LAB :: PGP (Pretty Good Privacy)

This guide is written based on users having access to a laptop or computer that can be used to install software on. Download Gpg4win (GNU Privacy Guard for Windows) from [https://www.gpg4win.org/index.html](https://www.gpg4win.org/index.html). The following software was used:

- Gpg4win-3.1.3.exe
- Windows 10 Enterprise version 1803

The guide will help participants to install and configure the software and will focus on:

- GnuPG - The heart of Gpg4win – the actual encryption software.
- Kleopatra - The central certificate administration of Gpg4win, which ensures uniform user navigation for all cryptographic operations.

### Install Gpg4Win on Windows 10

<table>
<thead>
<tr>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right-click on gpg4win-3.1.3.exe and click on Open to start the installation.</td>
<td><img src="https://via.placeholder.com/150" alt="Screenshot" /></td>
</tr>
<tr>
<td>Or Double-click on gpg4win-3.1.3.exe to start the installation.</td>
<td><img src="https://via.placeholder.com/150" alt="Screenshot" /></td>
</tr>
<tr>
<td>A message about User Access Control may appear. If so, Click on Yes.</td>
<td><img src="https://via.placeholder.com/150" alt="Screenshot" /></td>
</tr>
<tr>
<td>Select the appropriate language. In the example English is selected</td>
<td><img src="https://via.placeholder.com/150" alt="Screenshot" /></td>
</tr>
</tbody>
</table>
The installation wizard will start and you will see a welcome screen. Click on Next

On the page that contains the selection of components you can decide which programs you want to install. A default selection has already been made. Installation of individual components can be completed at a later time. Moving your mouse cursor over a component will display a brief description. Another useful feature is the display of required hard drive space for all selected components. Below are the applications and their function:

- **GnuPG**: Gnu Privacy Guard
- **Kleopatra**: Keymanager for OpenPGP
- **GPA**: GNU Privacy Assistant
- **GpgOL**: GnuPG for Outlook
- **GpgEX**: GnuPG Shell Extension
- **Browser integration**: Register GnuPG as native messaging service eg for the mailvelope extensions

Click on Next

The assistant will suggest a folder for the installation, e.g.: C:\Program Files (x86)\Gpg4win

Click on Install
When the installation finishes, 
Click on Next

On the completing the Gpg4win setup page, unselect 
the checkbox to run Kleopatra and click on Finish.

There should be a Kleopatra icon on the desktop. The 
icon can be used to start Kleopatra and is a shortcut to 
"C:\Program Files (x86)\Gpg4win\bin\kleopatra.exe"
On the right-mouse click context sensitive menu, there will be two options that can be used to sign and encrypt or decrypt files.

Using Kleopatra to create a key pair

<table>
<thead>
<tr>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right-click on Kleopatra icon and click on Open to start the program.</td>
<td>![Screenshot of Kleopatra icon and Open option]</td>
</tr>
<tr>
<td>Or Double-click on the Kleopatra icon</td>
<td>![Screenshot of Kleopatra icon]</td>
</tr>
</tbody>
</table>

Once the program opens, the main screen will be empty as no keys have been created. Click on New Key Pair.

Enter the details to create a new key.

1. Type in a name and email address
2. Click on the Advance settings button. Confirm the encryption algorithm, key usage and expiration. In this example, use the default settings.
3. Click on OK
4. Click on Next
Review the parameters.
1. Place a tick in the check box to show all details
2. After reviewing the settings click on create.

To create a key pair, you must enter a personal passphrase.

Choose a passphrase which is easy-to-remember but hard to break.

To make sure that no typing errors, the system will prompt you to enter the passphrase twice.

Click on OK

NOTE: A warning may appear if an insecure passphrase was used.

As soon as the key pair creation has been successful, you will see the following dialog. Please leave this window open as it will be used in later tasks.
The 40-digit “fingerprint” of the newly generated OpenPGP certificate is displayed in the results text field. This fingerprint is unique anywhere in the world, i.e. no other person will have a certificate with the same fingerprint.

Even at 8 digits it would already be quite unlikely that the same sequence would occur twice anywhere in world.

For this reason, it is often only the last 8 digits of a fingerprint which are used or shown, and which are described as the key ID. This fingerprint identifies the identity of the certificate as well as the fingerprint of a person.

You do not need to remember or write down the fingerprint. You can display it later in Kleopatra’s certificate details.

Troubleshoot Kleopatra

<table>
<thead>
<tr>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Kleopatra program does not start. Right mouse click on a file and click on sign and encrypt</td>
<td><img src="https://via.placeholder.com/150" alt="Screenshot" /></td>
</tr>
<tr>
<td>Click on cancel</td>
<td><img src="https://via.placeholder.com/150" alt="Screenshot" /></td>
</tr>
</tbody>
</table>
In the system tray, click on Kleopatra icon to open

Once the program opens, the main screen will be empty as no keys have been created.

To create a new key. Click on File and then click on New Key Pair

Double click on Create a personal OpenPGP key pair. This will start the Key Pair Creation wizard.

Following the steps in the previous section, to complete the wizard.
<table>
<thead>
<tr>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the Key Pair Created window, click on Make a Backup of Your Key Pair</td>
<td><img src="image1" alt="Key Pair Created window" /></td>
</tr>
<tr>
<td>Click on the folder icon to browse to a location to export the certificates</td>
<td><img src="image2" alt="Export Secret Certificate" /></td>
</tr>
</tbody>
</table>
| On the Save As window:  
1) Browse to the folder location  
2) Type in a file name  
3) Click on Save | For example: "C:\Users\NetSec\Documents\PGP lab Certificates\Example Key Creation.gpg" |
| Click on OK | ![Export Secret Certificate](image3) |
| NOTE: If you add a tick to the ASCII armor check box, the public key will be exported as well. | |
| Type in the Passphrase and Click on OK | ![Export Secret Certificate](image4) |
### Upload Public Key to directory server

<table>
<thead>
<tr>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the Key Pair Created window, click on Upload Public Key to Directory Service</td>
<td><img src="image1.png" alt="Screenshot" /></td>
</tr>
</tbody>
</table>

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

**Result**

- Key pair created successfully.
- Fingerprint: 58607903768386CA3417664C73D3521DA426C0F

**Next Steps**

- Make a Backup Of Your Key Pair...
- Send Public Key By Email...
- Upload Public Key To Directory Service...

Click on Continue

Click on OK

### Export Public Key and upload to server

<table>
<thead>
<tr>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click on Finish</td>
<td><img src="image2.png" alt="Screenshot" /></td>
</tr>
</tbody>
</table>

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

**Result**

- Key pair created successfully.
- Fingerprint: 58607903768386CA3417664C73D3521DA426C0F

**Next Steps**

- Make a Backup Of Your Key Pair...
- Send Public Key By Email...
- Upload Public Key To Directory Service...

Click on Finish
Right-mouse click on the Key and click on Export.

On the Save As window:
1) Browse to the folder location
2) The file name will be the fingerprint
3) Click on Save

The example location is: "C:\Users\NetSec\Documents\PGP lab Certificates\"

Browse to the location and open the exported file in notepad.

Select the public key block. Right-mouse click and select Copy.
Open any browser and go to http://pgp.mit.edu/

Paste the public key block text into the Submit a key area. Click on “Submit this key to the keyservers!” button.