DICT
DEPARTMENT OF INFORMATION
AND COMMUNICATIONS TECHNOLOGY

Downloading Authentication Certificate with User Generated Password Using Mozilla Firefox

Assumption

This document assumes that Firefox is already installed on your computer.

Note:

To be able to download and install the certificate, the user must have at least Firefox version 24 or higher installed on the computer. Also, other browsers like Google Chrome and Internet Explorer will not work.

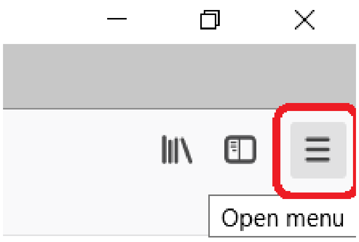
Prerequisite

The user must have an Internet connection.

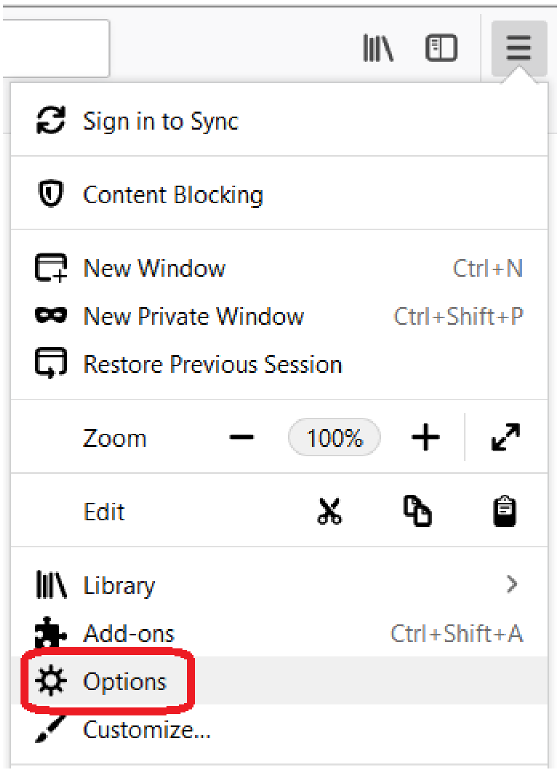
Setting up your environment

Before we proceed, you must first install the PNPKI certificate chain of trust.

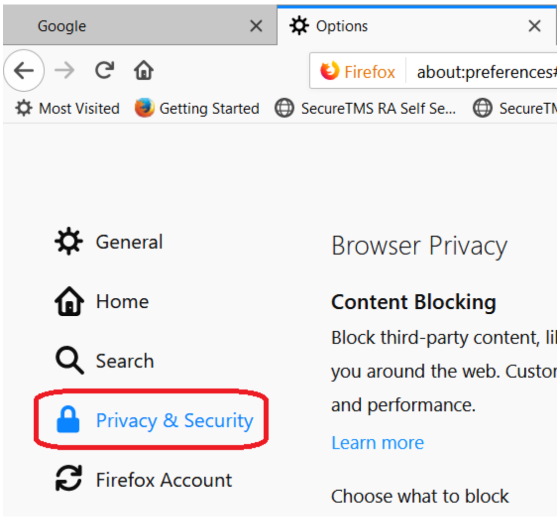
1. Download the PNPKI certificate chain PEM files here: https://drive.google.com/file/d/1Gzicyx4pd4xqONh_s-6kcb7mYM2kRxbx/view?usp=drive_web
2. Unzip the files
3. Launch your Mozilla Firefox browser. Click on the **Open Menu** at the top right corner.



4. Select **Options**



5. A new **Options** window will open. Select **Privacy & Security**



Browser Privacy

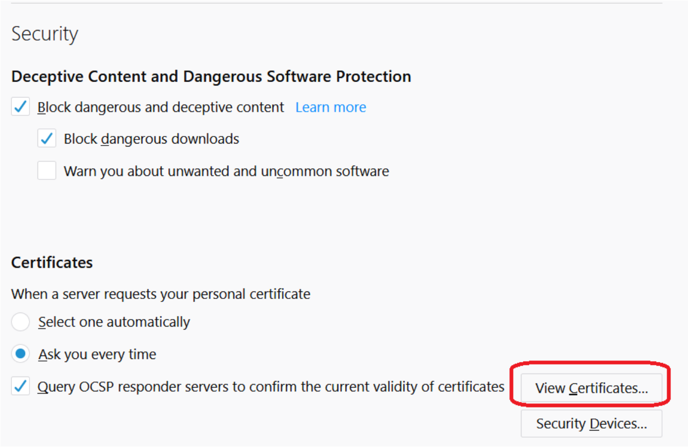
Content Blocking

Block third-party content, li you around the web. Custo and performance.

Learn more

Choose what to block

6. Scroll down to the bottom of the page, under the section for **Security,** look for the **View Certificates** button and click on it.



Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

□ Warn you about unwanted and uncommon software

Certificates

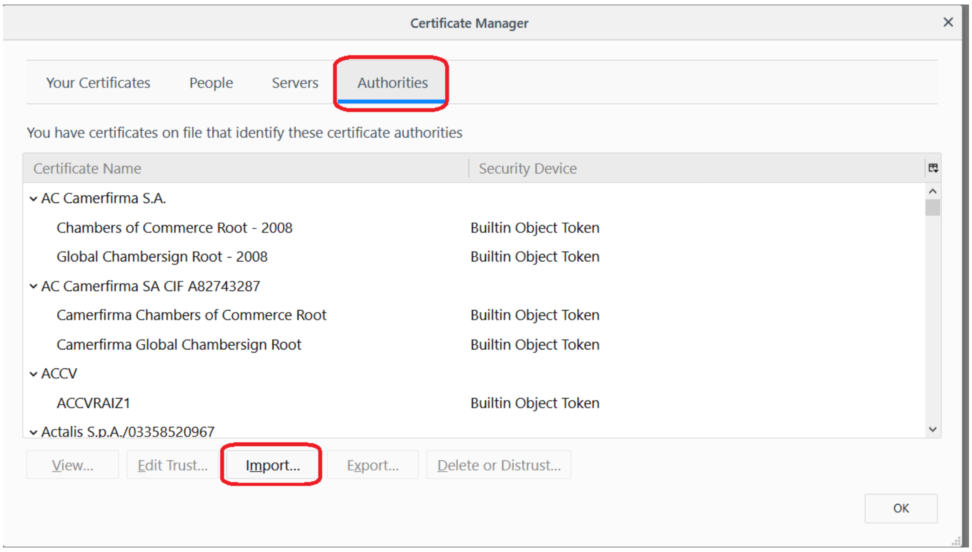
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

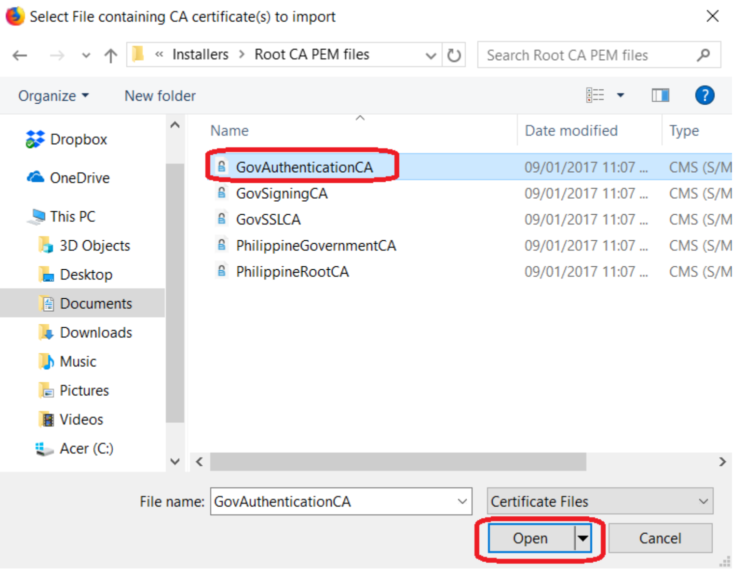
7. The **Certificates Manager** window will open. Go to the **Authorities** tab then click on **Import**



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌄ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⌄ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
⌄ ACCV	
ACCVRAIZ1	Builtin Object Token
⌄ Actalis S.p.A./03358520967	

8. Point it to the folder where you have unzipped the downloaded PEM files. Select one of the five files then click on Open



Select File containing CA certificate(s) to import

« Installers > Root CA PEM files

Search Root CA PEM files

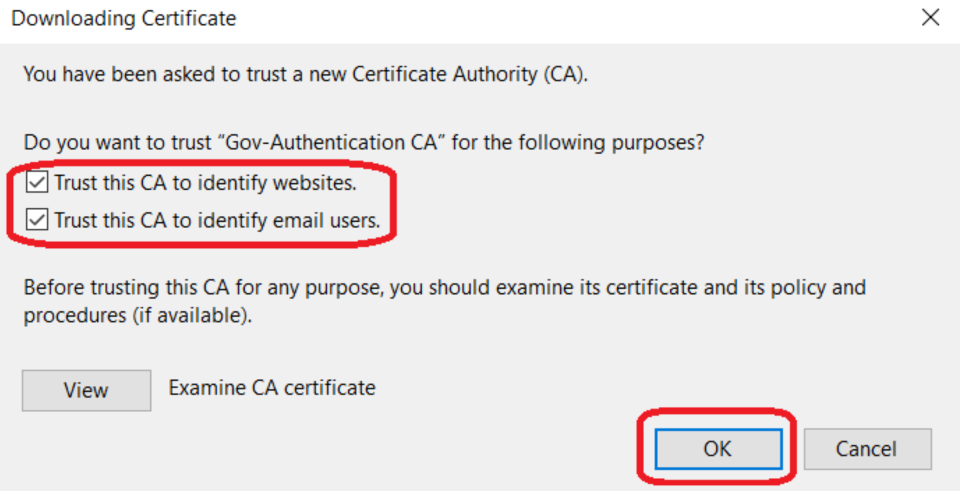
Organize ▾ New folder

Name	Date modified	Type
GovAuthenticationCA	09/01/2017 11:07 ...	CMS (S/M
GovSigningCA	09/01/2017 11:07 ...	CMS (S/M
GovSSLCA	09/01/2017 11:07 ...	CMS (S/M
PhilippineGovernmentCA	09/01/2017 11:07 ...	CMS (S/M
PhilippineRootCA	09/01/2017 11:07 ...	CMS (S/M

File name: GovAuthenticationCA

Certificate Files

9. The Downloading Certificate window will open. Put a check on both Trust this CA to identify websites and Trust this CA to email users then click on OK



Downloading Certificate

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

Do you want to trust “Gov-Authentication CA” for the following purposes?

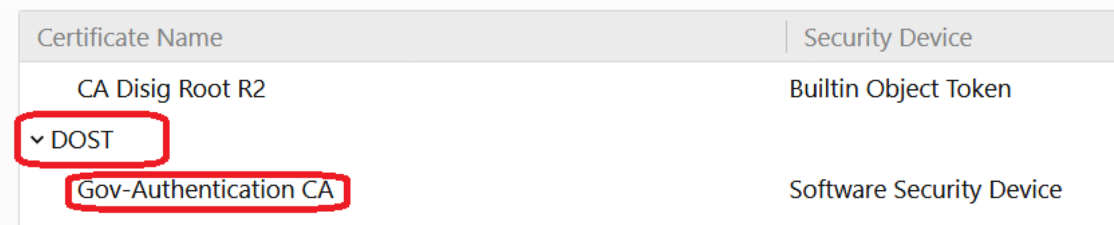
☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

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

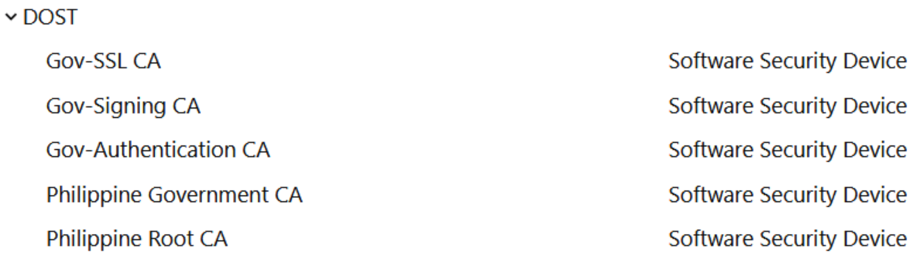
View Examine CA certificate

10. Back at the Certificate Manager window, if you scroll down the list, you should now see a section for DOST and the first PEM file you chose to install.



Certificate Name	Security Device
CA Disig Root R2	Builtin Object Token
⌄ DOST	
Gov-Authentication CA	Software Security Device

11. Just repeat the process until you have all five (5) PEM files installed.



⌄ DOST	
Gov-SSL CA	Software Security Device
Gov-Signing CA	Software Security Device
Gov-Authentication CA	Software Security Device
Philippine Government CA	Software Security Device
Philippine Root CA	Software Security Device

12. Click OK to close out the Certificate Manager window

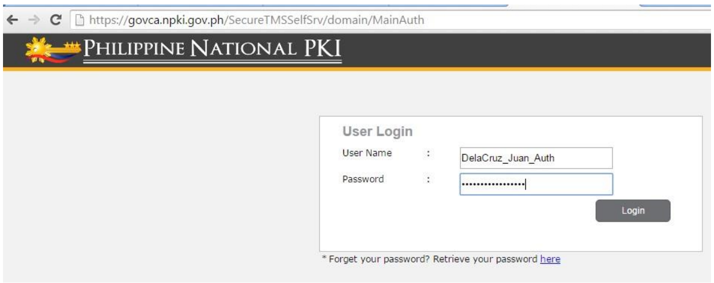
Now that you have finished setting up your environment, you can start downloading your certificate.

Start Downloading your PNPKI digital certificate

1. Login to the Self-Service Portal for your Authentication certificate

Access the self-service portal URL that your Registration Authority (RA) emailed to you. For the purposes of demonstration, we will be using this URL: https://govca.npki.gov.ph/SecureTMSSelfSrv/domain/MainAuth

Once you have accessed the appropriate URL, you should see the image below. Enter your username and password then click login.



https://govca.npki.gov.ph/SecureTMSSelfSrv/domain/MainAuth

PHILIPPINE NATIONAL PKI

User Login

User Name : DelaCruz_Juan_Auth

Password : ••••••••••••••••

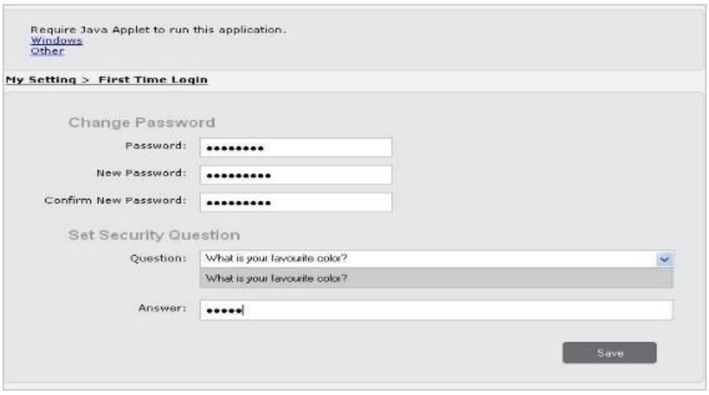
* Forget your password? Retrieve your password here

Figure 1. Logging in to the Self-Service Portal

Warning:

Be careful when entering your username and password. After **five (5) incorrect** log in attempts, your account will be **blocked**.

2. After logging in successfully for the first time, you will be prompted to **change your password**. Fill out all the fields and answer the security question.



Require Java Applet to run this application.
Windows
Other

My Setting > First Time Login

Change Password

Password: ••••••••

New Password: •••••••••

Confirm New Password: •••••••••

Set Security Question

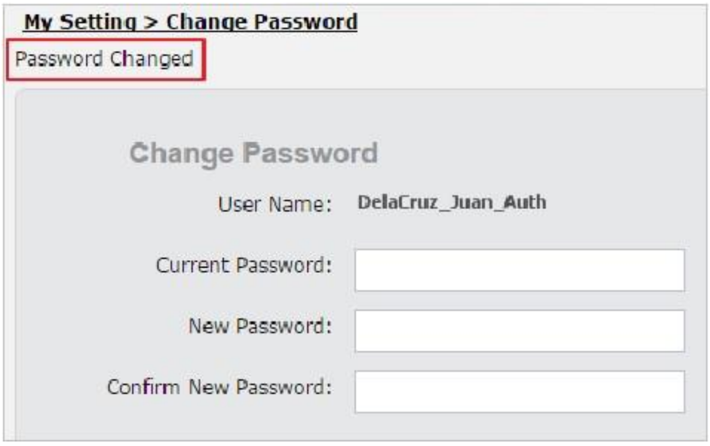
Question: What is your favourite color?

What is your favourite color?

Answer: •••••

Figure 2. Changing your password

3. Hit the Save button. If you encountered no errors, you should see this image:



My Setting > Change Password

Password Changed

Change Password

User Name: DelaCruz_Juan_Auth

Current Password:

New Password:

Confirm New Password:

Figure 3. Successfully changing your password

4. Click the Philippine National PKI logo on top of the page to get to the Home page.

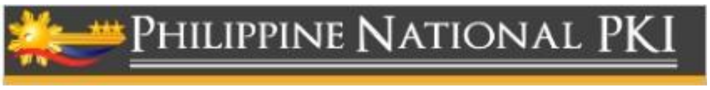


Figure 4. PNPKI logo

You may be logged out of the self-service portal. Login again with your new

Credentials.

5. Click Enrollment on the left side of the home page.

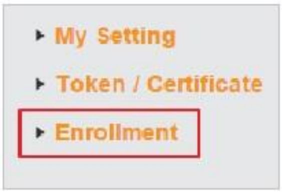
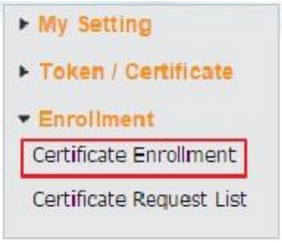


Figure 5. Selecting the Enrollment link

6. Select Certificate Enrollment form the dropdown list.



▸ My Setting

▸ Token / Certificate

▾ Enrollment

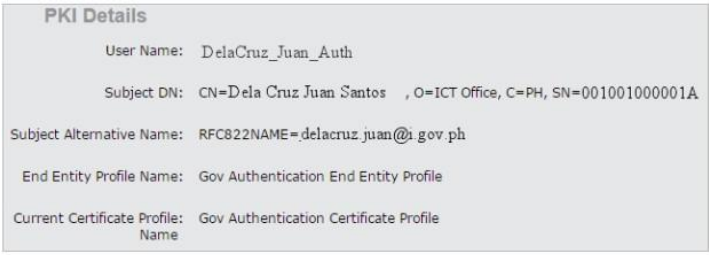
Certificate Enrollment

Certificate Request List

Figure 6. Selecting certificate Enrollment from the dropdown list

7. Check all details in your certificate. If you see any errors in your personal information, do not proceed. Notify your RA immediately.

Important:



PKI Details

User Name: DelaCruz_Juan_Auth

Subject DN: CN=Dela Cruz Juan Santos , O=ICT Office, C=PH, SN=001001000001A

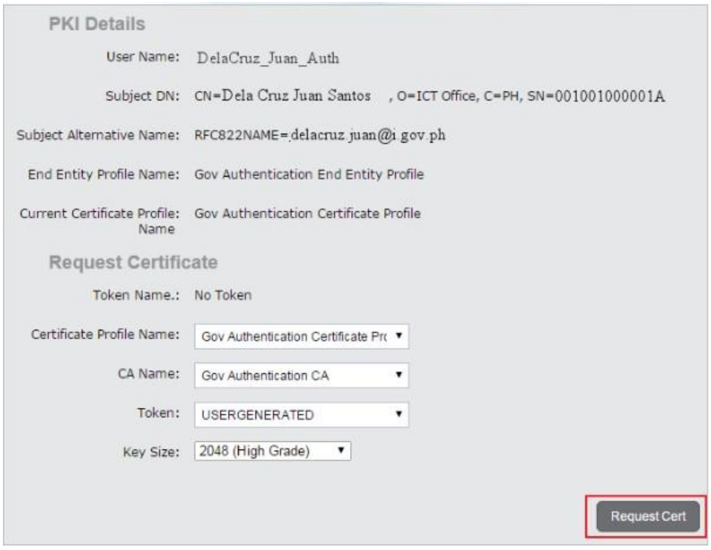
Subject Alternative Name: RFC822NAME=delacruz.juan@i.gov.ph

End Entity Profile Name: Gov Authentication End Entity Profile

Current Certificate Profile Name: Gov Authentication Certificate Profile

Figure 7. Certificate information

8. If your details are all correct, you can hit the Request Cert button at the lower right side of the page.



PKI Details

User Name: DelaCruz_Juan_Auth

Subject DN: CN=Dela Cruz Juan Santos , O=ICT Office, C=PH, SN=001001000001A

Subject Alternative Name: RFC822NAME=delacruz.juan@i.gov.ph

End Entity Profile Name: Gov Authentication End Entity Profile

Current Certificate Profile Name: Gov Authentication Certificate Profile

Request Certificate

Token Name.: No Token

Certificate Profile Name: Gov Authentication Certificate Prc ▾

CA Name: Gov Authentication CA ▾

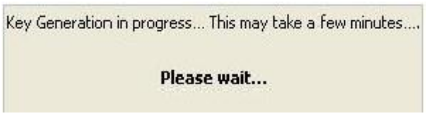
Token: USERGENERATED ▾

Key Size: 2048 (High Grade) ▾

Request Cert

Figure 8. Requesting for a certificate

9. The screen will display the generation of private key.



Key Generation in progress... This may take a few minutes....

Please wait...

Figure 9. Key generation

10. Click Certificate Request List to see the status of your certificate enrollment.

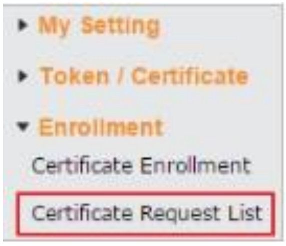
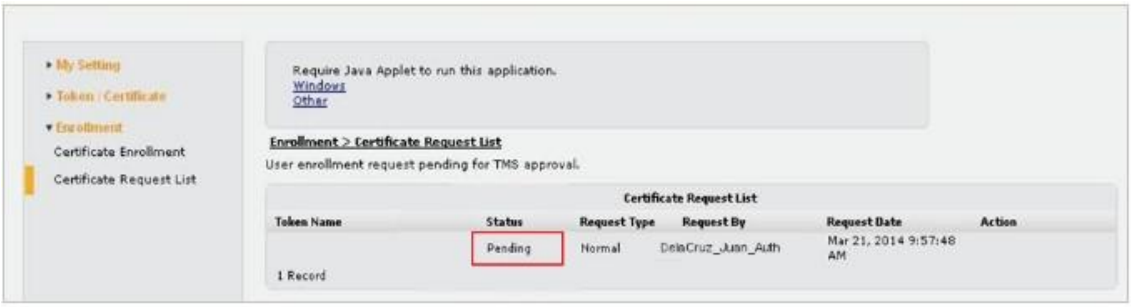


Figure 10. Selecting Certificate Request List

11. A “Pending” status will appear, which means your certificate enrollment is not yet issued. Notify your RA officer once you see the Pending status. The request certificate is subject to approval by the RA administrator.



Require Java Applet to run this application.
Windows
Other

Enrollment > Certificate Request List

User enrollment request pending for TMS approval.

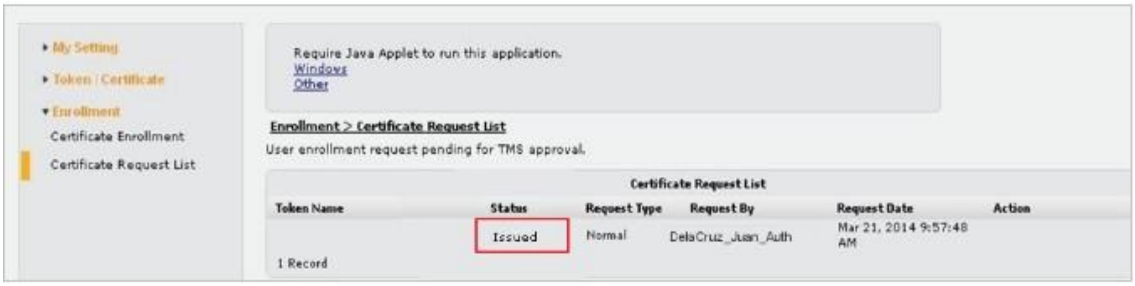
Certificate Request List

Token Name	Status	Request Type	Request By	Request Date	Action
	Pending	Normal	DelaCruz_Juan_Auth	Mar 21, 2014 9:57:48 AM	

1 Record

Figure 11. Pending status for certificate enrollment

12. Once approved, the status should be changed to Issued.



Require Java Applet to run this application.
Windows
Other

Enrollment > Certificate Request List

User enrollment request pending for TMS approval.

Certificate Request List

Token Name	Status	Request Type	Request By	Request Date	Action
	Issued	Normal	DelaCruz_Juan_Auth	Mar 21, 2014 9:57:48 AM	

1 Record

Figure 12. Issued status for certificate enrollment

13. Click Token Certificate list.

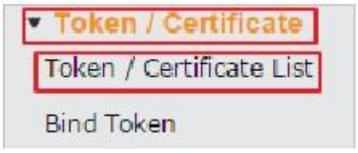
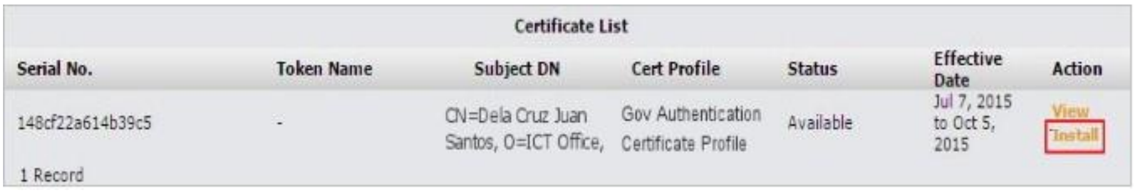


Figure 13. Selecting Token/Certificate list to see lists of certificates

14. Click Install on the right side of the page.

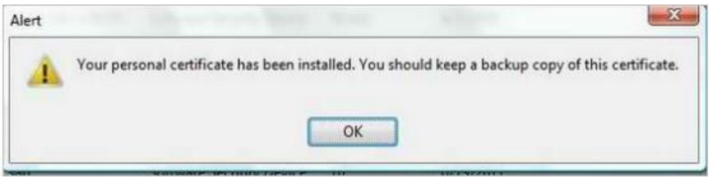

Certificate List

Serial No.	Token Name	Subject DN	Cert Profile	Status	Effective Date	Action
148cf22a614b39c5	-	CN=Dela Cruz Juan Santos, O=ICT Office,	Gov Authentication Certificate Profile	Available	Jul 7, 2015 to Oct 5, 2015	View Install

1 Record

Figure 14. Selecting Install button to install certificate in browser

15. A notification similar to the image below will pop up at the top of your browser, indicating that you have successfully installed your certificate.


Alert

Your personal certificate has been installed. You should keep a backup copy of this certificate.

Figure 15. Notification of the successful installation of your certificate into your browser.

Important:

If you clicked the **Request Cert** button and decided to download your certificate at a later time, make sure that you use the same browser and the same computer from where you requested the certificate, otherwise the Install option will freeze.

16. Click this icon ☰ located at the topmost right corner of your browser and go to Options.

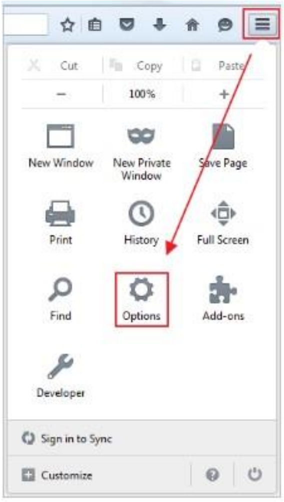
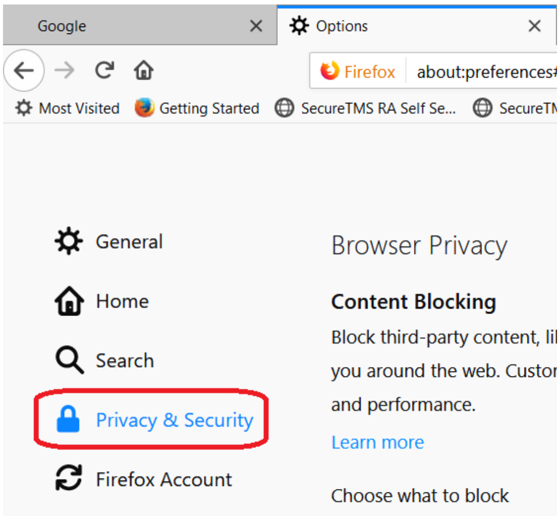


Figure 16. Getting to the option button

17. A new Options window will open. Select **Privacy & Security**



Browser Privacy

Content Blocking

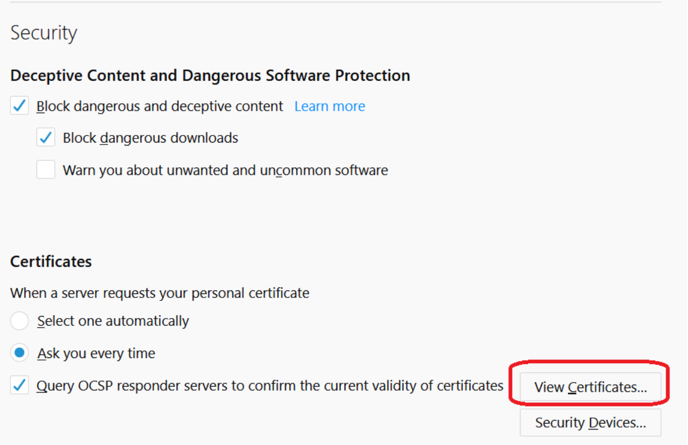
Block third-party content, li
you around the web. Custo
and performance.

Learn more

Choose what to block

Figure 17. Getting to the Privacy and Security

18. Scroll down to the bottom of the page, under the section for **Security**, look for the **View Certificates** button and click on it.



Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

□ Warn you about unwanted and uncommon software

Certificates

When a server requests your personal certificate

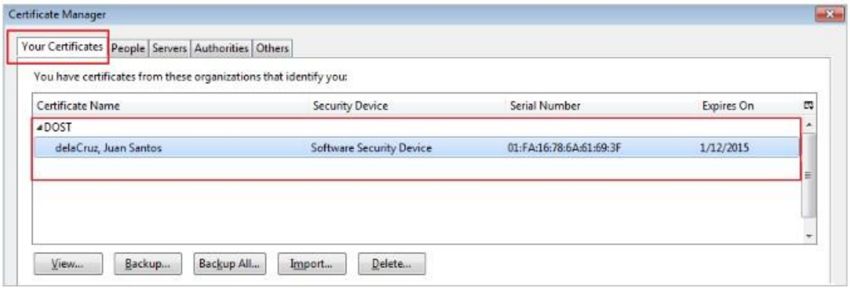
○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

Figure 18. Getting to the certificate manager

19. On the **certificate manager**, select **Your Certificates**. You should be able to see your certificate as show on the image below.

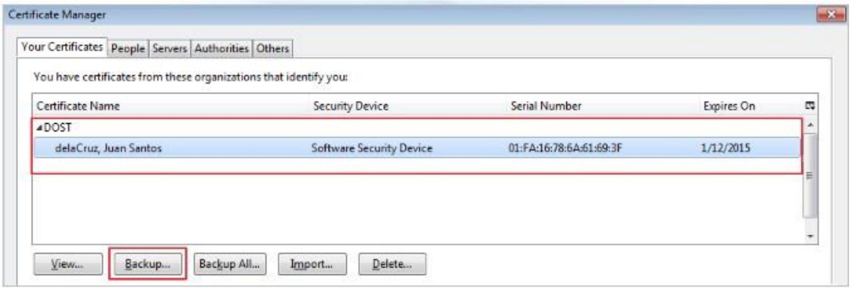


You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
◢DOST			
delaCruz, Juan Santos	Software Security Device	01:FA:16:78:6A:61:69:3F	1/12/2015

Figure 19. Viewing your certificate

20. Select your certificate then click **Backup**.

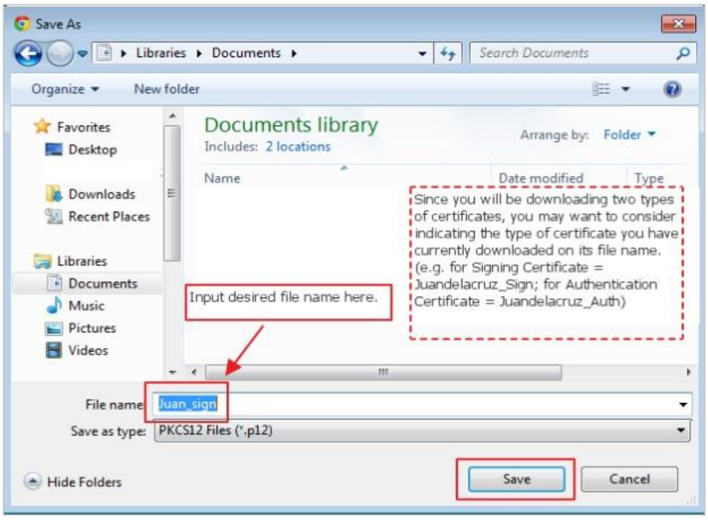


You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
◢DOST			
delaCruz, Juan Santos	Software Security Device	01:FA:16:78:6A:61:69:3F	1/12/2015

Figure 20. Backing up your certificate

21. Navigate to a secure directory where you will save your certificate. For purposes of demonstration, we will store the certificate on your documents folder. It is highly recommended, however, that you store it in a secure location.



Since you will be downloading two types of certificates, you may want to consider indicating the type of certificate you have currently downloaded on its file name. (e.g. for Signing Certificate = Juandelacruz_Sign; for Authentication Certificate = Juandelacruz_Auth)

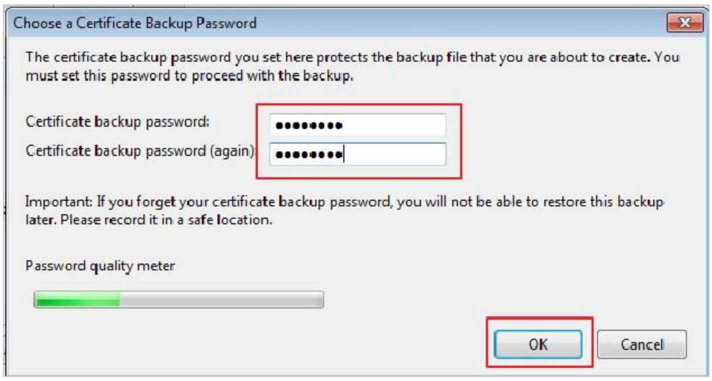
Input desired file name here.

File name: Juan_sign

Save as type: PKCS12 Files (*.p12)

Figure 21. Setting the name of your certificate

22. Set your password for the certificate then click **OK**.



The certificate backup password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.

Certificate backup password: ••••••••

Certificate backup password (again): ••••••••

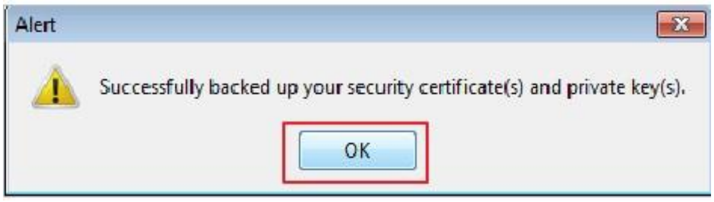
Important: If you forget your certificate backup password, you will not be able to restore this backup later. Please record it in a safe location.

Password quality meter

Figure 22. Setting your password

Note: The **password should be at least eight characters**. Consider a password that is hard to crack. It should contain at least a special character, a number, and capital and lower case letters.

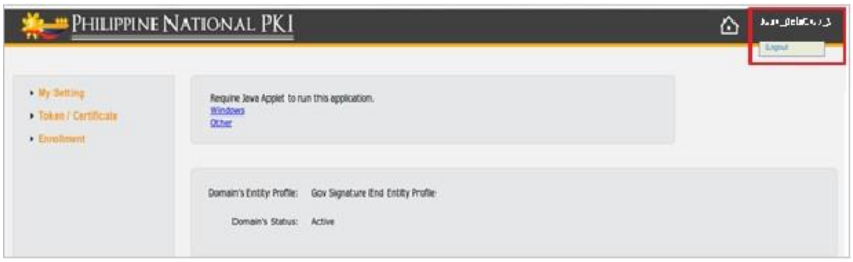
23. A success message should appear after clicking OK on the password window. Click OK to escape from the window.



Successfully backed up your security certificate(s) and private key(s).

Figure 23. Success message indicating you have successfully backed up your certificate

24. To log out of the Self-Service portal, hover you mouse over your user name located at the topmost right corner of the webpage. A Logout button should appear. Click it.



Require Java Applet to run this application.
Windows
Other

Domain's Entity Profile: Gov Signature End Entity Profile

Domain's Status: Active

Figure 24. Logging out of the self-service portal

25. Now you just need to follow the same steps to download and backup your Signing Certificate.