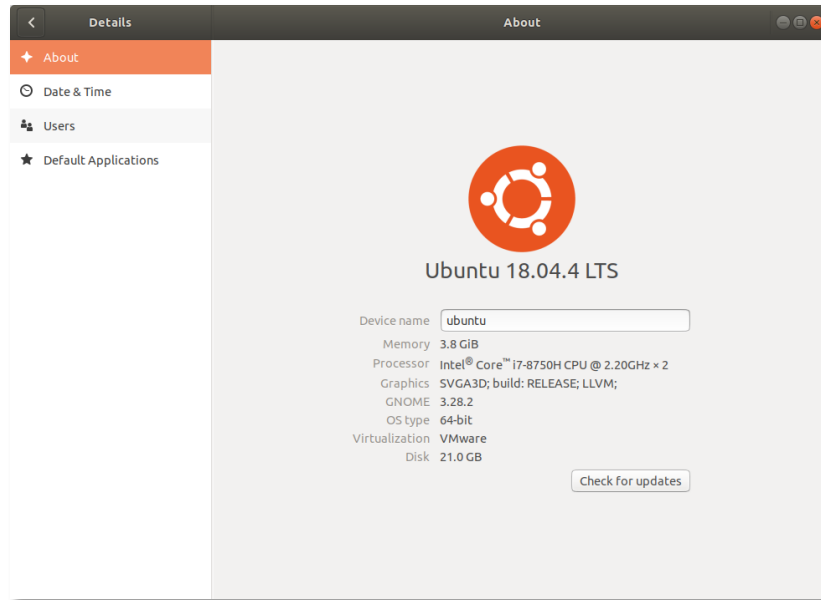
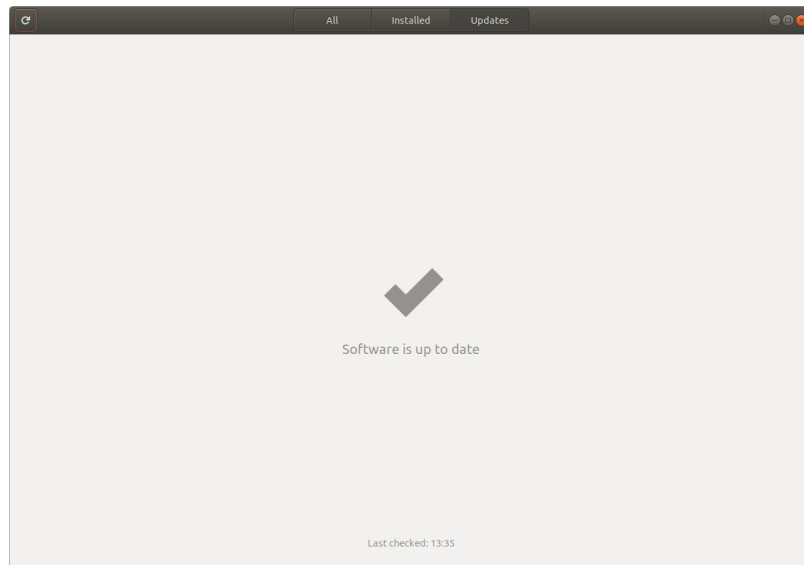


# Preparing Ubuntu 18.04 for DoD Use

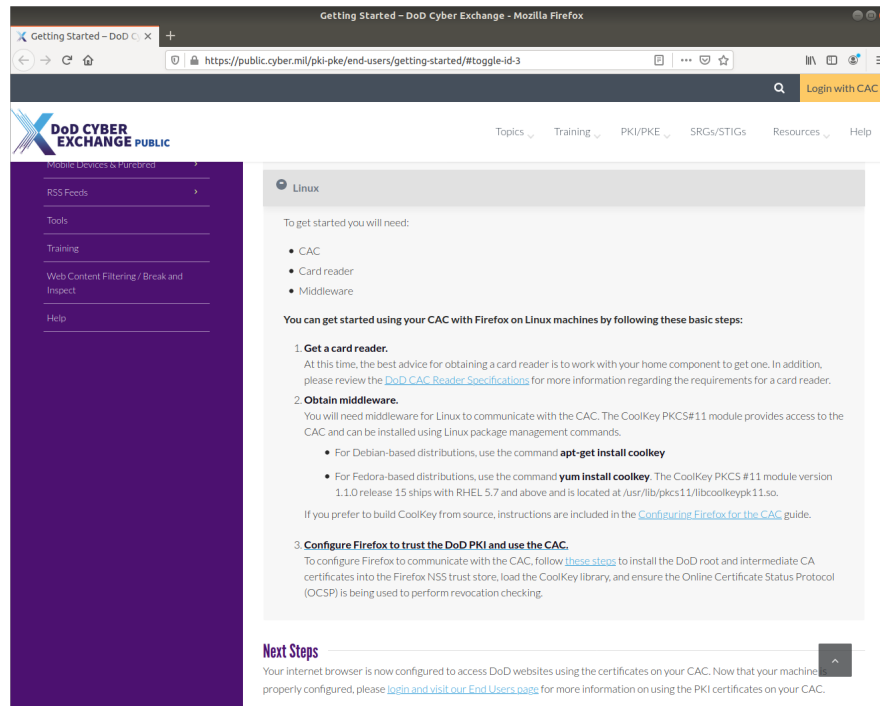
1. I am using Ubuntu 18.04.4 LTS to write this guide.



2. Make sure your Operating System is fully up to date. You can click the **Check for updates** button on the **About** page. You can also run the **Software Updater** utility to check for updates.

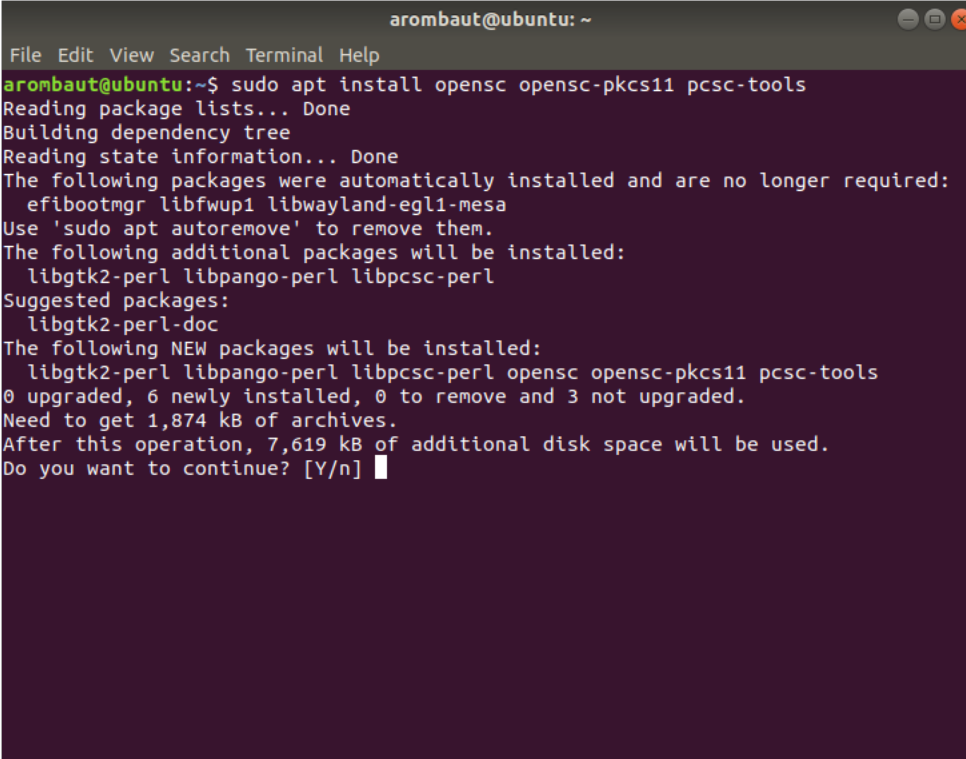


3. We are going to start by downloading everything we need. Navigate to the following URL <https://public.cyber.mil/pki-pke/end-users/getting-started/#toggle-id-3> to view the help from DoD Cyber Exchange. We are going to deviate from these instructions since they are not up to date for modern Mozilla Firefox installations, but the general workflow still is good.



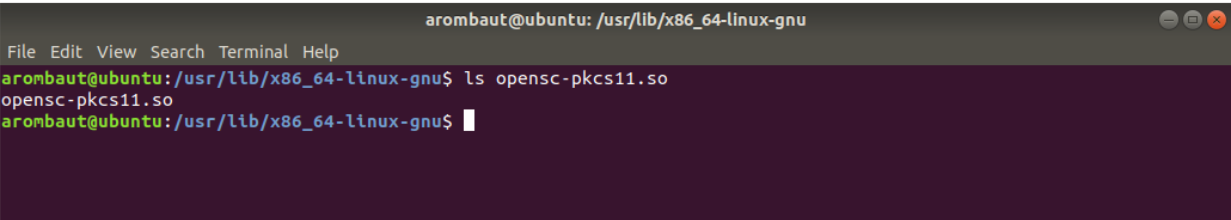
4. I'm assuming you already have a DoD Common Access Card (CAC) and a Smart Card Reader.

- Let's get the middleware. Unfortunately, the recommended CoolKey module is no longer valid on modern versions of Firefox (or at least I was unable to get this working). So, we will use OpenSC instead. Open **Terminal** and type `sudo apt install opensc opensc-pkcs11 pcsc-tools`. When asked, enter **Y** to continue.



```
arombaut@ubuntu: ~  
File Edit View Search Terminal Help  
arombaut@ubuntu:~$ sudo apt install opensc opensc-pkcs11 pcsc-tools  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  efibootmgr libfwup1 libwayland-egl1-mesa  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libgtk2-perl libpango-perl libpcsc-perl  
Suggested packages:  
  libgtk2-perl-doc  
The following NEW packages will be installed:  
  libgtk2-perl libpango-perl libpcsc-perl opensc opensc-pkcs11 pcsc-tools  
0 upgraded, 6 newly installed, 0 to remove and 3 not upgraded.  
Need to get 1,874 kB of archives.  
After this operation, 7,619 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

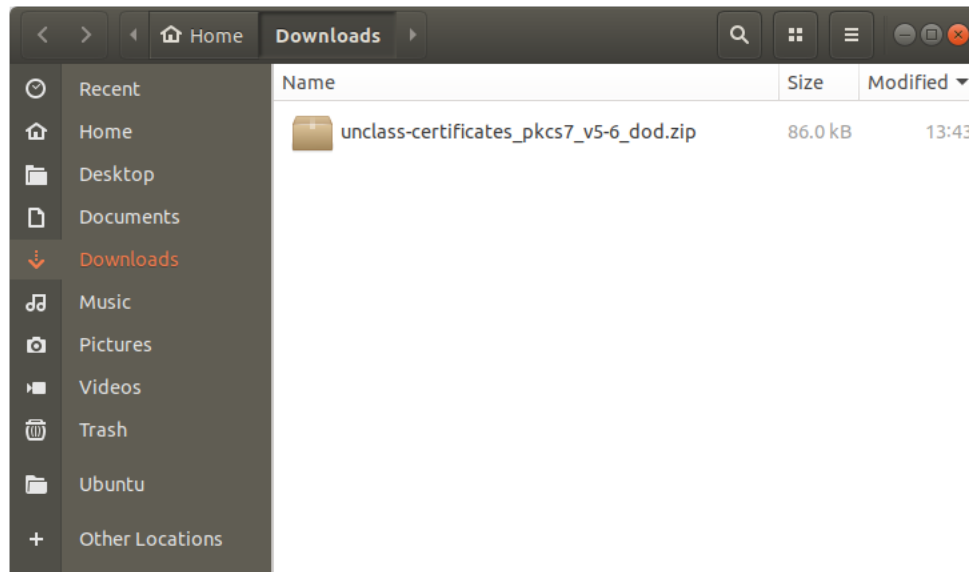
- Change directory to `/usr/lib/x86_64-linux-gnu/` and then list the directory contents to verify the `opensc-pkcs11.so` shared object is present.



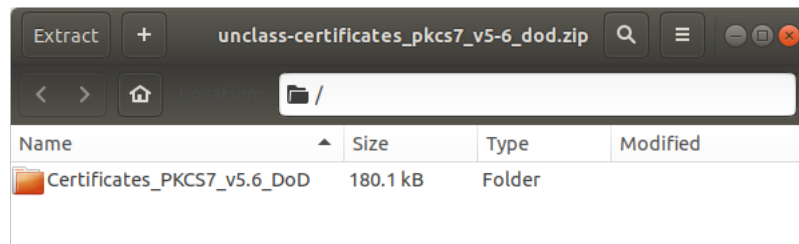
```
arombaut@ubuntu: /usr/lib/x86_64-linux-gnu  
File Edit View Search Terminal Help  
arombaut@ubuntu:/usr/lib/x86_64-linux-gnu$ ls opensc-pkcs11.so  
opensc-pkcs11.so  
arombaut@ubuntu:/usr/lib/x86_64-linux-gnu$
```

- After we install the DoD certificates in Firefox, we will add our Smart Card reader into the Firefox **Device Manager**. The path will be necessary in order to load the shared object.

8. Next, we are going to download the DoD certificates from Cyber.mil at [https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/zip/unclass-certificates\\_pkcs7\\_v5-6\\_dod.zip](https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/zip/unclass-certificates_pkcs7_v5-6_dod.zip).



9. Double-click the downloaded file to open **Archive Manager**. Click on the **Extract** button to open the Extract window. Click on the Extract button again to extract the file into the **Downloads** directory. Click **Close** on the **Extraction completed successfully** window. Close the **Archive Manager** window.

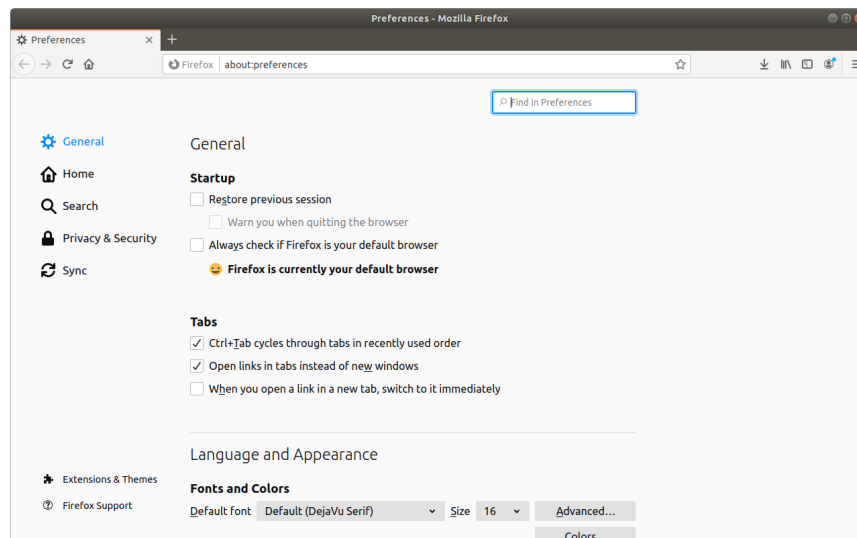


10. Open the **Downloads** folders if not already open. Verify that there is a DoD certificates folder (in addition to the zip file).

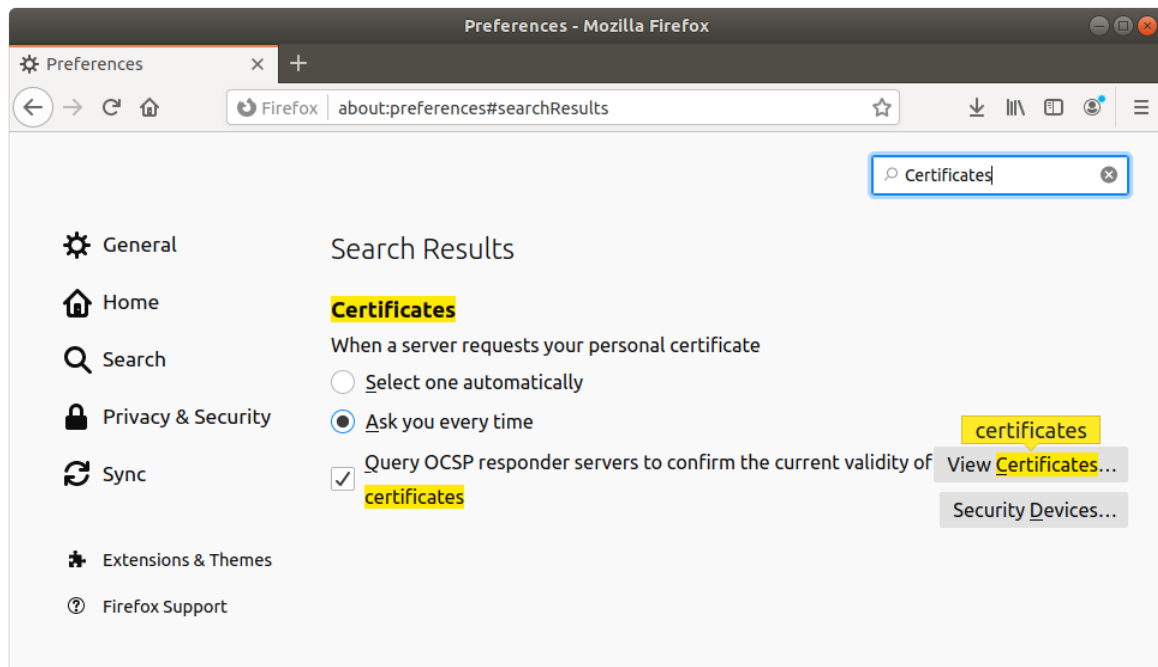
11. Now we will get to the configuring Firefox part of this guide. I am using Firefox 75.0 at the time of this writing, but this procedure has been similar for quite a few versions.



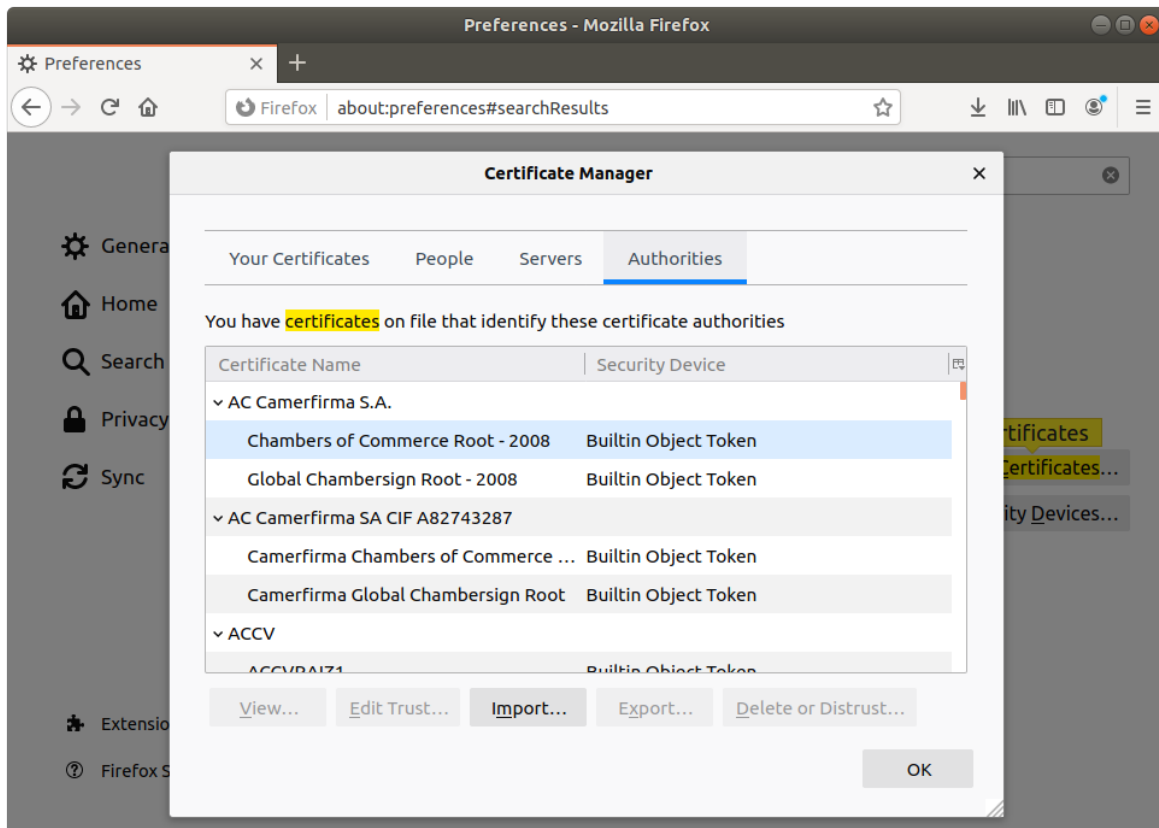
12. Open the Firefox menu by clicking on the three lines in the upper right corner of the browser window, select **Preferences**.



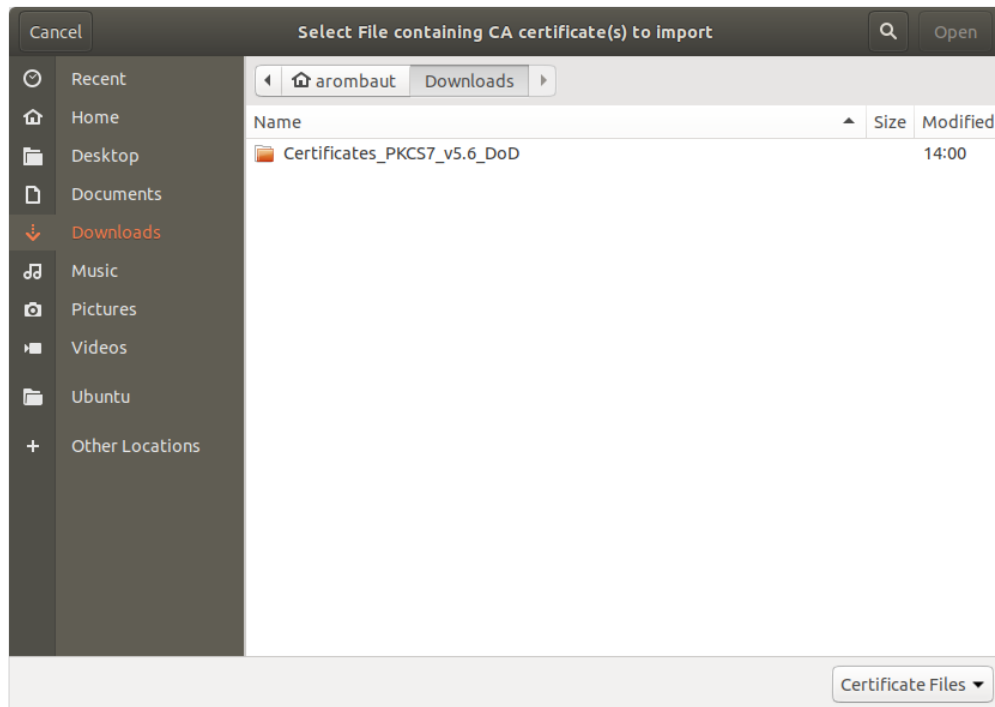
13. In the **Find in Preferences** search box, type **Certificates**.



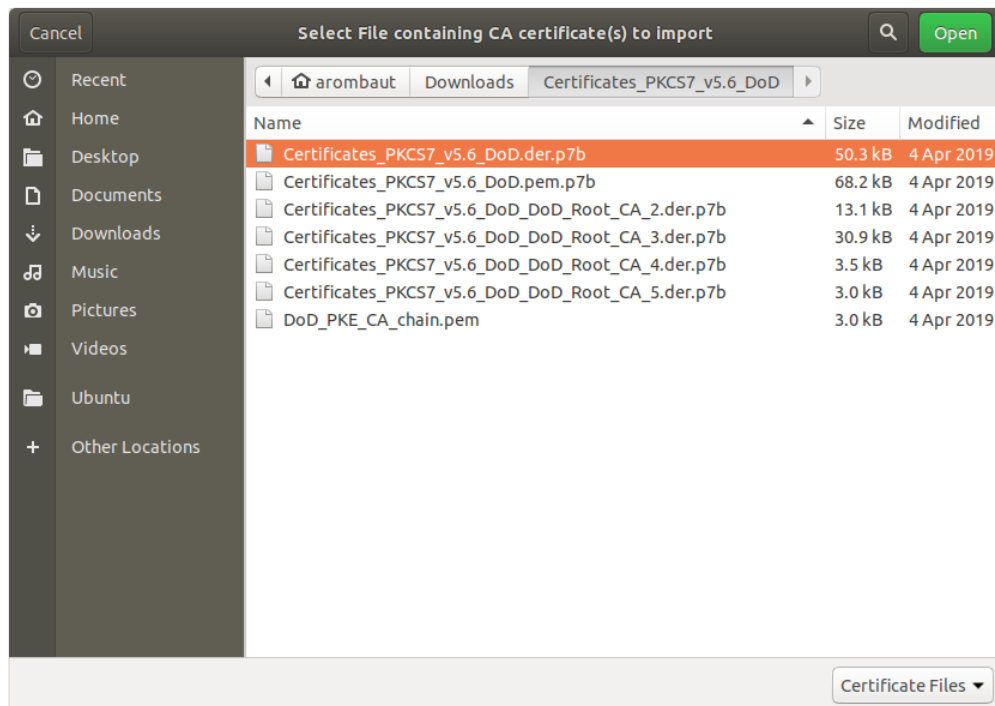
14. Click on the **View Certificates...** button to open the **Certificate Manager**.



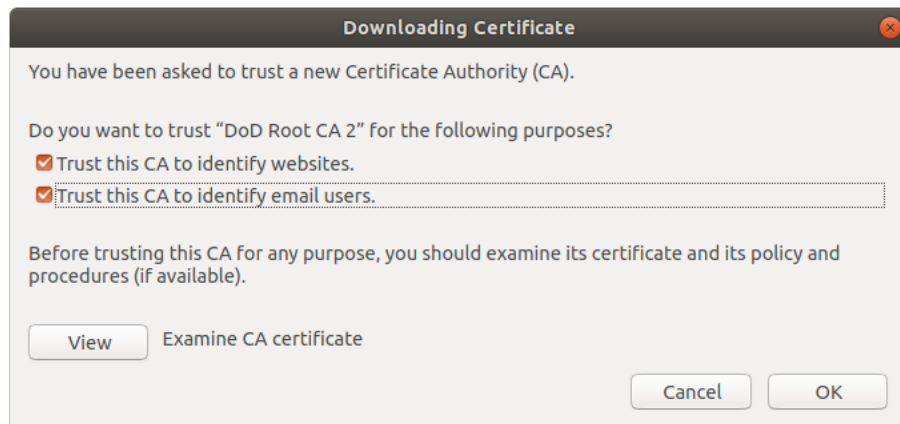
15. Click on the **Import...** button to open the **Select File containing CA certificate(s) to import** window.



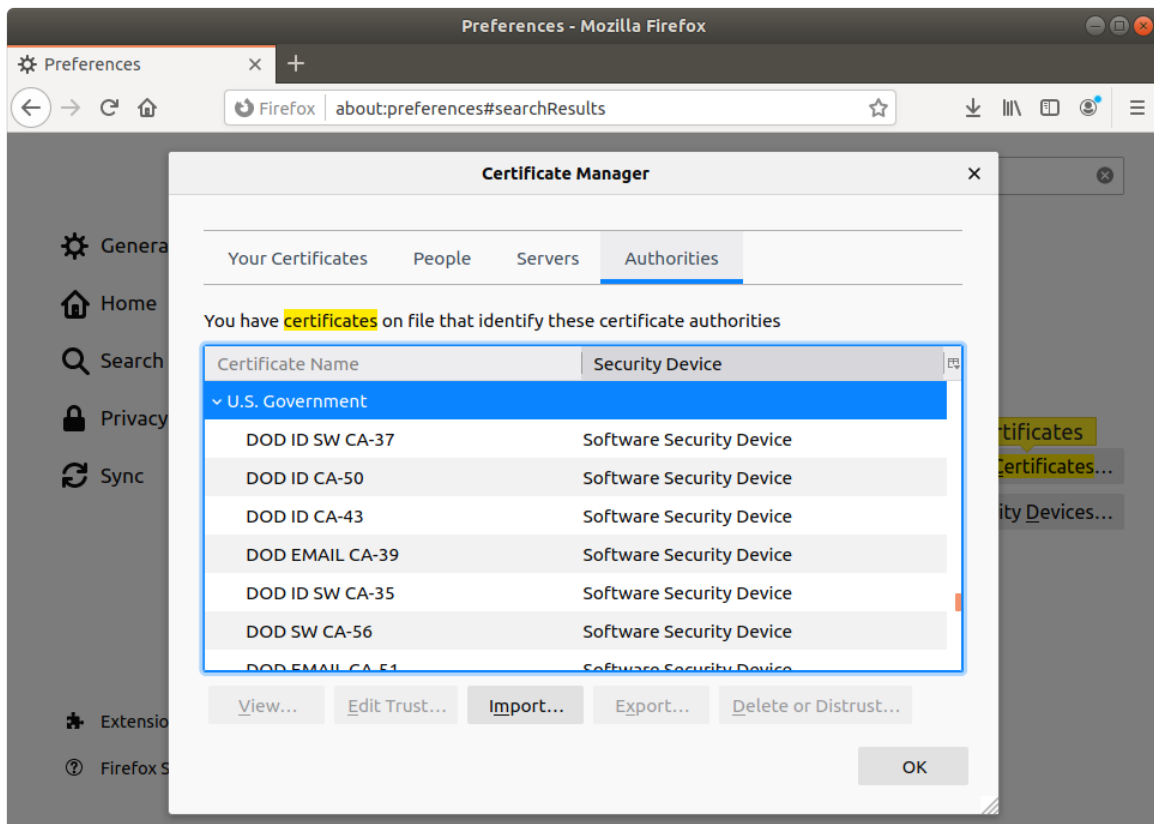
16. Navigate to the extracted folder (from step 10 above) to the **Certificates\_PKCS7\_v5.6\_DoD.der.p7b** file and click the **Open** button.



17. A **Downloading Certificate** window will open for the **DoD Root CA 2** certificate. Make sure both checkboxes are checked and click **OK**.

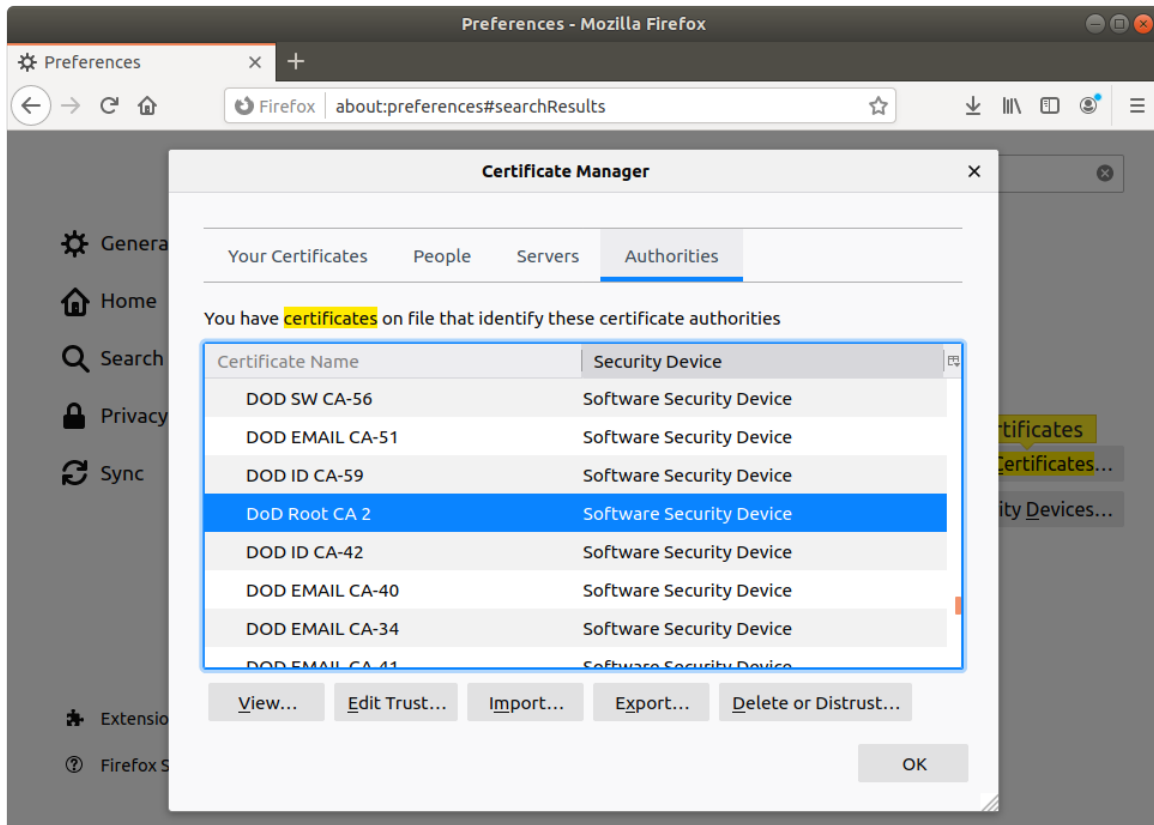


18. The certificates will be listed in the **Certificate Manager** under the **U.S. Government** heading.

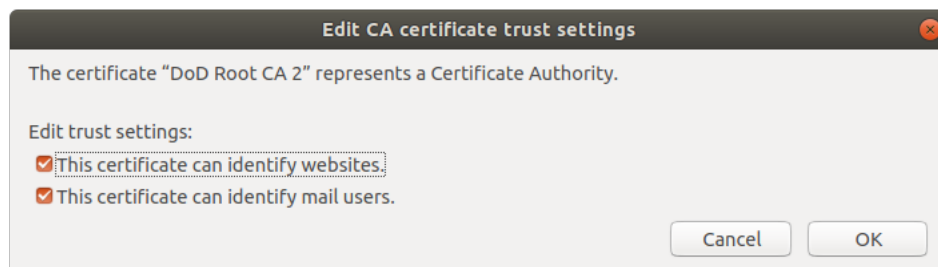




19. Navigate to **DoD Root CA 2** and click on the **Edit Trust...** button.

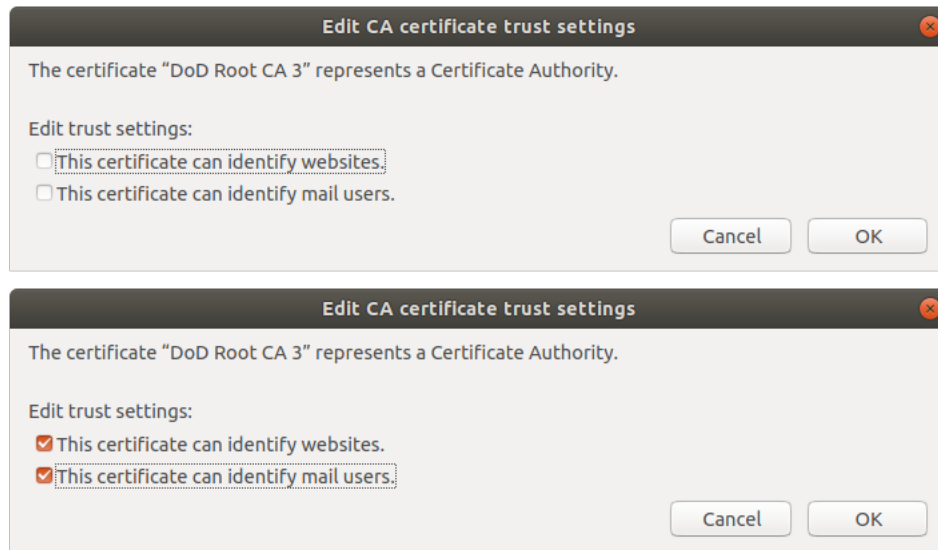


20. Ensure the two check boxes are checked.



21. Navigate to **DoD Root CA 3**, **DoD Root CA 4**, and **DoD Root CA 5** individually and check both boxes to edit the trust settings.

### DoD Root CA 3



**Edit CA certificate trust settings**

The certificate "DoD Root CA 3" represents a Certificate Authority.

Edit trust settings:

☐ This certificate can identify websites.

☐ This certificate can identify mail users.

Cancel OK

**Edit CA certificate trust settings**

The certificate "DoD Root CA 3" represents a Certificate Authority.

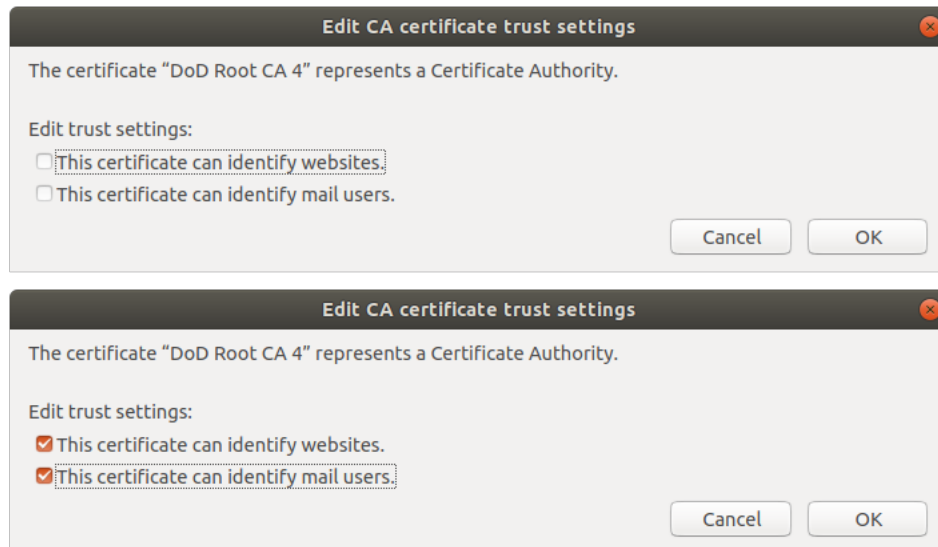
Edit trust settings:

☒ This certificate can identify websites.

☒ This certificate can identify mail users.

Cancel OK

### DoD Root CA 4



**Edit CA certificate trust settings**

The certificate "DoD Root CA 4" represents a Certificate Authority.

Edit trust settings:

☐ This certificate can identify websites.

☐ This certificate can identify mail users.

Cancel OK

**Edit CA certificate trust settings**

The certificate "DoD Root CA 4" represents a Certificate Authority.

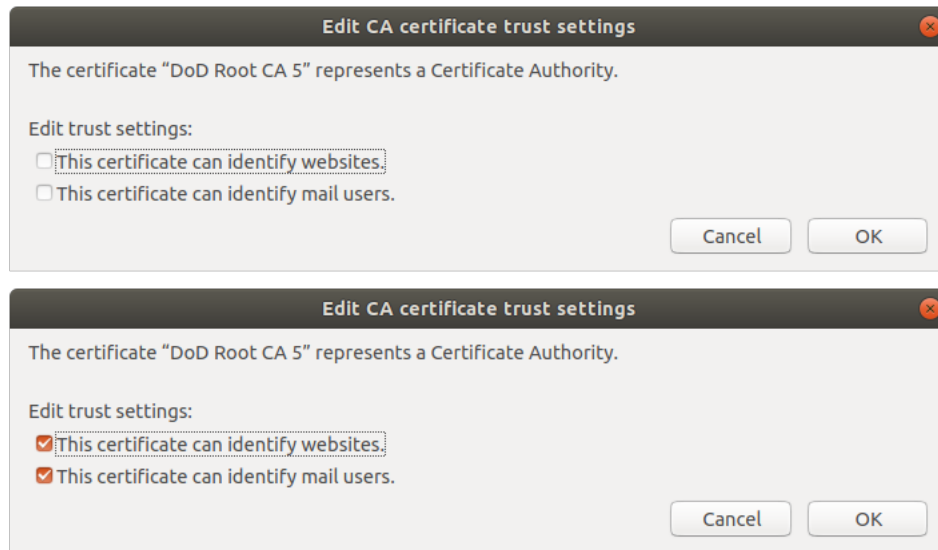
Edit trust settings:

☒ This certificate can identify websites.

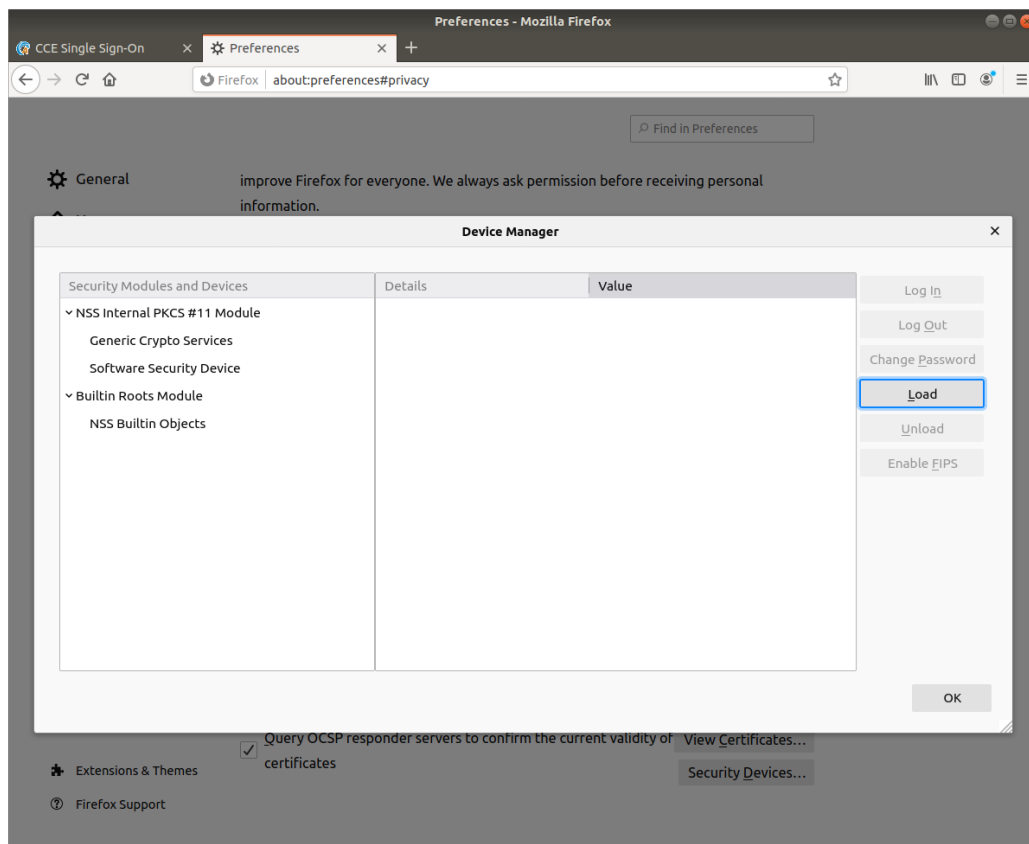
☒ This certificate can identify mail users.

Cancel OK

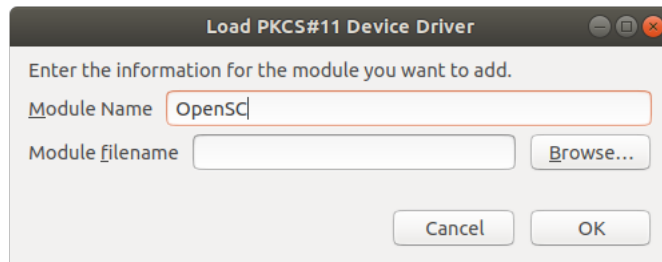
## DoD Root CA 5



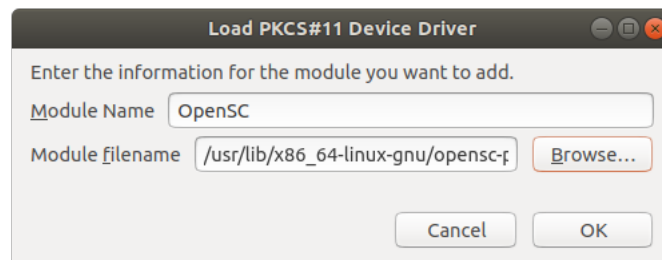
22. Once the Root CA certificates are trusted, close **Certificate Manager** or click **OK**.
23. While still on **Firefox Preferences**, click the **Security Devices...** button. The Firefox **Device Manager** opens. Click the **Load** button.



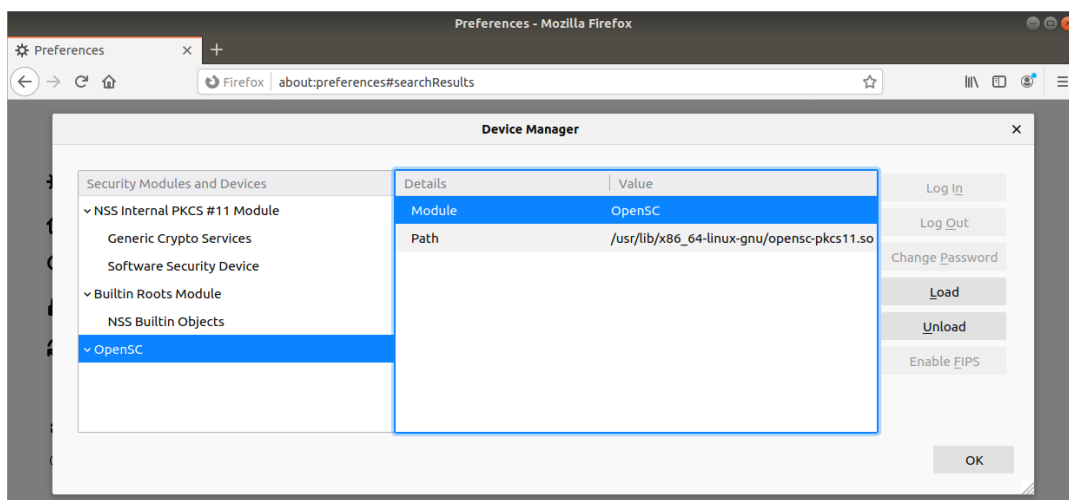
24. Replace the default text in the **Module Name** text box with **OpenSC**.



25. Click the **Browse** button next to the **Module filename** textbox. Click on **Other Locations** in the navigation pane. Double-click **Computer**. We are going to navigate to the directory listed in step 6 and 7 above. Double-click **usr**. Double-click **lib**. Double-click **x86\_x64-linux-gnu**. Start to type **opensc** and see that the folder starts to select the words for you as you type. Stop when you are on **opensc-pkcs11.so** and click the **Open** button. The **Module Filename** on the **Load PKCS#11 Device Driver** window will be populated with the shared object you selected.



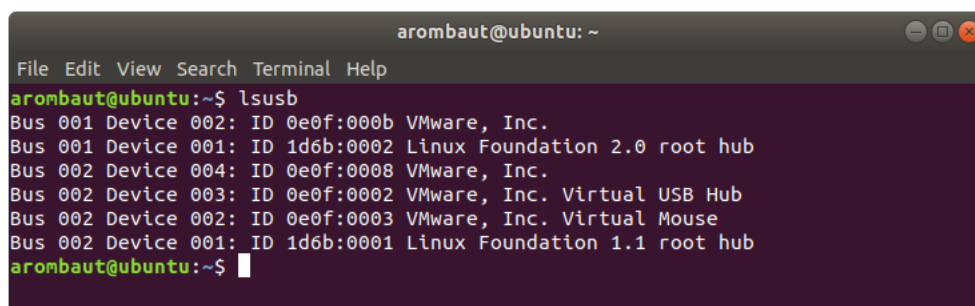
26. Click **OK** and verify the **OpenSC** module is in the list of **Security Modules and Devices**. You may have to select it to view the details.



27. Click **OK** to close the **Device Manager** window.
28. Close the **Preferences** tab.

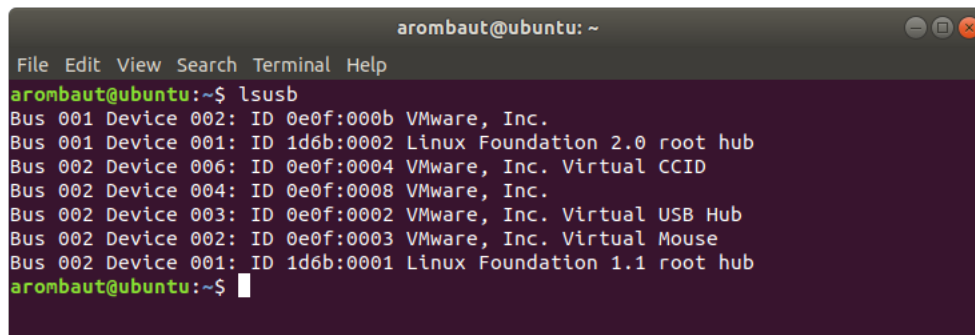
At this point, you should be good to go to navigate to CAC enabled DoD websites. Unlike Windows and macOS, you may have to go into the **Firefox Certificate Manager** to trust DoD certificates as you need them.

1. Let's verify that your Smart Card and reader are detected by your Ubuntu desktop.
2. Open **Terminal** and type **lsusb**. I am using a VMware virtual machine, but either way, your output should be different from mine. Here is an image of before I connected the Smart Card reader.



```
arombaut@ubuntu: ~  
File Edit View Search Terminal Help  
arombaut@ubuntu:~$ lsusb  
Bus 001 Device 002: ID 0e0f:000b VMware, Inc.  
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
Bus 002 Device 004: ID 0e0f:0008 VMware, Inc.  
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub  
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse  
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub  
arombaut@ubuntu:~$
```

3. Here is an image of after I connected the Smart Card reader.



```
arombaut@ubuntu: ~  
File Edit View Search Terminal Help  
arombaut@ubuntu:~$ lsusb  
Bus 001 Device 002: ID 0e0f:000b VMware, Inc.  
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
Bus 002 Device 006: ID 0e0f:0004 VMware, Inc. Virtual CCID  
Bus 002 Device 004: ID 0e0f:0008 VMware, Inc.  
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub  
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse  
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub  
arombaut@ubuntu:~$
```

4. Notice I now have a device listed on **Bus 002 Device 006** as **VMware, Inc. Virtual CCID**, where I did not have one before. This indicates that the USB bus has detected we have a Smart Card Reader plugged in.

5. Next, we need to verify that our DoD CAC (or Smart Card) is detected. In **Terminal**, type **pcsc\_scan** and look for **Card inserted**. You can test that it recognizes you removing your card and inserting your card back into the reader.

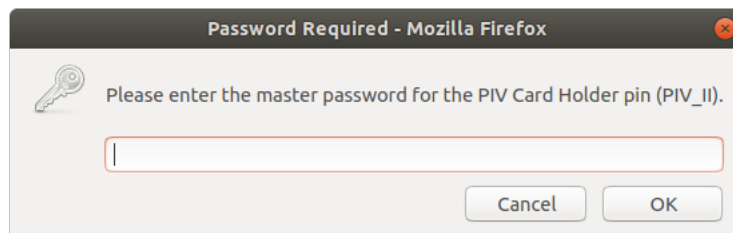
```
File Edit View Search Terminal Help
arombaut@ubuntu:~$ pcsc_scan
PC/SC device scanner
V 1.5.2 (c) 2001-2017, Ludovic Rousseau <ludovic.rousseau@free.fr>
Using reader plug'n play mechanism
Scanning present readers...
0: VMware Virtual USB CCID 00 00

Fri Apr 17 20:16:18 2020
Reader 0: VMware Virtual USB CCID 00 00
Card state: Card inserted,
ATR: 3B 7A 18 00 00 73 66 74 65 20 63 64 31 34 34

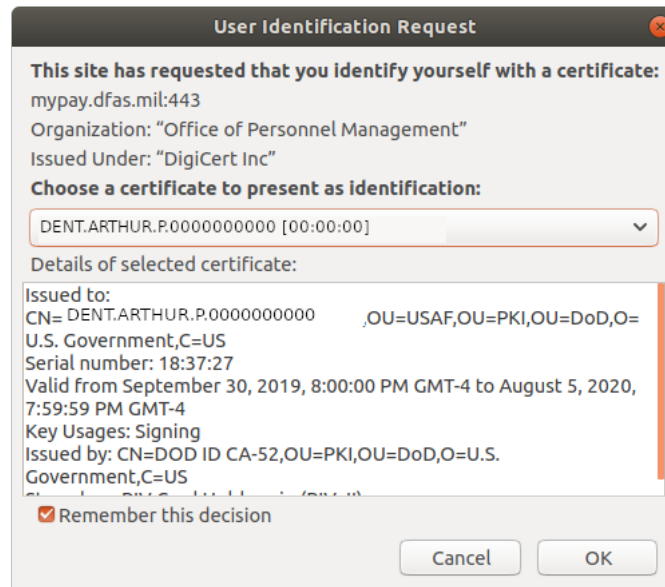
ATR: 3B 7A 18 00 00 73 66 74 65 20 63 64 31 34 34
+ TS = 3B --> Direct Convention
+ T0 = 7A, Y(1): 0111, K: 10 (historical bytes)
  TA(1) = 18 --> Fi=372, Di=12, 31 cycles/ETU
    129032 bits/s at 4 MHz, fMax for Fi = 5 MHz => 161290 bits/s
  TB(1) = 00 --> VPP is not electrically connected
  TC(1) = 00 --> Extra guard time: 0
+ Historical bytes: 73 66 74 65 20 63 64 31 34 34
  Category indicator byte: 73 (proprietary format)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 7A 18 00 00 73 66 74 65 20 63 64 31 34 34
  Republic Slovenia e-Gov, Ministry of Public Administration
  SIGOV-CA, Slovenian Governmental Certification Authority
/ █
```

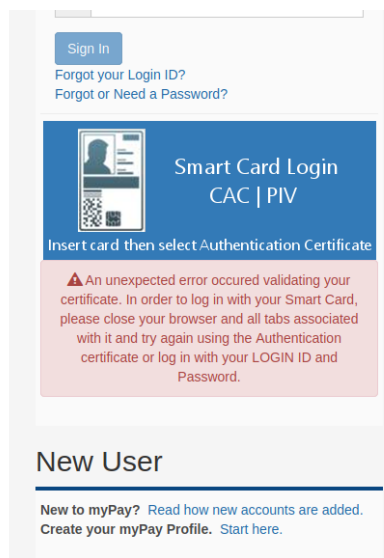
6. Now, let's test navigating to <https://mypay.dfas.mil/#/>. The myPay website does not use a DoD signed certificate. They use a commercially signed certificate from DigiCert, Inc. Open **Firefox** and type the URL in. Look for the CAC | PIV login box. Once you click on it, you should receive a **Password Required – Mozilla Firefox** window. Type in your **PIN** number here and click **OK**.



7. You should now receive a **User Identification Request** window asking what certificate you would like to use. Examine the **Details of selected certificate** in the lower portion of the window for more details. Click **OK** when you have chosen the correct certificate.

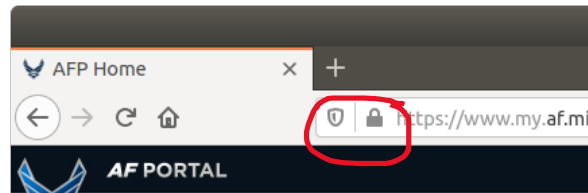


8. If you were able to get in, great! You are probably all set and do not need to continue this guide any longer. If you received an error, like I did below, then continue along.



9. In this case, you will want to close out **Firefox**, reopen, and navigate back to the website. This time around, it should work. If it still does not work, restart your computer and then open **Firefox** and try again.

10. Now let's try a site where a DoD certificate is in use. I will use the Air Force Portal as an example. The Air Force Portal is located at <https://www.my.af.mil>.
11. Navigate to the Air Force Portal and try to log in. You should be successful and also notice a lock symbol in the URL bar near the text. This indicates that **Firefox** is recognizing the certificates and that they are trusted.



This completes the help guide. I hope you have found it helpful and informative. If you are looking to use VMware Horizon Client for virtual desktops, such as in use by Air Force Reserve Command (AFRC) Desktop Anywhere, please be patient as I am working on that guide next. This guide should suffice for most people and be current and concise.

If you have any questions about the content presented here, please feel free to reach out to me via my email at [aaron.rombaut@gmail.com](mailto:aaron.rombaut@gmail.com) or Facebook messenger.