic.

 A digital signature authenticates a message. Authentication is about ensuring that the message is from whom it claims to be and that the message has not been tampered with. It does not matter who sees the message as long as they are assured that the message is authentic.