My previous attempts to get the DoD CAC/PKI system to work on Fedora and Ubuntu have been extremely painful and only occasionally successful. However, the process with **Ubuntu 11.04** was very straightforward. So simple even a pilot can do it – although maybe I just got lucky this time. While there are a number of different ways to do it, this is the way that worked for me using both the SCR 331 and SCR3310 card readers. These instructions assume a very basic level of knowledge about Linux.

To install the required card reader software:

1. To open the terminal (there are many ways to do this....this is one)

   - press the 'super' and 'a' keys at same time - the 'super' key is the windows icon key located between the <ctrl> and <alt> keys.
   - type 'terminal' (without the quotes)
   - click the 'terminal' icon

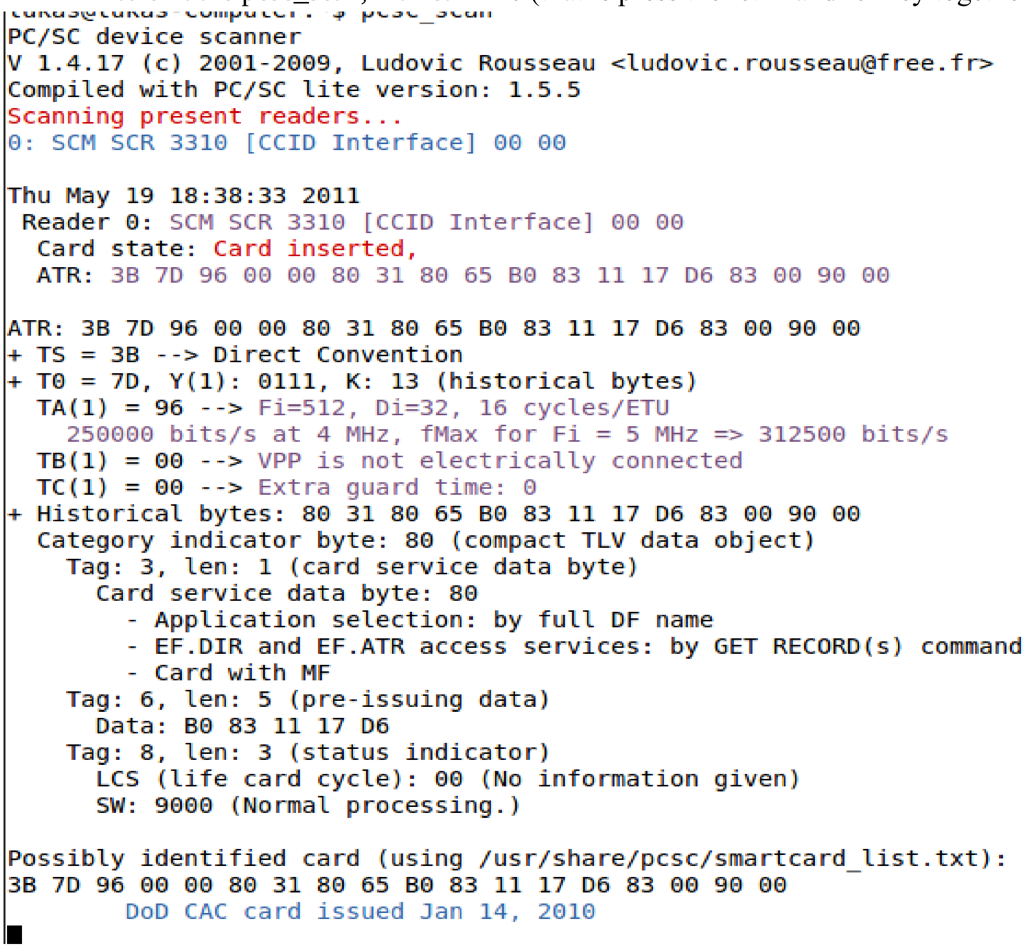
2. At command prompt, type:

   sudo apt-get install coolkey pcscd pcsc-tools

3. Enter your password if required
4. When complete, plug in (or re-plug in) your card reader and insert CAC card.
4. Check to see if your card reader is recognized by typing

   pcsc_scan

   - you should see something similar to this:
   - to exit the pcsc_scan, hit <ctrl> - c (that is press the 'ctrl' and 'c' key together)



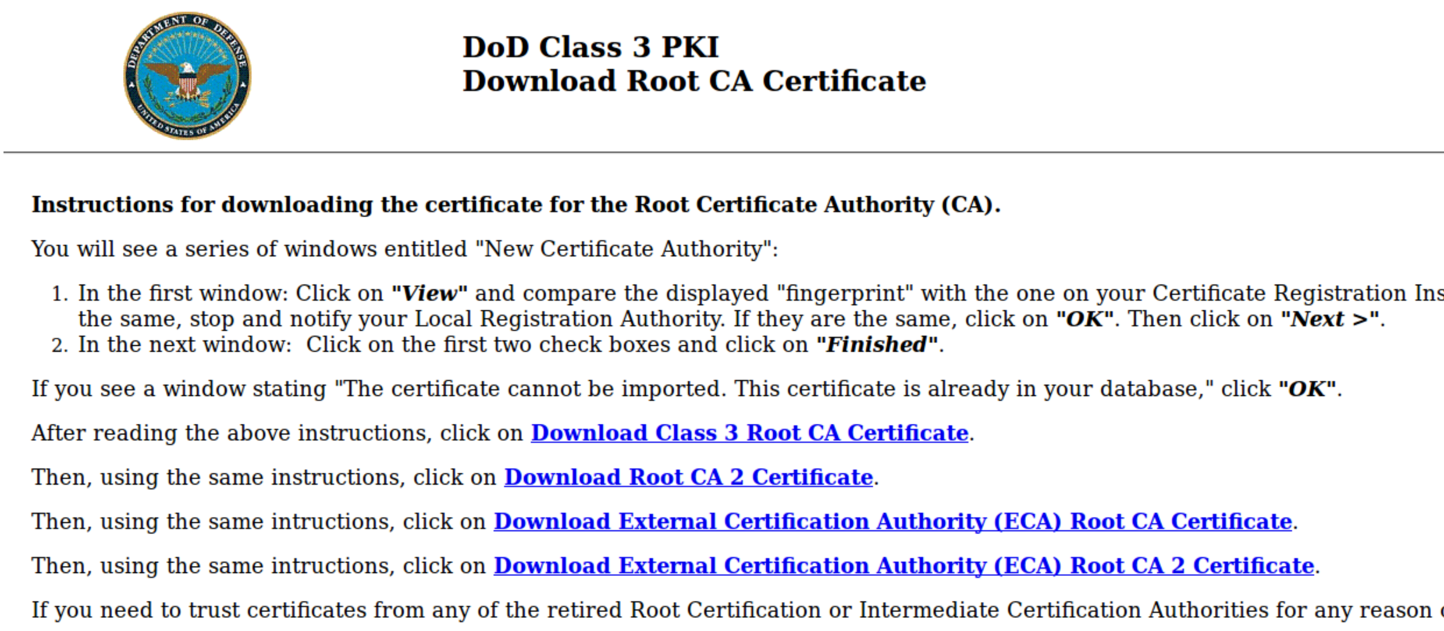
```
lukas@lukas-computer:~$ pcsc_scan
PC/SC device scanner
V 1.4.17 (c) 2001-2009, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.5.5
Scanning present readers...
0: SCM SCR 3310 [CCID Interface] 00 00

Thu May 19 18:38:33 2011
 Reader 0: SCM SCR 3310 [CCID Interface] 00 00
  Card state: Card inserted,
  ATR: 3B 7D 96 00 00 80 31 80 65 B0 83 11 17 D6 83 00 90 00

ATR: 3B 7D 96 00 00 80 31 80 65 B0 83 11 17 D6 83 00 90 00
+ TS = 3B --> Direct Convention
+ T0 = 7D, Y(1): 0111, K: 13 (historical bytes)
  TA(1) = 96 --> Fi=512, Di=32, 16 cycles/ETU
    250000 bits/s at 4 MHz, fMax for Fi = 5 MHz => 312500 bits/s
  TB(1) = 00 --> VPP is not electrically connected
  TC(1) = 00 --> Extra guard time: 0
+ Historical bytes: 80 31 80 65 B0 83 11 17 D6 83 00 90 00
  Category indicator byte: 80 (compact TLV data object)
    Tag: 3, len: 1 (card service data byte)
      Card service data byte: 80
        - Application selection: by full DF name
        - EF.DIR and EF.ATR access services: by GET RECORD(s) command
        - Card with MF
    Tag: 6, len: 5 (pre-issuing data)
      Data: B0 83 11 17 D6
    Tag: 8, len: 3 (status indicator)
      LCS (life card cycle): 00 (No information given)
      SW: 9000 (Normal processing.)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 7D 96 00 00 80 31 80 65 B0 83 11 17 D6 83 00 90 00
        DoD CAC card issued Jan 14, 2010
```

- if you get any kind of error message, you may need to update the drivers for your card reader. That is more complicated and you should use other resources to figure out how to do this (there is plenty of info online about this although it is not an easy process). For both of my readers, updating the driver was not necessary.

You will then need to download the DoD CA Certificates for Firefox:

There are many ways to do this too. This is not always the fastest but it should work for most people. You must use Firefox to access this website, Chrome will not work.

1. Go to: http://dodpki.c3pki.chamb.disa.mil/rootca.html



DoD Class 3 PKI
Download Root CA Certificate

Instructions for downloading the certificate for the Root Certificate Authority (CA).

You will see a series of windows entitled "New Certificate Authority":

1. In the first window: Click on ***"View"*** and compare the displayed "fingerprint" with the one on your Certificate Registration Ins
the same, stop and notify your Local Registration Authority. If they are the same, click on ***"OK"***. Then click on ***"Next >"***.
2. In the next window: Click on the first two check boxes and click on ***"Finished"***.

If you see a window stating "The certificate cannot be imported. This certificate is already in your database," click ***"OK"***.

After reading the above instructions, click on **Download Class 3 Root CA Certificate**.

Then, using the same instructions, click on **Download Root CA 2 Certificate**.

Then, using the same intructions, click on **Download External Certification Authority (ECA) Root CA Certificate**.

Then, using the same intructions, click on **Download External Certification Authority (ECA) Root CA 2 Certificate**.

If you need to trust certificates from any of the retired Root Certification or Intermediate Certification Authorities for any reason (

2. Click on all four Certificates, one at a time.

- these are ‘Download Class 3 Root CA Certificate’, ‘Download Root CA 2 Certificate’, ‘Download External Certification Authority (ECA) Root CA Certificate’, ‘Download External Certification Authority (ECA) Root CA 2 Certificate’.

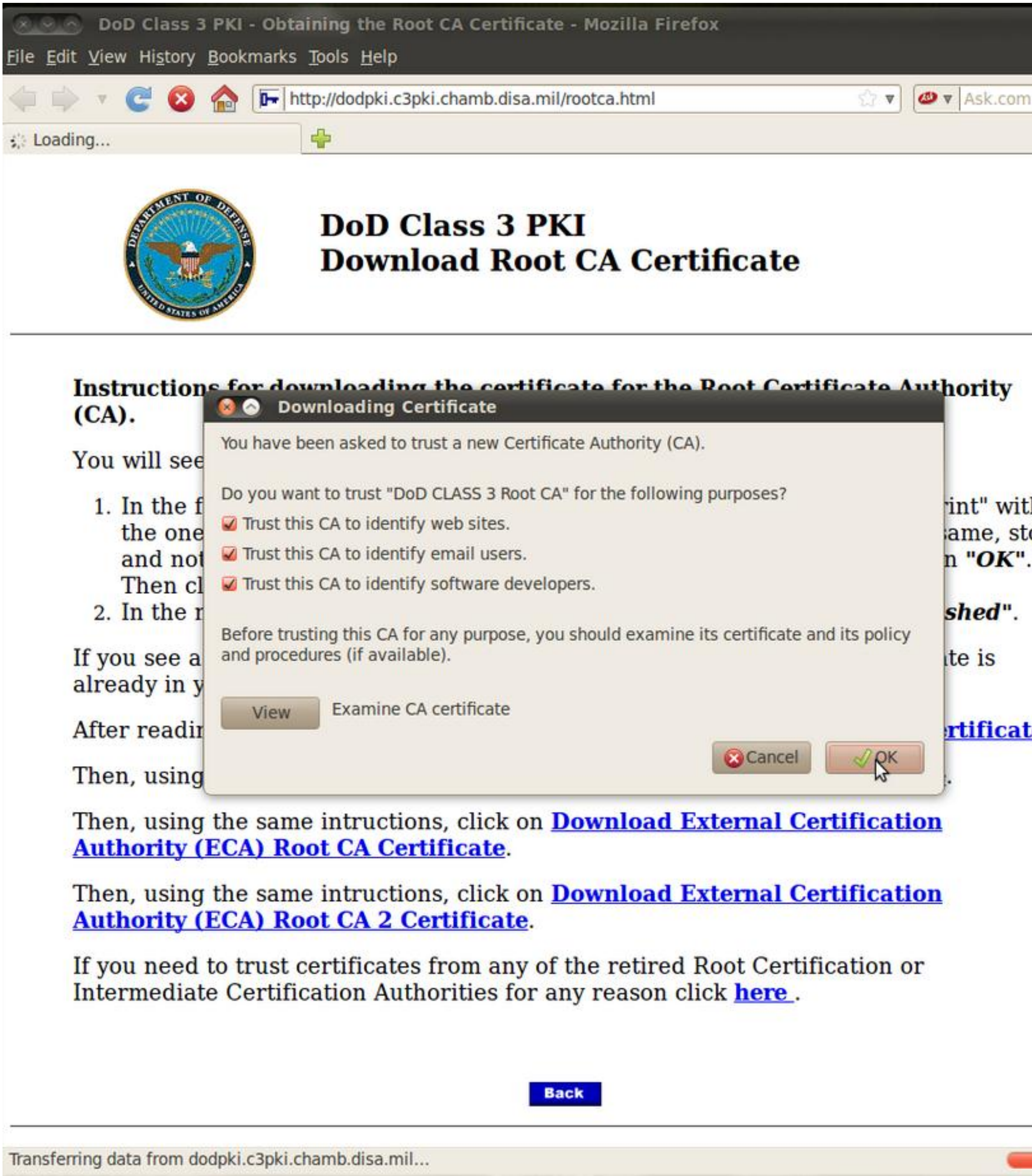
3. For each one, the process is the same. A notification box will appear. Check all three **or** the top two boxes.

- that is check ‘Trust this CA to identify web sites.’, ‘Trust this CA to identify email users’, and ‘Trust this CA to identify software developers’.

- At different installs, I have selected all three and just the top two. They both work. But, I have heard it is better for security to do only the top two but am unsure why.

4. Click ‘view’ to confirm the certificates then click ‘enter’

NOTE **- You may receive the error message (below) when you do this. THIS IS NOT A PROBLEM; the certificate has been installed anyway. No need to worry or do anything further.**


DoD Class 3 PKI - Obtaining the Root CA Certificate - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://dodpki.c3pki.chamb.disa.mil/rootca.html
Ask.com
Loading...

DoD Class 3 PKI
Download Root CA Certificate

Instructions for downloading the certificate for the Root Certificate Authority (CA).

You will see

1. In the f… …int" with the one… …ame, sto and not… …n "*OK*". Then cl…
2. In the r… …*shed*".

If you see a… …te is already in y…

After readin… …rtificat

Then, using… …

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "DoD CLASS 3 Root CA" for the following purposes?

☑ Trust this CA to identify web sites.
☑ Trust this CA to identify email users.
☑ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

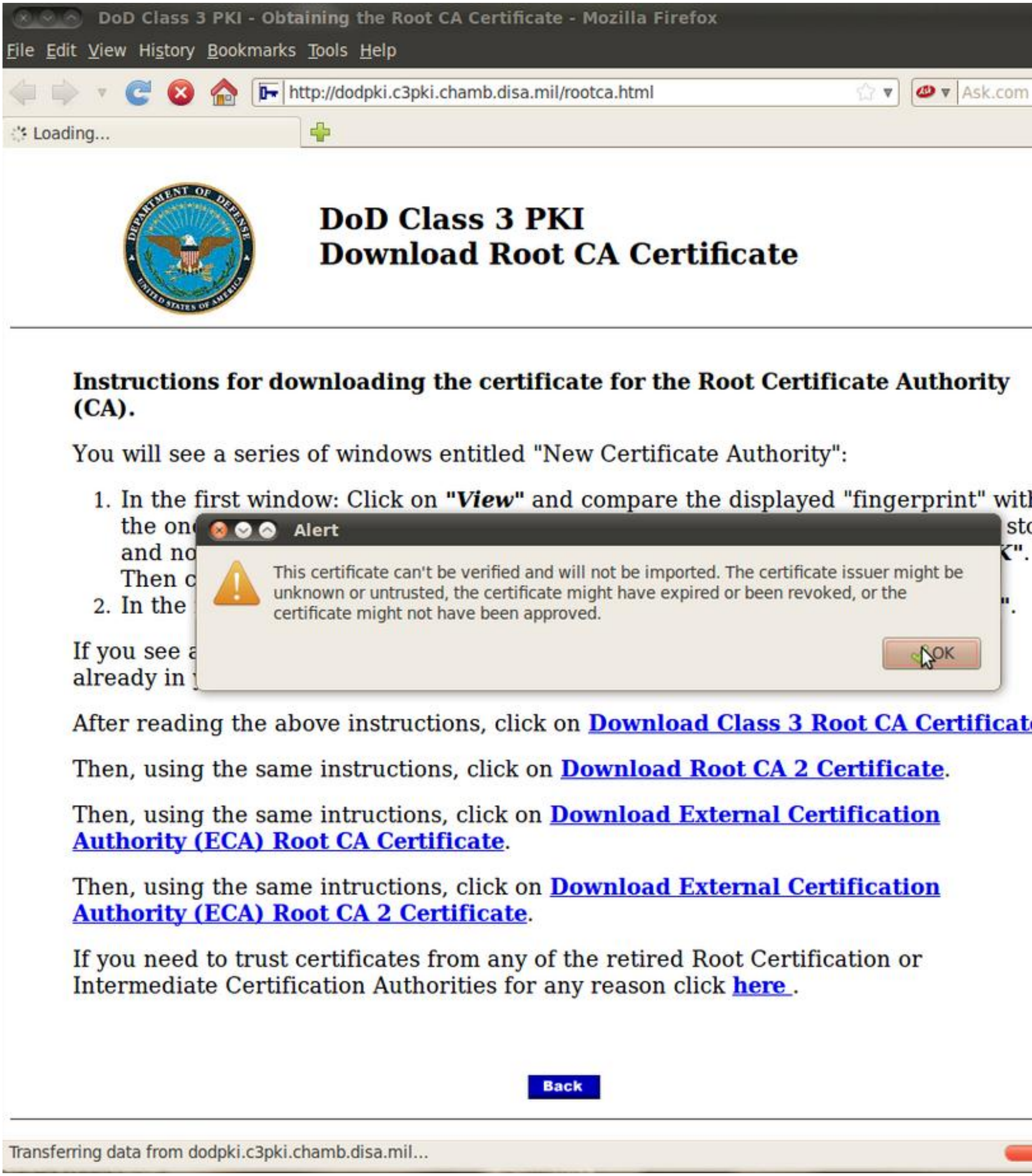
Then, using the same intructions, click on **Download External Certification Authority (ECA) Root CA Certificate**.

Then, using the same intructions, click on **Download External Certification Authority (ECA) Root CA 2 Certificate**.

If you need to trust certificates from any of the retired Root Certification or Intermediate Certification Authorities for any reason click **here** .

Transferring data from dodpki.c3pki.chamb.disa.mil...

- Again, you may receive the error message below when you do this. THIS IS NOT A PROBLEM; the certificate has been installed anyway. No need to worry or do anything further.


DoD Class 3 PKI - Obtaining the Root CA Certificate - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://dodpki.c3pki.chamb.disa.mil/rootca.html
Ask.com
Loading...
Alert
OK
Back

DoD Class 3 PKI
Download Root CA Certificate

Instructions for downloading the certificate for the Root Certificate Authority (CA).

You will see a series of windows entitled "New Certificate Authority":

1. In the first window: Click on **"*View*"** and compare the displayed "fingerprint" wit
   the on sto
   and no K".
   Then c
2. In the ".

If you see a
already in

This certificate can't be verified and will not be imported. The certificate issuer might be unknown or untrusted, the certificate might have expired or been revoked, or the certificate might not have been approved.

After reading the above instructions, click on Download Class 3 Root CA Certificat

Then, using the same instructions, click on Download Root CA 2 Certificate.

Then, using the same intructions, click on Download External Certification Authority (ECA) Root CA Certificate.

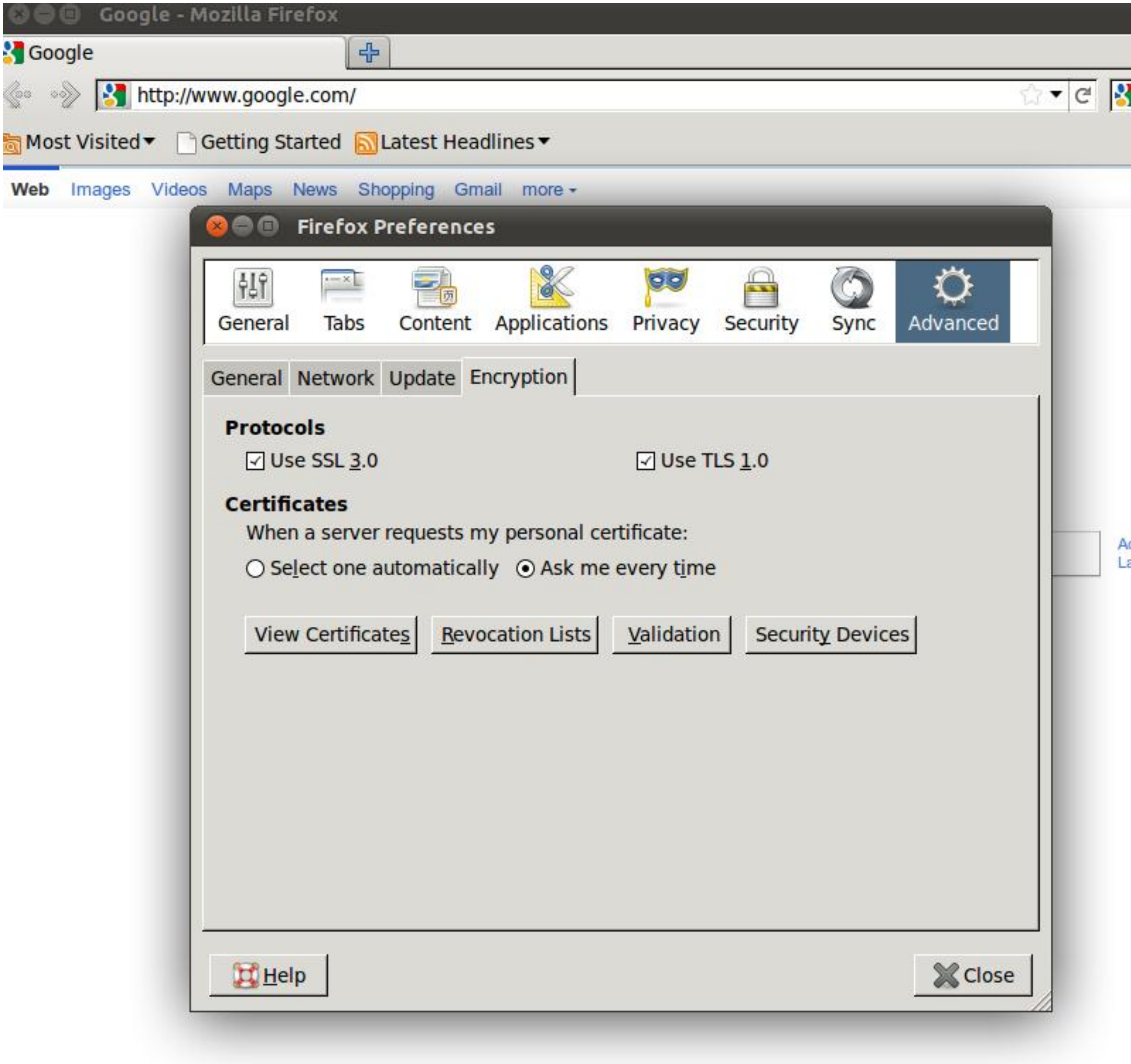
Then, using the same intructions, click on Download External Certification Authority (ECA) Root CA 2 Certificate.

If you need to trust certificates from any of the retired Root Certification or Intermediate Certification Authorities for any reason click here .

Transferring data from dodpki.c3pki.chamb.disa.mil...

Adding your smartcard reader to Firefox:

1. Open Firefox
2. On the menu bar (at top of screen), go to Edit->Preferences
3. Click on Advanced tab



Protocols

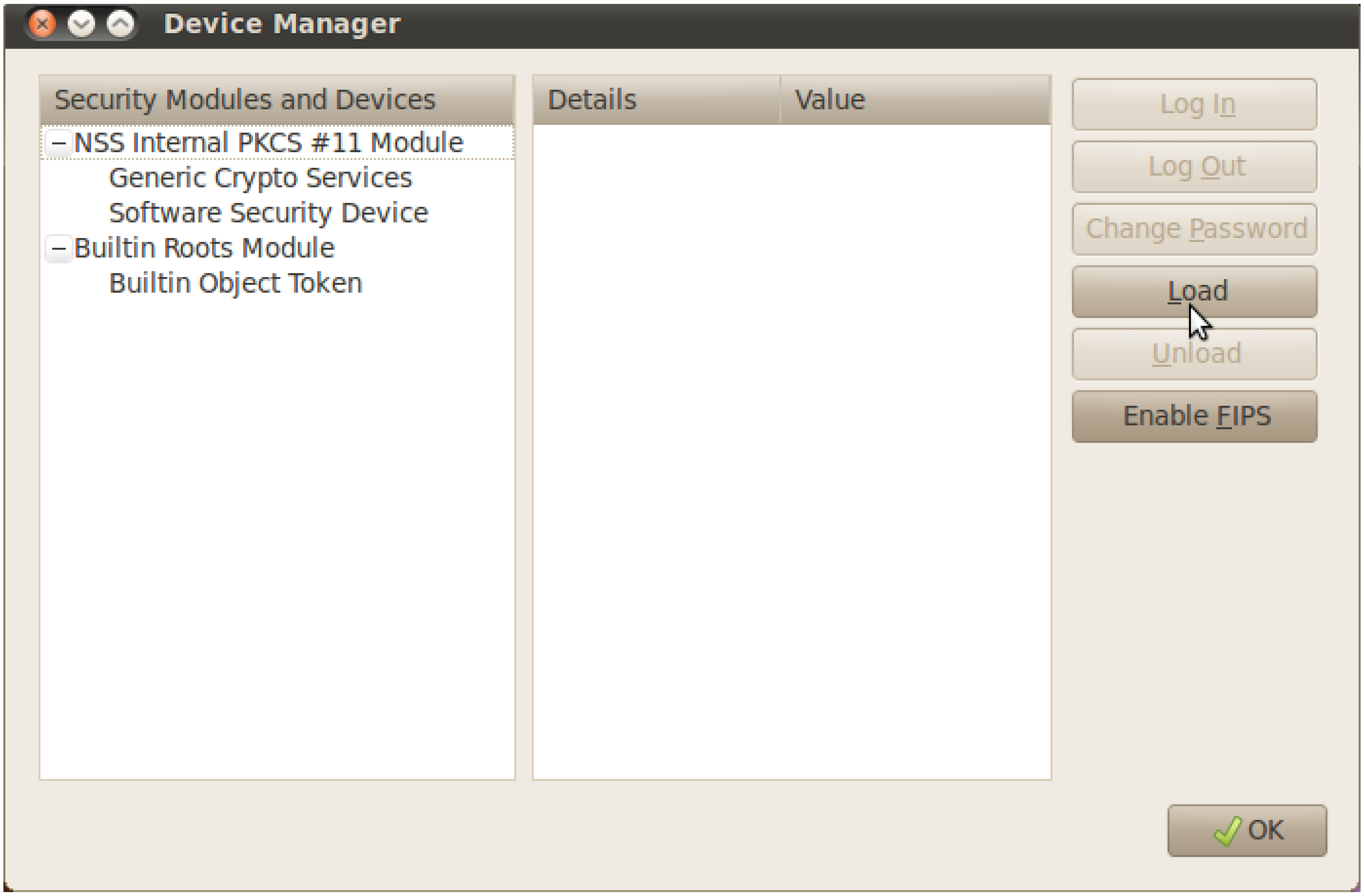
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

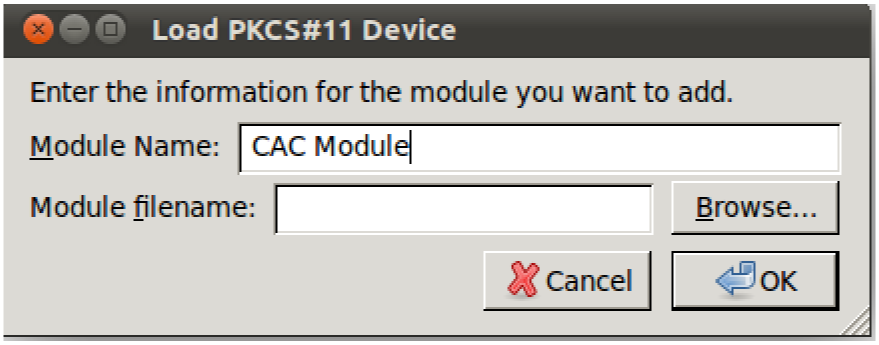
○ Select one automatically ● Ask me every time

4. Click on Security Devices



5. Click ‘Load’

6. For Device name type in ‘CAC Module’ (without the quotes)

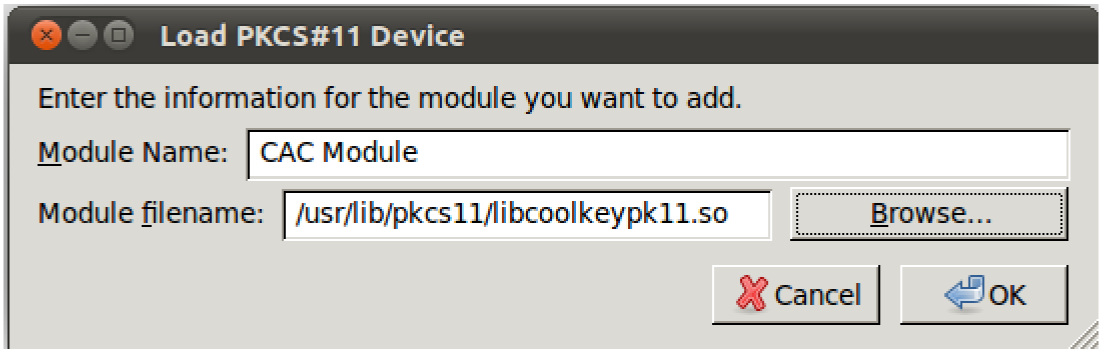


Enter the information for the module you want to add.

Module Name: CAC Module

Module filename:

7. For Module Filename, click Browse and go to and select
   /usr/lib/pkcs11/libcoolkeypk11.so
   - for me, this worked even though I use the 64-bit Ubuntu OS)
   - do not mistakenly select ‘/home/<yourname>/usr/lib’ you won’t find the file there



Enter the information for the module you want to add.

Module Name: CAC Module

Module filename: /usr/lib/pkcs11/libcoolkeypk11.so

8. Select ‘OK’, ‘OK’, etc. until back to normal browser.

9. Restart computer and test by loading Firefox with card reader plugged in and your CAC card inserted.

- For the SCR331 card reader, there should be a green light illuminated when the reader is plugged in. It flashes when the card is inserted AND Firefox is running. If Firefox is not running, the light may not illuminate or it may not flash (**until** Firefox is started).

- For the SCR3310 card reader, the green light will turn on when Firefox is running AND your CAC card is inserted. It will never blink.

10. Log onto a CAC/PKI website to test

- When prompted for your ‘Master Password’, this is your normal PIN that you use when logging on at work.

- When logging onto PKI required sites, you will be prompted by a warning box that is titled ‘**User Identification Request**’. There will be a drop-down menu directly below the line ‘**Choose the certificate to present as identification**’. One option will say ‘**CAC ID Certificate**’ and the other will say ‘**CAC Email Signature Certificate**’ as well as your name and a bunch of other info. You must select the ‘**CAC Email Signature Certificate**’ for OWA and the ‘**CAC ID Certificate**’ for non-email sites (such as NKO). If you select the incorrect one and have the ‘**Remember this decision**’ box checked, you may need to delete all your history/cookies/etc in order to get back the option to select certificates for future logins to that website.

NOTES:

- I have not tried to log onto DTS so I don’t know if further adjustments may be necessary to do this. I also usually access US Navy sites so there may be issues with non-Navy ones.

- Some screenshots are not mine, they were taken from the following blog: http://zxq9.com/dodcac/U10.4-LTS-32/Ubuntu10.4-LTS-32.html

- To use DBSign, you may need to do further adjustments including some changes to Java. One good resource for how to do this is DBSign Java .