



# Linux and LibreOffice User Guide for HYP2003

## HyperPKI USB Token

09/09/2022

HSTE-NB0066-IND-RV1.0

HYPERSECU INFORMATION SYSTEMS INC

200-6191 Westminster Hwy, Richmond BC, V7C 4V4 Canada  
1-604-279-2000 | [hypersecu.com](http://hypersecu.com)

# Table of Contents

Getting Started.....	1
Installing HYP2003 Token Driver in Linux Ubuntu.....	1
Setting Up Chrome to Use the HYP2003 Token for PDF Signing .....	2
Setting Up LibreOffice to Use Chromium Certificates .....	6
Setting up Mozilla Firefox to Use the HYP2003 Token to Sign PDFs in LibreOffice .....	8
Digital Signing with LibreOffice .....	12
Digitally Signing ODF Documents.....	12
Digitally Signing Existing PDF Documents .....	16
Checking the Digital Signature on ODF Documents and Existing PDF Documents .....	17

# Document History

Version	Release Date	Description of Changes	Document Owner	Approved By
1.0	2022-09-09	Original document	NB	JL

# Getting Started

## Installing HYP2003 Token Driver in Linux Ubuntu

1. Open the terminal and execute the command `uname -m` to determine if your system is 32-bit or 64-bit.
2. Extract the downloaded files, then find and open the config folder.
3. Right-click and select the open terminal here or open that path in terminal.
4. Enter the following command:

```
sudo sh config.sh
```

5. Enter the sudo user password.
6. After entering the password, you will receive the message `Run Finish >`
7. Enter the following command:

```
cd ../redist >
```

8. Enter the following command:

```
sudo chmod a+x pkimanager >
```

9. Enter the following command:

```
sudo chmod 775 >
```

10. Enter the following commands:

```
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 >
```

11. Plug the token into the system and double-click to open the pkimanager from redist folder.
12. Check the status of the token to make sure you receive the message that the token is inserted and ready to use.

---

**NOTE:** This works for only CSP 2.0 tokens (as per CCA Guidelines for PKI Hardware, issued in 2018). `libcastle_v2.so.1.0.0` is the PKCS#11 library file which communicates with the token for the certificate.

In the application where you want to use the certificate, that application must be able to browse PKCS#11 lib (`libcastle_v2.so.1.0.0`) in it.

If you are using a token with CSP V.10, you can update your existing token to CSP V2.0 from <https://update.epasstokens.com>.

---

## Setting Up Chrome to Use the HYP2003 Token for PDF Signing

Chrome for Linux manages digital certificates similarly to Firefox by using Mozilla NSS as the backend. However, unlike Firefox, Chrome does not provide a graphical user interface to install PKCS#11 modules. Therefore, to set up Chrome you will need to use the command line.

---

**NOTE:** Make sure your token contains the user certificate and is plugged in before proceeding. You must also be using a HYP2003 token with **CSP V2.0**.

---

1. Open the terminal and install Mozilla NSS Tools if it is not 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
```

2. `modutil` will alert you that you need to close your browser if it is not already closed. Type `q` `<enter>` to abort or `<enter>` to continue.
3. Once any running browsers are closed, press **Enter**. When the command finishes, you can reopen your browser.

---

**WARNING:** Performing this operation while the browser is running could corrupt your security databases.

---

4. Module "epass2003" is added to the database.
5. Verify that the token has been successfully added by running the following command:

```
$ modutil -dbdir sql:~/.pki/nssdb/ - list
```

6. As root, to load the root CA (CCA India 2022, 2014) certificate into the NSS database, enter the following command:

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

7. To root load each sub CA's public certificate into the NSS database, enter the following command:

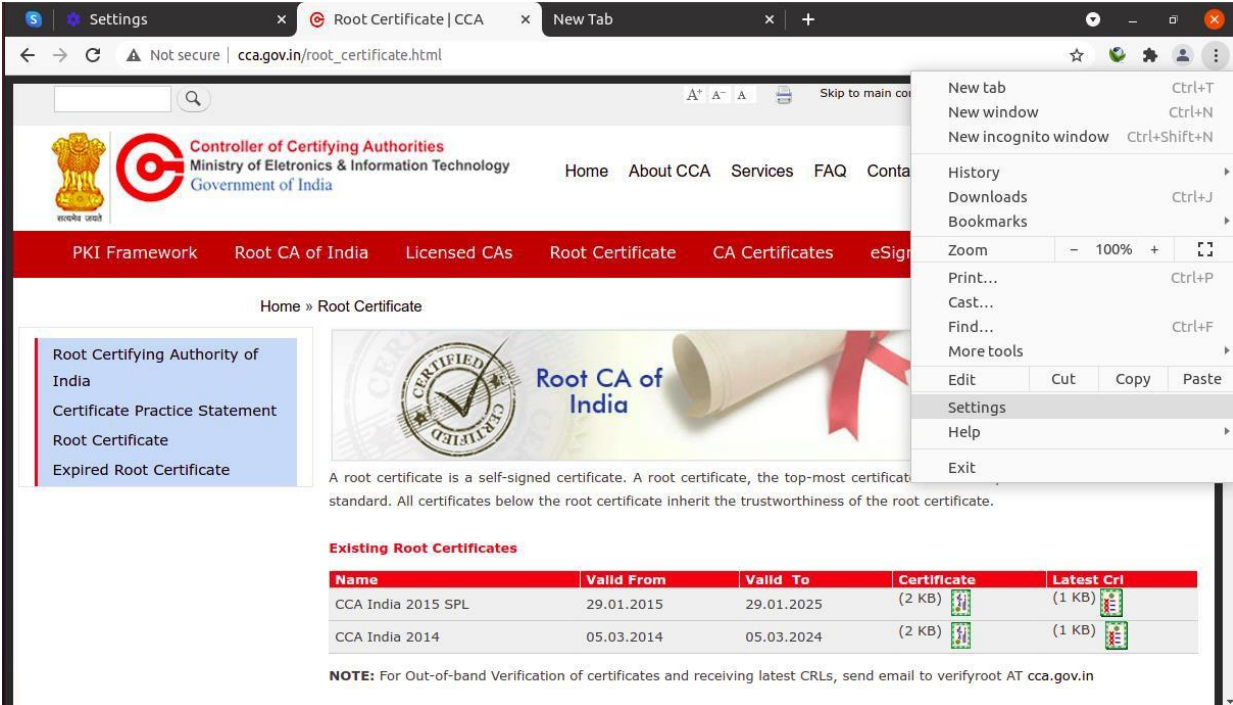
```
certutil -A -n subca -i /location_of_subca_root_cert/rootcert.pem -t "CT,CT,CT" -d ~/.pki/nssdb
```

8. To verify that the certificates have loaded, as root, enter the following command:

```
certutil -L -d ~/.pki/nssdb
```

It is also possible to verify the trust of a root CA certificate through the Chrome browser.

1. Open Chrome, then open the menu and click **Settings**.

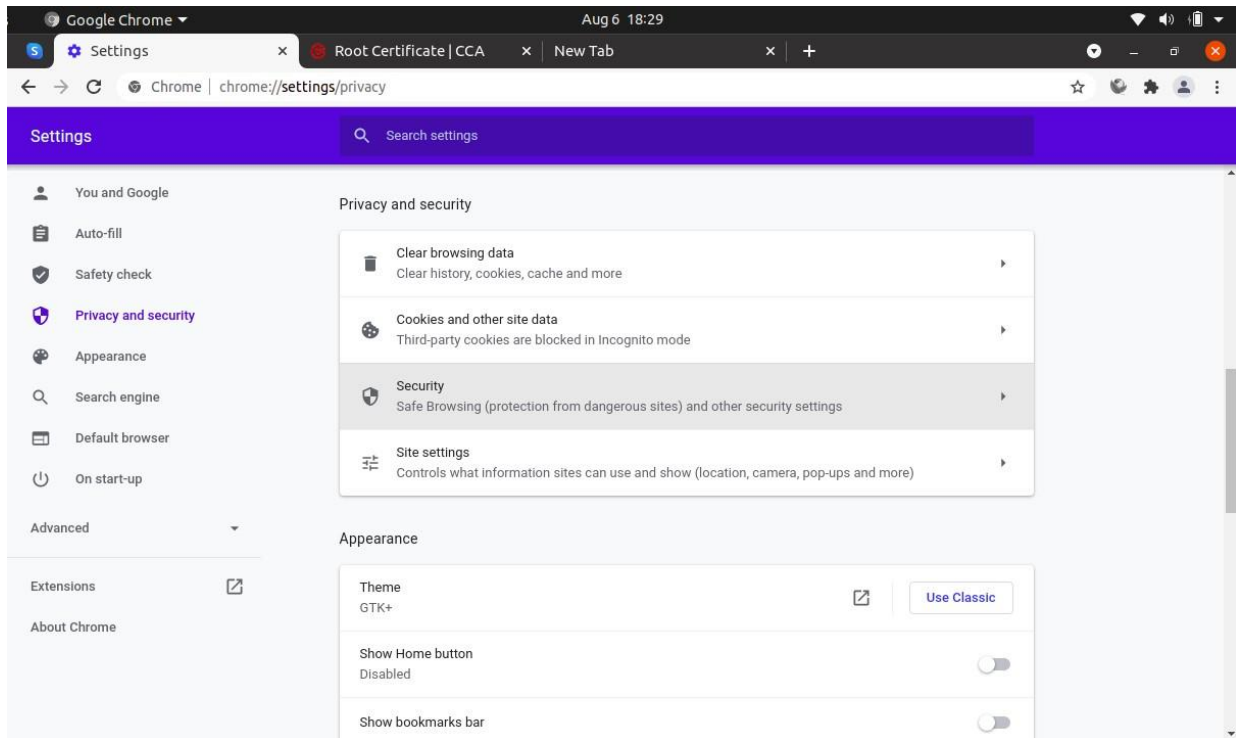


The screenshot shows a Chrome browser window with the address bar displaying 'cca.gov.in/root\_certificate.html'. The page content includes the CCA logo and navigation menu. A table titled 'Existing Root Certificates' is visible, listing two certificates: 'CCA India 2015 SPL' and 'CCA India 2014'. A Chrome menu is open, showing the 'Settings' option highlighted.

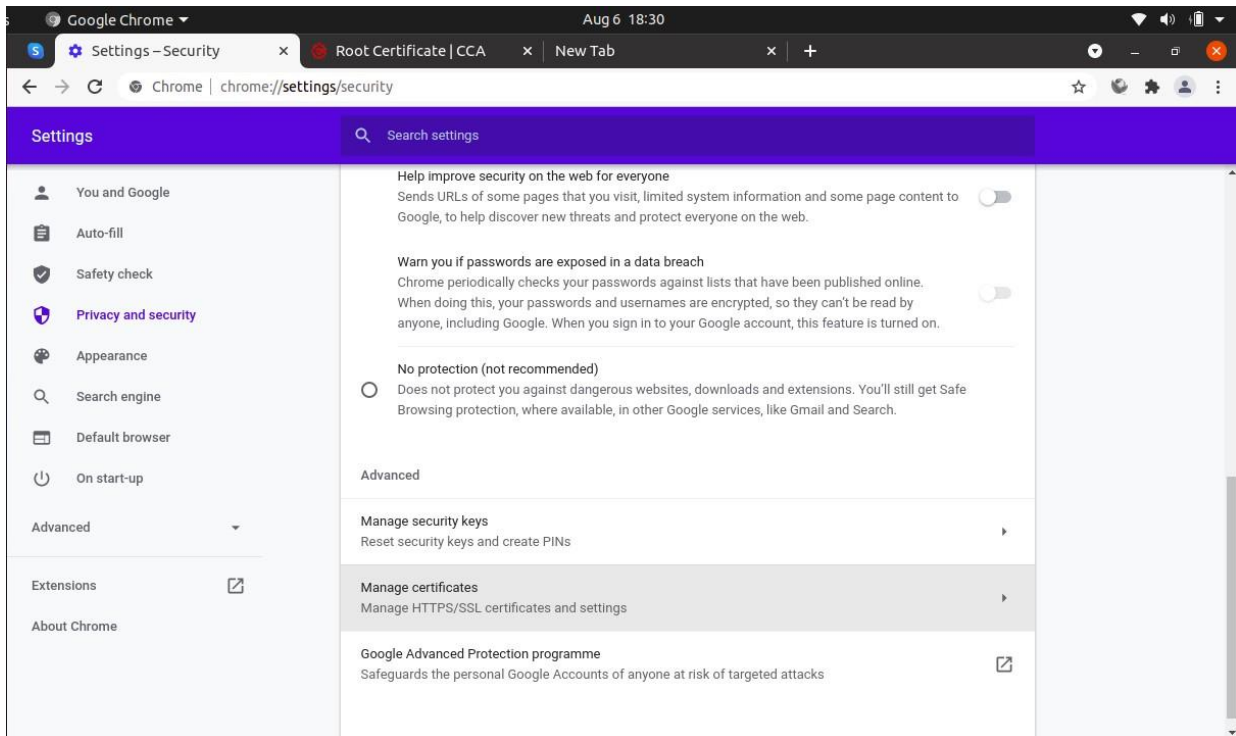
Name	Valid From	Valid To	Certificate	Latest Crl
CCA India 2015 SPL	29.01.2015	29.01.2025	(2 KB)	(1 KB)
CCA India 2014	05.03.2014	05.03.2024	(2 KB)	(1 KB)

**NOTE:** For Out-of-band Verification of certificates and receiving latest CRLs, send email to verifyroot AT cca.gov.in

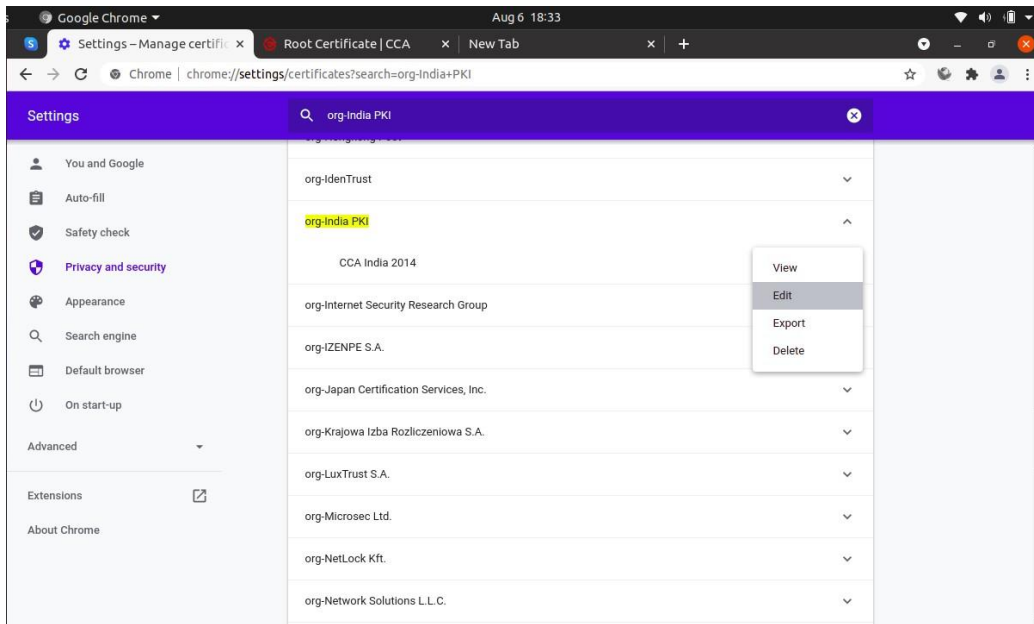
2. Select **Privacy and Security**, then select **Security**.



3. Navigate to **Manage Certificates** and click on the **Authorities** tab.



4. Navigate to **org-India PKI** and expand the section to find the CCA India 2014, which is the root-certifying authority in India. Root certificates available on the HYP2003 token will appear in the list here.

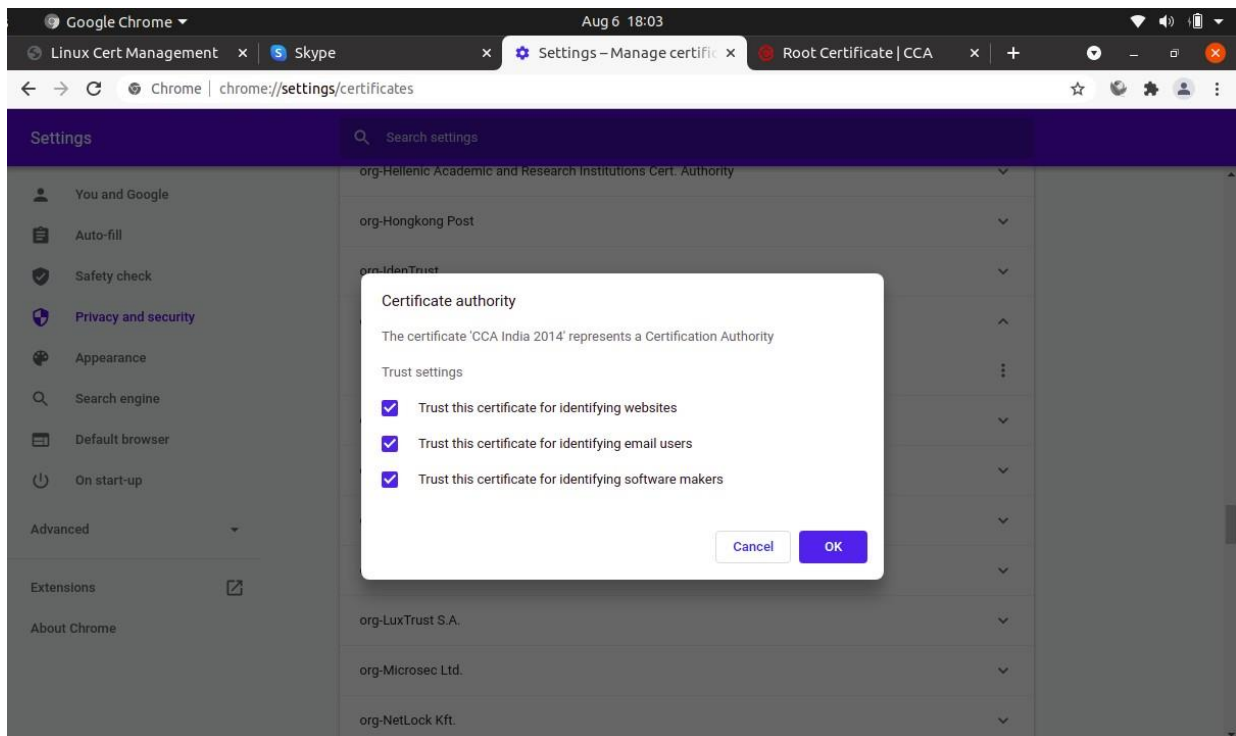


---

**NOTE:** If you can't find the CCA India 2014, you will need to import manually.

---

5. Click **Edit**, then check all available checkboxes and click **OK**.



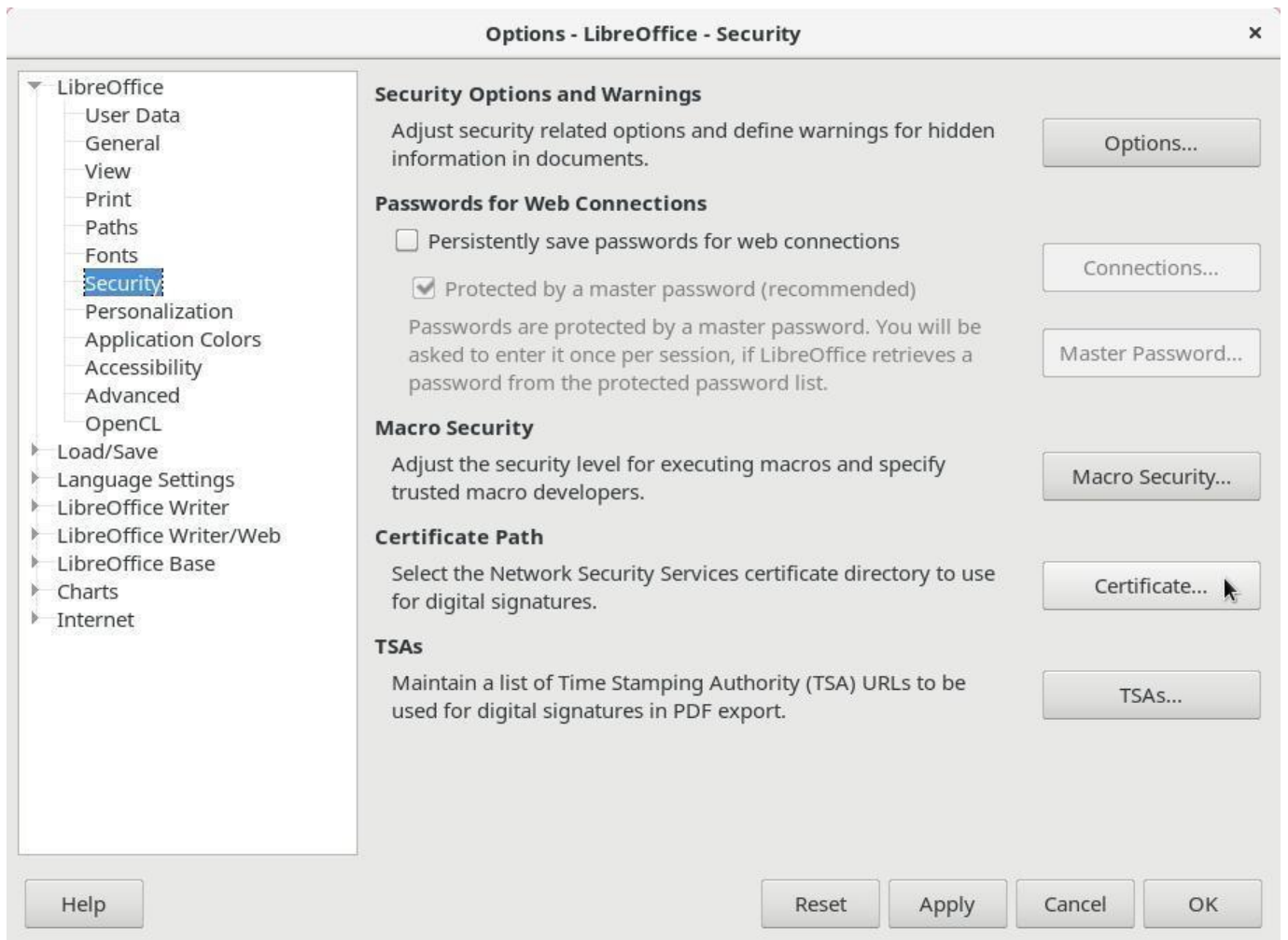


## Setting Up LibreOffice to Use Chromium Certificates

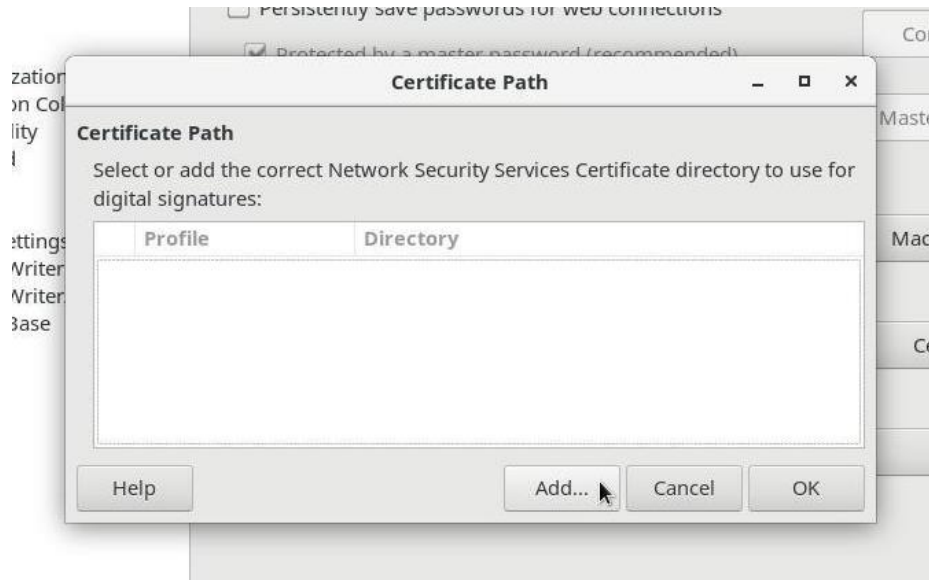
Chromium users do not need to install and set up Firefox to sign documents with LibreOffice. Instead, they can set up LibreOffice to use the Chromium public key infrastructure.

To do so:

1. Open the Tools menu, then click **Options**.
2. Click **LibreOffice** to expand the tree on the left side panel, then select **Security** and click **Certificate**.



3. In the Certificate Path window, click **Add**.

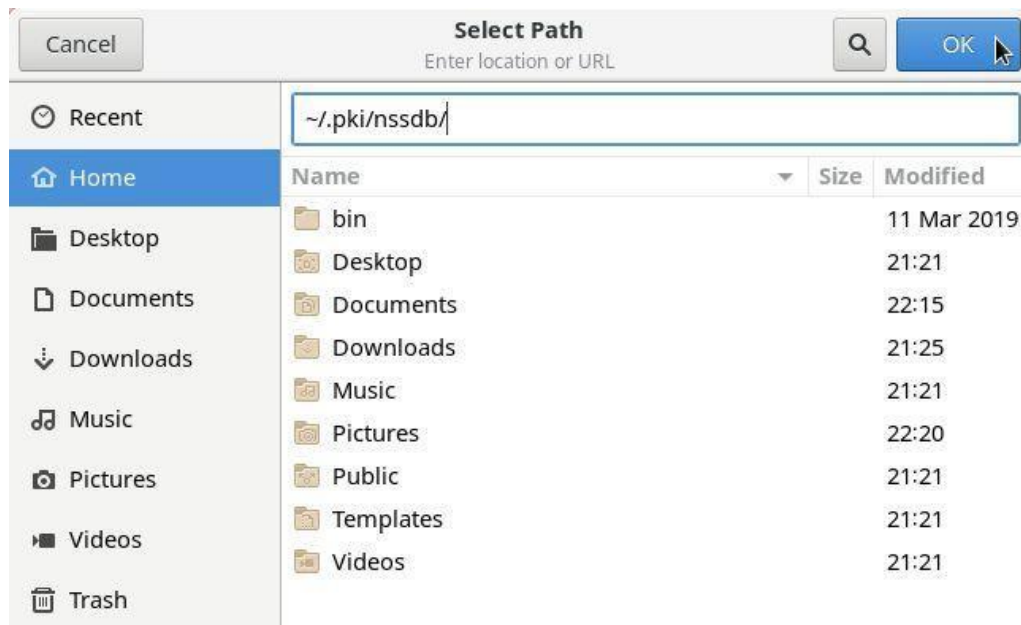



---

**NOTE:** Chromium stores its certificate configuration in `~/.pki/nssdb/`

---

4. In the Select Path field, press **Ctrl+L** to manually enter the location.
5. Enter `~/.pki/nssdb/` and click **OK**.

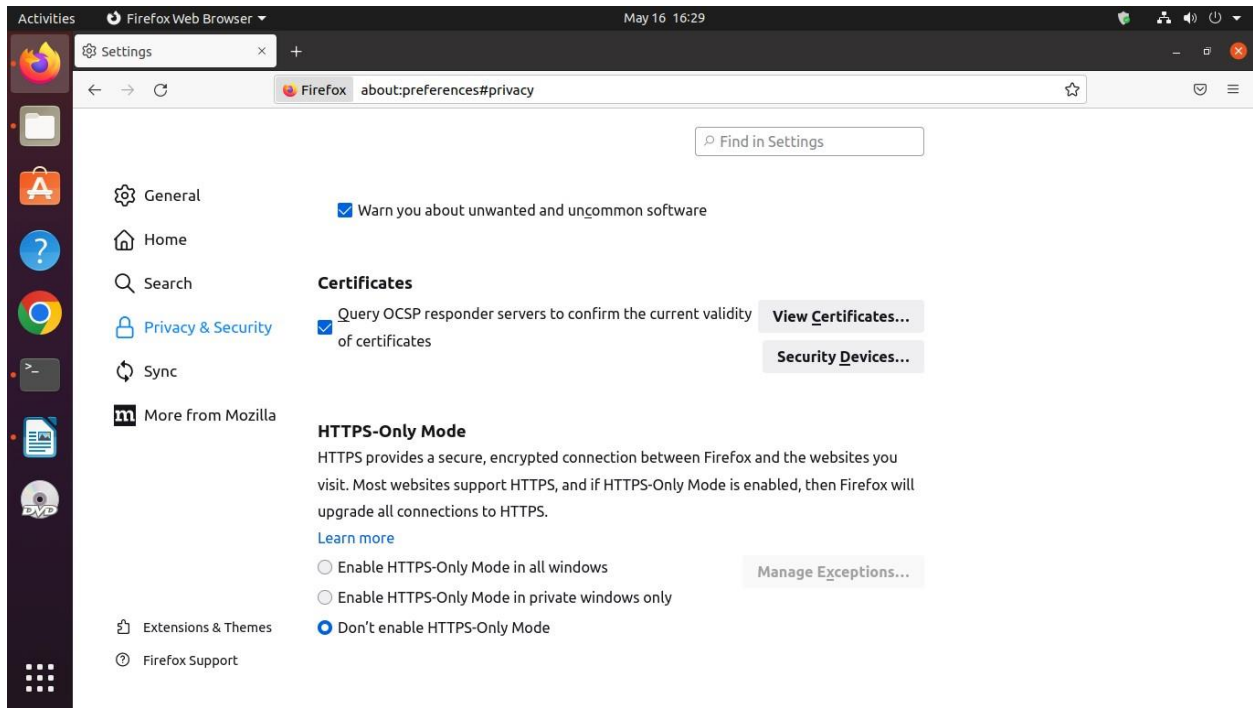


6. Click **OK** in the Certificate Path window to close the window, then click **OK** in the Options window to close the window.
7. Restart LibreOffice to complete setup.

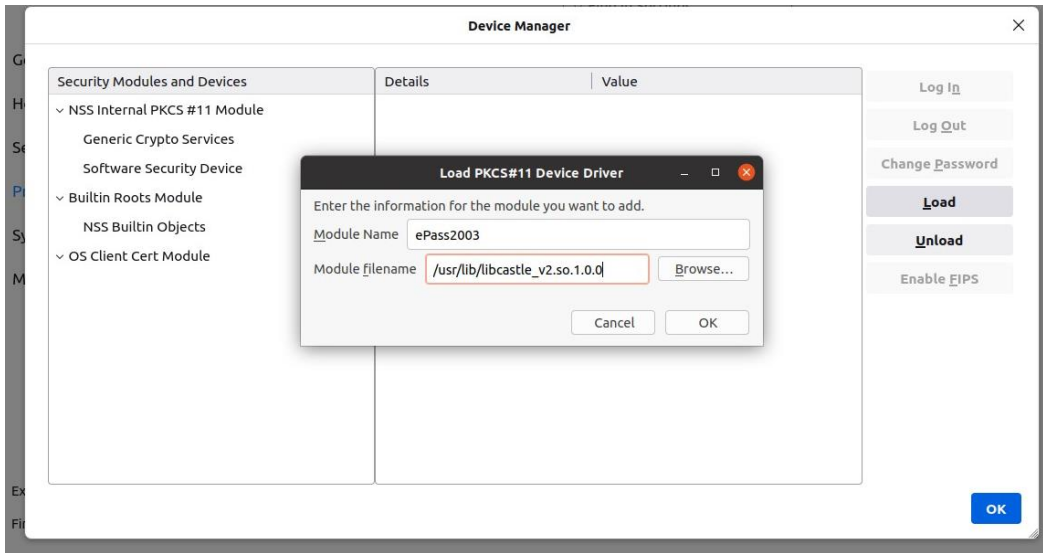
# Setting up Mozilla Firefox to Use the HYP2003 Token to Sign PDFs in LibreOffice

**NOTE:** Before getting started, be sure Mozilla Firefox can browse PKCS#11 lib (libcastle\_v2.so.1.0.0) in it.

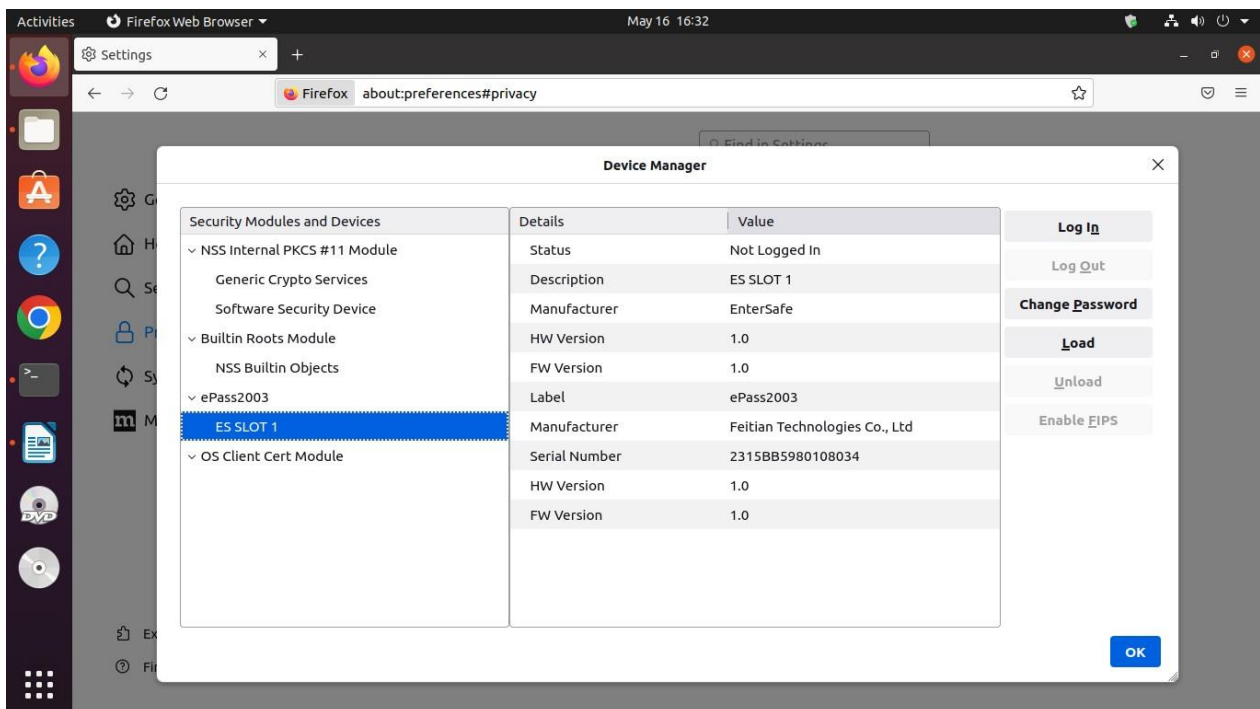
1. Open Firefox, then enter `about:preferences#privacy` into the address bar and press **Enter**.
2. Click **Security Devices** to open the Device Manager.



3. Click **Load**.
4. In the Module Name field, enter `ePass2003`.
5. In the Module File Name field, enter `/usr/lib/libcastle_v2.so.1.0.0`.



6. Click **OK** to close the Device Manager.



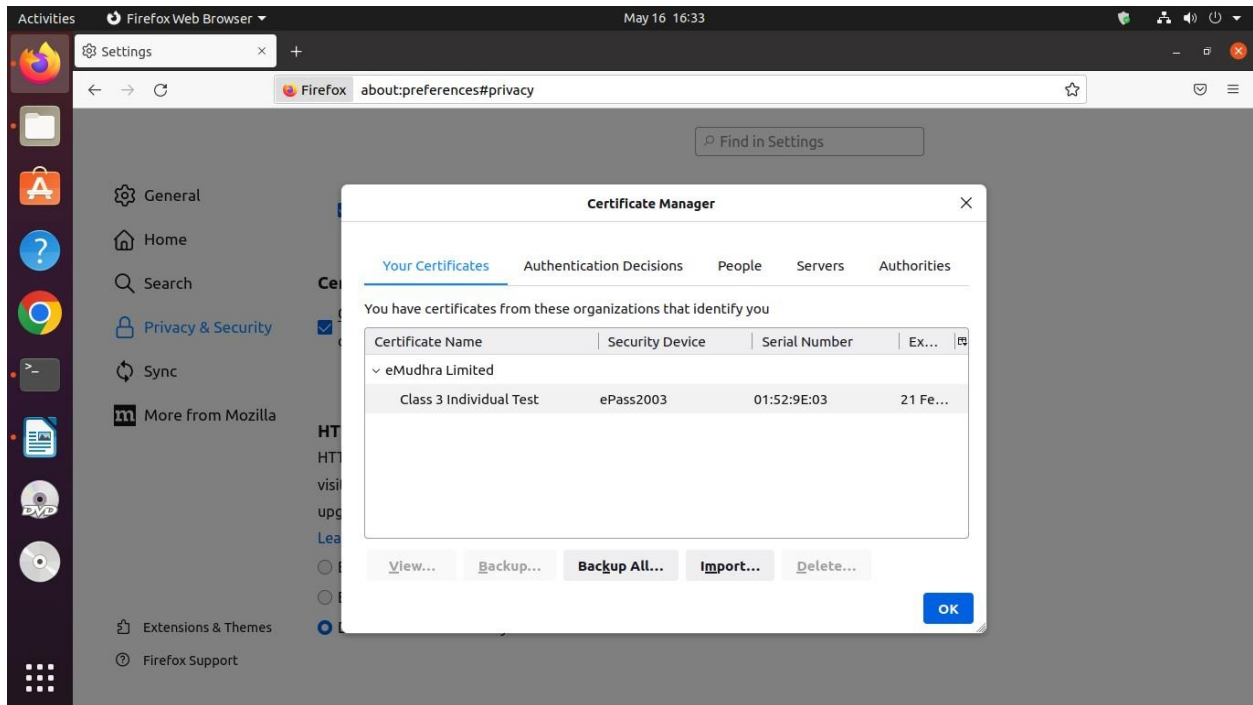
7. Click **Certificate**.

8. In the Your Certificates tab, you can view the current user certificate on the HYP2003 token.

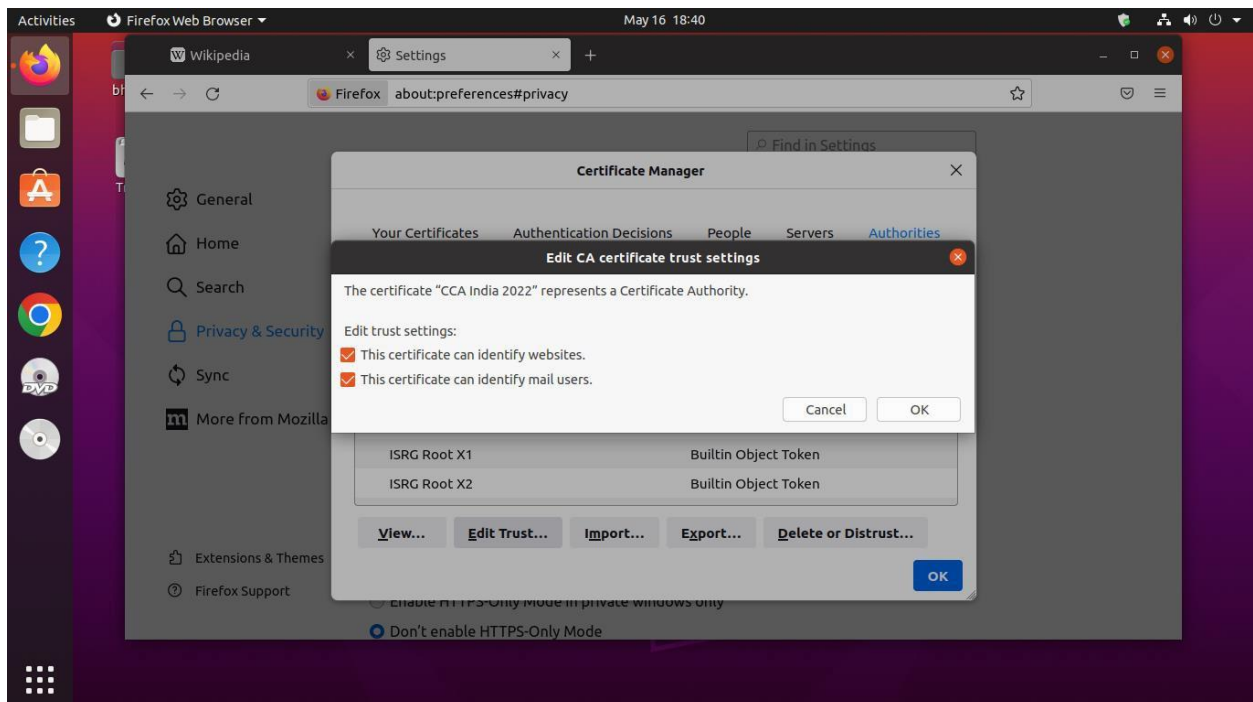
---

**NOTE:** Make sure the token is with root chain of CCA and Issuer CA.

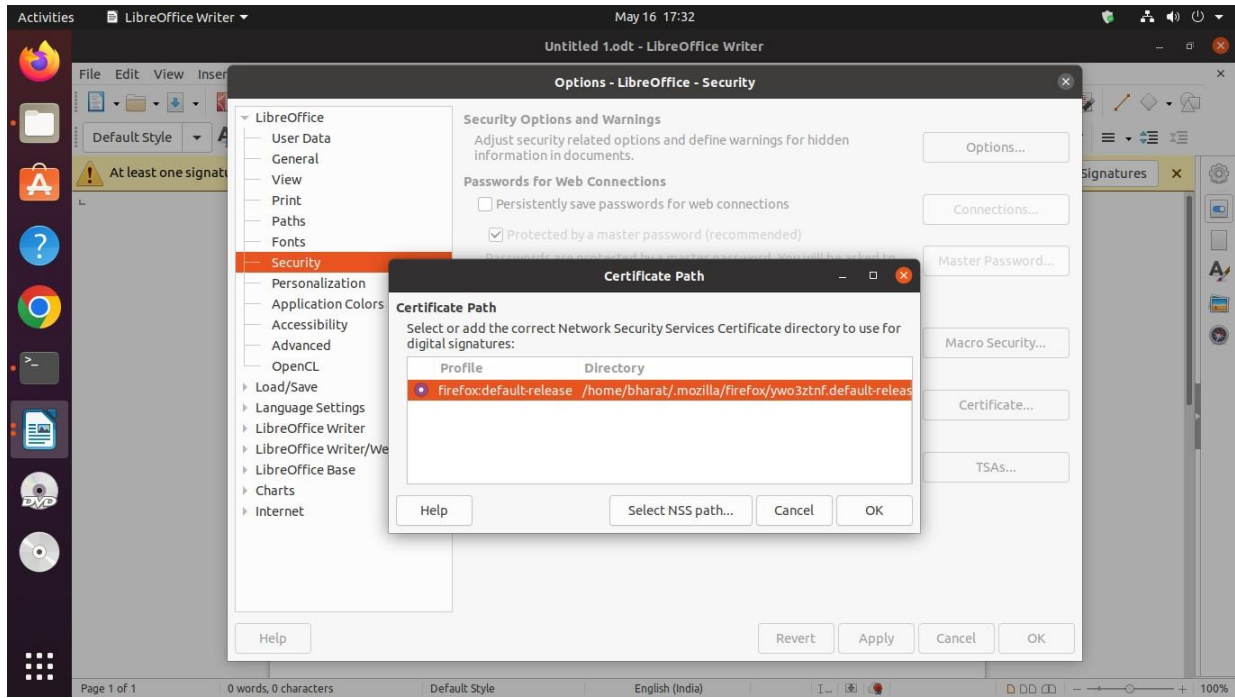
---



9. Click the **Authorities** tab and find the India PKI. Click **Edit Trust**, then check both checkboxes and click **OK**.



10. Open the LibreOffice writer and go to **Tools > Options > Security > Certificate**.
11. Make sure `Firefox:default-release` is selected, then click **OK**.



# Digital Signing with LibreOffice

If you have a digital certificate, you can sign documents before sending them to ensure the recipient is confident about the documents' authenticity and integrity. LibreOffice can sign not only Open Document Format (ODF) documents, but also any PDF documents including those created by other programs.

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

## Mozilla Firefox Browser

By default, LibreOffice looks for certificates and cryptographic media in the Mozilla Firefox configuration. If you use Firefox, you must set it up before signing documents with LibreOffice. To do so, follow the procedures described in the documents below:

- [How to install website certificates on Linux](#)
- [Using smart cards on openSUSE Linux](#)

## Chromium-Based Browsers

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.

To do so, follow the procedures described in the document below:

- [Setting up smart card authentication on Google Chrome / Chromium](#)

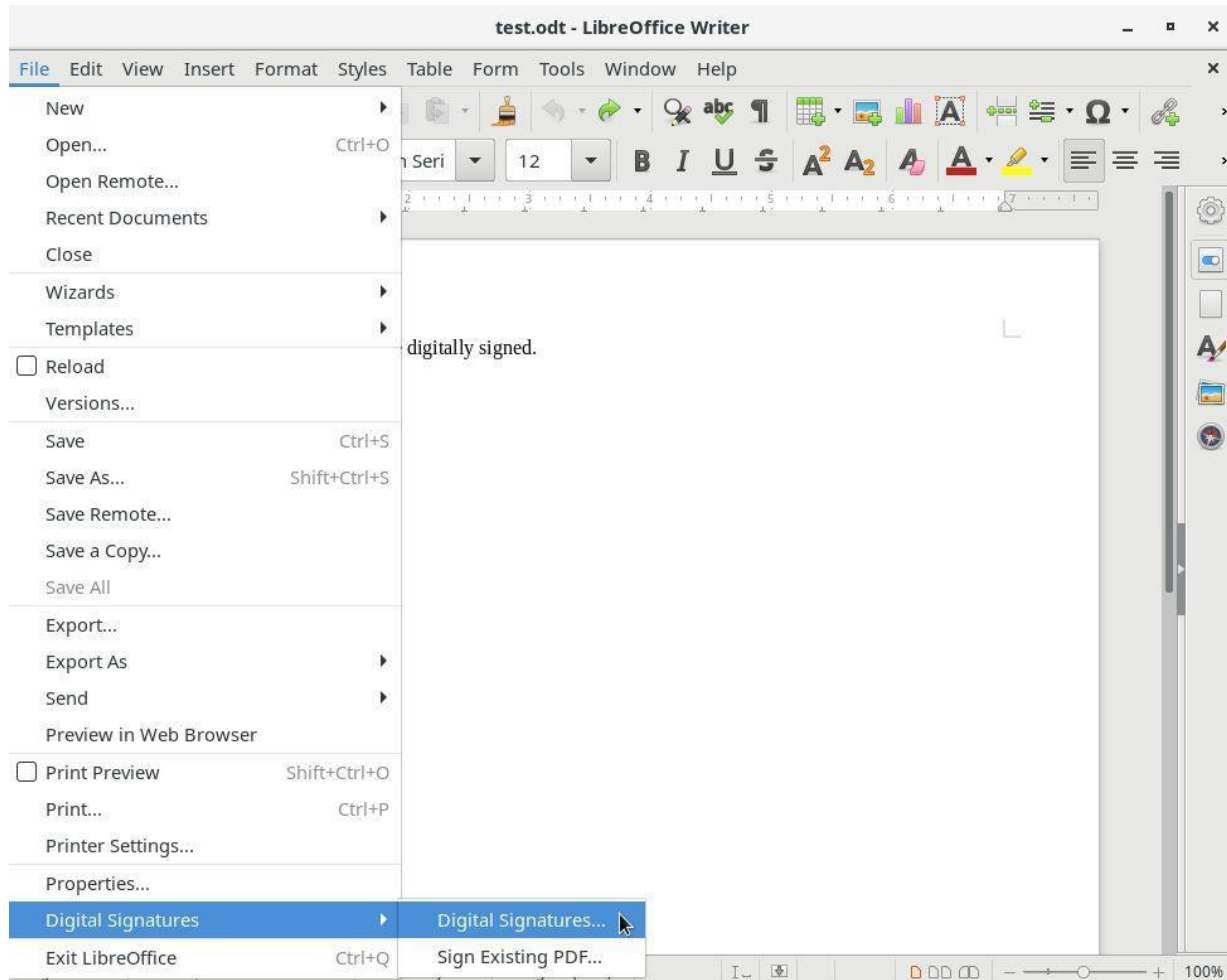
## Digitally Signing ODF Documents

The Open Document Format (ODF) is the default file format for LibreOffice. The following file types and extensions are all considered ODF documents and can be digitally signed:

- `.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
- `.odf` for mathematical equations (formulas), opened with Math

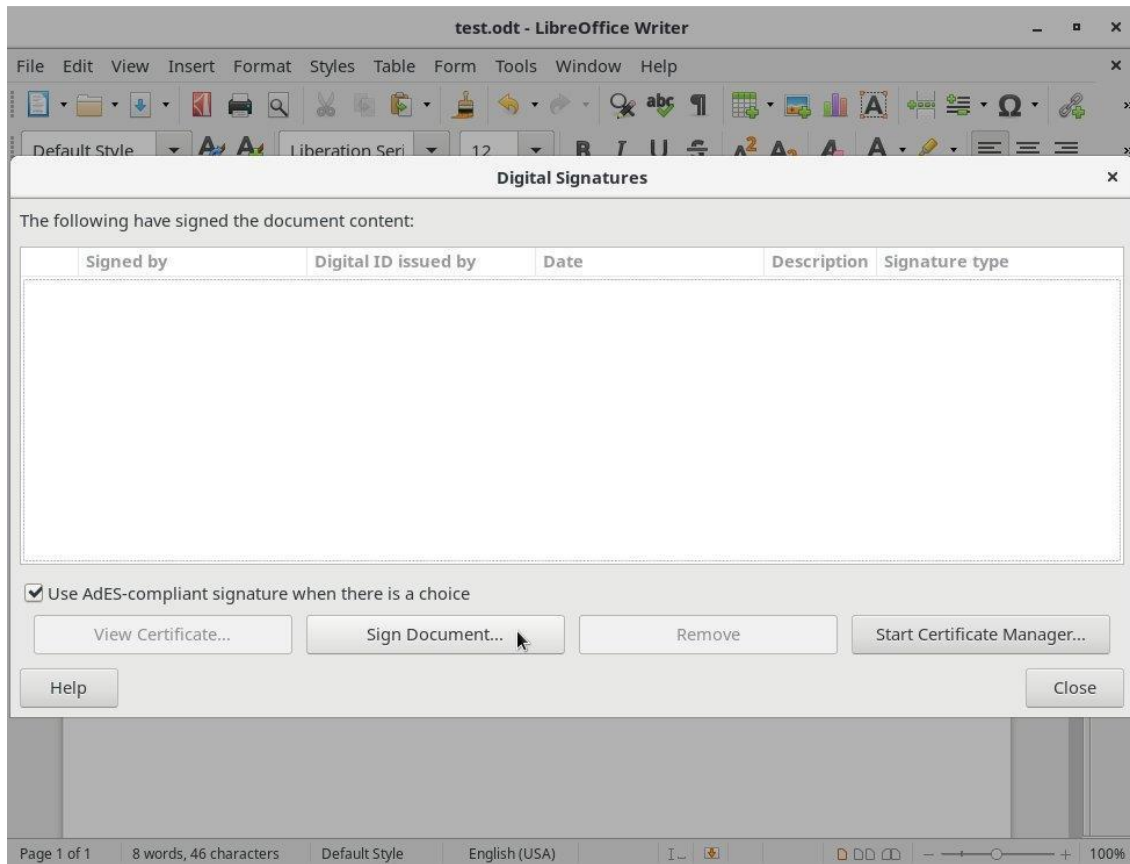
This section will use a .odt file to demonstrate how to digitally sign an ODF document. The steps will be similar for all ODF files using a LibreOffice Suite application.

1. Open the **File** menu, then navigate to Digital Signatures and click **Digital Signatures**.

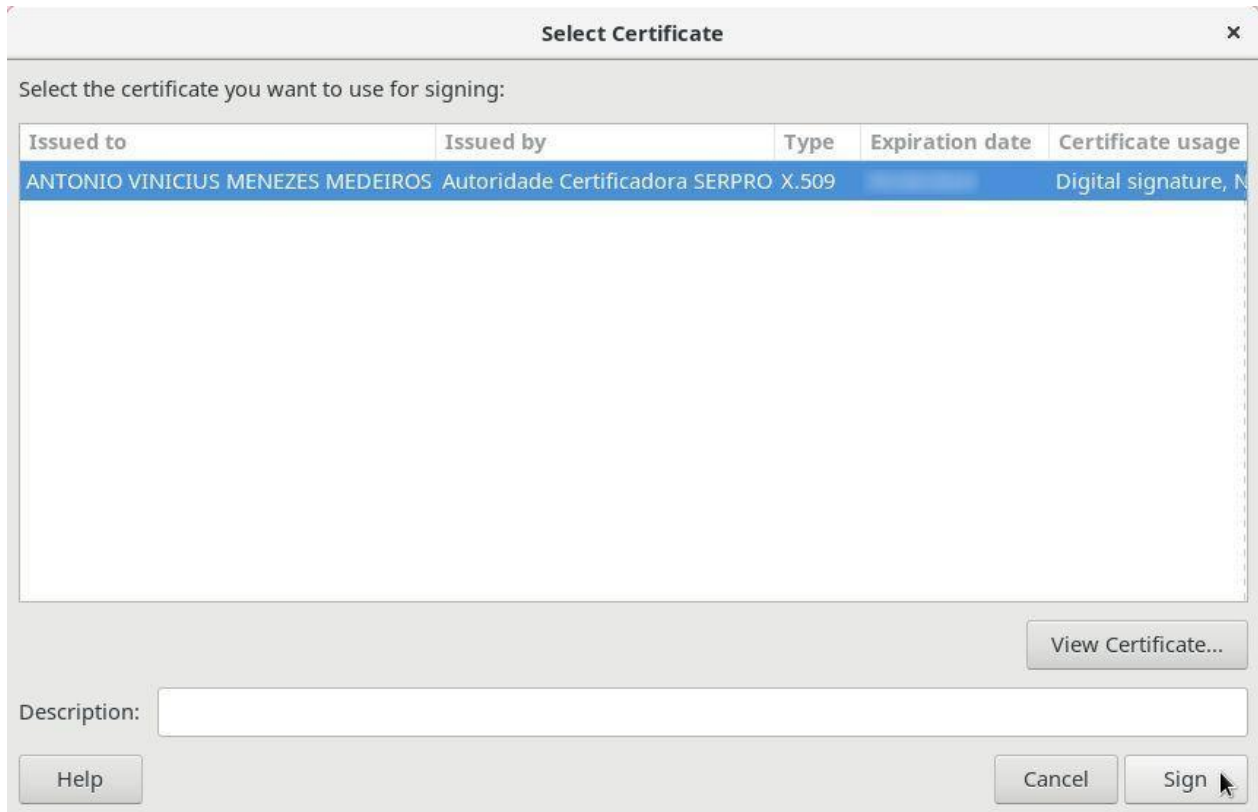


2. If you are prompted to save the document, click **Yes**.
3. In the Digital Signatures window, click **Sign Document**.

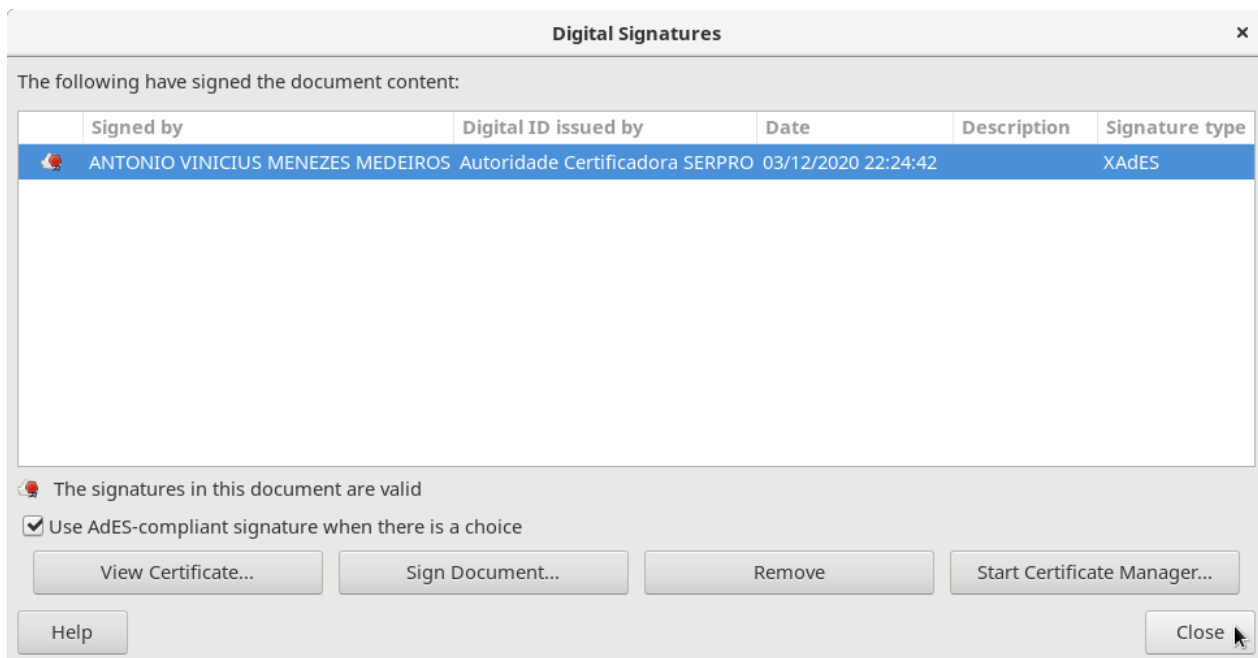


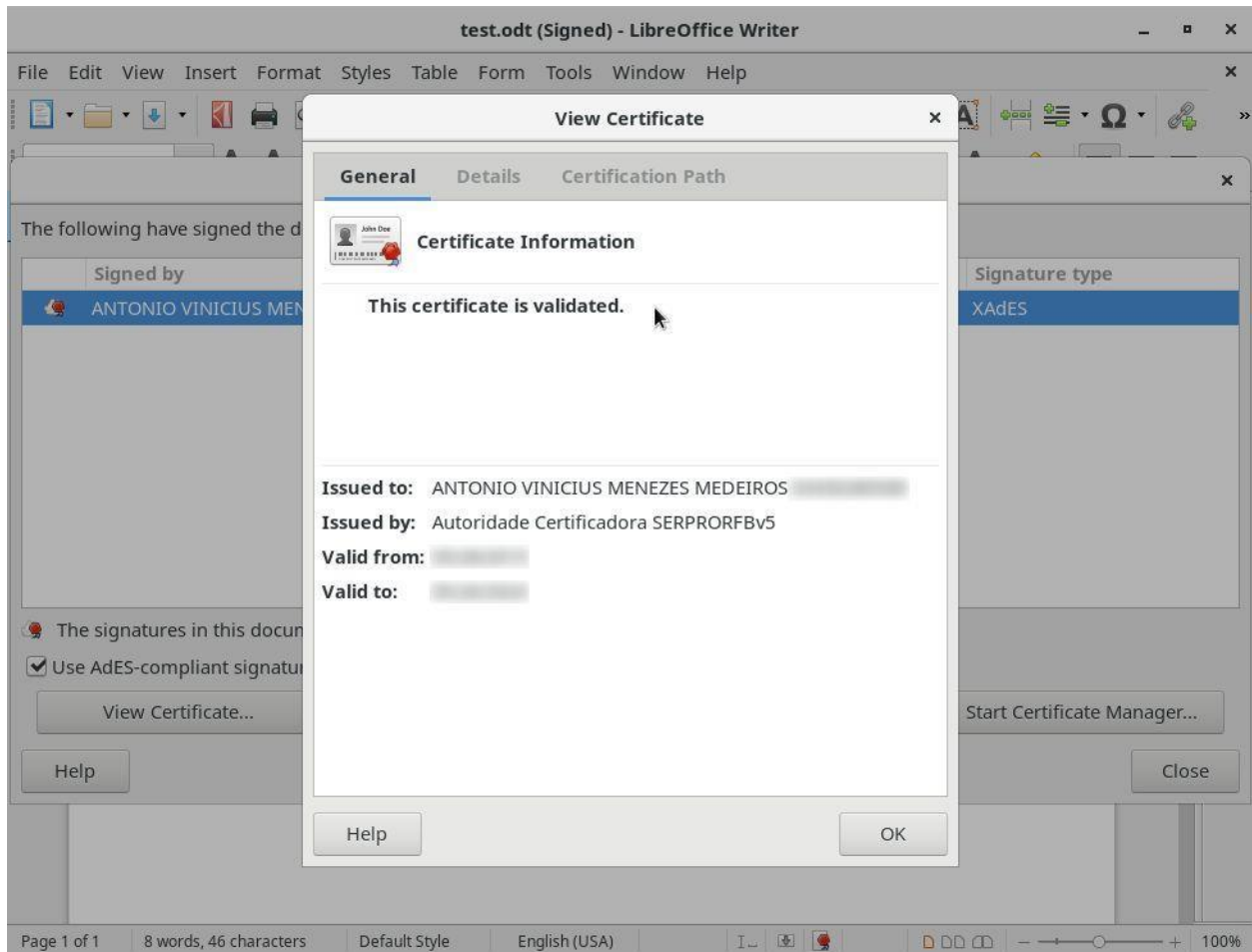


4. Enter the token's PIN, then select the certificate you want to use to sign the document and click **Sign**.



- In the Digital Signatures window, confirm that the document has been digitally signed and click **Close**.



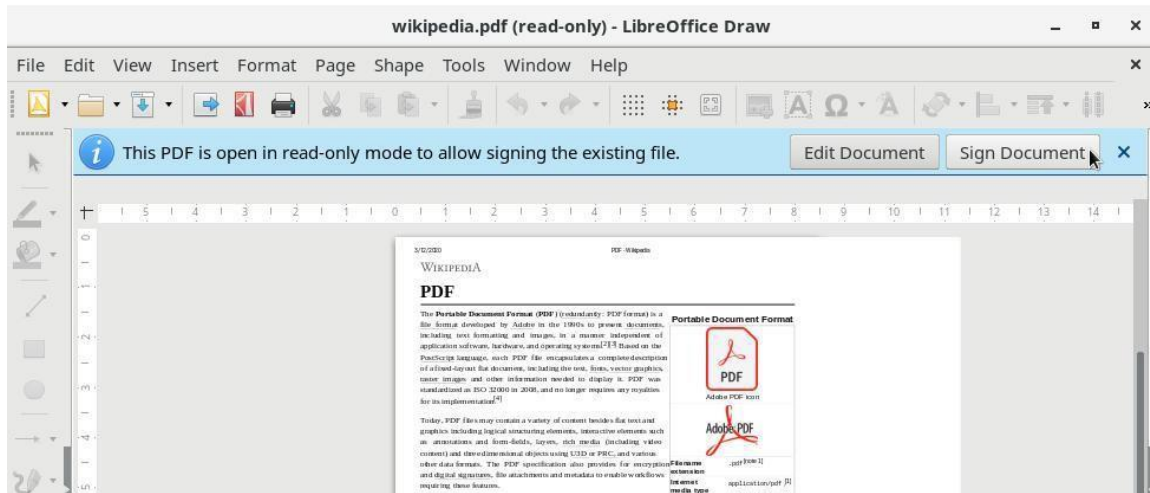


## Digitally Signing Existing PDF Documents

LibreOffice also sign any existing PDF documents, including those created by other applications outside LibreOffice.

To sign an existing PDF document using LibreOffice:

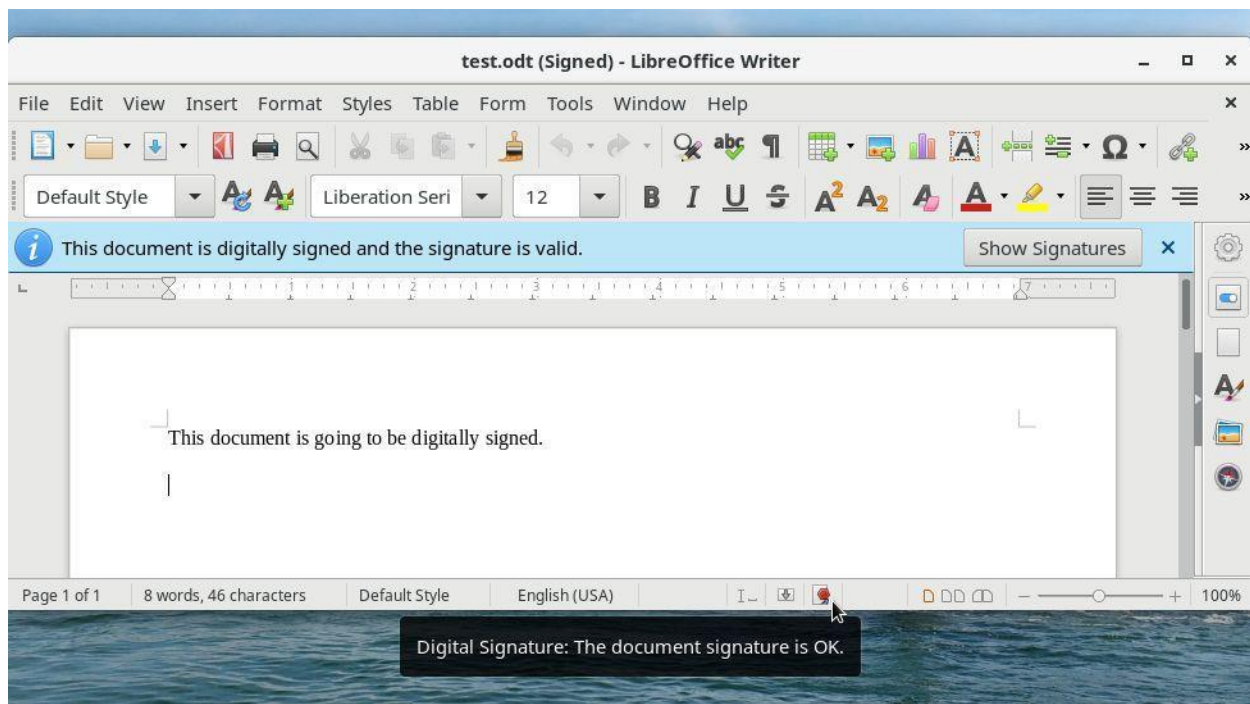
1. Open the **File** menu, then navigate to Digital Signatures and click **Sign Existing PDF**.
2. Open the PDF document you want to sign. LibreOffice will open the document in Read-Only mode.



3. Click **Sign Document** and follow the procedures described in steps 3-5 in *Digitally Signing ODF Documents* to complete the digital signing process.

## Checking the Digital Signature on ODF Documents and Existing PDF Documents

When you open a digitally signed ODF document or a digitally signed existing PDF document, LibreOffice will inform you that the document is signed. It will also display the Digital Signature icon on the status bar.



To view the document's digital signature:

1. Double-click the **Digital Signature** icon on the status bar or click **Show Signatures** on the system message.
2. In the Digital Signatures window, select a digital signature and click **View Certificate** to view more details.

---

**NOTE:** The Certificate Information “This certificate is validated” and the Certification status “This certificate is OK” indicates that LibreOffice has established the Certification Path up to the certificate of a known certificate authority.

---