**Cybersecurity 401**

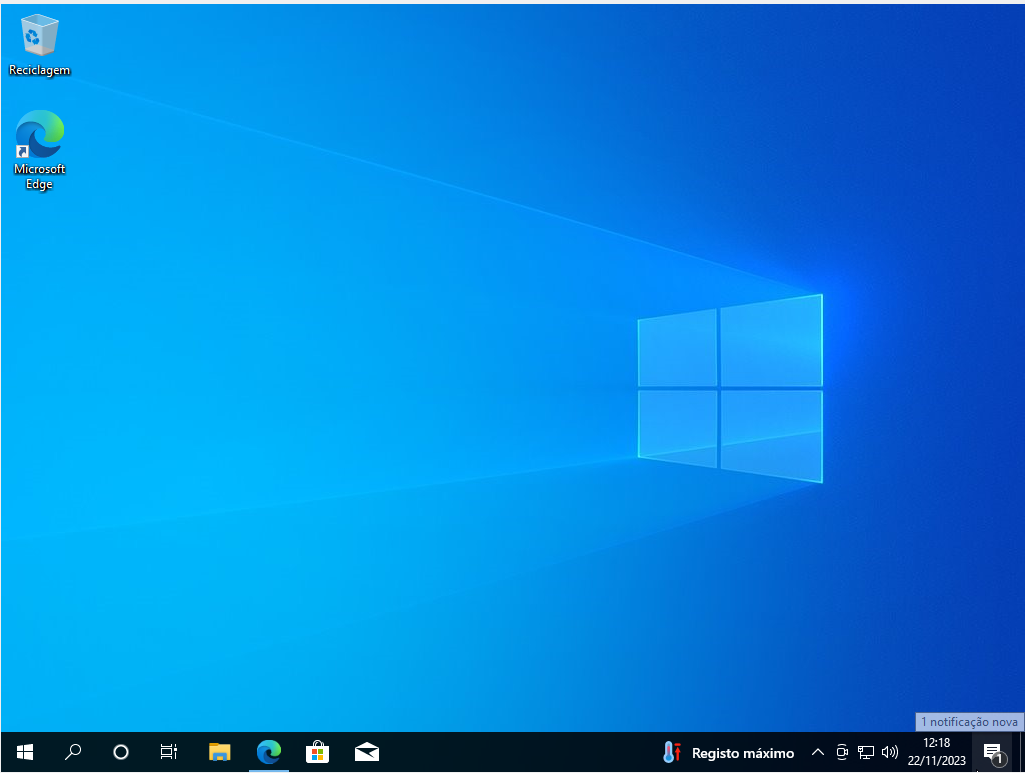
**Module 2 - Data Security**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

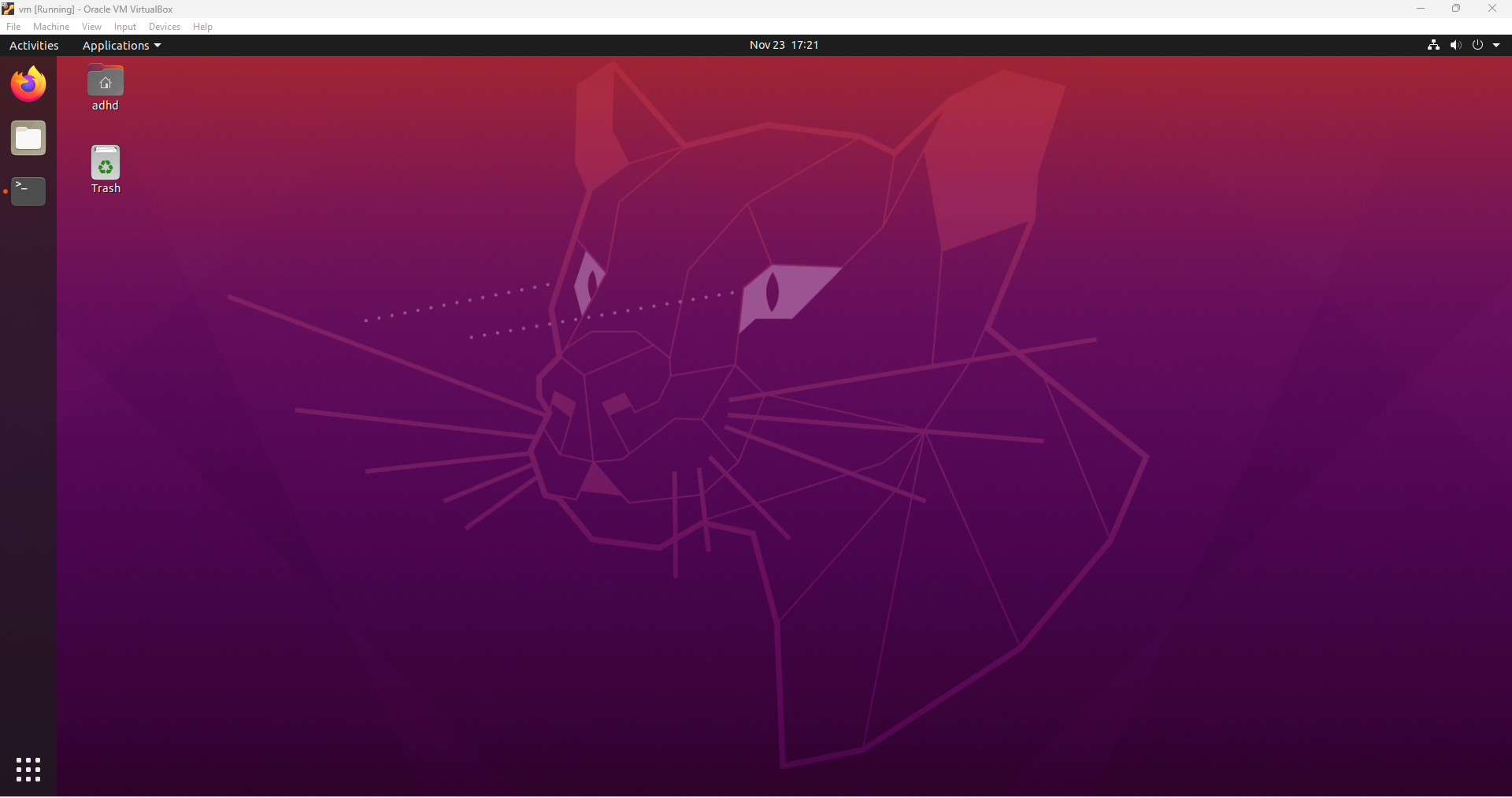
# **Lab 09 - Public Key Infrastructure (PKI)**

**| Rodrigo Brasil 11/2023 |**

## **Part 1: Staging**



Windows 10 VM



Ubuntu VM

### Windows VM Setup

#### Download Gpg4win

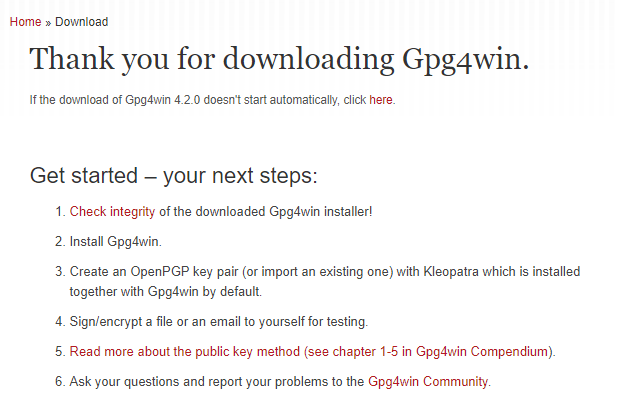
### 

Gpg4win stands for (GNU Privacy Guard for Windows) and is free software for file and email encryption.  
You can download Gpg4win in here: <https://www.gpg4win.org>

Click the big green download button



It will ask if we want to donate to support development, feel free to do it if you want but we will click the $0 to download without donating



After downloading, it will show this page and it will start downloading automatically



It will download an exe file to your Downloads folder



It will look like this

#### Install Gpd4win

### 

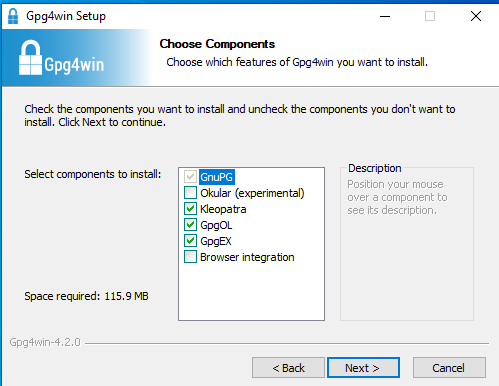
When executing the exe file, it will asks to choose a language for the setup

Feel free to choose your language or one that you understand

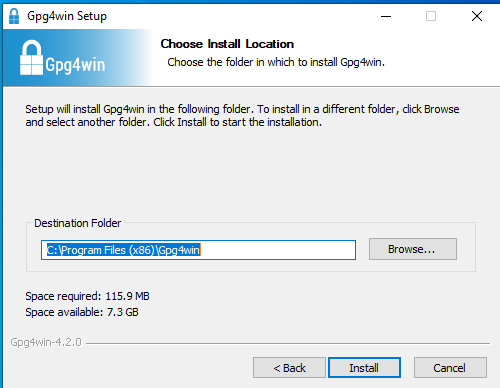
For the purpose of this exercise i will choose English



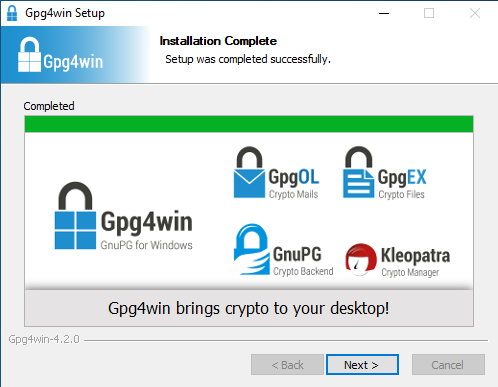
After choosing a language it will show a welcome message, click next



Next it will ask to choose components we will leave them at default, and click next



Next it will ask where we want to install it, we will leave it at its default location and click install

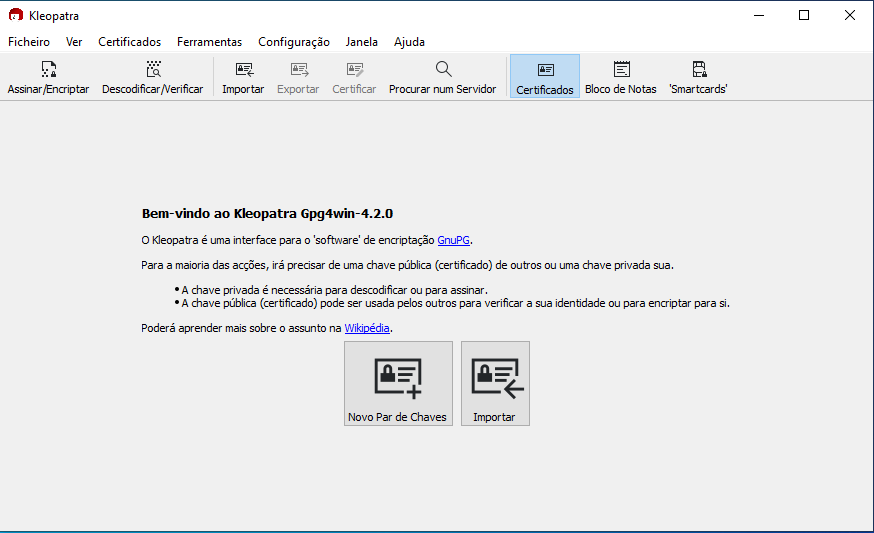


It will start installing, when complete click next.



After completing, there will be 2 checkboxes, one opens kleopatra and the other one shows the README file.

Leave them at default

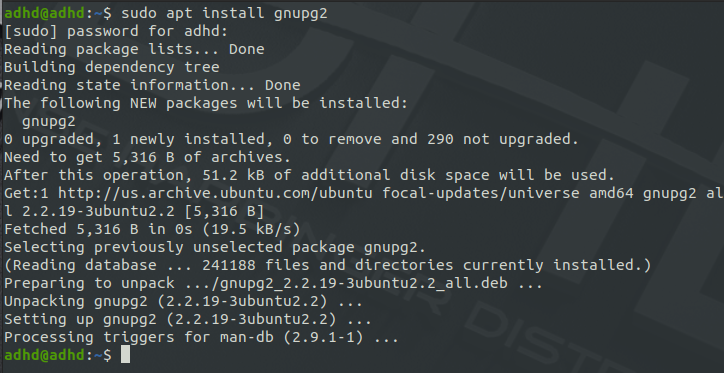


Kleopatra will look like this

Has it says in the program its a encryption software to create and manage asymmetric encryption keys.

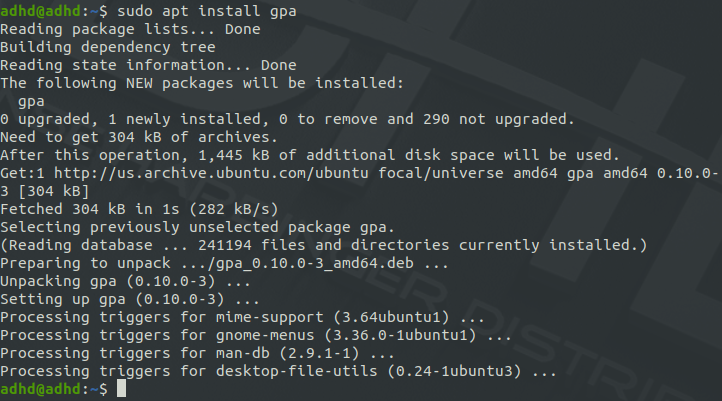
### Ubuntu VM Setup

#### Download and install gnupg2 and gpa



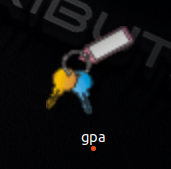
To install gnupg2 and depending on the distro you are using open the terminal and type the command:

“**sudo apt install gnupg2**”

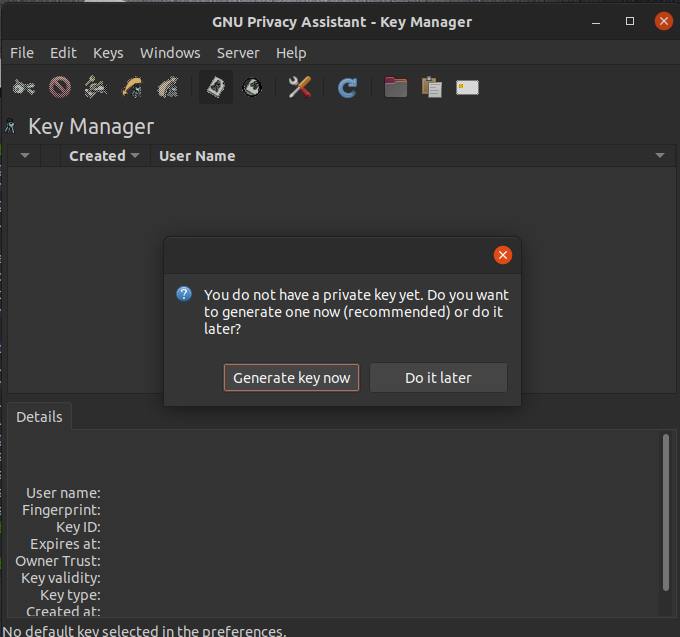


To install gpa type the following command:

“**sudo apt install gpa**”



After installing gpa depending on your distro you will have this icon on your applications



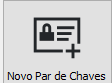
After opening it it will look like this

## 

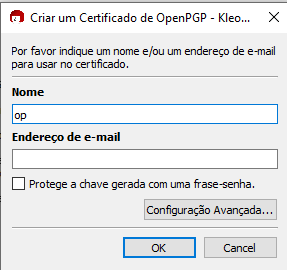
## 

## 

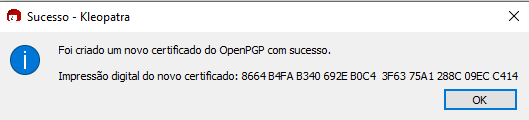
## **Part 2: Message Encryption with Gpg4win on Windows 10**



To create new keys click the new key pair

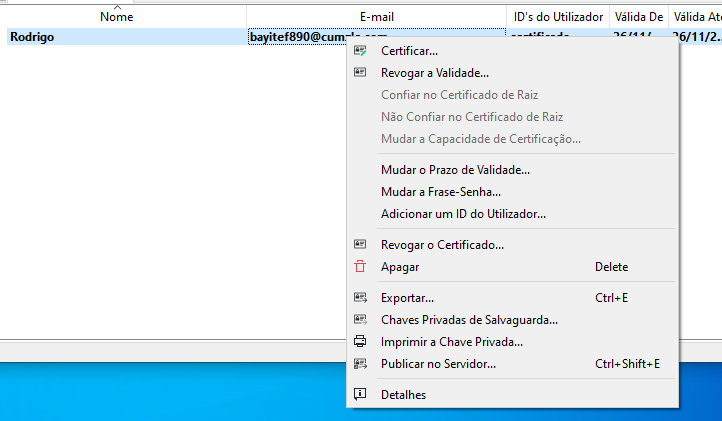


In here we will give a name and a email address to associate with the keys



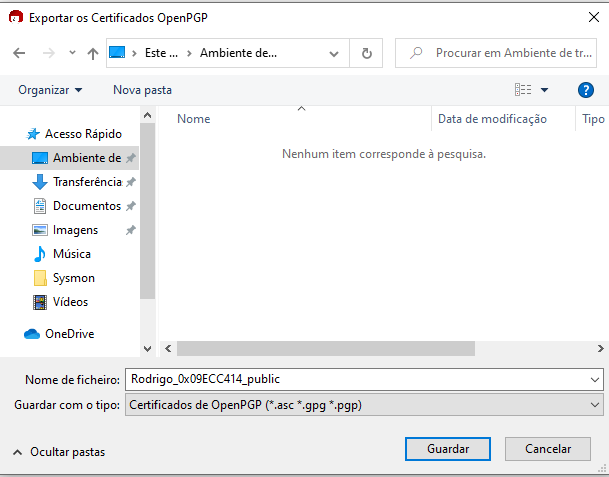


After providing the details it will look like this



Now we need to export the key as an OpenPGP certificate.

To do so right click it and click export

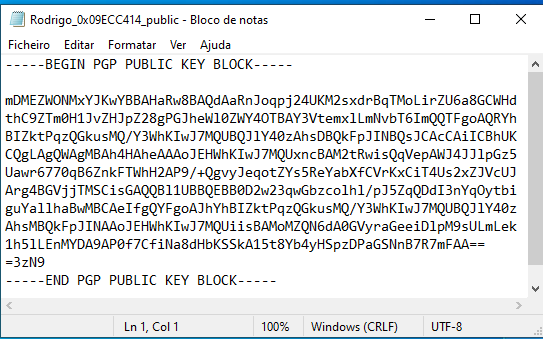


It will ask where we want to save it.

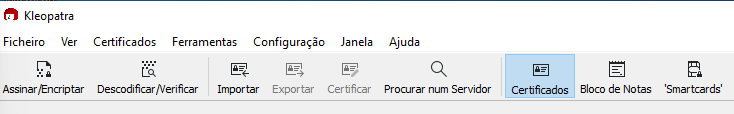
We will save it to the desktop for convenience.



The certificate file will look like this

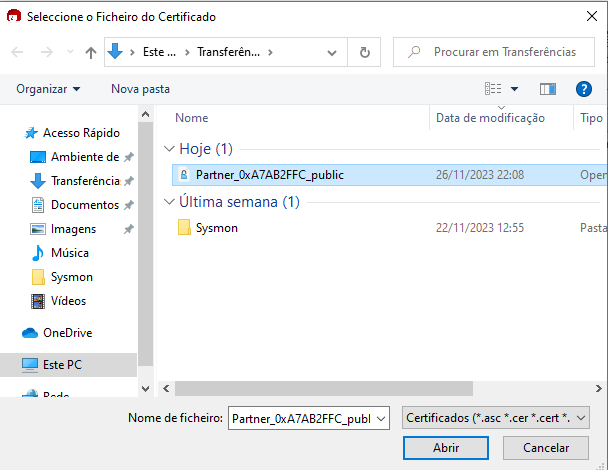


The certificate seen in notepad shows the public key





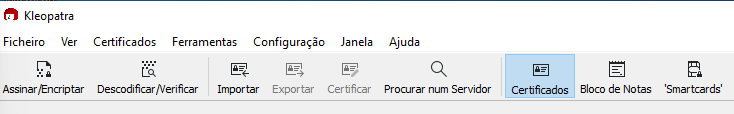
To import the key from the partner you need to import it using the import button located on the top of the GUI.



When clicked it will ask where it is, in this case is in downloads

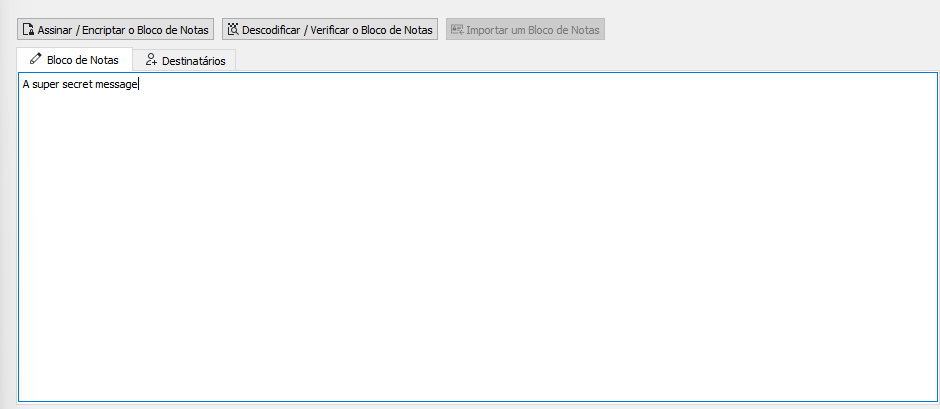


After being imported it will look like this



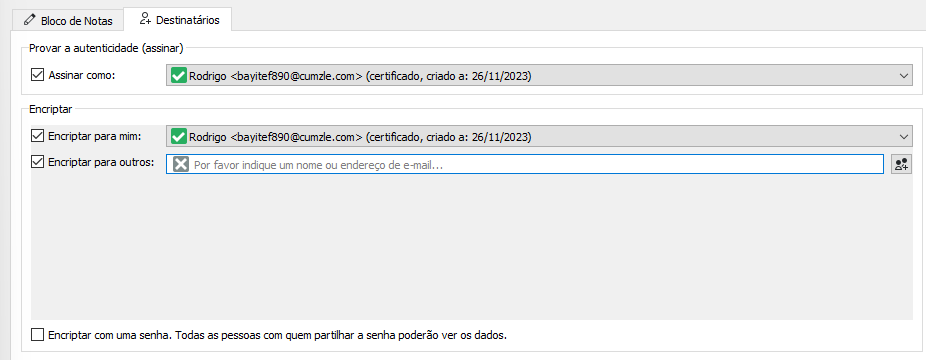


To send a message click the notepad icon located on the top bar as well.



The notepad will look like this.

Inside, write your super secret message!



To send to your partner click recipients and in encrypt to others

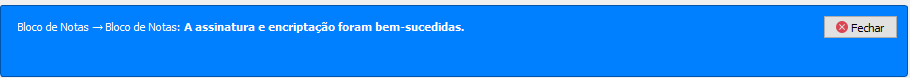




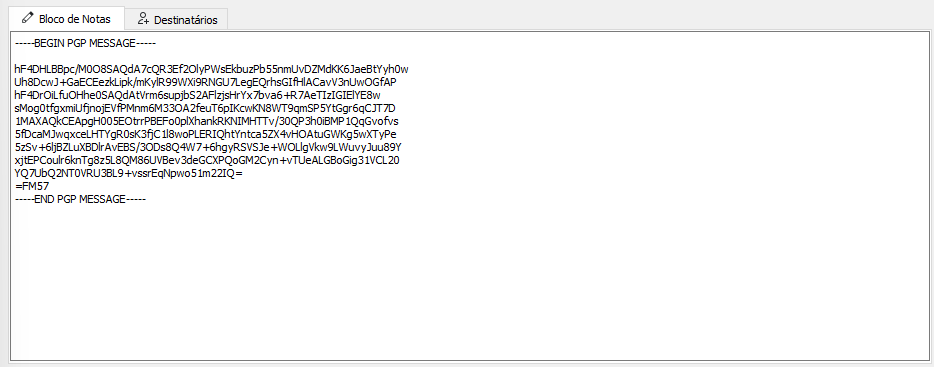
Search the name of your partner and select it



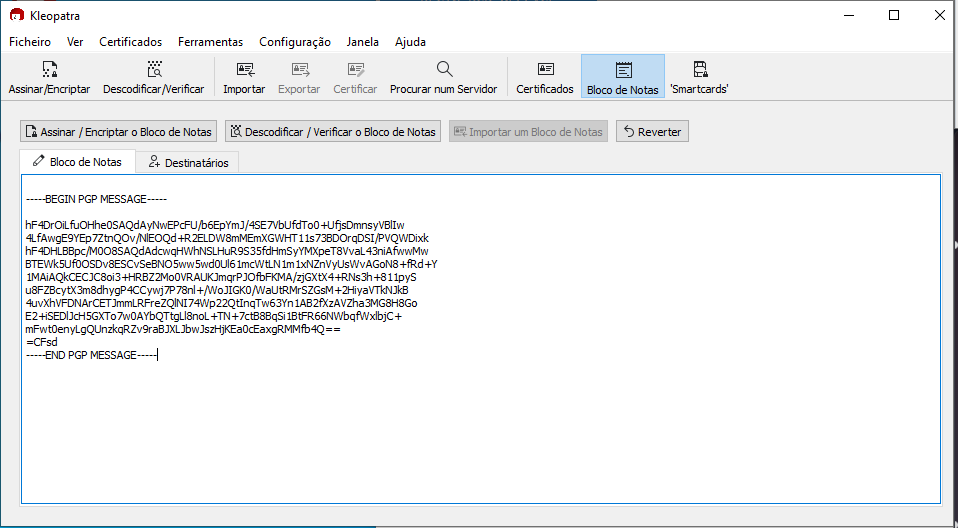
And click sign/encrypt notepad



It will give this message

Click again on notepad and your super secret message will now be encrypted!

Copy it, send to your partner and wait for his encrypted message



After receiving your partner encrypted message, paste it on the notepad



And click decode/verify notepad



And the message will be decrypted with information validating the message came from your partner!

### 

## **Part 3: Email Encryption with GPG on Ubuntu Linux Desktop**

### 

## **Part 4: Certificates and SSL with OpenSSL**

### 

## **Part 5: Reporting**

* How can public key encryption utilities ensure integrity and confidentiality of data between two parties?
* Is PGP a secure protocol to be using?
* Why is PGP not very popular among casual computer users?

Identify a website on the internet that does NOT have HTTPS (SSL) encryption in place.

* Why do you think the website lacks SSL encryption?
* What steps should the web administrator take in order to reconfigure the site to use SSL encryption?