Linux and Libre Office User Guide for HYP2003/ePass2003 Tokens

1. Installation of Token Drivers in Linux
2. Setting up Token in Chrome Browser to sign PDF in Libre Office
3. Setting up Libre Office to use Chrome Certificates
4. Setting up Token in Mozilla Firefox Browser to sign PDF in Libre Office
5. Settings for Signing ODF and PDF Documents using Libre Office
6. Checking the digital signature on ODF documents signed with Libre Office
7. Signing PDF Documents using Libre Office
8. Checking the digital signature on PDF documents signed with Libre Office

INSTALLATION OF **HYP2003/EPASS2003** TOKEN DRIVER IN LINUX UBUNTU

1. Open the terminal and execute the command uname –m to know whether your system is 32-bit or 64-bit. It shows if your system is running 32-bit (i686 or i386) or 64-bit(x86_64) >
2. Unzip/extract the downloaded files >
3. Find and open the config folder >
4. Right Click and select the open terminal here or open that path in terminal >
5. Enter the command sudo sh config.sh
6. Enter the sudo user password >
7. After Enter Password You will get the massage Run Finish >
8. cd ../redist >
9. sudo chmod a+x pkimanager >
10. sudo chmod 775 >

11. sudo cp libcastle_v2.so.1.0.0 /usr/lib/ >
    sudo chmod 700 /usr/lib/libcastle_v2.so.1.0.0 >
    sudo chown user:group /usr/lib/libcastle_v2.so.1.0.0 >
12. Plug the token into the system and double click and open the pkimanager from redist folder. Check the status of token and if you get the massage token is inserted and ready to use.
    It's work for only CSP 2.0 token. (As per CCA Guidelines for PKI Hardware, issued in 2018)
    libcastle_v2.so.1.0.0 is the PKCS 11 library file which communicate with token for certificate.
    In which application you want to use certificate, that application need to have provision to browse PKCS11 lib (libcastle_v2.so.1.0.0) in it.

    Note: In case you are using Token with CSP V1.0 you can update your existing token to CSP V2.0 from https://update.epasstokens.com

SETTING UP CHROME TO USE YOUR HYP2003/EPASS2003 TOKEN TO SIGNE PDF IN LIBREOFFICE

Chrome for Linux manages digital certificates similarly to Firefox — using Mozilla NSS as backend. However, unlike Firefox, Chrome does not provide a graphical user interface to install PKCS11 modules. Therefore, to set up Chrome you need to use the command line.

Plug in your token before proceeding and plug ePass2003 having the user certificate along with all root CA certificate. Make sure your supplier has provided you Token with CSP V2.0

First, start by opening the terminal and installing Mozilla NSS Tools (they may be already installed on your system):

```
$ sudo apt-get install libnss3-tools
$ sudo mkdir ~/.pki/nssdb
$ sudo chmod -R 0700 $HOME/.pki
$ sudo modutil -dbdir ~/.pki/nssdb/ -add "ePass2003" -libfile /usr/lib/libcastle_v2.so.1.0.0
```

modutil alerts you that you need to close your browser:

WARNING: Performing this operation while the browser is running could cause corruption of your security databases. If the browser is currently running, you should exit browser before continuing this operation.
Type 'q <enter>' to abort, or <enter> to continue:

Close any running web browsers and hit Enter. When the command finishes, you can reopen them:

Module "ePass2003" added to database.

You can verify that the token has been successfully added by running:

```
$ modutil -dbdir sql:.pki/nssdb/ -
list
```
As root, load the root CA (CCA India 2022 , 2014)certificate into the NSSdb

certutil -A -n rootca -i /location_of_ca_root_cert/rootcert.pem -t "CT,CT,CT" -d ~/.pki/nssdb

If needed as root load each sub CA's public certificate into the NSSdb

certutil -A -n subca -i /location_of_subca_root_cert/rootcert.pem -t "CT,CT,CT" -d ~/.pki/nssdb

Verify expected certificates have loaded, as root:

certutil -L -d ~/.pki/nssdb

Below is the another way to trust the Trust a root CA certificate.

Once done Open the Chrome and open the Settings

Select the Privacy and security from left and then select the security.
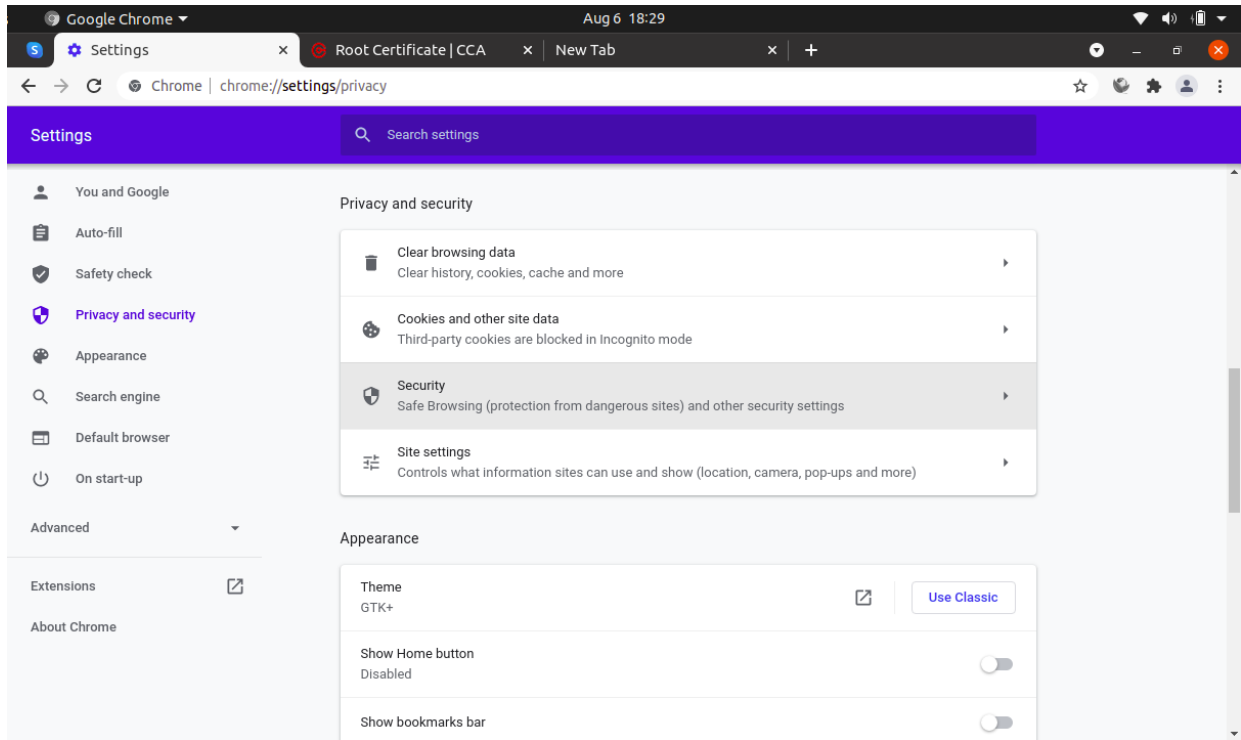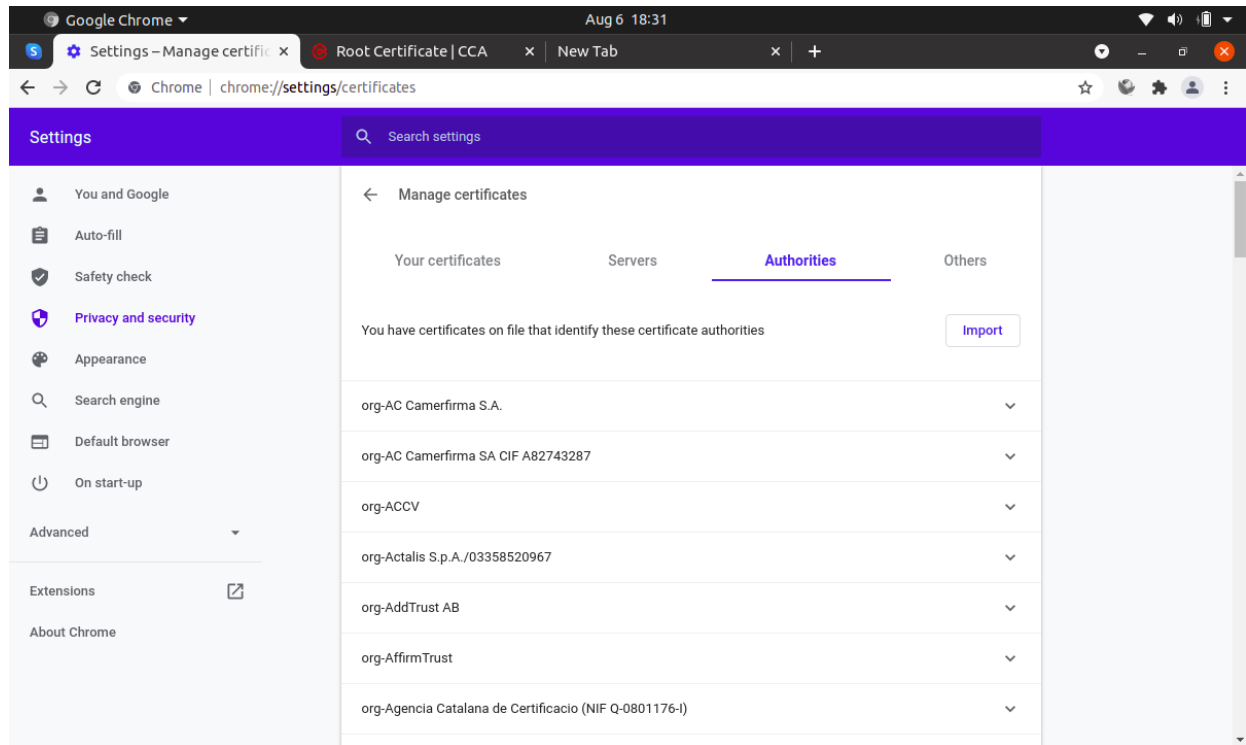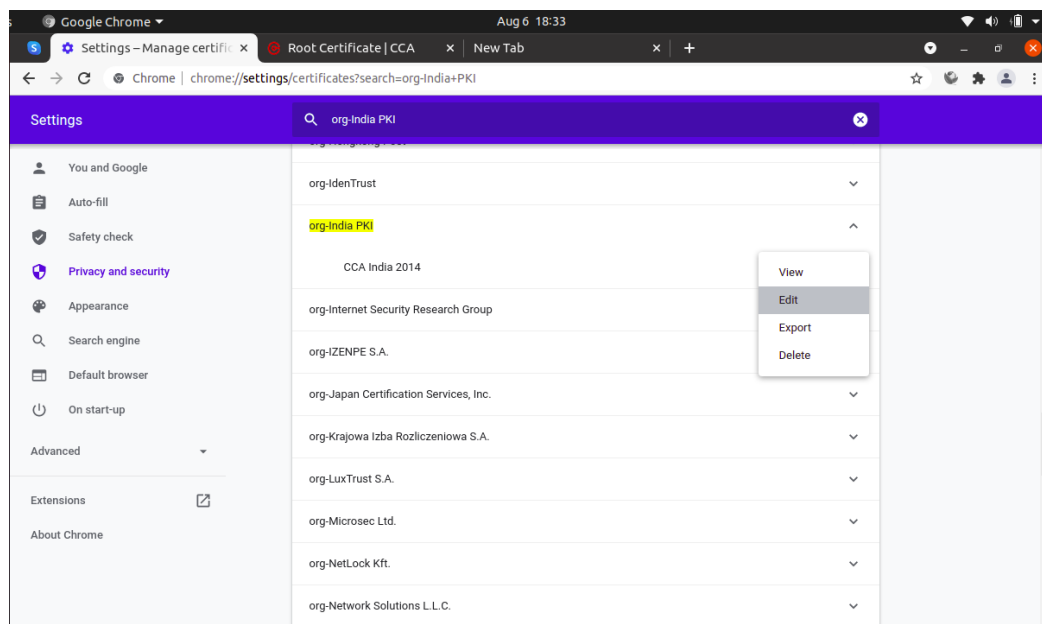
Find the option mange certificate.
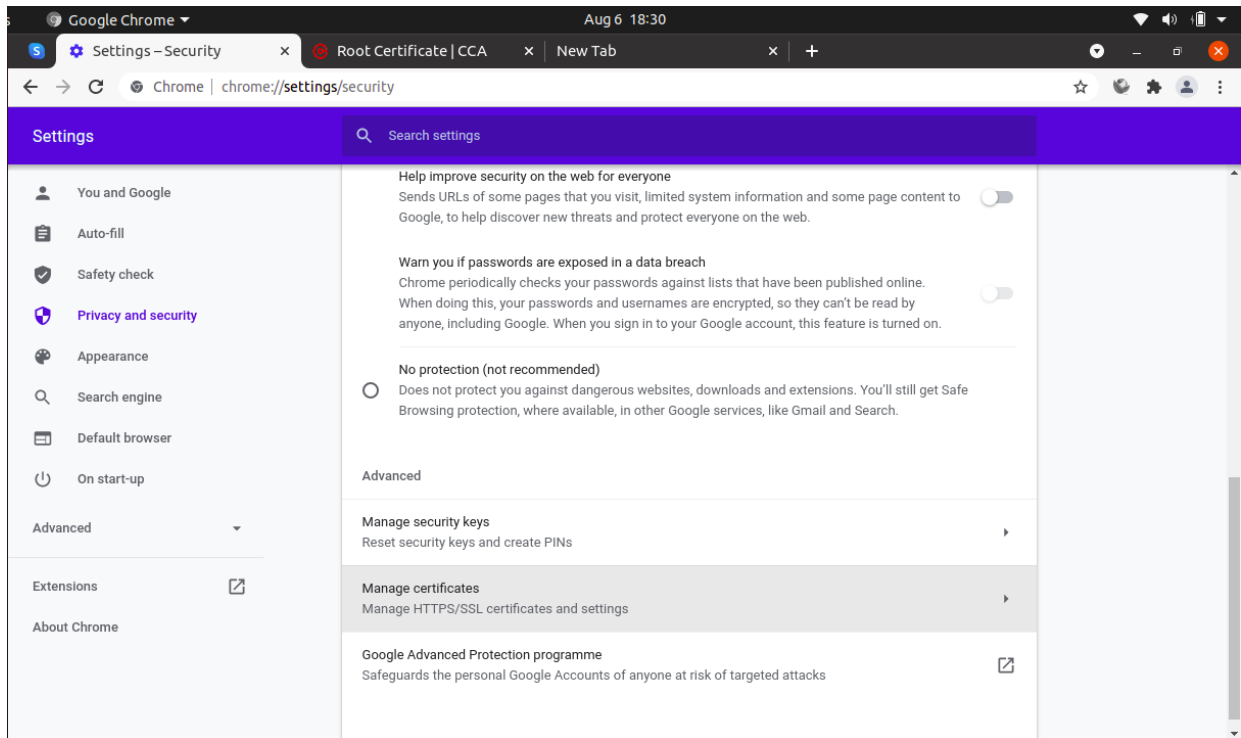
Click on Authorities Tab

Find the "org-India PKI" and expand it. Here you will find the CCA India 2014, which is root-certifying authority on India. If you can't find it then you need to import manually. T the root certificates are available on the HYP2003/ePass2003 token it will appear in the list here.

Click on Edit and mark the all check box.
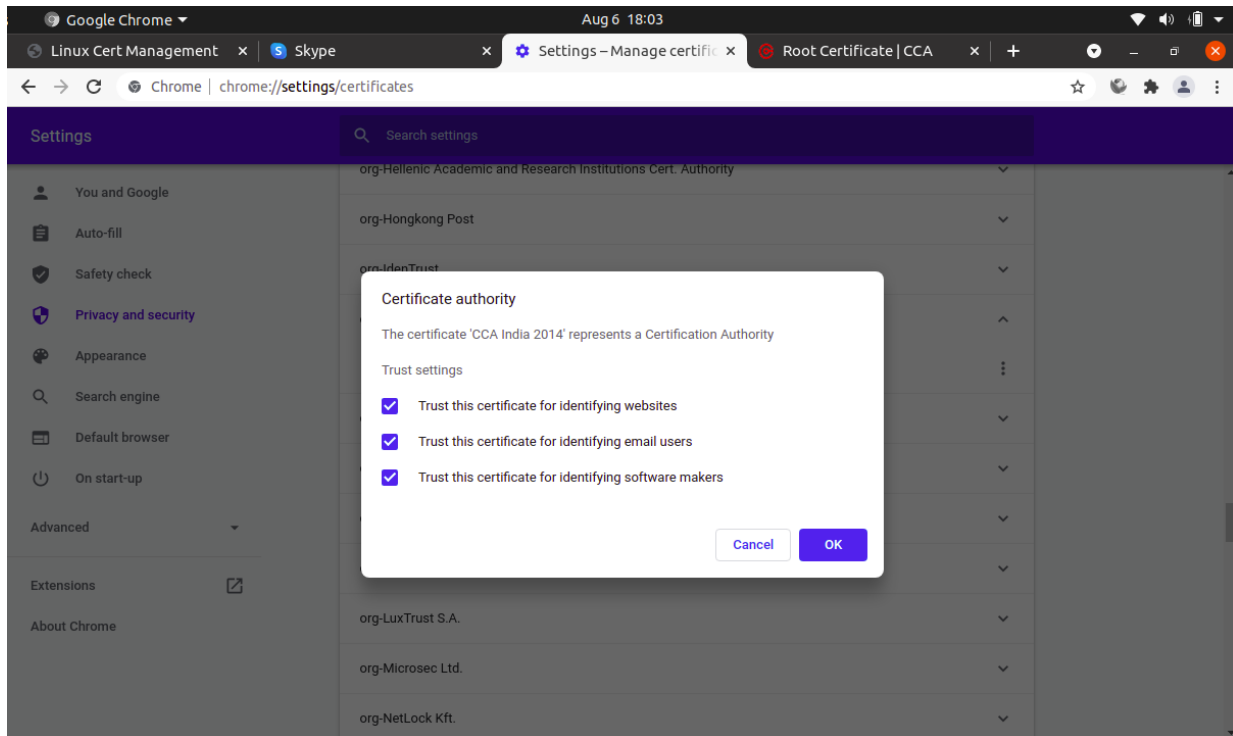
Chromium users don't need to install and set up Firefox to sign documents with LibreOffice: they can set up LibreOffice to use the Chromium public key infrastructure.

To do that, open the **Tools** menu and click **Options**.

On the tree by the left, expand **LibreOffice**, then select **Security**:
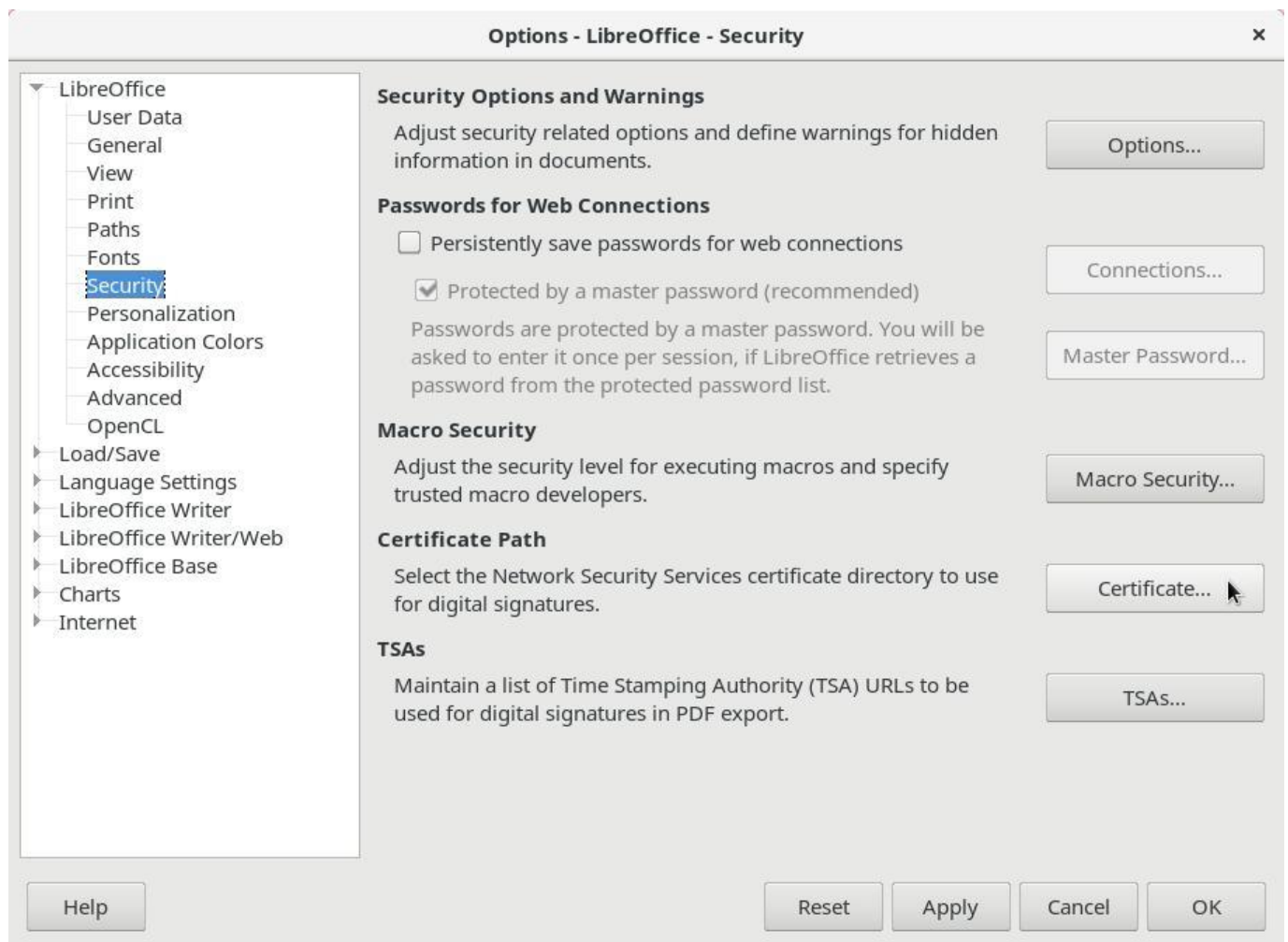
By the right, under **Certificate Path**, click the **Certificate** button.

On the **Certificate Path** dialog box, click **Add**:

Chromium stores its certificate configuration in ~/.pki/nssdb/.

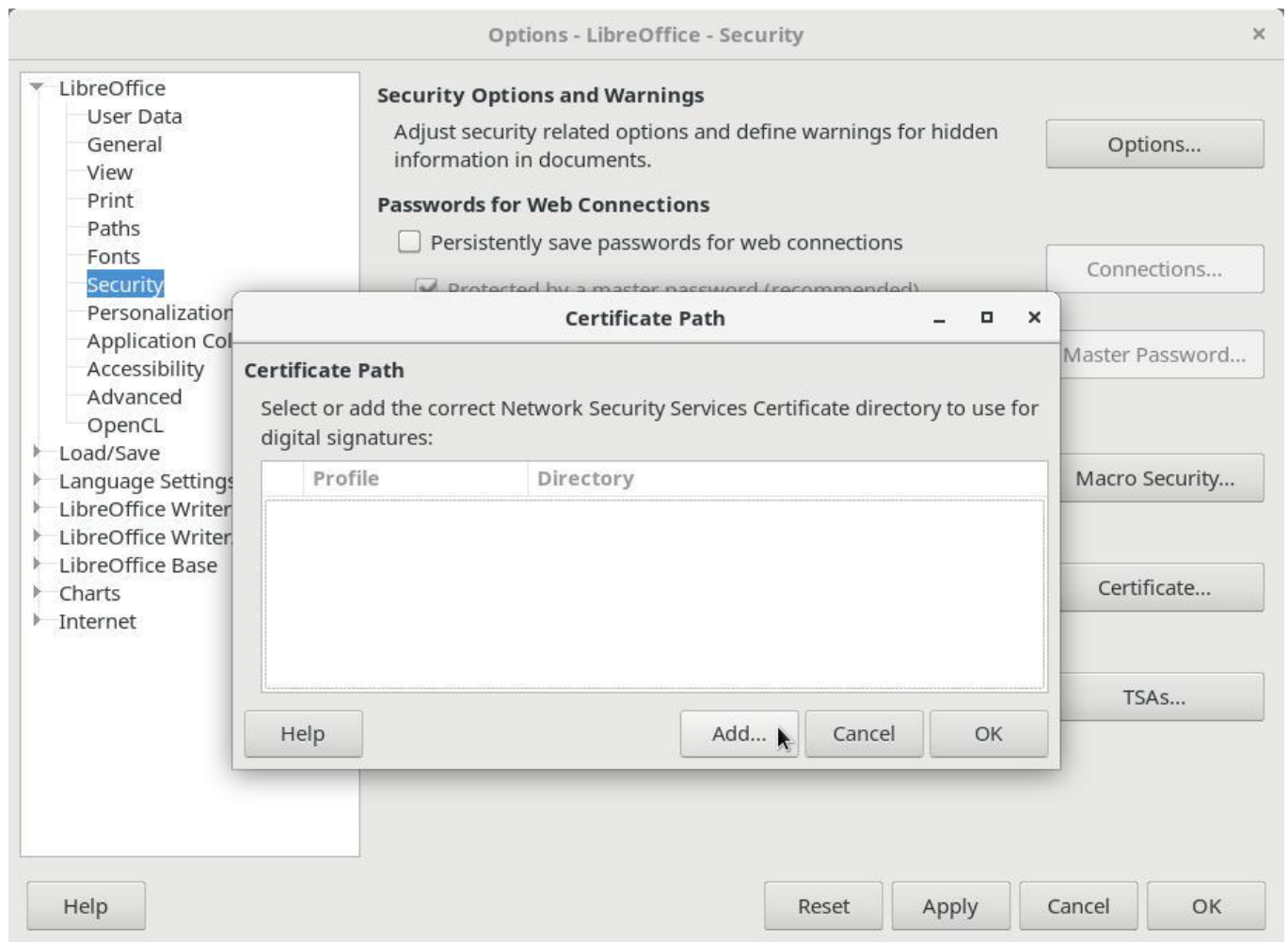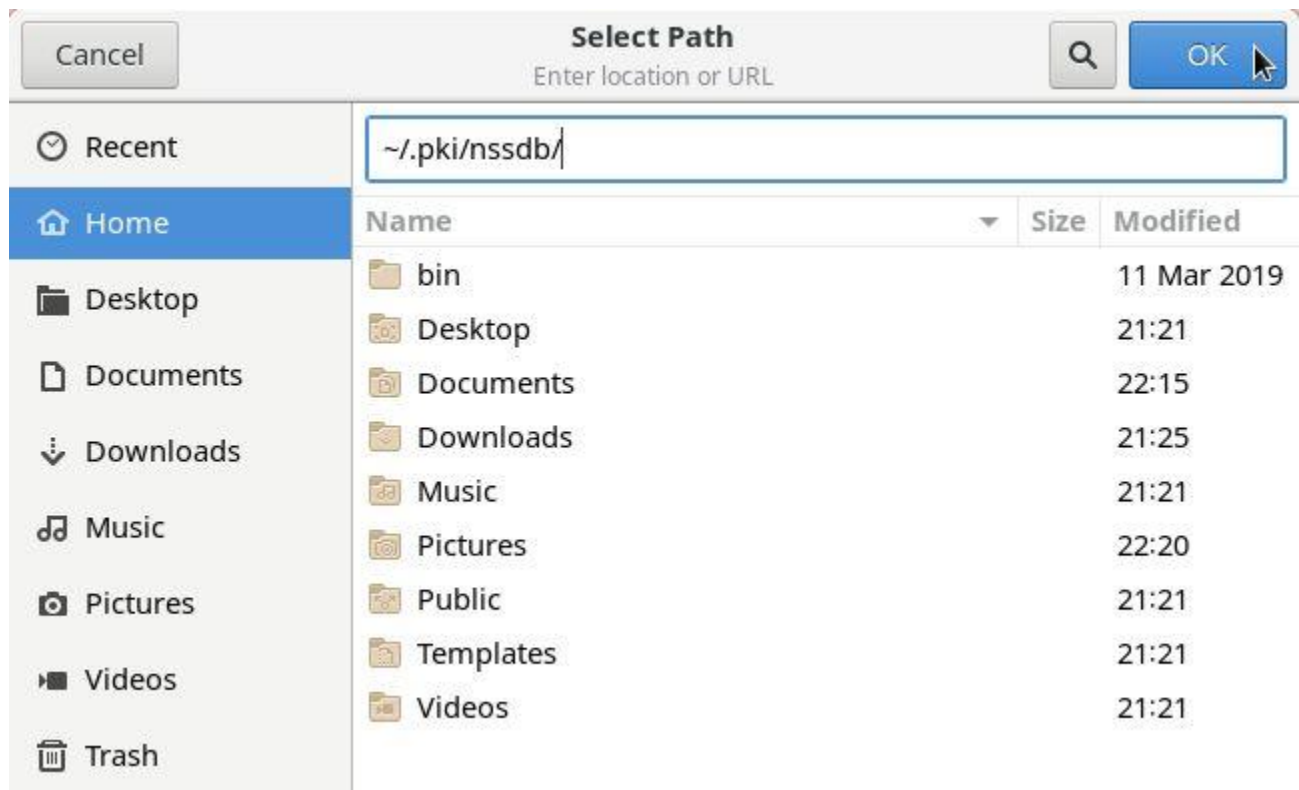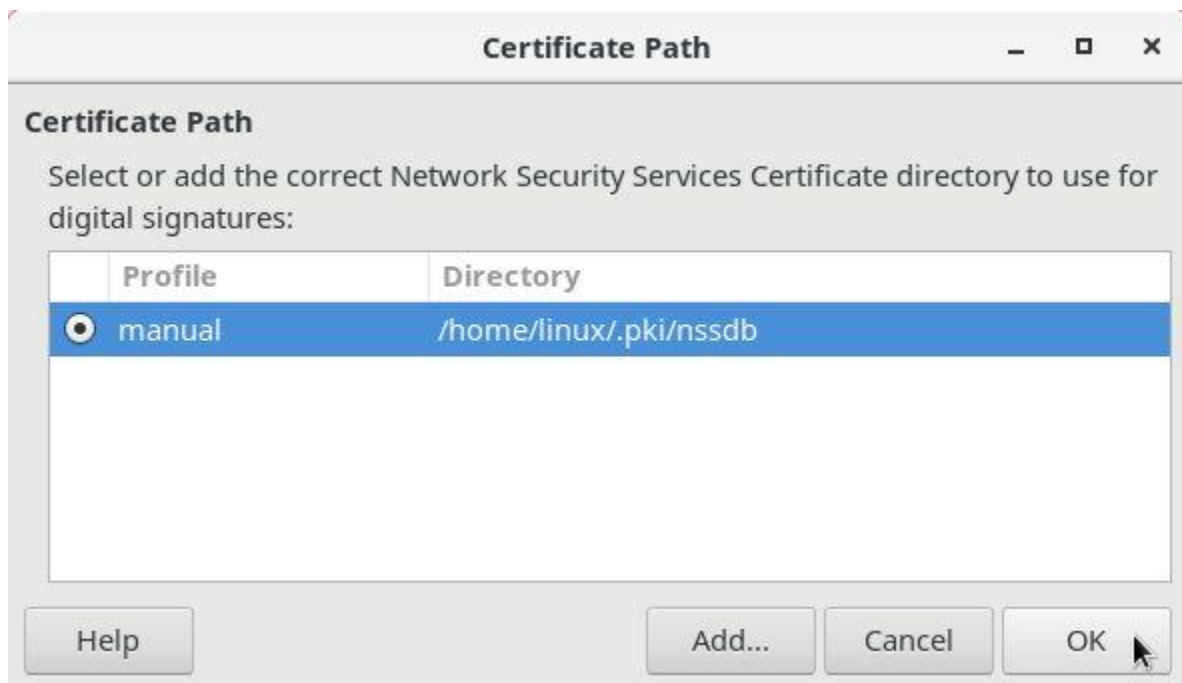On the **Select Path** dialog box, press **Ctrl + L** to manually enter the location, type ~/.pki/nssdb/ and click **OK**:

Cancel	**Select Path** Enter location or URL	Q	OK

~/.pki/nssdb/|

⊘ Recent

⌂ Home

▤ Desktop

🗋 Documents

⬇ Downloads

🎵 Music

📷 Pictures

▸▪ Videos

🗑 Trash

Name	▼	Size	Modified
📁 bin			11 Mar 2019
📁 Desktop			21:21
📁 Documents			22:15
📁 Downloads			21:25
📁 Music			21:21
📁 Pictures			22:20
📁 Public			21:21
📁 Templates			21:21
📁 Videos			21:21

Back to the **Certificate Path** dialog box, click **OK** to close it:

Certificate Path   — ◻ ✕

Certificate Path

Select or add the correct Network Security Services Certificate directory to use for digital signatures:

	Profile	Directory
⦿	manual	/home/linux/.pki/nssdb

Help		Add...	Cancel	OK

Back to the **Options** dialog box, click **OK** to close it.
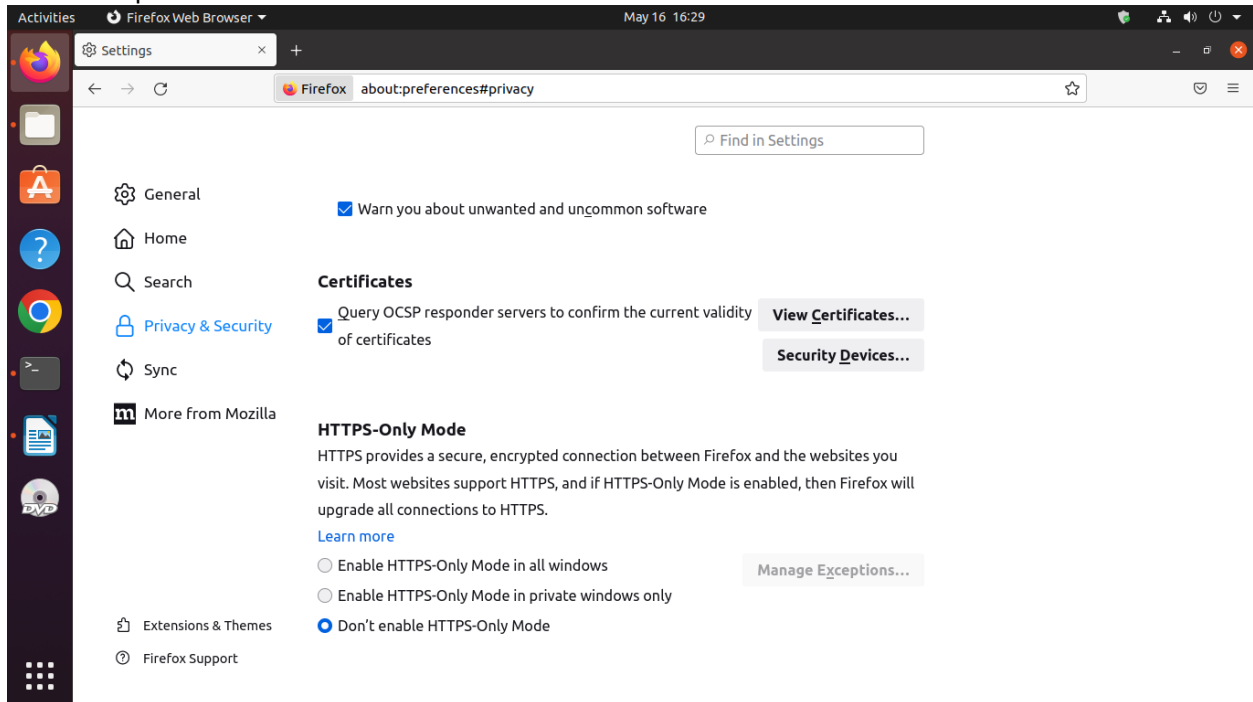
Restart LibreOffice and you are ready to go!

SETTING UP MOZILLA FIREFOX TO USE YOUR EPASS2003 TOKEN TO SIGNE PDF IN LIBREOFFICE

Start Mozilla and paste about:preferences#privacy into the address bar and hit enter.

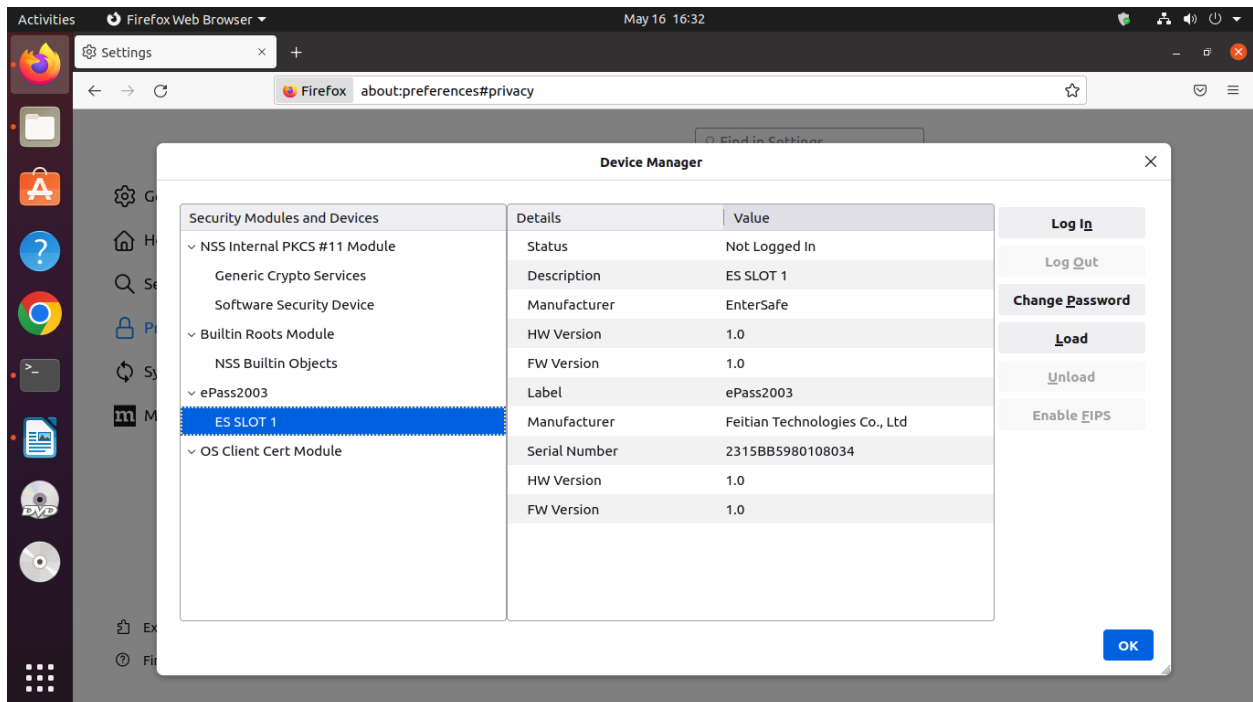Scroll and find the Security Devices Button.

Click and open it.

It will Open the Device Manager.

Click on Load button and enter Module Name ePass2003 and Module File Name /usr/lib/libcastle_v2.so.1.0.0 as shown in below image. (it will not work if Point No. 12 is not done in Installation process).
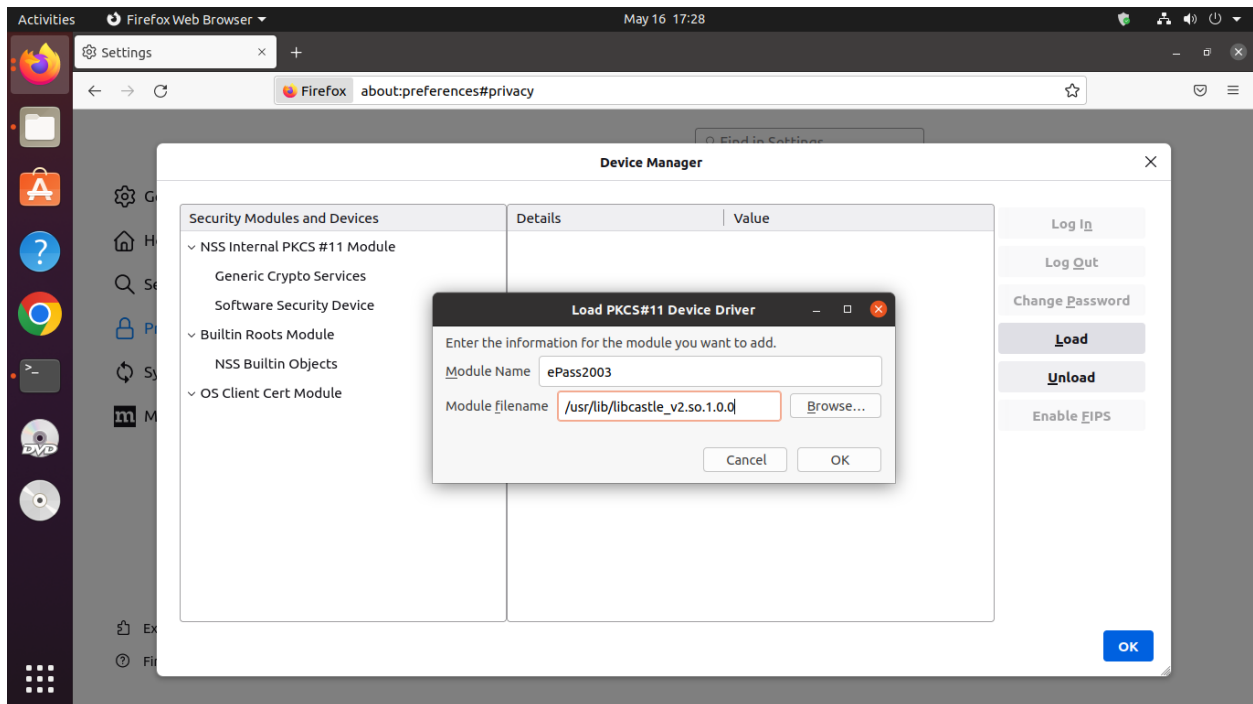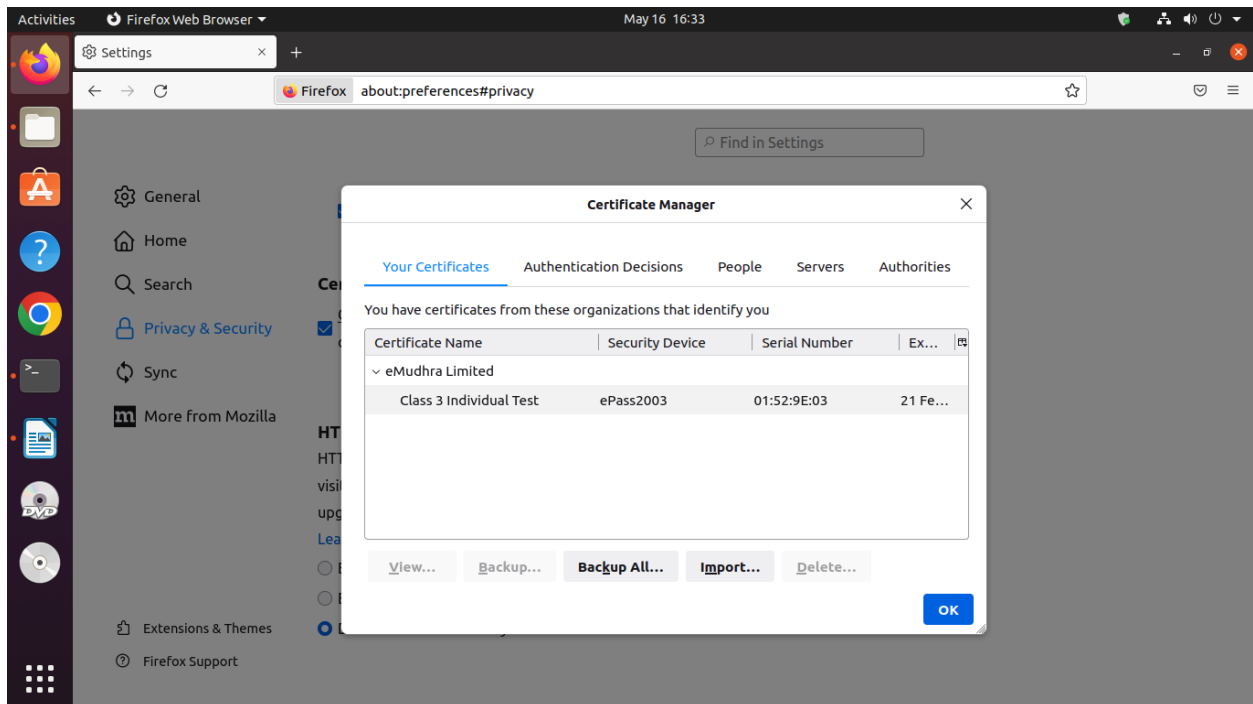
Once Module is successfully added you will get the below screen.

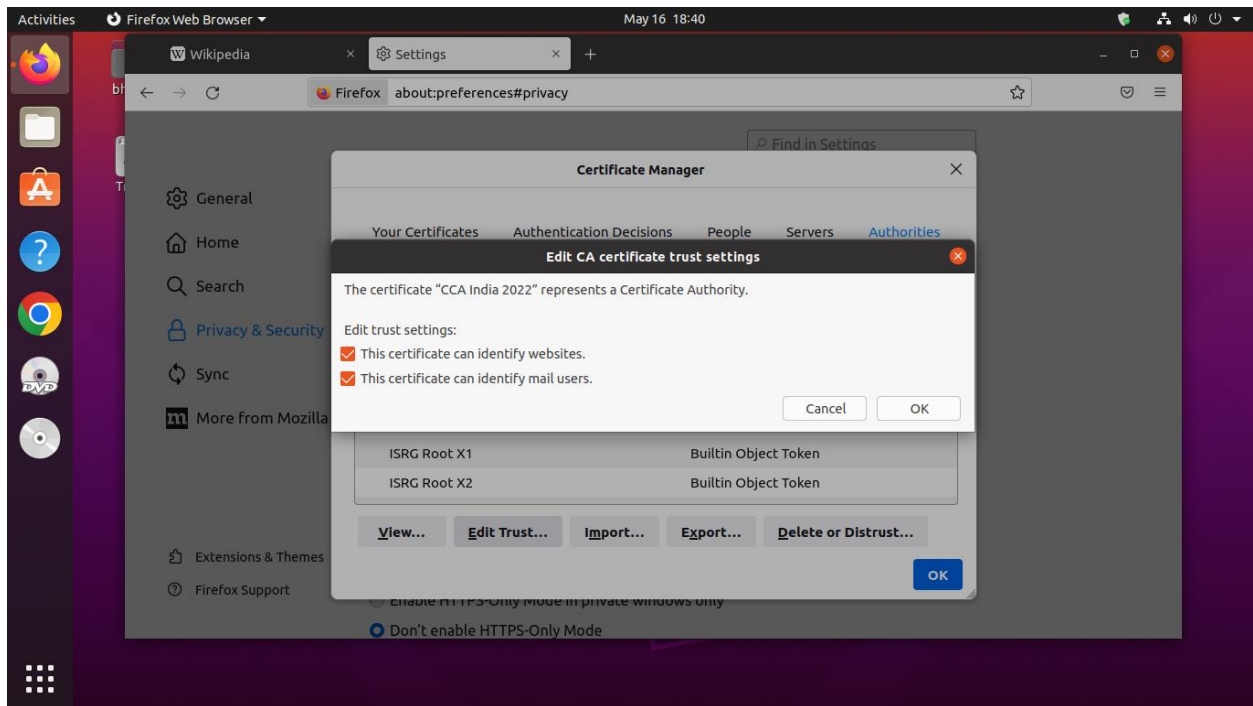Click on Ok and Close the Device manager and then click on certificate button.

In your certificate Tab you will get the present user certificate into the token.

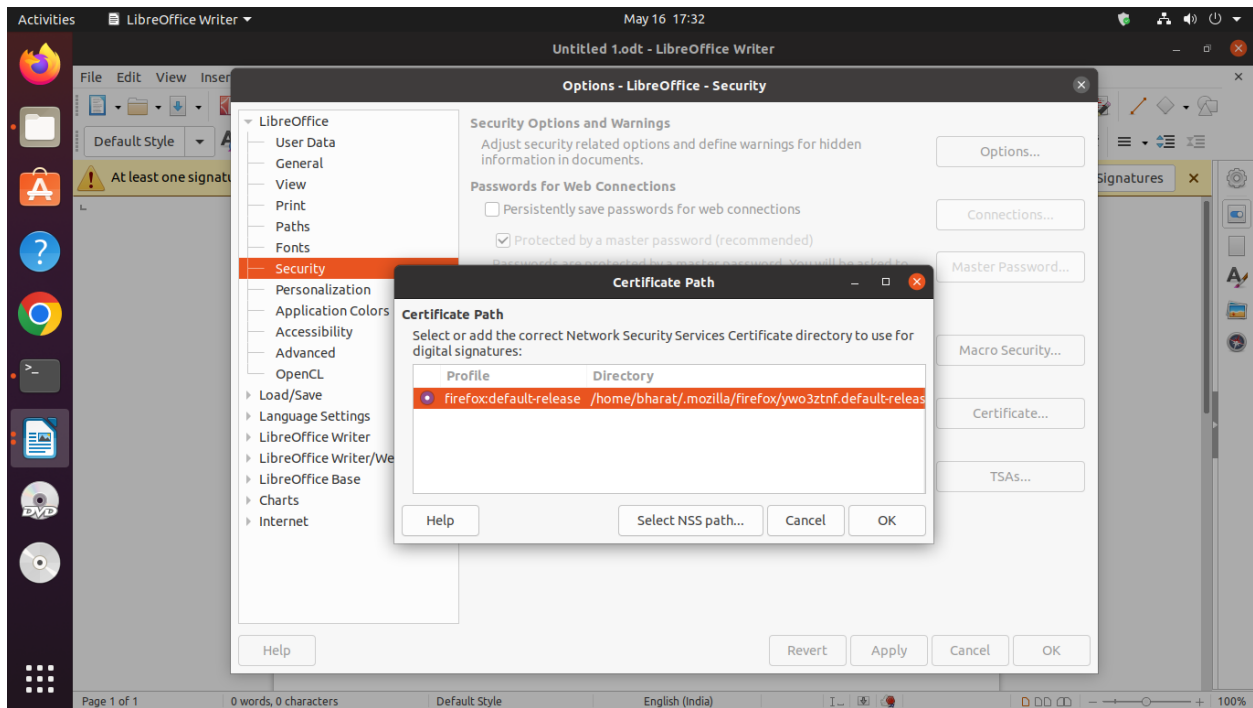Make sure token with Root chain of CCA and Issuer CA

Click on Authorities Tab and find the India PKI. Click on Edit Trust button and select the both check box and click on OK Button.
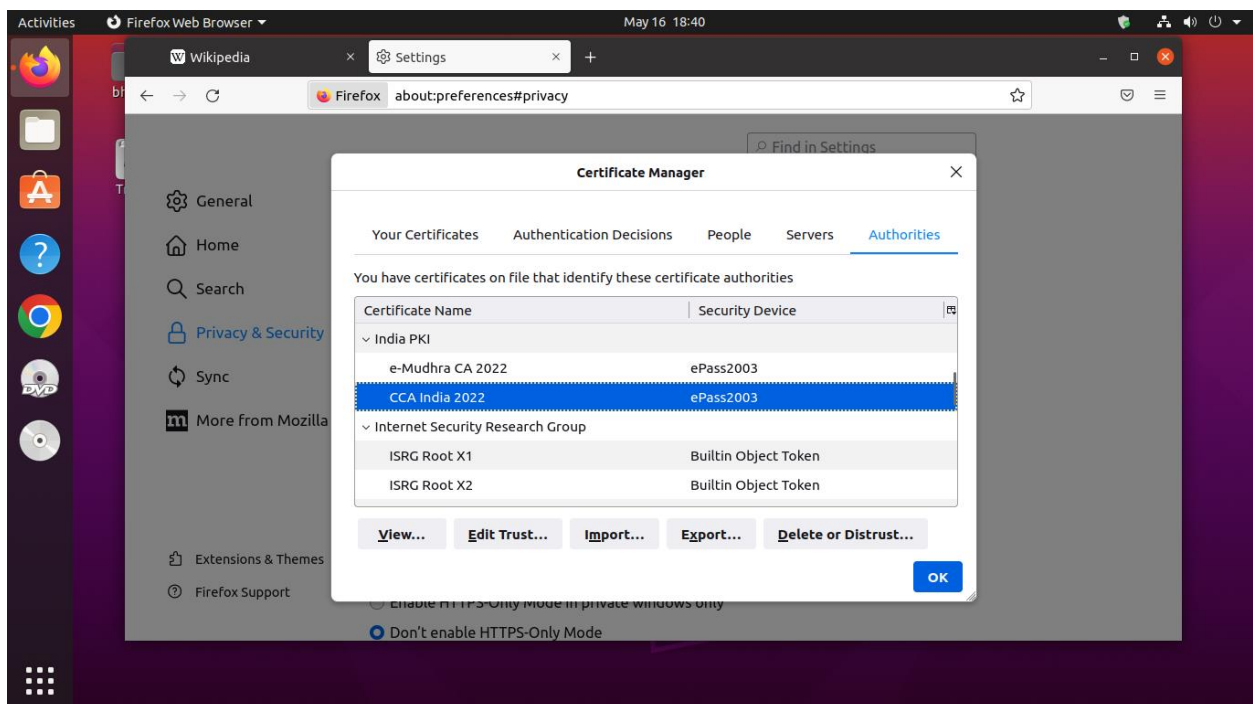
Once done open the LibreOffice writer and Go to Tools ➔ Options ➔ Security ➔ Certificate

By default, it is selected but if not select it (firefox:default-release)

SIGNING ODF AND PDF DOCUMENTS WITH LIBREOFFICE

If you have a digital certificate, you can sign documents before sending them, so that who receives them feels confident about their authenticity and integrity.

Today you are going to see how to do that with the LibreOffice office suite, which is able to sign not only ODF documents created by itself, but also any PDF documents (even those created by other programs).

Although capable of signing, LibreOffice does not have its own public key infrastructure. Instead, it uses the infrastructure of a web browser to sign documents.

By default, LibreOffice looks for certificates and cryptographic media in the Mozilla Firefox configuration. Therefore, if you use Firefox, you need to set it up before signing documents with LibreOffice. These two posts show how you can get everything working:

- How to install website certificates on Linux
- Using smart cards on openSUSE Linux

Linux Kamarada 15.1 brings Chromium as default web browser. If you use Chromium (or a Chromium-based browser, such as Google Chrome, Opera, Vivaldi or Brave), you can set up LibreOffice to use it instead of Firefox. But also in that case your browser must be setup first:

- Setting up smart card authentication on Google Chrome / Chromium

Then, refer to the end of this post to see how to set up LibreOffice to use Chromium.

Everyone on the same page (tokens and browsers setup), let's move on to LibreOffice!

Signing an ODF document

The Open Document Format (ODF) is the default file format for LibreOffice. The most common filename extensions used for Open Document files are:

- .odt for *text* documents, opened with Writer;
- .ods for *spreadsheets*, opened with Calc;
- .odp for *presentations*, opened with Impress;
- .odg for *graphics* (diagrams, vector images), opened with Draw;
- .odb for *databases*, opened with Base; and
- .odf for mathematical equations (*formulas*), opened with Math.

Let's see how to sign a text document (a .odt file) with LibreOffice Writer (steps are similar for any application of the LibreOffice suite).

Open the **File** menu, **Digital Signatures** submenu, and click **Digital Signatures**:
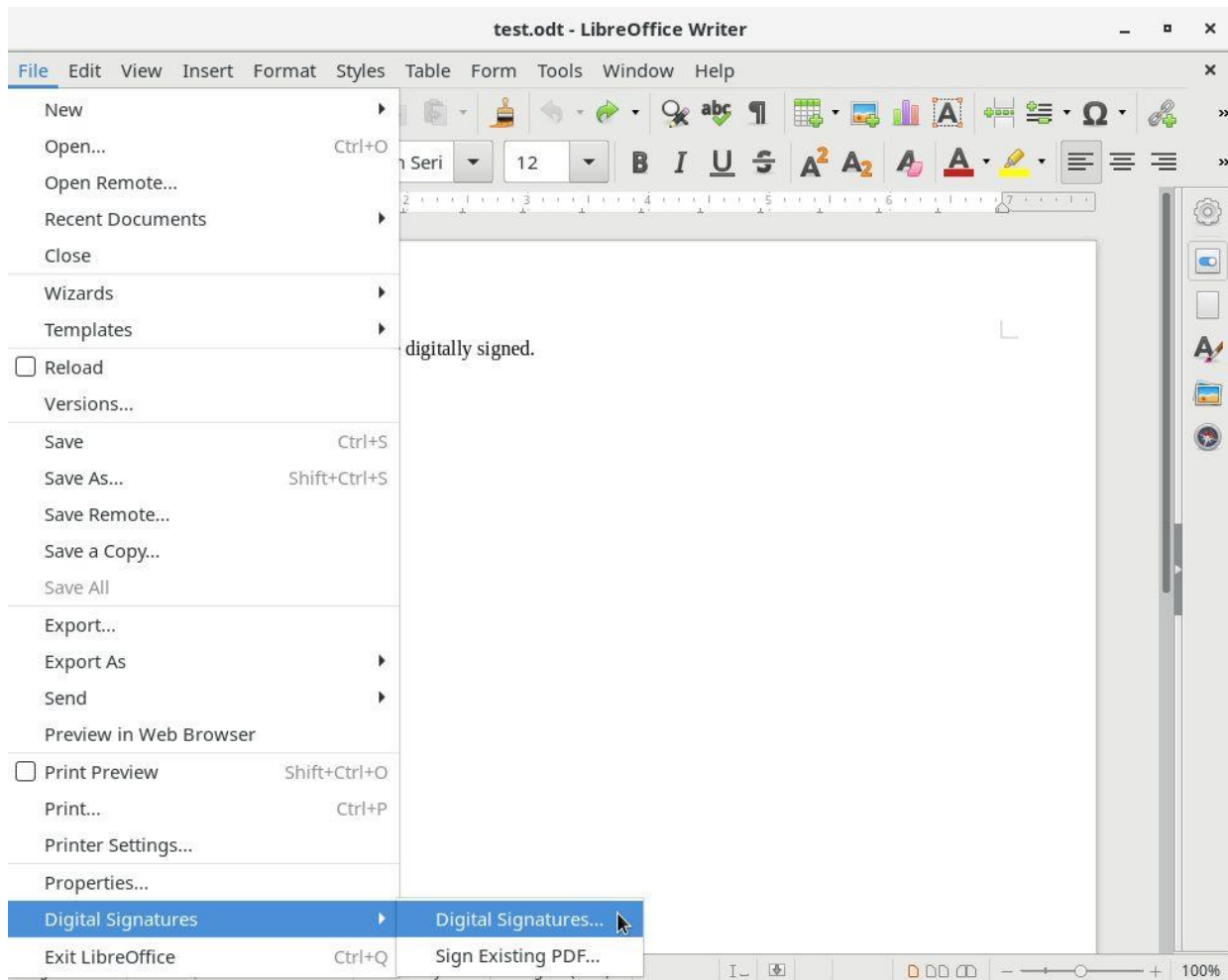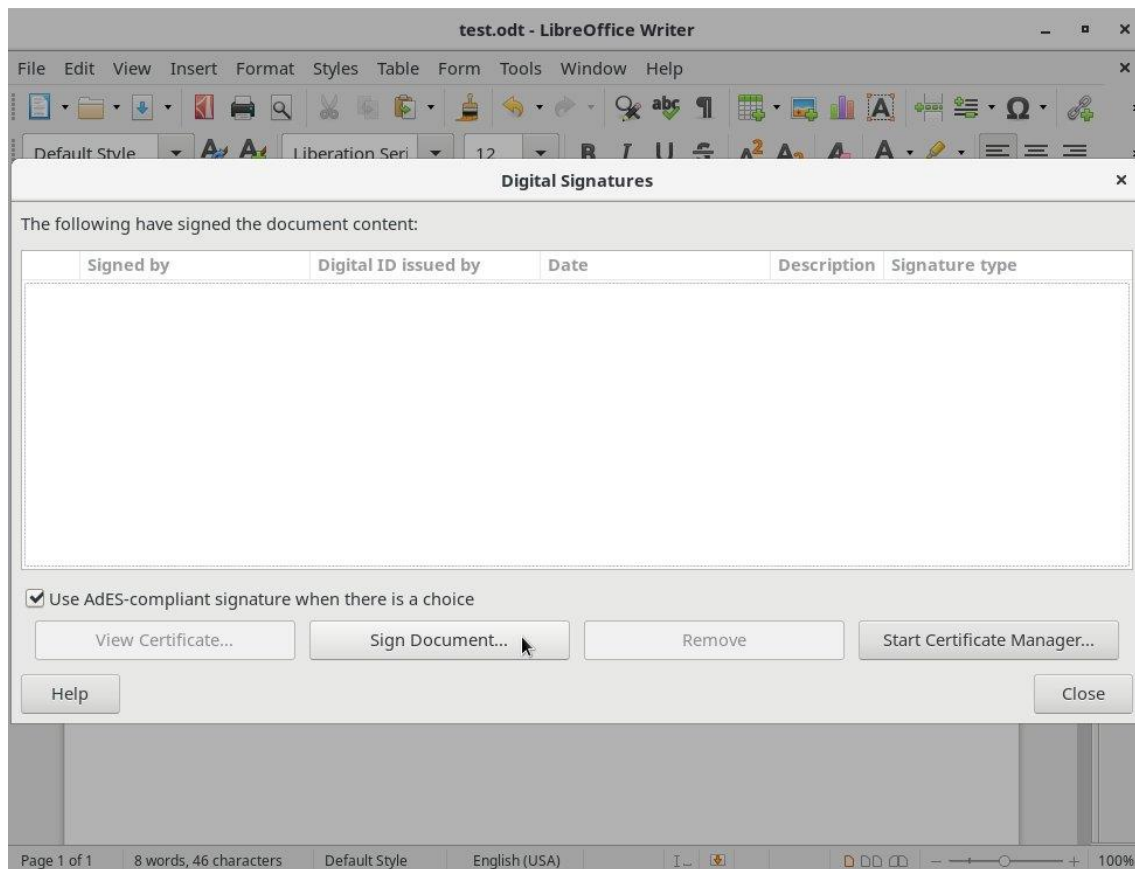
If you have not previously saved the document, LibreOffice alerts you that it has to be saved before it can be signed, and asks if you want to save it. Click **Yes** and save the document:
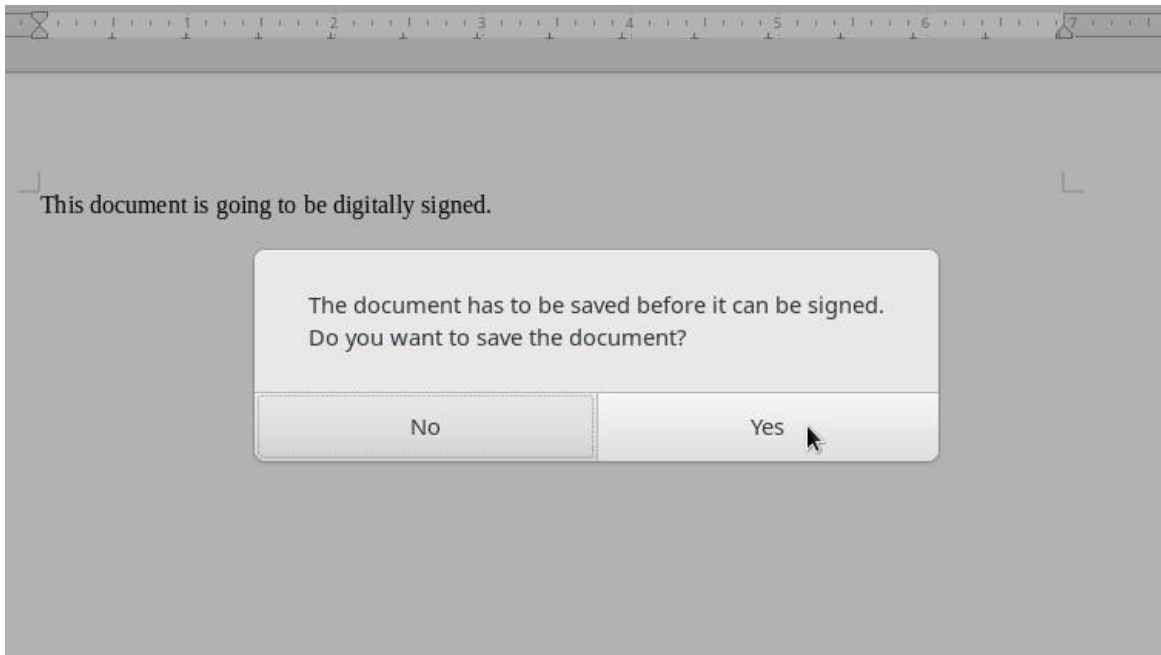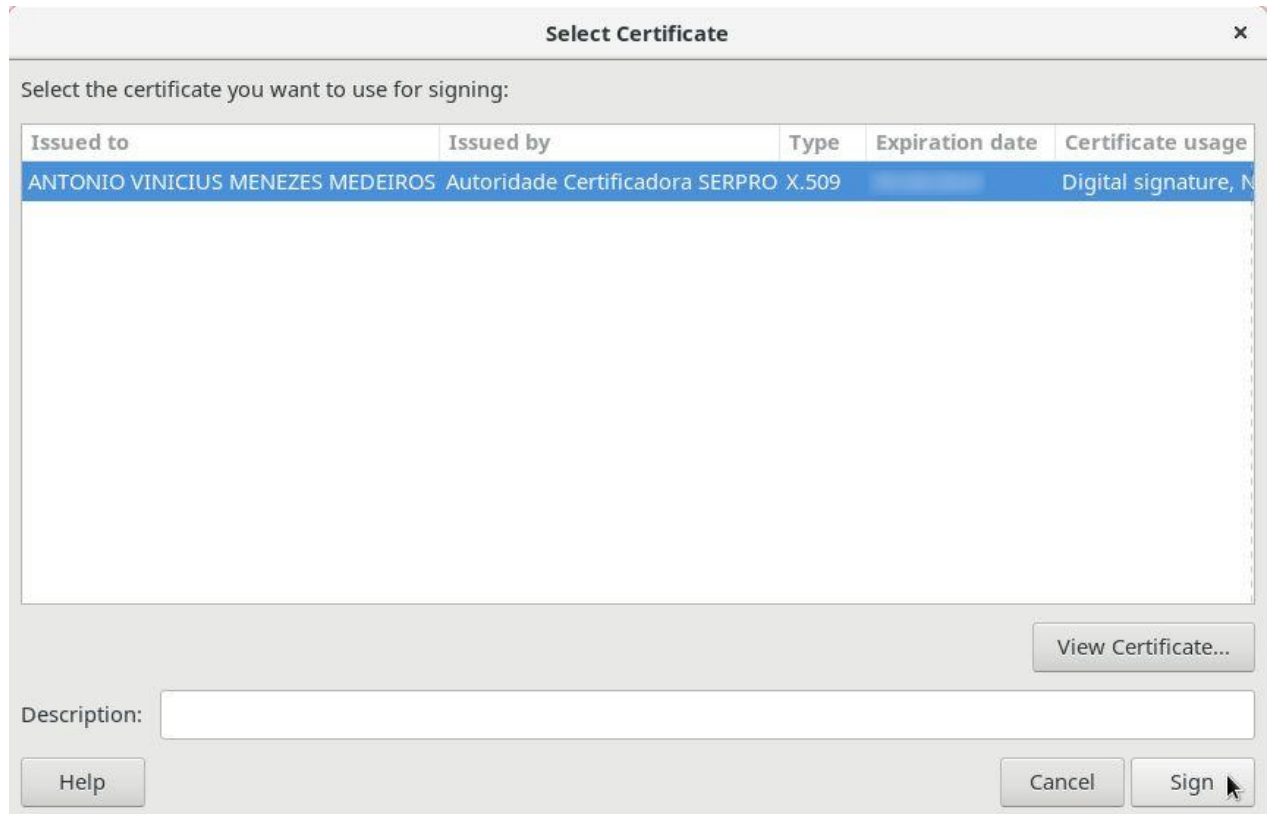
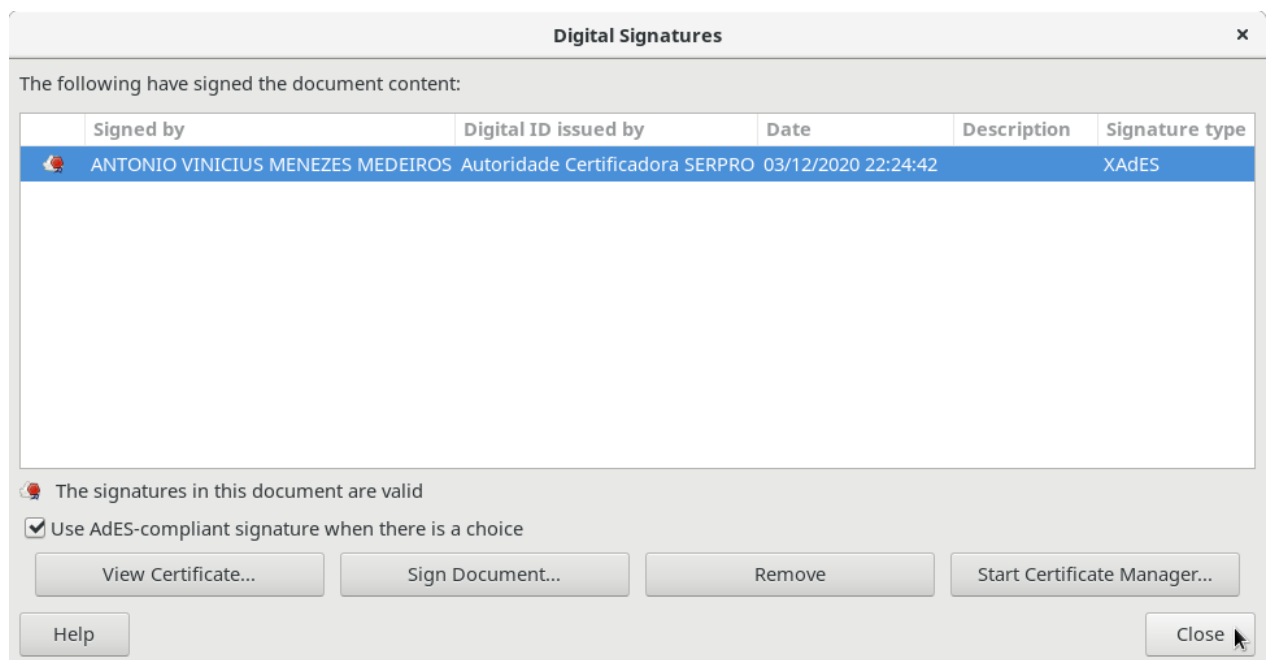On the **Digital Signatures** dialog box, click **Sign Document**:

LibreOffice asks for your token's PIN password. Type it and click **OK**.

On the **Select Certificate** dialog box, choose the certificate to be used to sign and click **Sign**:
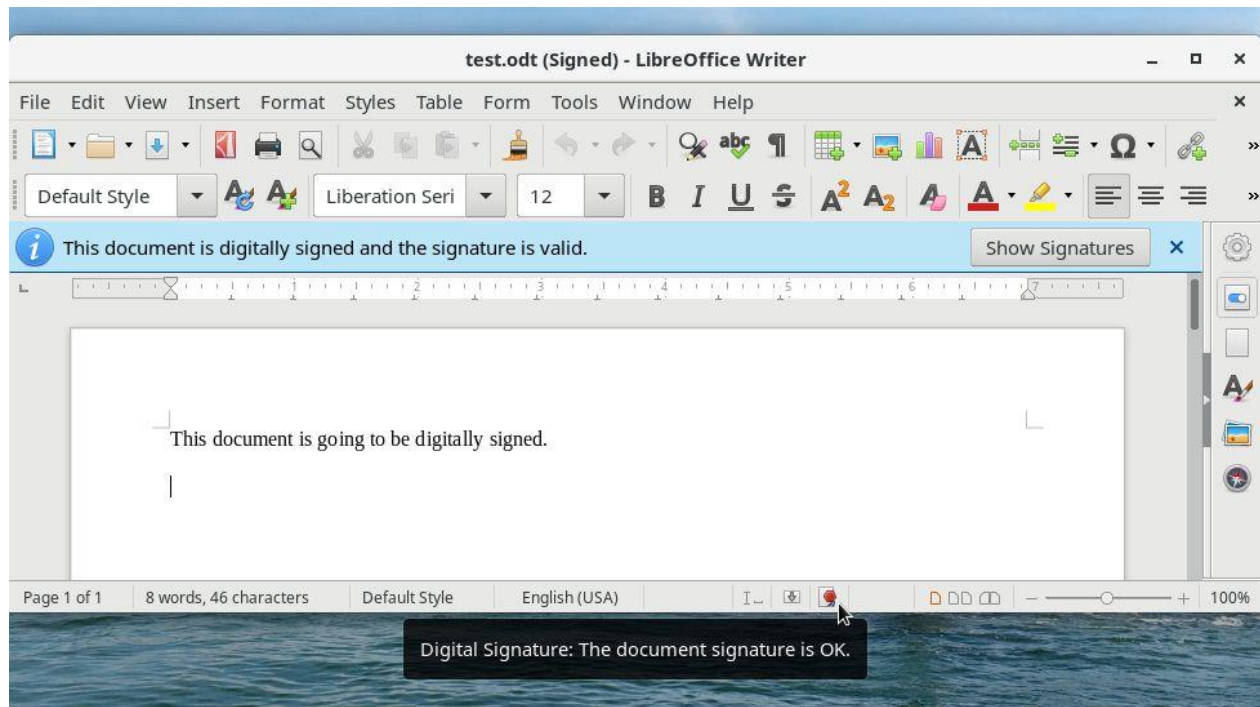

Back to the **Digital Signatures** dialog; note that the digital signature of the document is shown:


Click **Close**.

CHECKING THE DIGITAL SIGNATURE ON ODF AND PDF DOCUMENTS

When you open a signed ODF document, LibreOffice informs that the document is signed. In other words, you are seeing the original, unchanged document. It also shows the **Digital Signature** icon on the status bar:

To view the digital signature of the document, you can either double-click the **Digital Signature** icon on the status bar, or click the **Show Signatures** button on the alert.

On the **Digital Signatures** dialog box, you can select a signature and click **View Certificate** to see more information about the signer:
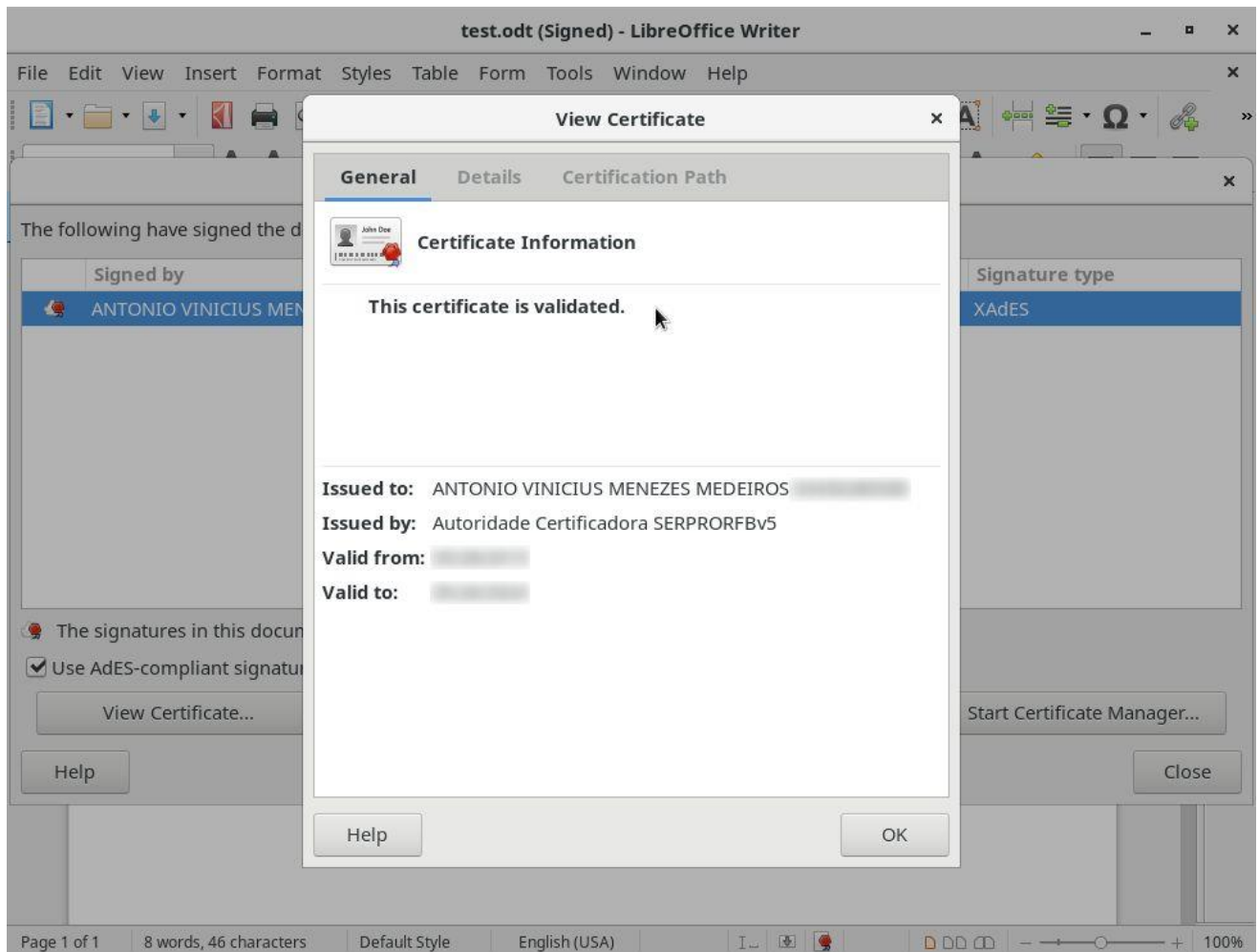
The message **This certificate is validated** indicates that LibreOffice was able to establish the **Certification Path** up to the certificate of a known certification authority:

That is similar to a web browser displaying a lock icon when you access an HTTPS website.
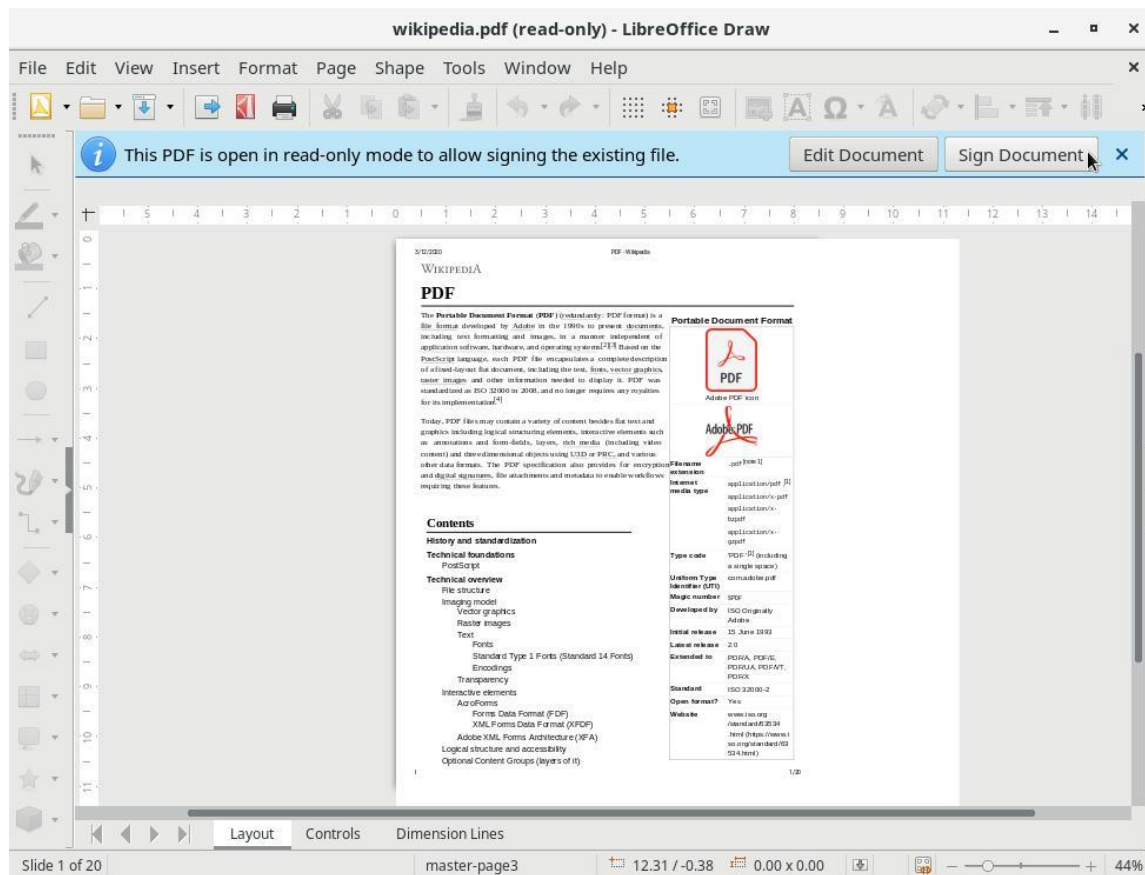

DIGITAL SIGNATURE ON PDF DOCUMENTS WITH LIBREOFFICE

LibreOffice is able to sign PDF documents created not only by the office suite itself, but also any existing PDF documents, even those created by other applications (outside LibreOffice).

You can sign an existing PDF document from any application of the LibreOffice suite: just go to the **File** menu, **Digital Signatures** submenu, click **Sign Existing PDF** and open the PDF document that you want to sign. LibreOffice Draw opens the document in read-only mode:

Click **Sign Document**. LibreOffice Draw presents the **Digital Signatures** dialog box.

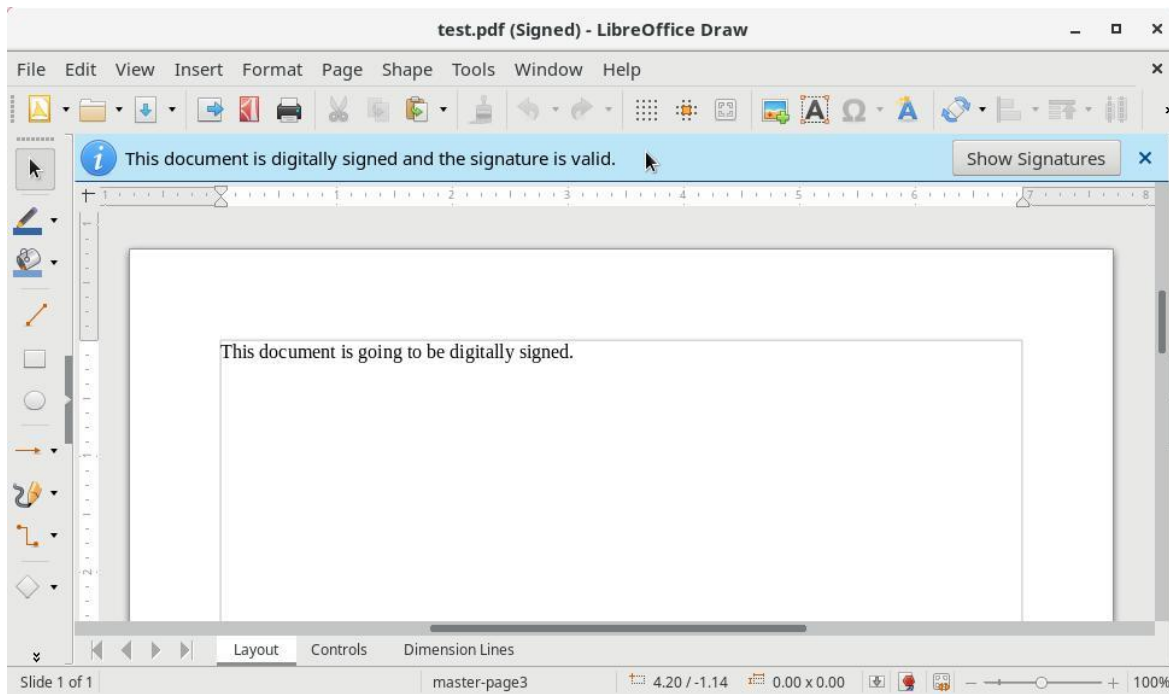Now you can sign the PDF document the same way you would sign an ODF document.

CHECKING THE DIGITAL SIGNATURE ON PDF DOCUMENTS

LibreOffice Draw can open PDF documents.

When you open a signed PDF document, LibreOffice Draw notifies you that the document is signed, it also shows the **Digital Signature** icon on the status bar (just as it does with signed ODF documents):

To view the signature, you can either double-click the **Digital Signature** icon on the status bar, or click the **Show Signatures** button on the alert.