

DSCSigner Installation Manual for Ubuntu

Contents

1. DSCSigner installation in Ubuntu.....	3
1.1. DSC token driver installation	3
1.2. DSCSigner installation	3
2. Browser Configuration.....	6
2.1. Mozilla Firefox	6
2.2. Google Chrome.....	9

1. DSCSigner installation in Ubuntu

For Ubuntu operating system the following prerequisites are required:

- DSC token driver
- Java8

However, Java 8 runtime is bundled along with the DSCSigner Debian package and will be installed and configured along with installation.

1.1. DSC token driver installation

To install DSC driver,

- Make sure you have JRE 1.8 installed
- Use key combination **Ctrl+Alt+t** open terminal
- Enter **java -version** to check installed java version
- Proceed installation, if **java -version** shows to be **1.8**, otherwise install and proceed

```
gst@gstnode1:~$ java -version
java version "1.8.0_144"
Java(TM) SE Runtime Environment (build 1.8.0_144-b01)
Java HotSpot(TM) 64-Bit Server VM (build 25.144-b01, mixed mode)
```

- Copy driver to Desktop. Here for Eg: ProxKey Token.



- To install token driver, open terminal **Ctrl+Alt+t**
- Type **cd Desktop** to go to Desktop
- Install driver using command:

```
sudo dpkg -i wdtokentool-proxkey_1.1.0-1_all.deb
```

```
gst@gstnode1:~$ cd Desktop
gst@gstnode1:~/Desktop$ sudo dpkg -i wdtokentool-proxkey_1.1.0-1_all.deb
[sudo] password for gst:
(Reading database ... 524714 files and directories currently installed.)
Preparing to unpack wdtokentool-proxkey_1.1.0-1_all.deb ...
```

If installation Completes successfully, we can proceed with DSCSigner Installation.

1.2. DSCSigner installation

To install DSCSigner, open the Terminal and type the following command

```
sudo dpkg -i DCSigner.deb
```

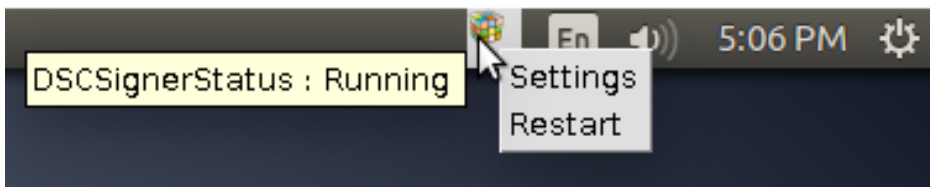
```
gst@gstnode1:~/Desktop$ sudo dpkg -i DCSigner.deb
```

After installation, DCSigner will start automatically once DSC token is connected to the system.

DCSigner will attempt to initialize using token, which was installed on the previous step. DCSigner can be seen in the top bar with running status.

If the token fails to start for any reason, DCSigner can be restarted by connecting token to the system, right clicking on the DCSigner icon in the top bar and then clicking on the Restart button.

- On Initial run you can see if DCSigner is running by looking at top bar



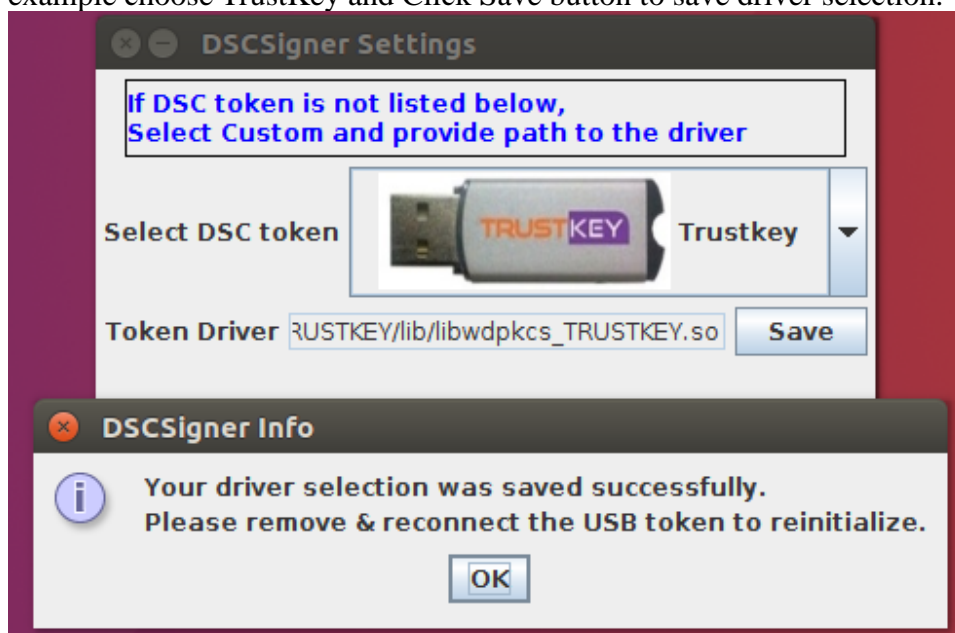
- To select the token driver to TrustKey, Install Trustkey driver in your machine and **Right Click DCSigner Icon -> Settings.**



If DSC token is not listed by default, a custom driver selection is made available where user can provide their custom driver and reinitialize with new driver next time.



If DSC token is listed by default then use the dropdown and select appropriate driver, here for example choose TrustKey and Click Save button to save driver selection.



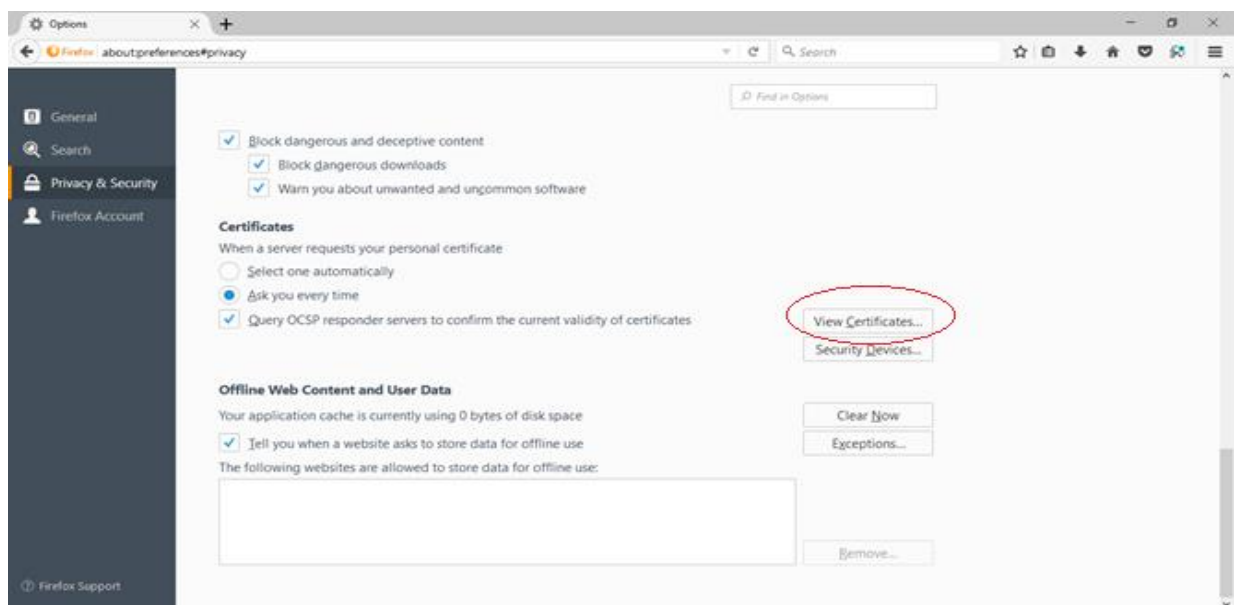
Then you will be shown a message saying token driver saved successfully. Now remove and reconnect your token to reinitialize with new driver.

2. Browser Configuration

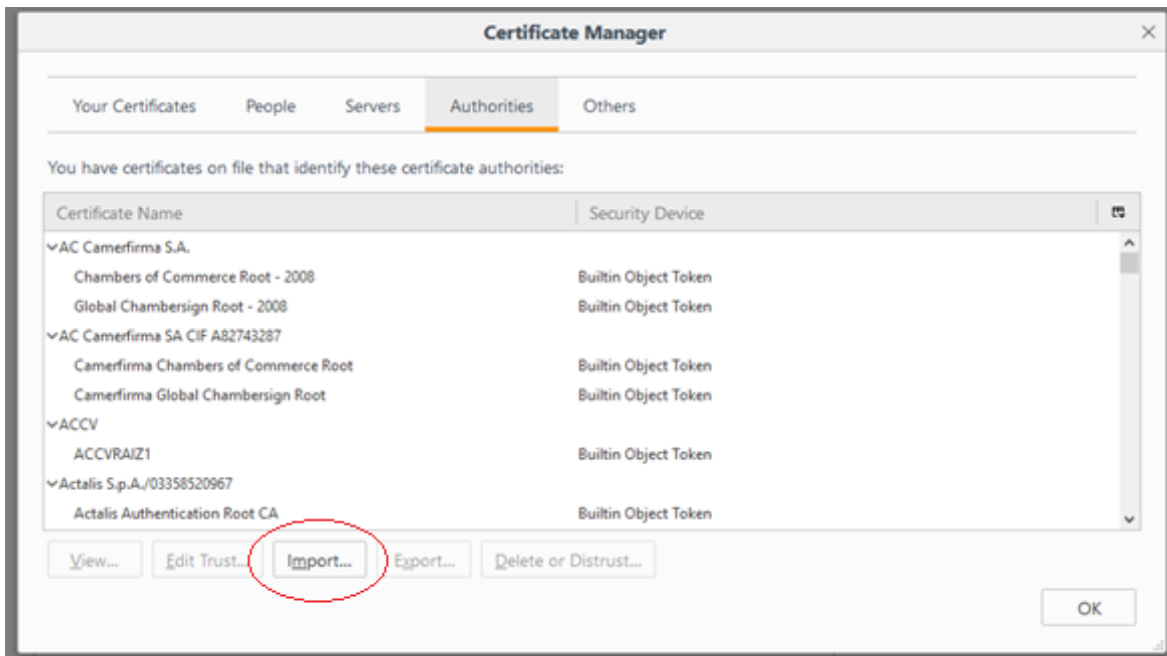
The browser must be configured prior to the use of DSCSigner tool to configure the browser to trust the DSCSigner Client. The configuration for the browsers are given below.

2.1. Mozilla Firefox

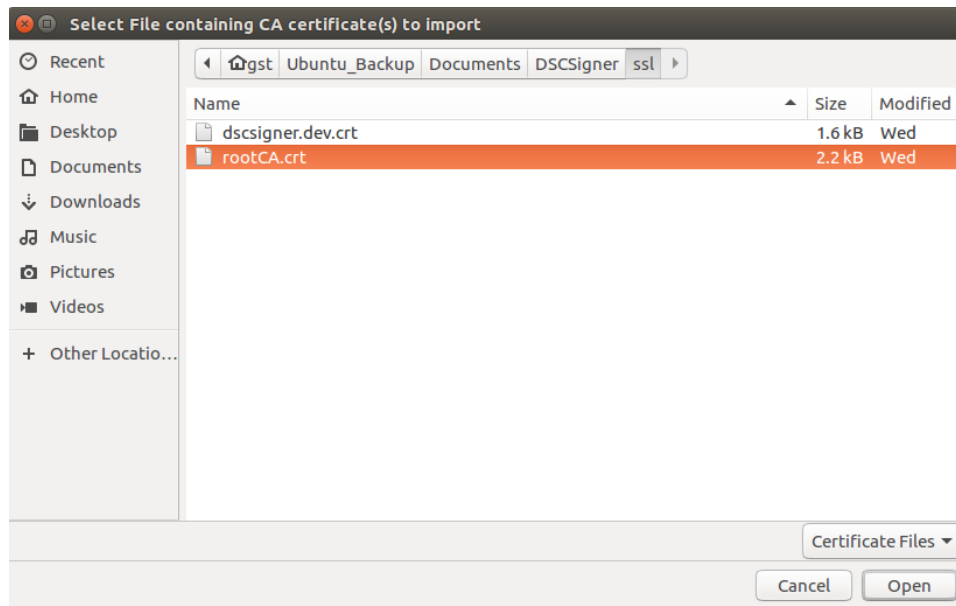
1. Open Mozilla Firefox and type the following in the address bar and press enter.
about:preferences#privacy
2. Scroll down to view the Certificate section and click on the **View Certificates** button to open the certificate manager.



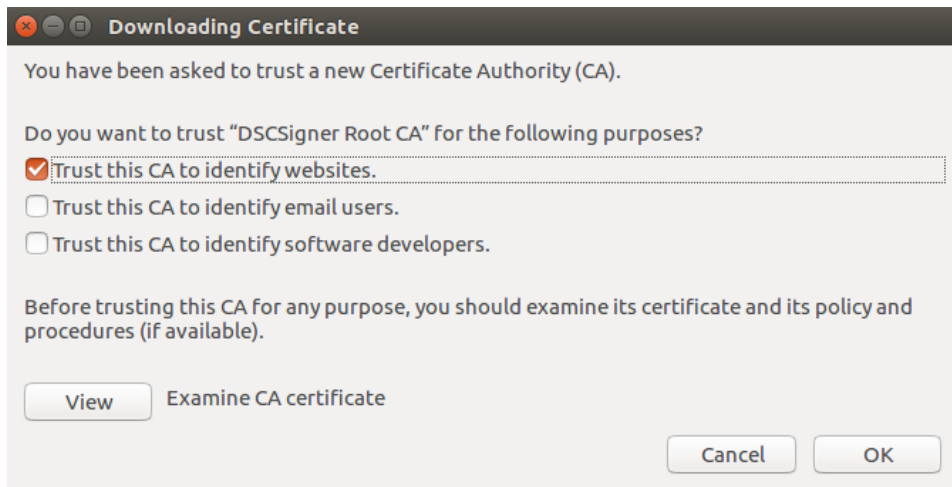
3. In the Certificate Manager popup, click on the Authorities tab and then click on Import button.



4. Browse to DSCSigner/ssl folder and select the rootCA.crt file and click on the Open button.



5. Check the **Trust this CA to identify websites** and click on OK button to complete the root certificate export.

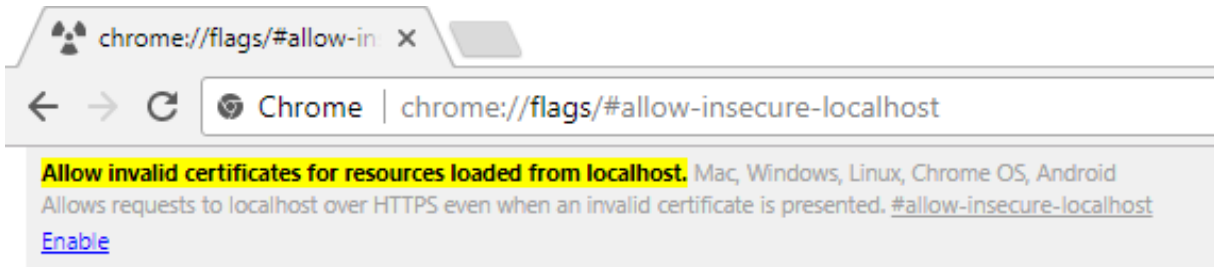


6. The configuration is complete and now you can use Mozilla Firefox for digital signing using DSCSigner.

2.2. Google Chrome

1. Open Google Chrome browser and type the following in the address bar and press enter:

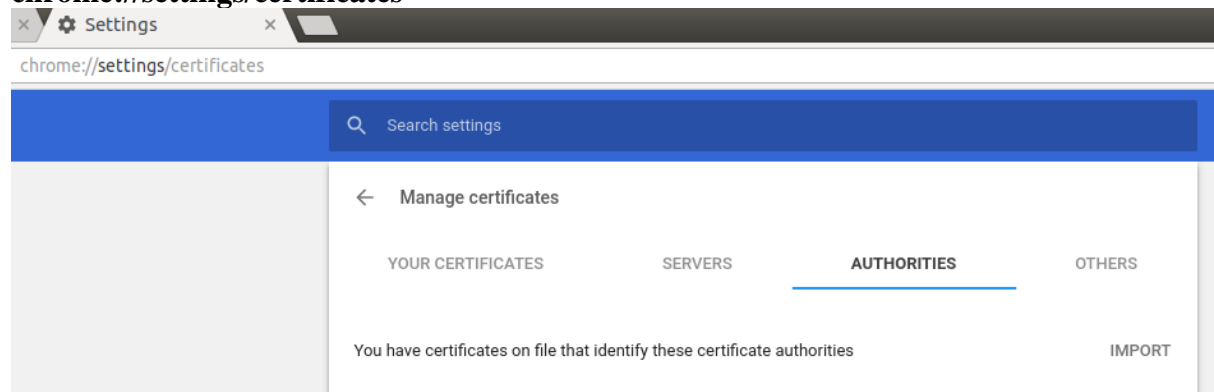
chrome://flags/#allow-insecure-localhost



Click on Enable link to enable

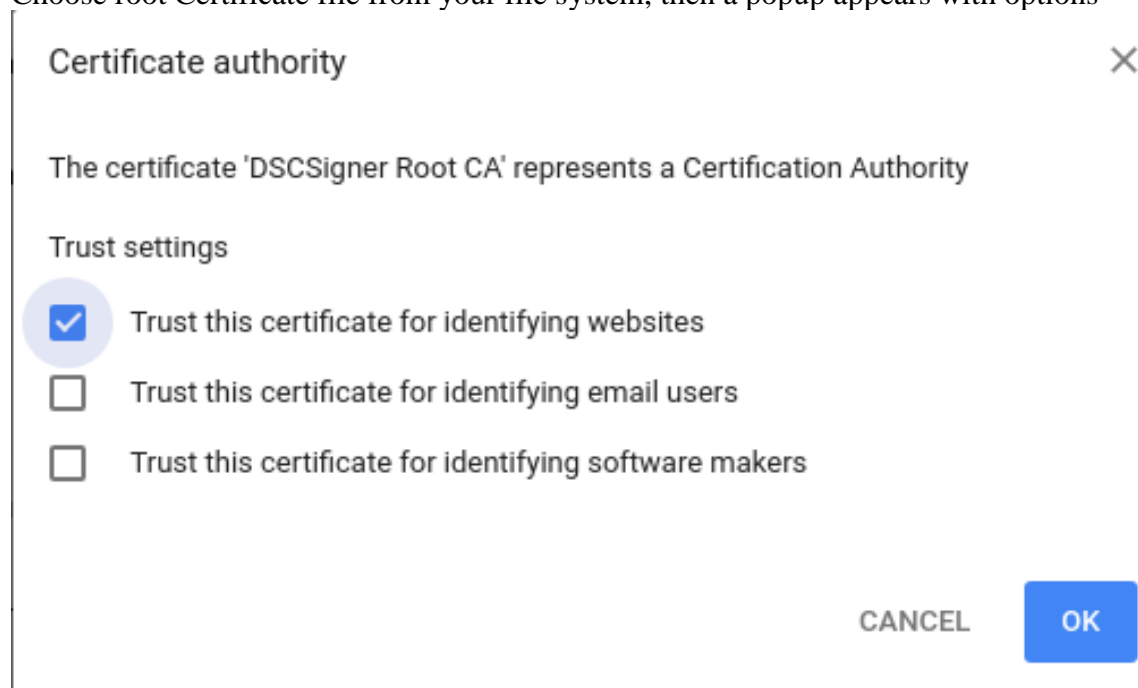
2. On the address bar type

chrome://settings/certificates

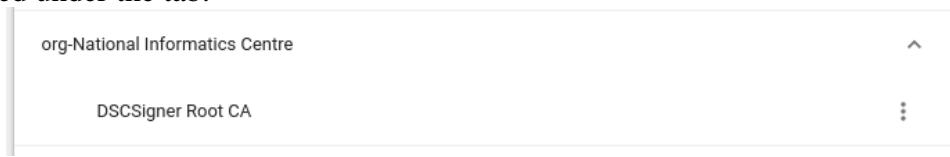


Choose Authorities tab from available tabs and click on the IMPORT link

Choose root Certificate file from your file system, then a popup appears with options



Choose 'Trust this certificate for identifying website' and click OK. The root certificate will be listed under the tab.



Now chrome can be used for signing in Ubuntu.