How to encrypt email on Microsoft Outlook

Outlook in Microsoft Office's office suite is one of the popular Windows email tools used by professionals and businesses.

Outlook in Microsoft Office's office suite is one of the popular Windows email tools used by professionals and businesses. Therefore, there will be several times when you want to send sensitive emails or confidential documents to ensure only recipients can access them. Therefore, most of the current email services mostly use email encryption (SSL / TLS) to ensure absolute security. However, this type of encryption can only protect email when it is transmitted over the Internet. When email is in a static state in the inbox, anyone who has access to your email account can read it.

How to encrypt email on Microsoft Outlook?

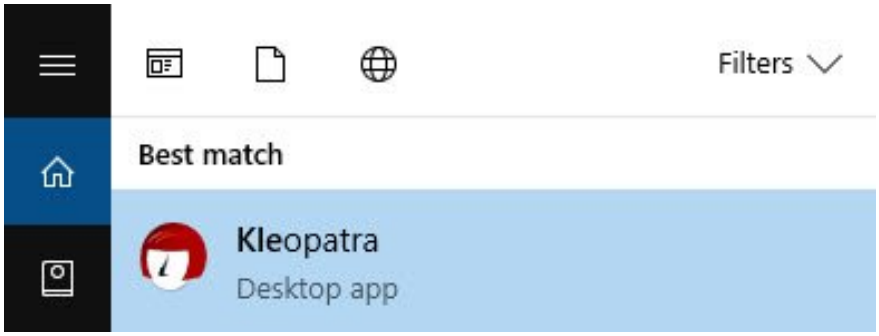
1. Encrypt Email in Outlook with GPG
2. Encrypt email in Outlook with a digital certificate
    1. Get a free digital certificate
    2. Enter a digital certificate (Chrome User)
    3. Install S / MIME Control

Encrypt Email in Outlook with GPG

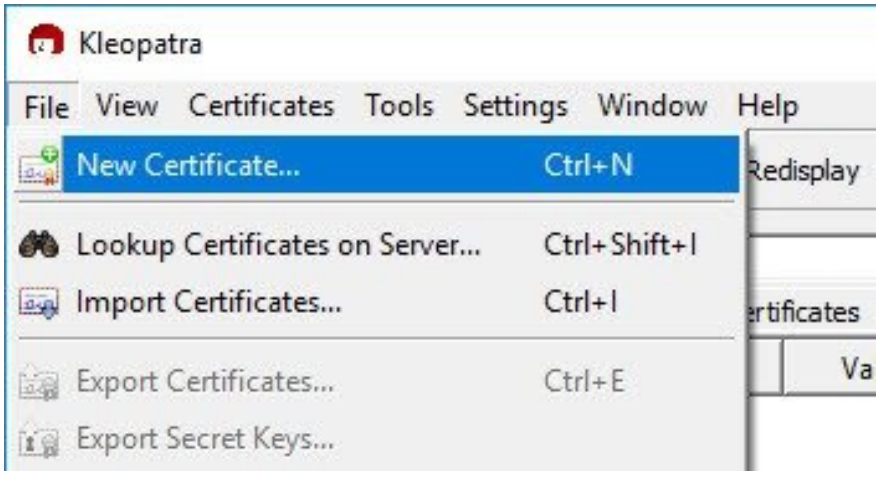
To ensure that only recipients can access your email, you can encrypt your email using GPG (GNU Privacy Gaurd) to use the public and private key. Here's how to encrypt emails in Outloook using GPG.

In Outlook, we will use free software **Gpg4win** (OpenPGP support) to encrypt email. Download and install Gpg4win like other software. This software will install the **plugin that** requires encryption and decoding of recipient email in Outlook.

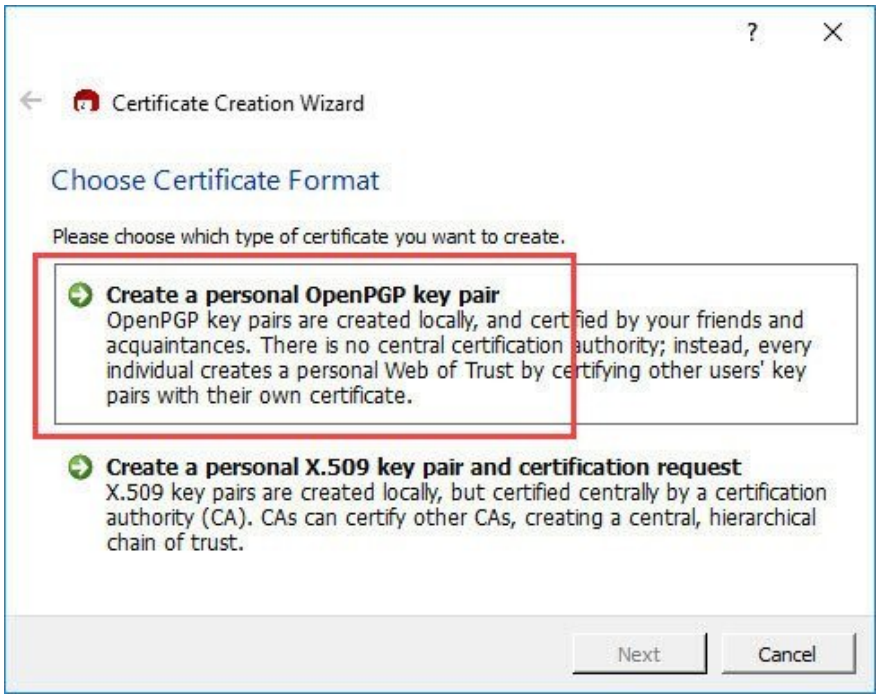
Complete installation, search and open **Kleopatra** in the **Start** menu. Here, you can create the primary key and enter the public key if necessary.



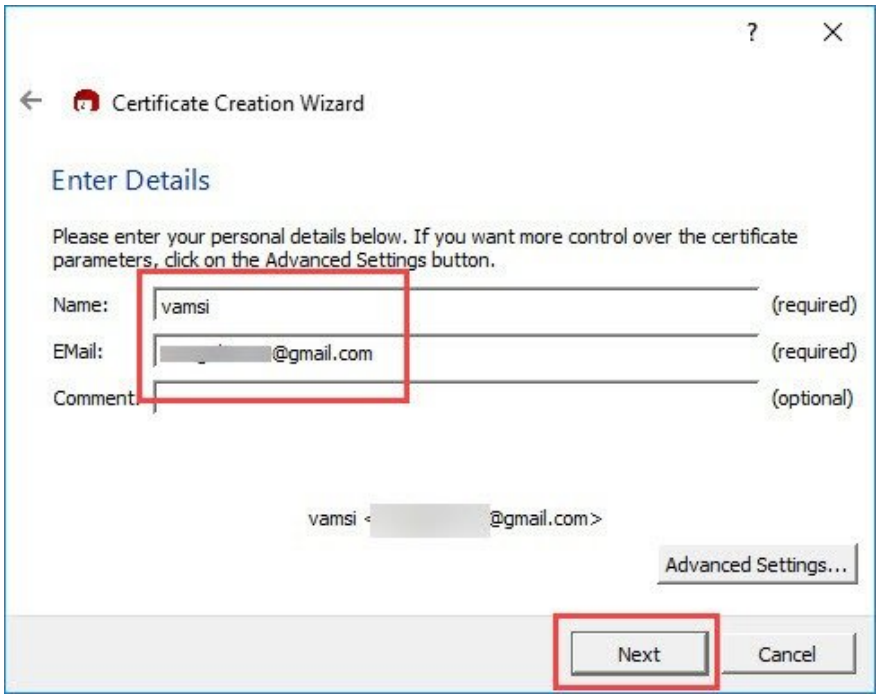
After Kleopatra opens, click **File** and select the **New Certificate** option.



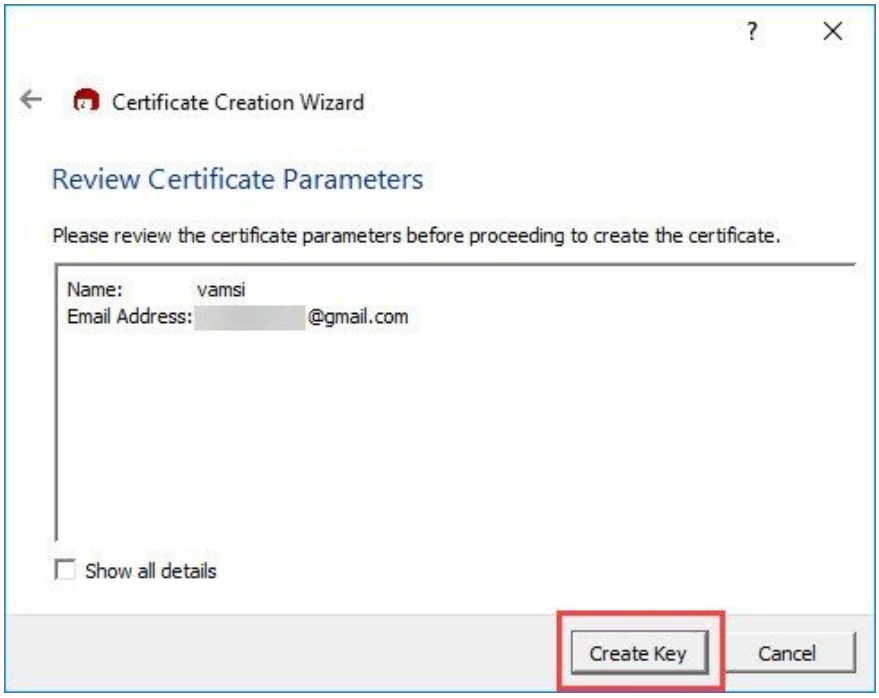
The new window appears, select the first option **Create a personal OpenPGP key pair** and click the **Next** button.



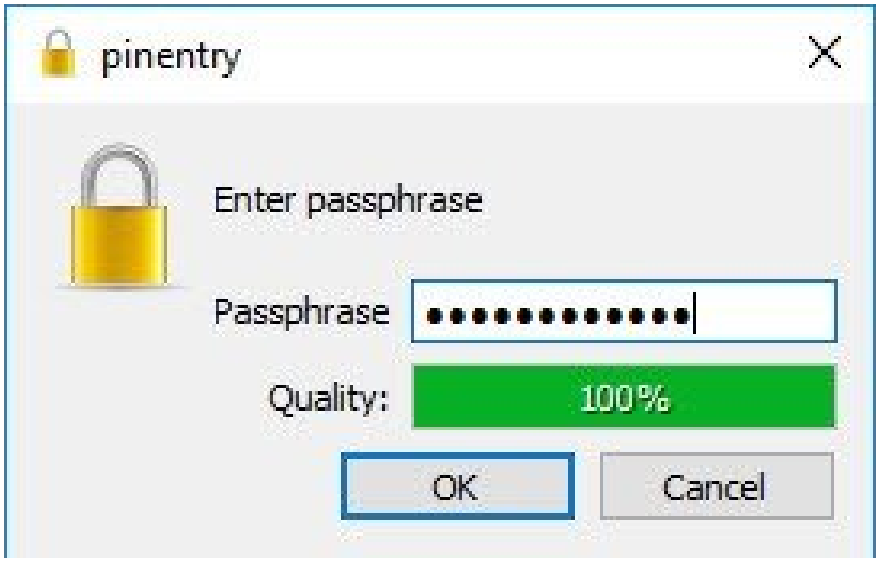
Next, enter the name and email address you want to create the primary key. The key pair will be associated with that email address.



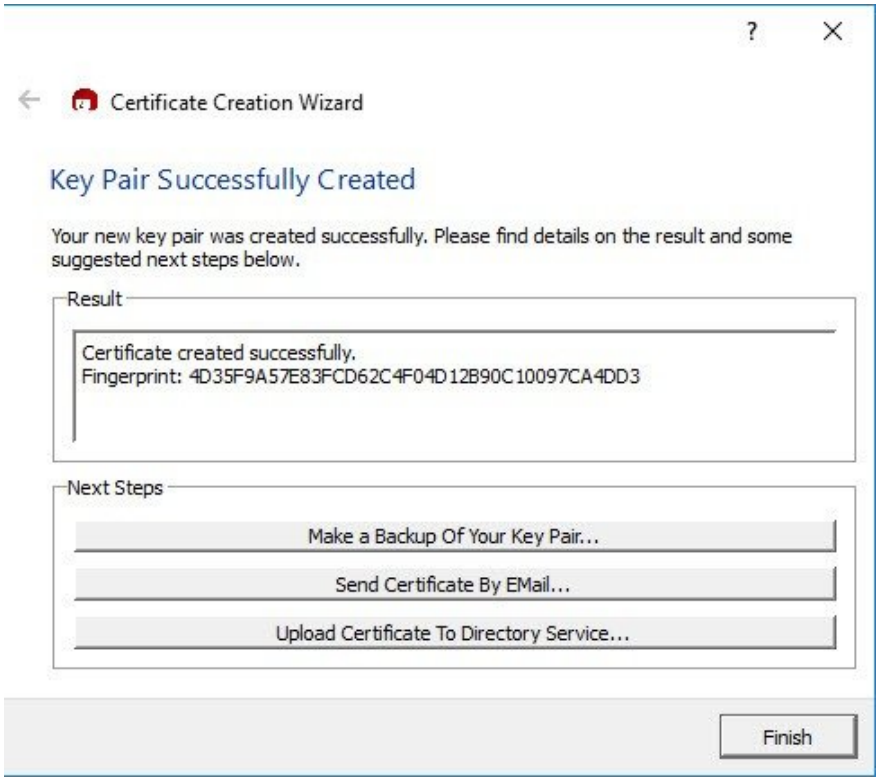
Now, review your information and click **Create Key** .



Enter the strongest security password for the lock code and click **OK** . You will be prompted to re-enter the password, enter the same password to continue.



This will create a code containing the public and private keys. In addition, a backup copy of the key pair can be created to keep it safe by clicking **Make a Backup of Your Key Pair** .

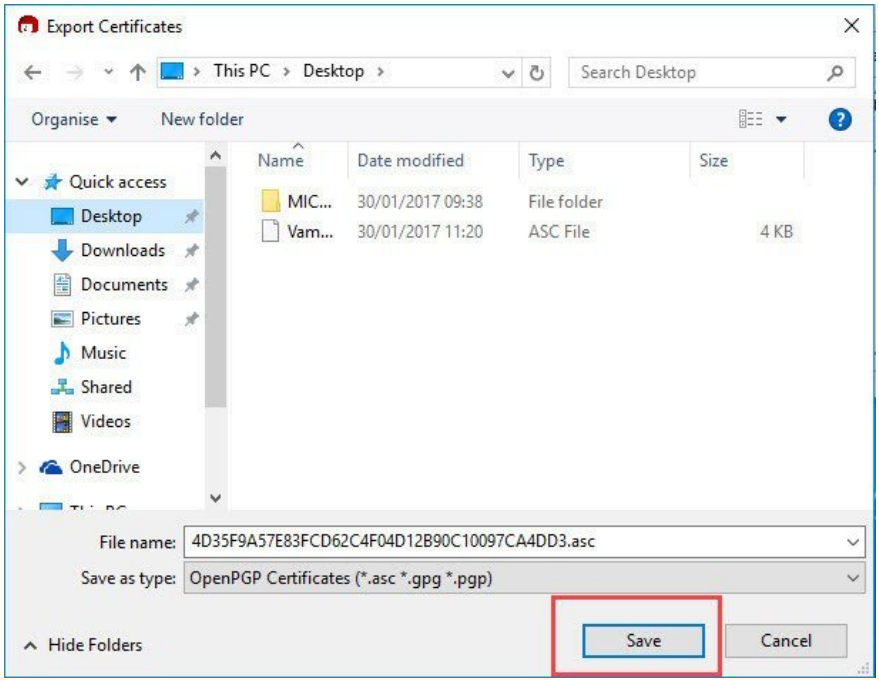


Public Key : Use to encrypt email. So you can share the public key for anyone you want. If someone wants to send you an encrypted email, they must use your public encryption to encrypt the mail.

Private Key : Use to decrypt encrypted email. You should never share personal code. Furthermore, the private key decodes only the messages encrypted by your own public key.

To export the public code, select **Your Certificate** on the main window and select **Export Certificate** .

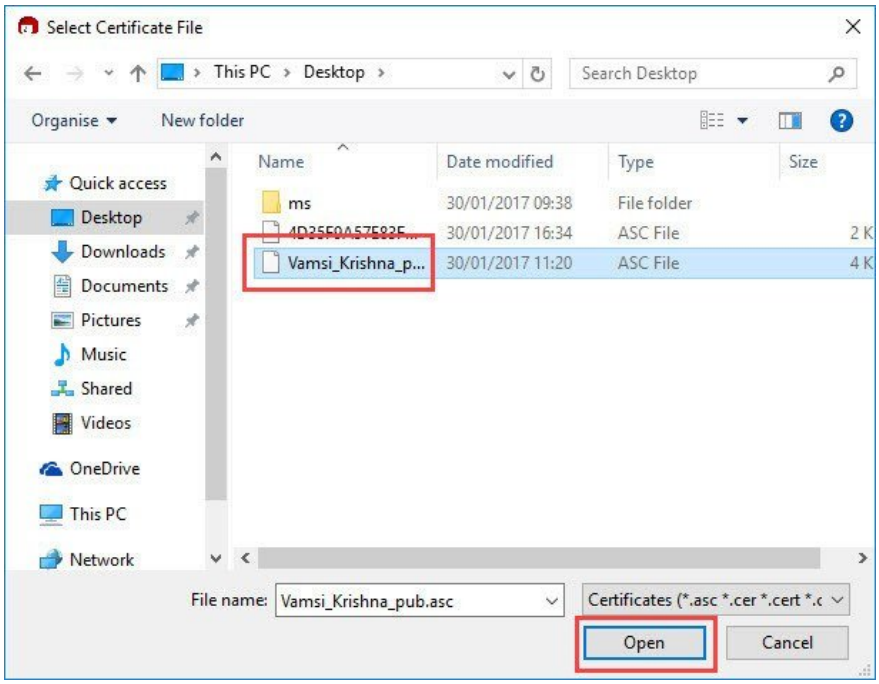
Select the destination and click **Save** . By default, the fingerprint will be used as the file name. You can change the file name if necessary.



Once the email has been exported and saved, you can share it publicly anywhere like forum or website, .

As I said earlier, if you want to send encrypted email, you must use the recipient's public key to encrypt the email. You must enter the recipient's public key before performing that task.

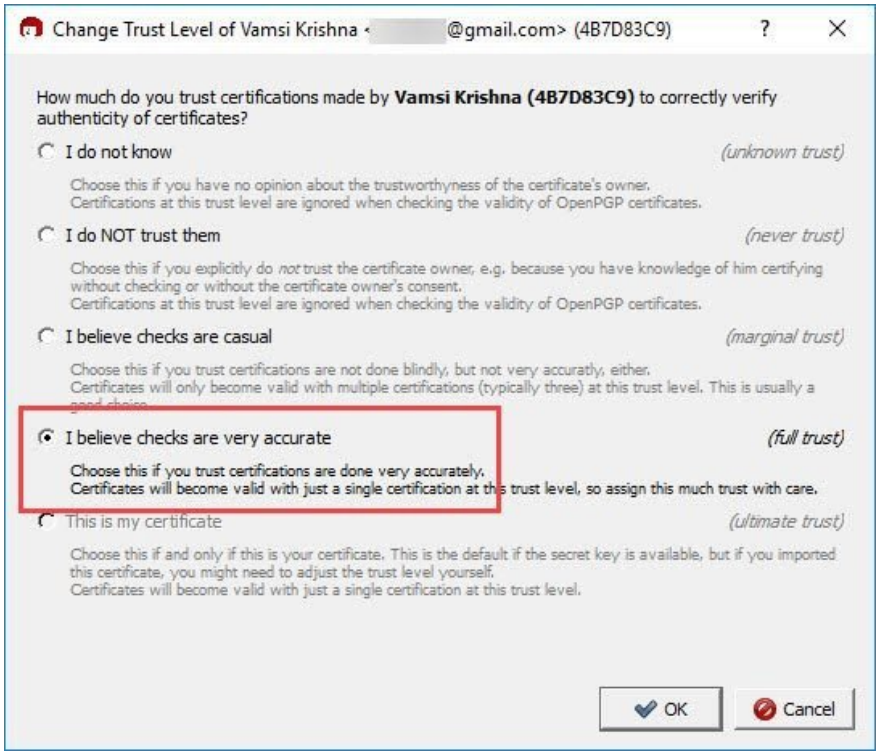
To receive the public key, ask them and download it. In Kleopatra's main window, click **Import Certificate** . Choose that information.



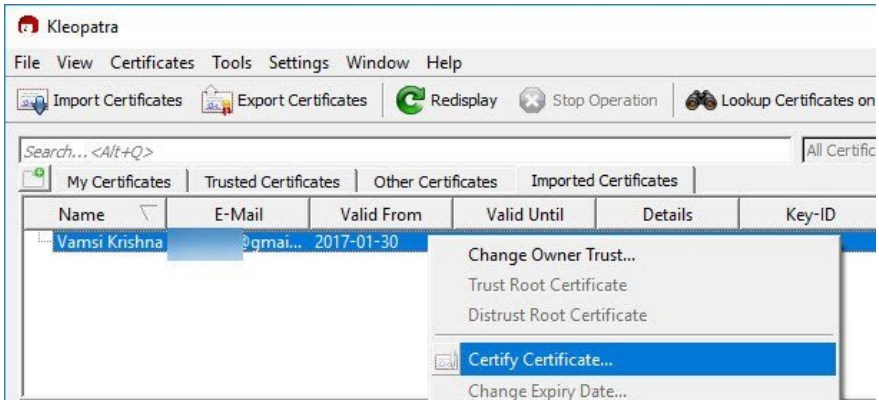
The above operation will enter the public key. Before using it, you need to make sure it is transmitted from a source of trust. First, move to the **Imported Certificates** tab on the main window. Right-click the information

you entered and select **Change Owner Trust** .

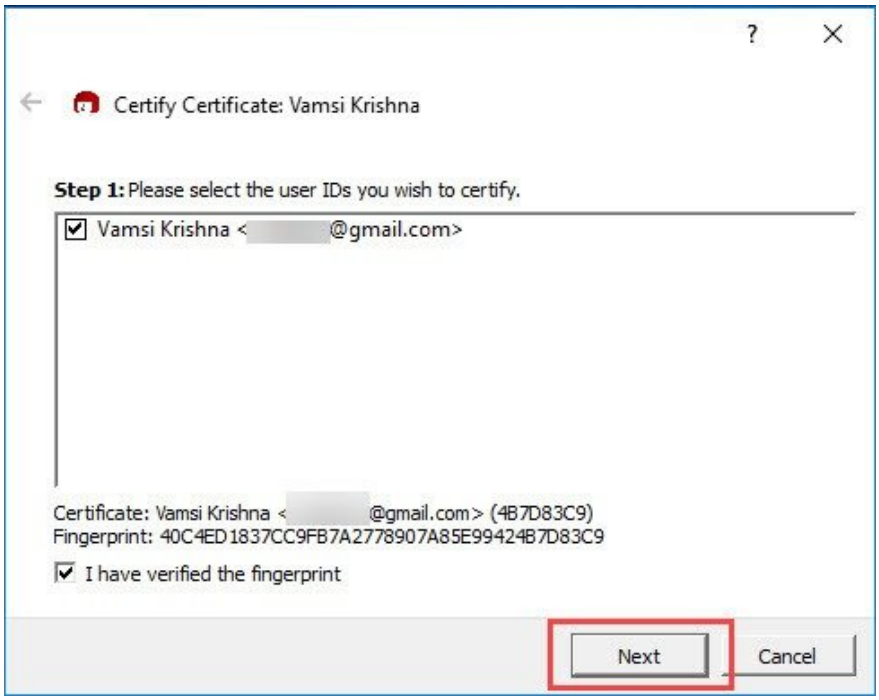
Next, click on **I believe checks are very accurate** and click **OK** .



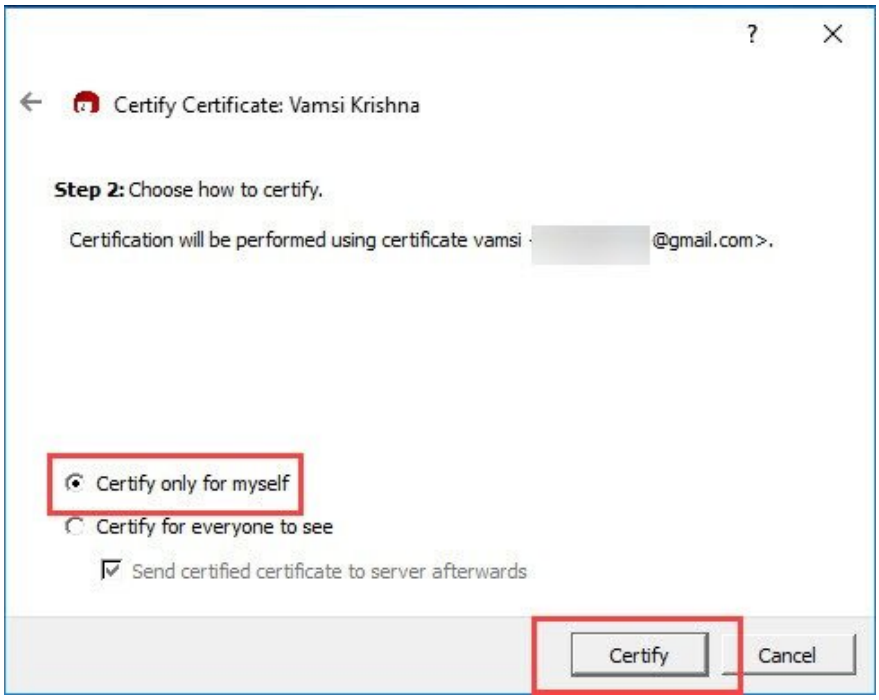
Go back, right-click that information and select **Certify Certificate** .



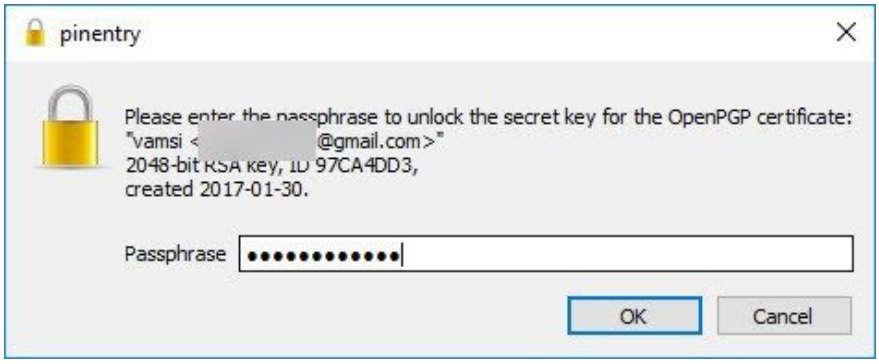
Next, tick both **checkboxes** to confirm and click **Next** .



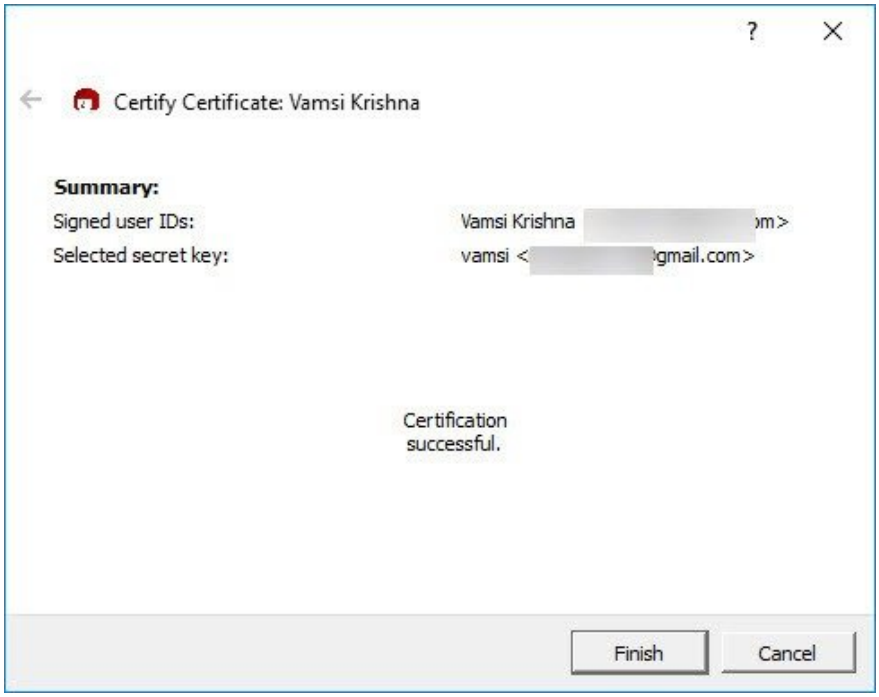
Select **Certify only for myself** and **Certify** .



You will be prompted to enter the entered password when creating the key pair. Enter the password and **OK** .



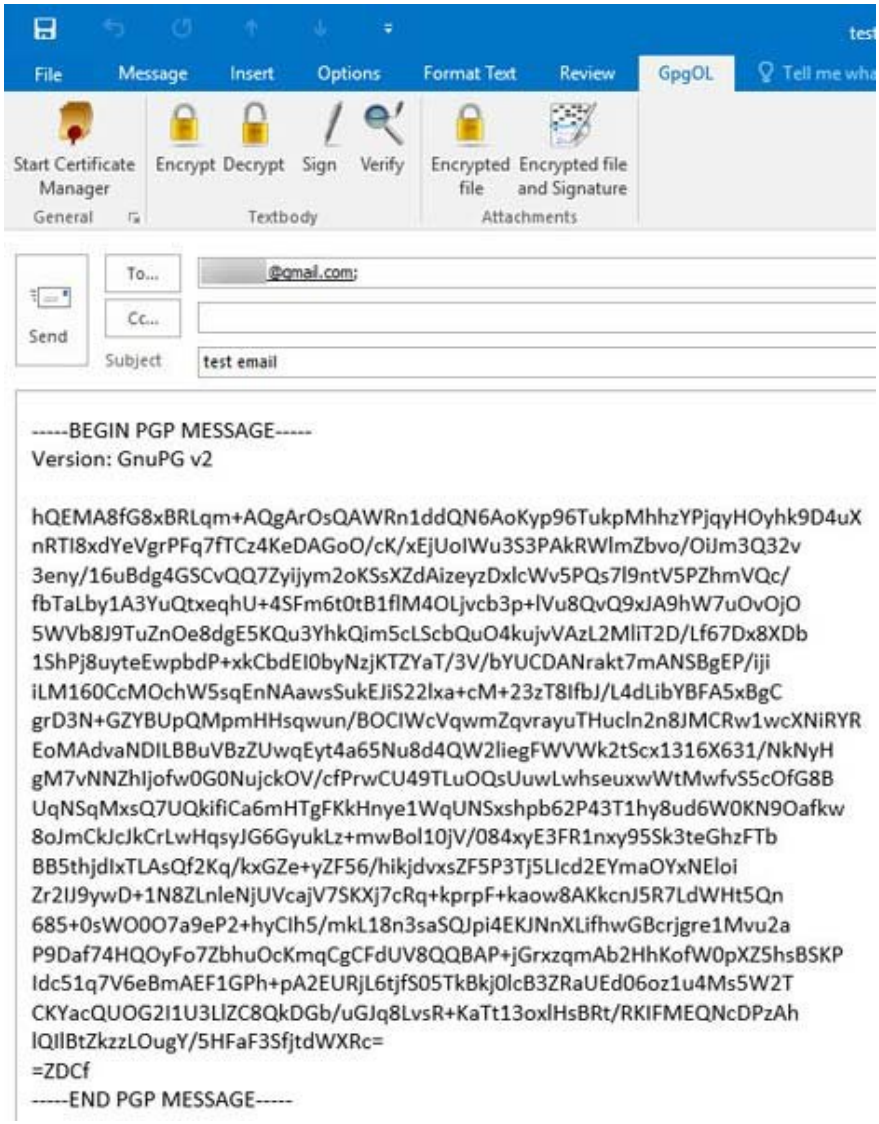
You will see a confirmation window appear. Click **Finish** to close the window.



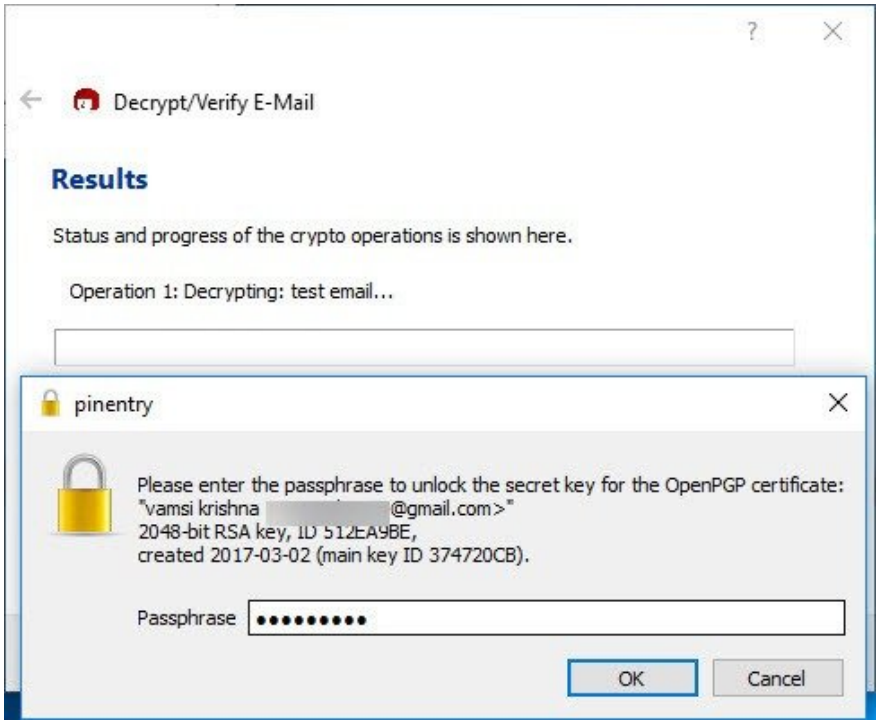
When you're done entering the public key, use it to encrypt email for specific users in Outlook.

Finally, to encrypt emails, open **Outlook** and create new messages as you normally would. After creating the mail, go to **GpgOL** tab and click **Encrypt** .

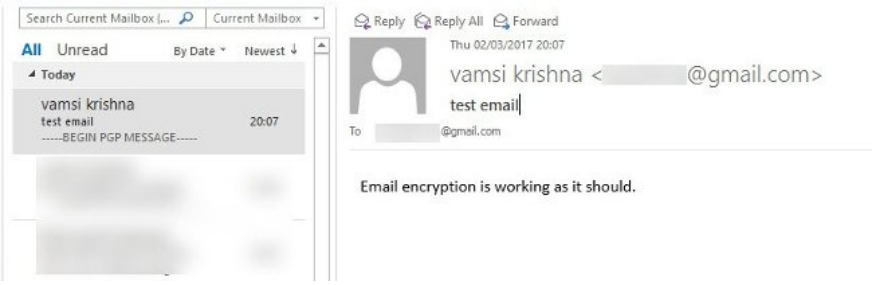
As soon as the button is clicked, Gpg4win will encrypt the email if the recipient's public key is available. When encrypted, the email will look like this. The recipient will be able to decrypt the email with his private key.



If you receive email encryption from other users with a public key, Outlook will ask for your password. Enter the password and click **OK** .



If not, you will see the decrypted message in Outlook.



Encrypt email in Outlook with a digital certificate

Office 365 subscribers have the option to add S / MIME encryption to their Outlook.com account. Free users will have to stick with one of the other options and the free options above are probably also easier to use (refer to the article How to encrypt Gmail, Outlook and other webmail for more details).). Users also need Digital Certificate for personal S / MIME encryption of Outlook.com.

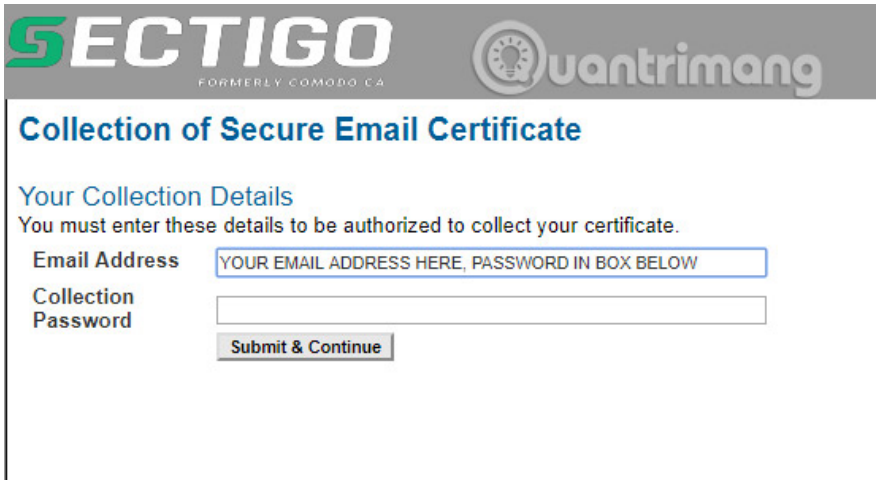
Get a free digital certificate

1. Use Mozilla Firefox, visit Comodo InstantSSL website. (You cannot use Microsoft Edge or Google Chrome for this task).

2. Scroll to and next to **Trial Certificates,** select **Free.**

3. Enter details for the email account you want to secure, use in Microsoft Outlook. Add a password. Accept the terms in **Subscriber Agreement** and click **Next,** then follow the instructions on the screen.

4. Go to the email account and open the email collection (authorized details to collect into the certificate) of Comodo. Copy the collection link, paste it into the Mozilla Firefox address bar and press **Enter.** Enter the corresponding email address. Now, copy **Collection Password** from the email into the **Collection Password** field and press **Enter.** The digital certificate will immediately begin downloading (it takes only 1 or 2 seconds).



5. Next, still in Mozilla Firefox, users need to extract the digital **certificate** from **Certificate Store.** The reason is that the automatic download certificate is in an incorrect format. In Mozilla Firefox, go to **Menu> Options> Privacy & Security** , then scroll down to the **Security** section and select **View Certificates.**

6. Select **Your Certificates** tab **,** then select **Certificate Name** for the relevant email address and click **Backup.** Select a relevant and easy-to-remember file name, then save the file in a memorable location. Now, the user must create another password. This password is very important. It protects the backup file being created, as well as when installing a digital certificate in another program.

The free certificate will last for 90 days .

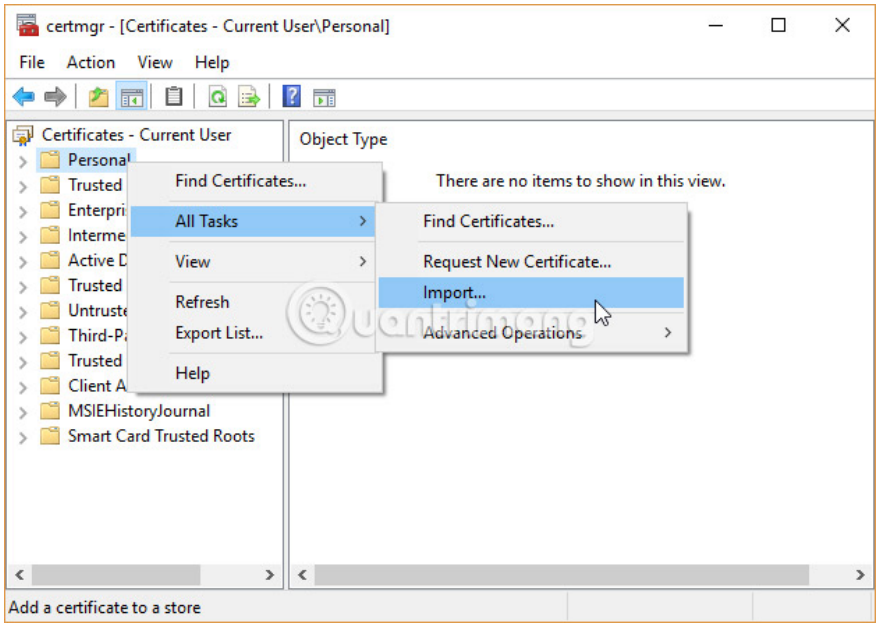
Enter a digital certificate (Chrome User)

At this time, Google Chrome users must import a new digital certificate into the **Windows Certificate Store** . Chrome uses Windows Certificate Store to authenticate users' digital certificates, so it is necessary to enter a digital certificate to use S / MIME encryption of Outlook.com.

Please note that if you are using Firefox, the reader may switch to the next section because the digital certificate is ready to use (Chrome and Firefox use different digital certificate authentication methods).

1. In Windows, press **Windows + R** key, then enter **certmgr.msc** and press **Enter.**

2. Highlight **Personal** folder **.** Now, right-click and select **All tasks> Import** .



3. Browse to the location of the backup digital certificate, identify the digital certificate, and then select **Open.**

4. Enter the password created during the backup process in the previous section. Now, select **Mark this key as Exportable** and leave the **Include all extended properties** option selected, then click **Next.**

5. Select **Place all certificates in the following store** .

6. Make sure the folder is selected as **Personal,** then click **OK,** followed by **Next.**

4. Finish the import process. Users will see a message that the process was successful.

Install S / MIME Control

The Outlook.com account uses S / MIME Control to manage encryption certificates.

1. Open an Outlook.com account in the browser.

2. Create a new email, select the option icon (three dots), then select **Message options> Encrypt this message (S / MIME)** .

3. When the **'Install S / MIME Control'** prompt appears, select **Run,** verify the Windows Account Control prompt and select **Run.**

When installing and configuring S / MIME encryption options, users can use the **Gear icon> S / MIME Settings menu** to choose whether to encrypt the content of all emails.

It's simple to send and receive encrypted emails using Outlook. Note, never share a private key with anyone.

You finished reading the article "**How to encrypt email on Microsoft Outlook**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.