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 <u>https://public.cyber.mil/pki-pke/end-users/getting-started/#toggle-id-3</u> 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.

5. 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 Unfortunately, the recommended CoolKey module is no longer valid on modern versions of Firefox (or at least I was unable to get this working).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	
<pre>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 requir 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 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]</pre>	red :

6. 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.



7. 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.

 Next, we are going to download the DoD certificates from Cyber.mil at <u>https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/zip/unclass-certificates_pkcs7_v5-6_dod.zip</u>.

<	> 🔸 🏠 Home	Downloads > Q		
Ø	Recent	Name	Size	Modified \bullet
ŵ	Home	unclass-certificates_pkcs7_v5-6_dod.zip	86.0 kB	13:43
	Desktop			
۵	Documents			
÷				
99	Music			
٥	Pictures			
⊨	Videos			
1	Trash			
	Ubuntu			
+	Other Locations			

 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.

Extract + unclass-certi	ficates_pkcs7_	v5-6_dod.zip	Q = 8
< > 🔂 Location 🖿 /			
Name 🔺	Size	Туре	Modified
Certificates_PKCS7_v5.6_DoD	180.1 kB	Folder	

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**.

	Preferences - Mozilla Firefox		● ● ⊗
☆ Preferences ×	+		
← → ♂ ✿	Sirefox about:preferences	\$	± ⊪\ ⊡ ® ≡
	> Find in Preferences	כ	
🔆 General	General		
Home	Startup		
Q Search	Restore previous session		
Privacy & Security	Always check if Firefox is your default browser		
C Sync	😑 Firefox is currently your default browser		
	Tabs Image: Ctrl+Tab cycles through tabs in recently used order Image: Open links in tabs instead of new windows Image: When you open a link in a new tab, switch to it immediately		
 Extensions & Theme Firefox Support 	Language and Appearance Fonts and Colors Default font Default (DejaVu Serif) v Size 16 v Advanced		
	Colors		

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.

Can	icel	Select File containing CA certificate(s) to import	٩	Open
Ø	Recent			
企	Home	Name 🔺	Size	Modified
	Desktop	Certificates_PKCS7_v5.6_DoD		14:00
D	Documents			
÷				
99	Music			
ø	Pictures			
H	Videos			
	Ubuntu			
+	Other Locations			
		Ce	rtificat	e Files 🔻

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.

Car	ncel	Select File c	ontaining CA c	ertificate(s) to import		٩	Open
Ø	Recent	• 🏠 arombaut	Downloads	Certificates_PKCS7_v5.6_DoD			
企	Home	Name			٠	Size	Modified
	Desktop	📔 Certificates_PK	CS7_v5.6_DoD.(der.p7b		50.3 kB	4 Apr 2019
۵	Documents	Certificates_PK	CS7_V5.6_DoD.	pem.p7b DoD. Poot. CA. 2 dec.p7b		68.2 kB	4 Apr 2019
\$	Downloads	Certificates_PK	CS7_V3.0_D0D_ CS7_V5.6_D0D	DoD_Root_CA_2.der.p7b		30.9 kB	4 Apr 2019
44	Music	Certificates_PK	CS7_v5.6_DoD_	DoD_Root_CA_4.der.p7b		3.5 kB	4 Apr 2019
ž	Disturas	Certificates_PK	CS7_v5.6_DoD_	DoD_Root_CA_5.der.p7b		3.0 kB	4 Apr 2019
0	Pictures	DoD_PKE_CA_c	hain.pem			3.0 kB	4 Apr 2019
	Videos						
	Ubuntu						
+	Other Locations						
						Certific	ate Files 🔻

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.



	P	references - Mozilla Firefox		-	-		
Preferences	× +						
← → ♂ ☆	Sirefox about:preference	s#searchResults	☆	$\overline{\mathbf{A}}$	III\ 🗉	۲	≡
		Certificate Manager		×		8	
🔆 Genera	Your Certificates People	Servers Authorities					
Home	You have <mark>certificates</mark> on file that	identify these certificate auth	orities				
Q Search	Certificate Name	Security Device		E.			
	DOD SW CA-56	Software Security	/ Device				
	DOD EMAIL CA-51	Software Security	/ Device		tificat	es	
Sync Sync	DOD ID CA-59	Software Security	/ Device		<u>l</u> ertifica	tes	
	DoD Root CA 2	Software Security	Device		ity <u>D</u> evi	ces	
	DOD ID CA-42	Software Security	/ Device				
	DOD EMAIL CA-40	Software Security	/ Device				
	DOD EMAIL CA-34	Software Security	/ Device	1			
		Coffware Security	Dovico				
🔹 Extensio	<u>V</u> iew <u>E</u> dit Trust	I <u>m</u> port E <u>x</u> port	Delete or Distrust				
⑦ Firefox S			ок	:			
					8		

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

20. Ensure the two check boxes are checked.

Edit CA certificate trust settings	8
The certificate "DoD Root CA 2" represents a Certificate Authority.	
Edit trust settings: This certificate can identify websites. This certificate can identify mail users.	Cancel OK

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

DoD Root CA 4



DoD Root CA 5

8
Cancel OK
8

- 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.

	Preferences - Mozilla Fire	fox			•	•
Image: Weight of the standard	× +					
← → C ⁱ	ces#privacy		☆	III\ 🗊	۲	Ξ
		♀ Find in Preferences				
General improve Firefox for	everyone. We always ask permissio	n before receiving personal				
information.	Device Manager				×	
	Device Manager				^	1
Security Modules and Devices	Details	Value		Log In		
~ NSS Internal PKCS #11 Module				Log Out		
Generic Crypto Services				Charace Deserves		
Software Security Device				Change <u>P</u> assword		
✓ Builtin Roots Module				Load	J	
NSS Builtin Objects				<u>U</u> nload		
				Enable <u>F</u> IPS		
				OK		
				ŬŔ.		
Query OCSP re	sponder servers to confirm the curre	ent validity of View Certificates			Í	2
Extensions & Themes certificates		Security <u>D</u> evices				
③ Firefox Support						

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

Load PKCS#11 Device Driver	● 🛛 😣
Enter the information for the module you want to add.	
Module Name OpenSC	
Module <u>f</u> ilename	Browse
Cancel	ОК

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.

			Preference	s - Mozilla Firefox				- • •	
🔅 Prefe	erences X	+							
\leftrightarrow	C' 🕜	Sirefox about:preferen	ces#searchResults		☆	lii\	•	\$ ≡	
F			Device	Manager			×	1	
ł	Security Modules a	and Devices	Details	Value		Log I <u>n</u>			
1	∼ NSS Internal PKC	5 #11 Module	Module	Module OpenSC		Log Out			
	Generic Crypto	Services	Path	/usr/lib/x86_64-linux-gnu/opensc-pl	kcs11.so				
C	Software Secu	ity Device					Change Password		
	✓ Builtin Roots More	dule							
	NSS Builtin Obj	ects							
ŕ	✓ OpenSC								
c						ОК			
								1.	

- 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 **Isusb**. 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 S	Search	Ter	minal Help		
агог	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	
агор	nbaut	@ubunt	u:~\$_				

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.

 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.



 Now, let's test navigating to <u>https://mypay.dfas.mil/#/</u>. 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.

	Password Required - Mozilla Firefox 🛛 🔗
Jan Contraction	Please enter the master password for the PIV Card Holder pin (PIV_II).
	Cancel 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.

User Identification Request 😣						
This site has requested that you identify yourself with a certificate: mypay.dfas.mil:443						
Organization: "Office of Personnel Management"						
Issued Under: "DigiCert Inc"						
Choose a certificate to present as identification:						
DENT.ARTHUR.P.0000000000 [00:00:00]						
Details of selected certificate:						
Issued to: CN= DENT.ARTHUR.P.0000000000 U.S. Government,C=US Serial number: 18:37:27 Valid from September 30, 2019, 8:00:00 PM GMT-4 to August 5, 2020,						
Key Usages: Signing Issued by: CN=DOD ID CA-52,OU=PKI,OU=DoD,O=U.S. Government,C=US						
🖾 Remember this decision						
Cancel OK						

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 <u>https://www.my.af.mil</u>.
- 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 <u>aaron.rombaut@gmail.com</u> or Facebook messenger.