HOW TO CONNECT TO eCLAIMS WEB SERVICE WITH DIGITAL CERTIFICATES USING THE PROXYSERVER

Things you will need:

a. Computer with Windows OS (Windows XP or later and Windows 2003 or Later) with direct **Internet Connection** and **WinRAR** installed.
b. Claims Web Service package named "eClaims Web Service.rar" which contains the following:
   - OpenSSL application
   - .Dll files
        i. libeay32.dll
        ii. ssleay32.dll
   - Cert folder containing
        i. Certificate (.pfx file) - This is your philhealth assigned client digital certificate
        ii. Root certificate (.cer file)
   - Proxy Server Application (ProxyServer.exe)
   - Client Test Application (ClientTest.exe)
c. Email from PhilHealth informing you of the following passwords:
   - certificate password
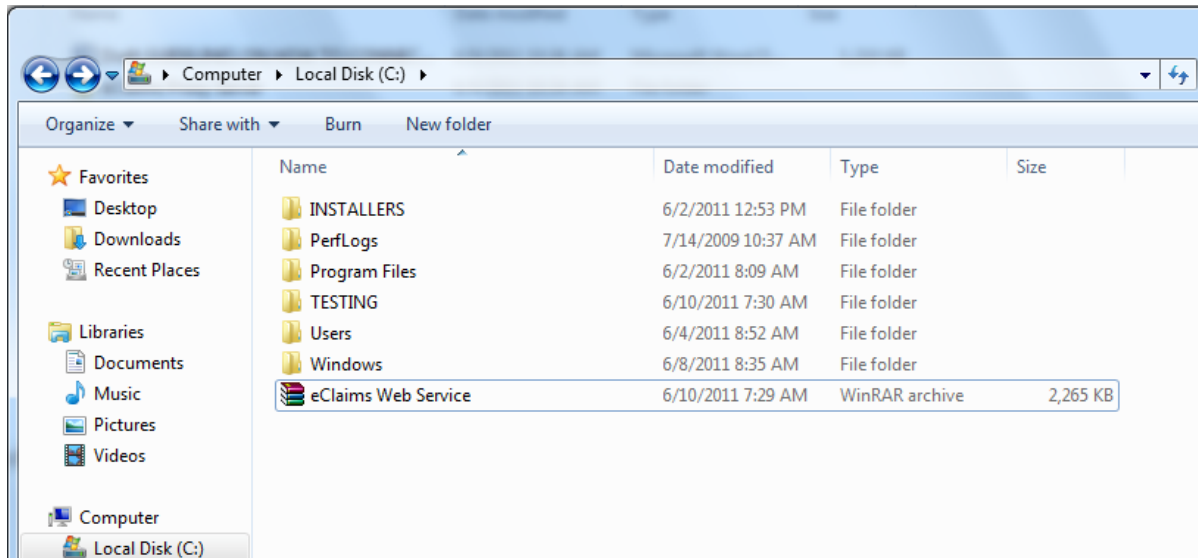   - password of the "eClaims Web Service.rar"

Overview:

a. Extract the package, i.e., "eClaims Web Service.rar"
b. Extract the key and certificate from the .pfx file.
   a. Extract the certificate file (.pem) from the client certificate (.pfx), i.e.

   openssl.exe pkcs12 -clcerts -nokeys -in "C:\eClaims Web Service\cert\phichospital.pfx" -out "C:\eClaims Web Service\Cert\phichospitalcert.pem"

   b. Extract the certificate key (.pem) from the same client certificate (.pfx), i.e.

   openssl.exe pkcs12 -nocerts -in "C:\eClaims Web Service\cert\phichospital.pfx" –out "C:\eClaims Web Service\Cert\phichospitalkey.pem"

c. Run the Proxy Server and point to the URLs to connect to the eClaims web services and certificates, i.e.,
   i. For eClaims Phase I, use
       https://eclaims.philhealth.gov.phh/soap and/or
       https://eclaims1.philhealth.gov.ph/soap
   ii. For eClaims Phase II (testing stage), use
       https://cws.philhealth.gov.ph/soap
   iii. c:\eClaims web service\cert*phichospitalcert.pem*
   iv. c:\eClaims web service\cert*phichospitalkey.pem*
   v. c:\eClaims web service\cert*phicrootca.cer*
   vi. Enter the *passprase*
   vii. Start the Server

d. Point your Hospital IS to connect to the computer where the PROXY SERVER is running, i.e.,
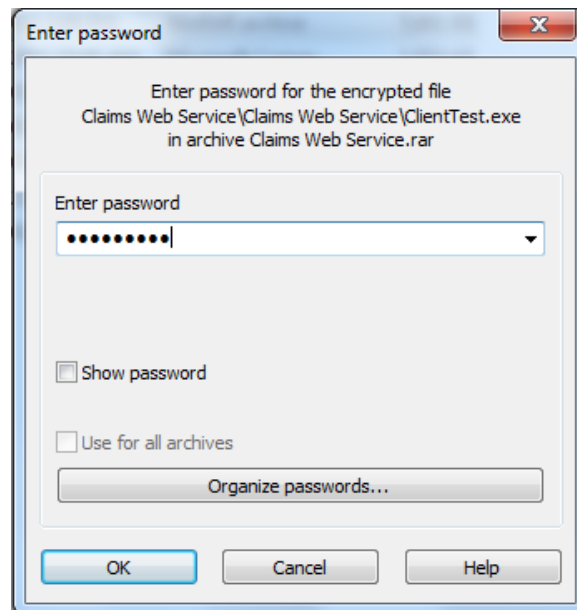   http://computername:8098/soap

Step by Step:

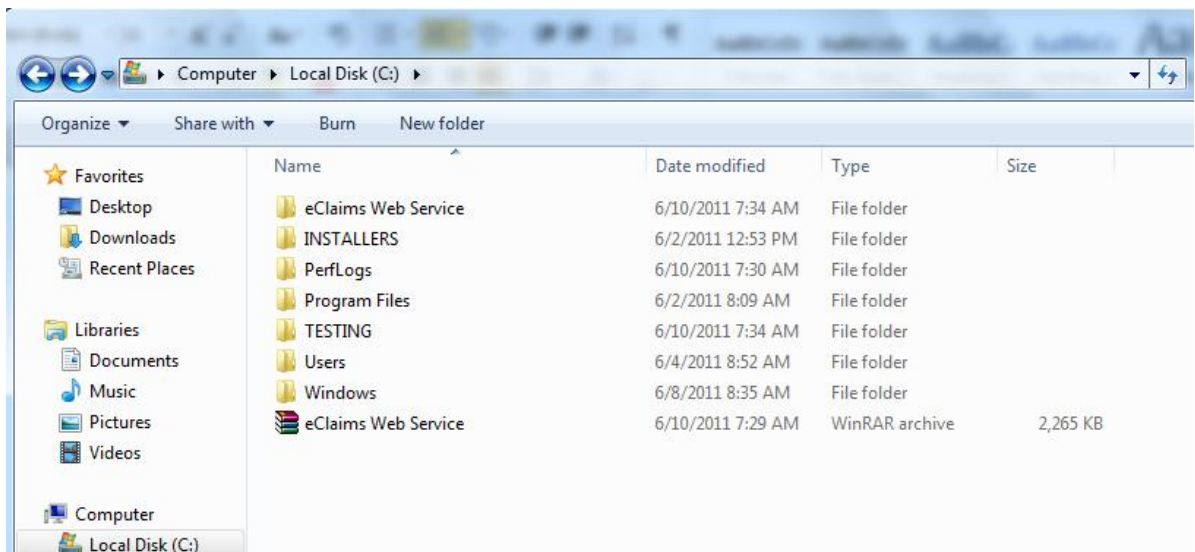1. Save the "eClaims Web Service.rar" in drive "C" or any drive in your workstation


2. Extract the .rar file
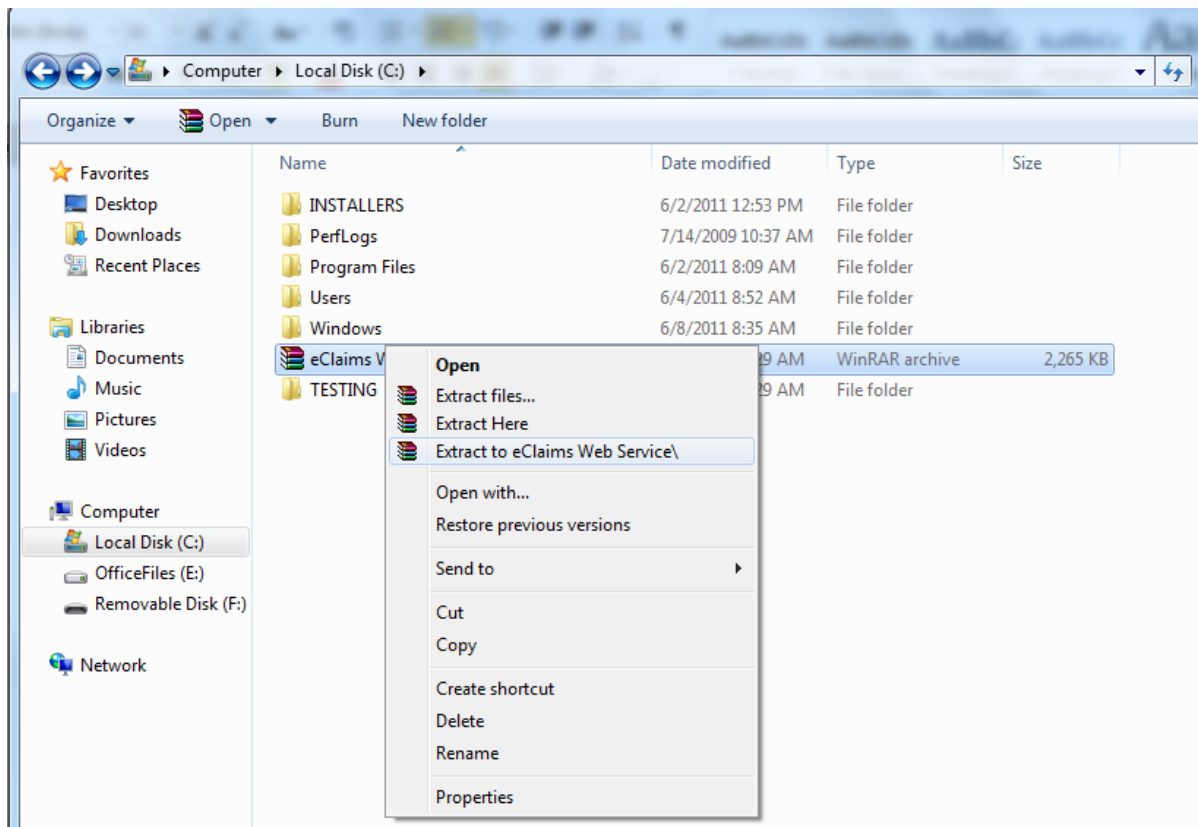
3. Input the password provided in the email that was sent by PhilHealth then click "**OK**".


4. Click on the *eClaims Web Service* folder to open.

5. The contents of the folder should be the following: *OpenSSL folder* containing the openSSL application*, libeay32.dll* file, *ssleay32.dll* file, "*cert*" folder, *"Proxy Server" Application* and the "*Client Test" Application*.
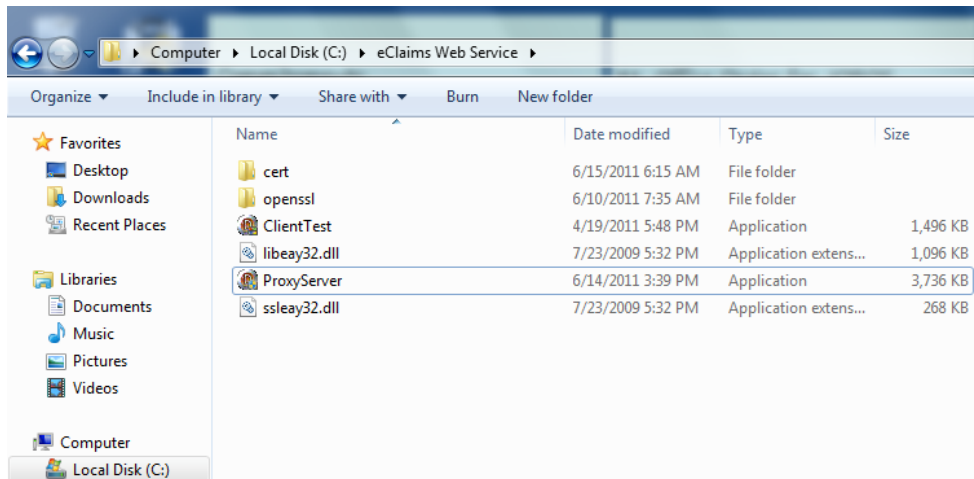
6. After checking the contents of the folder, click on the "*Start*" button or the "*Windows Logo*" button then go to "*Accessories*" then right click on the "Command Prompt" application. Click on "*Run as Administrator*" the command prompt should appear.
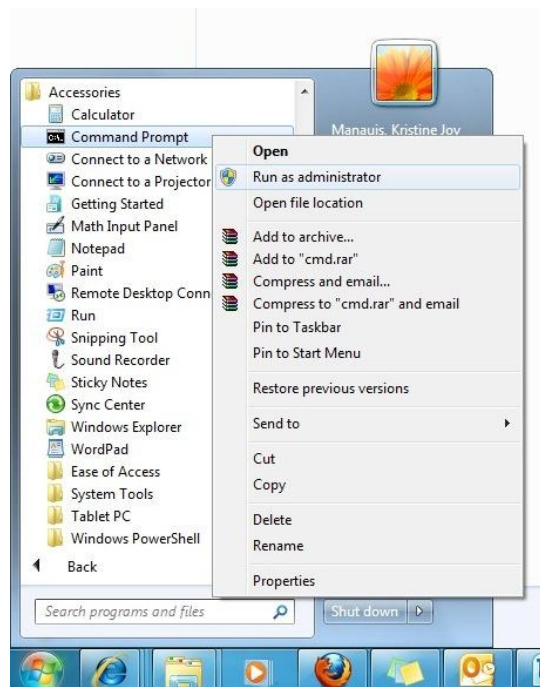
7. We are now ready to extract the **Key file (***phichospitalkey.pem***)** and **Client certificate (***phichospitalcert.pem***)** which will be used by the Proxy Server Application to connect to the Claims Web Service. On the Command Prompt window, go to the folder where the **openssl.exe** resides. In this guideline, the openssl.exe resides on the "**C:\eClaims Web Service\openssl\bin** ".
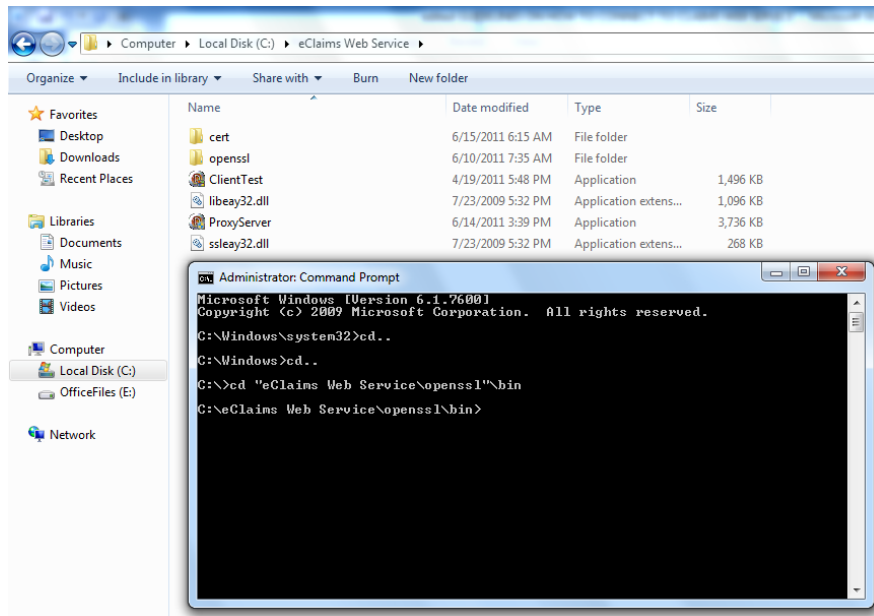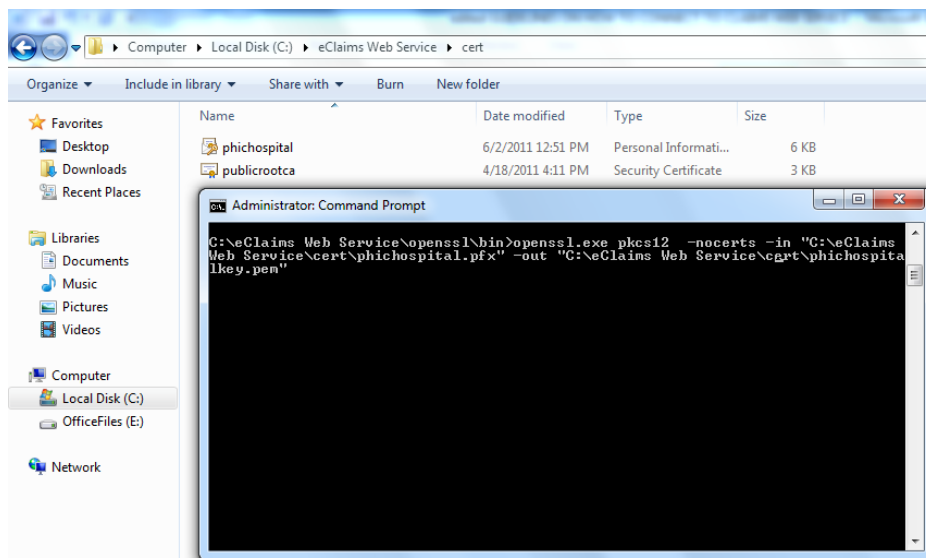

8. To extract the **Key file (***phichospitalkey.pem***)** type the following script into the Command Prompt then press ENTER:

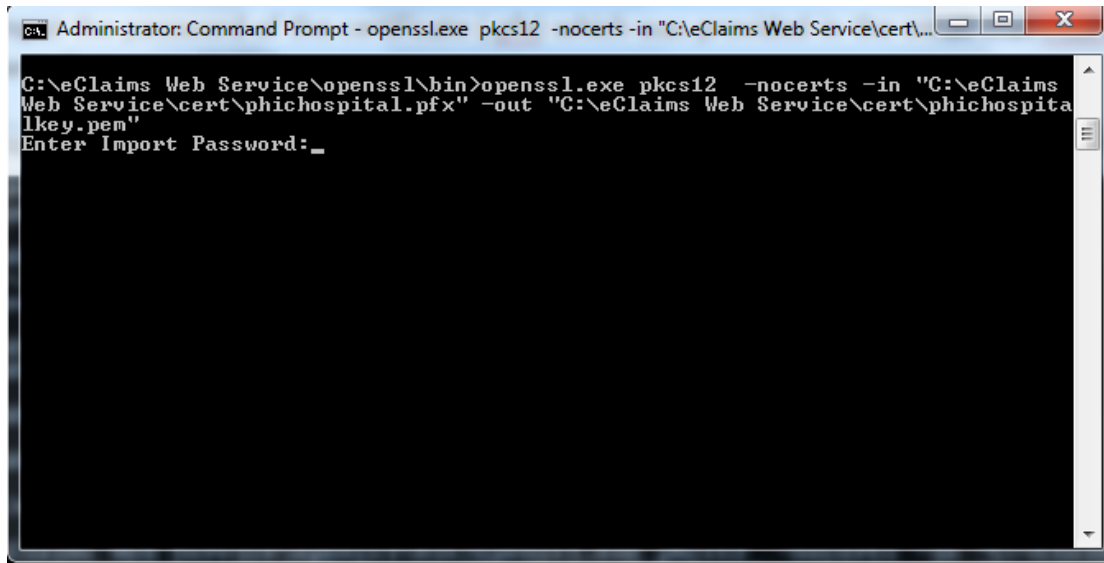> **openssl.exe pkcs12 -nocerts -in "<***path where the .pfx file resides***>\certificate.pfx"-out "<***path where you want to save the .pem file***>\key.pem"**

In this guideline, the script that we will use is:

> *openssl.exe pkcs12 -nocerts -in "C:\eClaims Web Service\cert\phichospital.pfx" -out "C:\eClaims Web Service\cert\phichospitalkey.pem"*
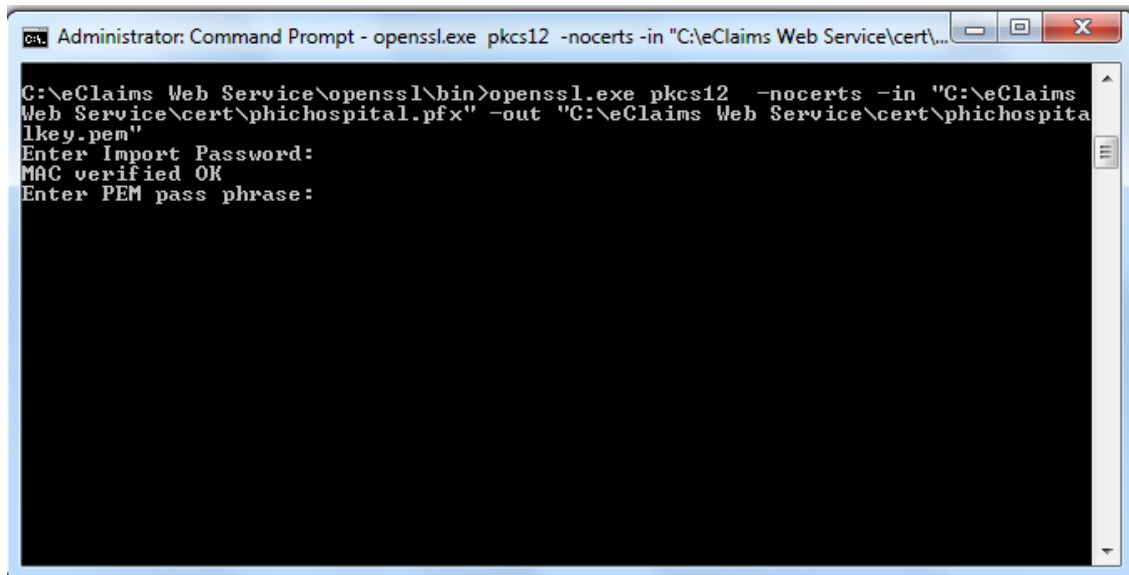
9. Input the password of the certificate (.pfx) which was provided in the email that PhilHealth has sent then press ENTER.
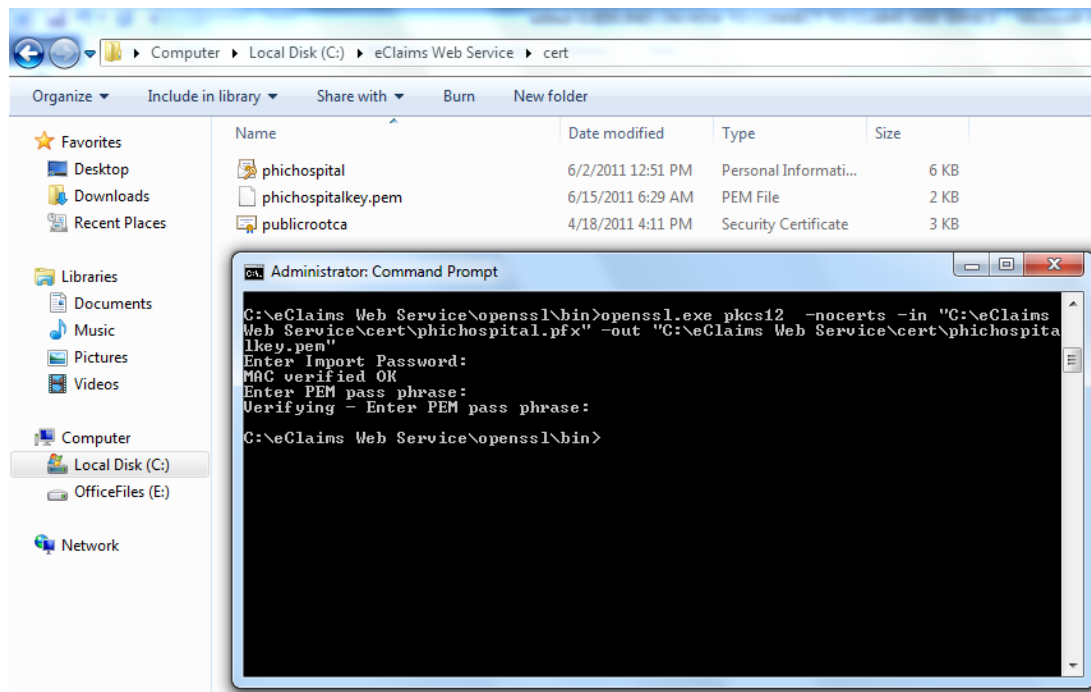

10. If you have entered the password successfully, the command prompt will ask you to provide a "**PEM pass phrase**" for the "Key file". *Please take note of the PEM pass phrase you will input*.

11. After successfully inputting the "PEM pass phrase". A new file (*phichospitalkey.pem*) should be created in the "cert" folder. This is the certificate key file.
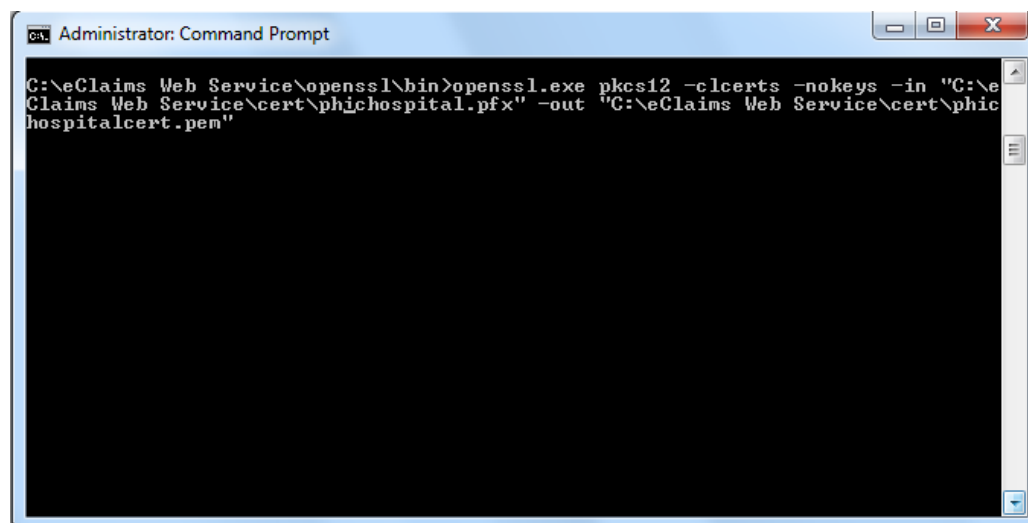

12. To extract the *Client certificate file (phichospitalcert.pem)* type the following script into the Command Prompt then press ENTER:
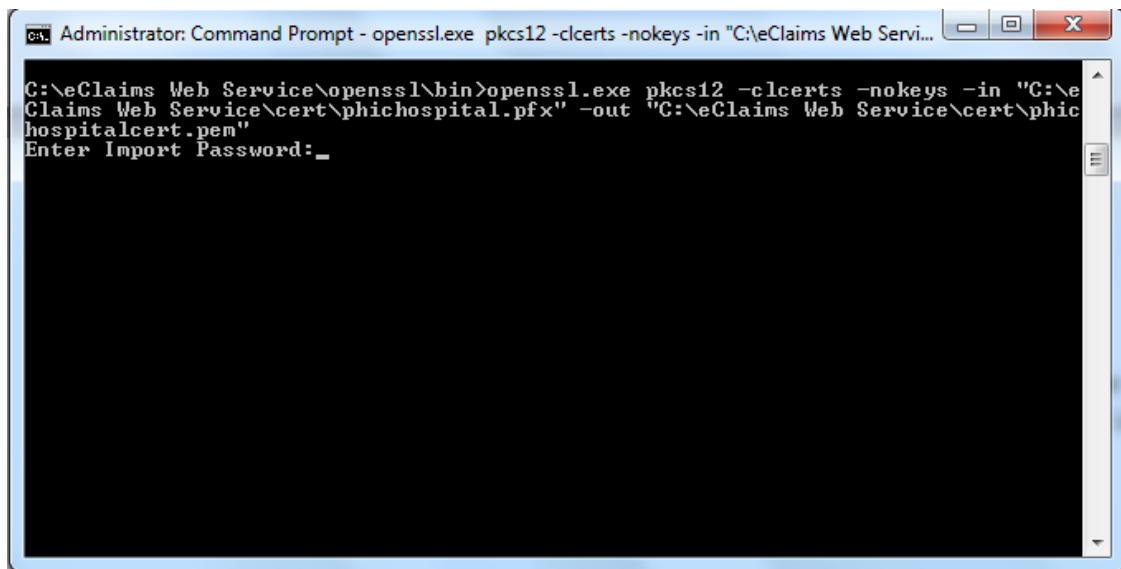
openssl.exe pkcs12 -clcerts -nokeys -in "*<path where the .pfx file resides>*\certificate.pfx" –out"*<path where you want to save the .pem file>*\cert.pem"
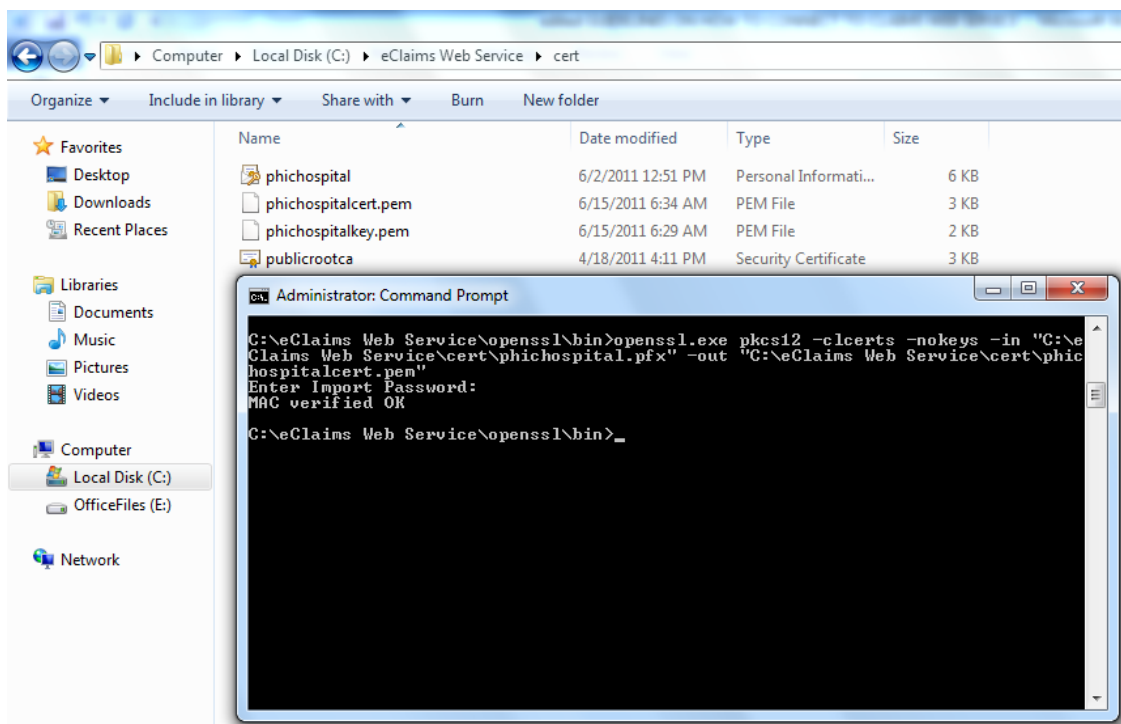
In this guideline, the script that we will use is:

openssl.exe pkcs12 -clcerts -nokeys -in "C:\eClaims Web Service\cert\phichospital.pfx" -out "C:\eClaims Web Service\cert\phichospitalcert.pem"

13. Input the password of the certificate (.pfx) which was provided in the email that PhilHealth has sent then press ENTER. A new file (*phichospitalcert.pem*) should be created in the "cert" folder. This is the certificate file.

14. We have successfully extracted the Key and the Client Certificate which are both in .pem file. We will now use these files together with the Root Certificate to run the Proxy Server Application. But before running, we must set first the compatibility properties of the said application. Right click the "**Proxy Server**" application then click on "**Properties**".
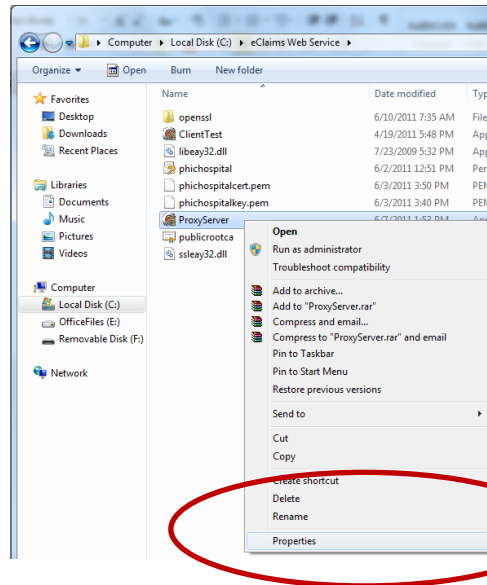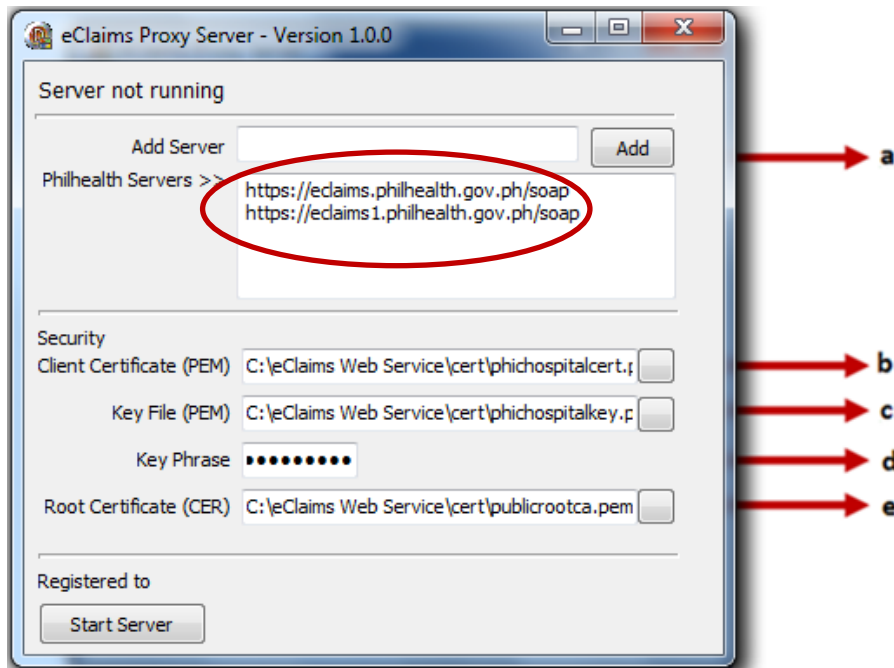

15. The **Proxy Server Properties** window will appear. Click on the "**Compatibility**" tab then check if the "**Run this program in compatibility mode**" is enabled then select "**Windows XP (Service Pack3)**" on the drop down list under the Compatibility mode. Click "**OK**".
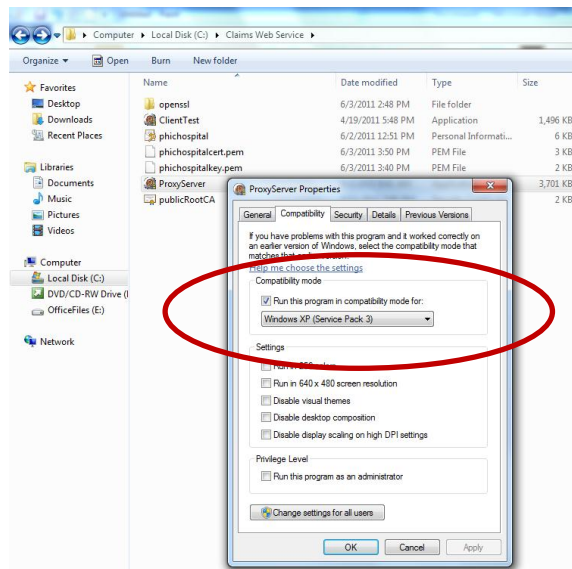
16. Double click "**Proxy Server**" application ⊞ ProxyServer to open.

17. The Proxy Server application will appear. Input the following then click **"Start Server"** button:

a. At the "Add Server" portion, input **https://eclaims1.philhealth.gov.ph/soap** then click "Add", and input **https://eclaims.philhealth.gov.ph/soap** then click "Add" again. The proxy server will load balance on the two sites.

b. Select the "**Client Certificate**" **(.pem)** that you created on Step 11. In this guide, we shall input **"C:\eClaims Web Service\cert\phichospitalcert.pem"**

c. Select the **"Key file" (.pem)** that you created on Step 8. In this guide, we shall input **"C:\eClaims Web Service\cert\phichospitalkey.pem"**

d. Key in the **PEM Pass Phrase** you created on Step 10**.**

e. Select the **Root Certificate**. In This guide, we shall input **"C:\eClaims Web Service\cert\publicRootCA.cer"**
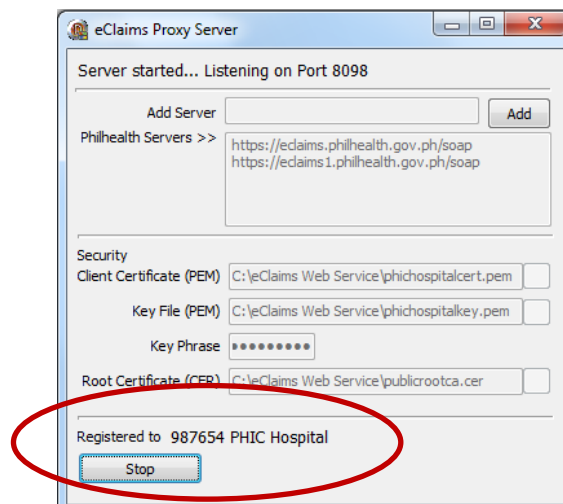
18. To test whether your application is now connected to PhilHealth's Claims Web Service, use the "**Client Test***"* application. But before opening the "Client Test" application, check first the compatibility properties of the application if the compatibility mode is enabled. Kindly do Steps 14 and 15 on the "Client Test" application.
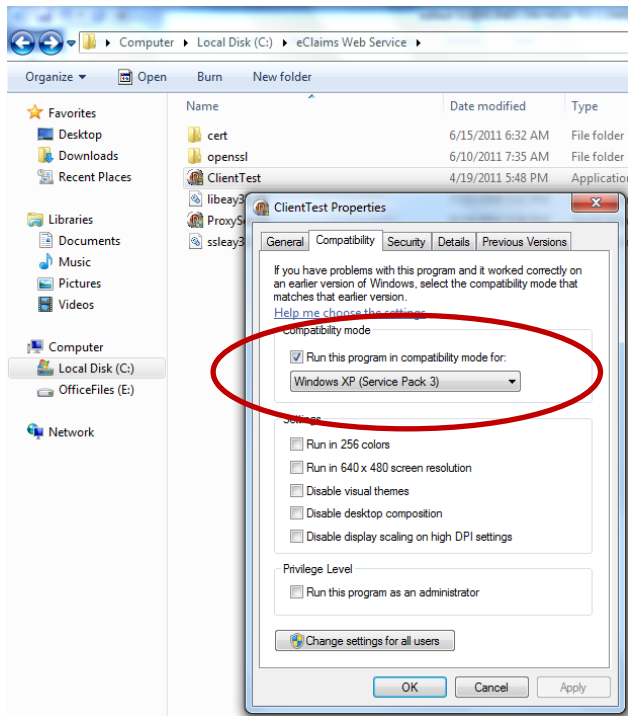
19. Double click on the to open. Then click on the **"Server Date Time"** button. The application should display the correct date and time of the server. If the application has minimize its window, kindly click the maximize window button to see whether the application got the correct date and time of the server.
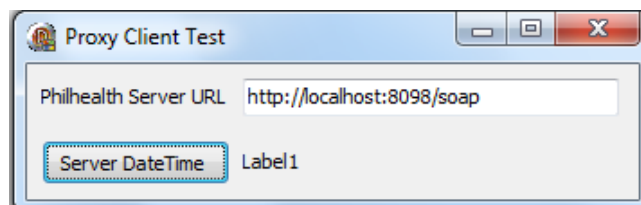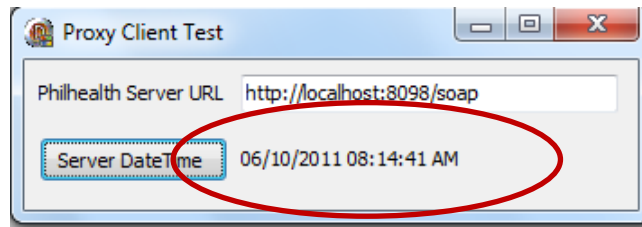
Congratulations! You have successfully connected to the Philhealth Web Service with Digital Certificates using the Philhealth Proxy Server.

20. To use this proxy, point your application or programs to connect to http://locahost:8098/soap (for local clients) or http://<PCNAME>:8098/soap replacing <PCNAME> with the IP address or computer name of the workstation where the proxy runs.

Revocation of the "Certificate" (.pfx):

Certificate revocation may be necessary when, prior to the expiration of a certificate, there has been a compromise in security or the certificate is no longer valid for legal or business reasons.

Certificate revocation begins with the subscriber questioning the validity of a particular certificate. Any number of reasons may exist which would invalidate a certificate for its intended purpose.

The PhilHealth issued certificates may be revoked under the following circumstances:

- The certificate corresponding to the root certificate has been
    - Lost
    - Disclosed without authorization
    - Stolen
    - Compromised in any way
- The subscriber does not meet the obligations of its Non-Disclosure Agreement with PhilHealth, which processed the certificate application.
- There is an improper or faulty issuance of a certificate due to:
    - A prerequisite to the issuance of the certificate not being satisfied;
    - A fact in the certificate is known, or reasonably believed, to be false.
- Any other circumstance that may reasonably be expected to affect the reliability, security, integrity or trustworthiness of the certificate or the cryptographic key pair associated with the certificate.
- The subscriber requests the revocation for any reason whatsoever of its certificate.

Procedure for revocation request:

Revocation shall be requested **PROMPTLY** after detection of a compromise or any other event giving cause for revocation.

A revocation request may be generated in the following ways, in order of preference:

- Electronically by a digitally signed message
- By personal representation to PhilHealth
- By a signed fax message
- Electronically by a non-signed message
- By telephone call to PhilHealth

Those wishing to revoke a certificate may contact:

> **PhilHealth**
> **IT Management Department**
> **Tel: +63 (02) 6376293**
> **Trunkline: +63 (02) 4417444 local: 7604,7606, or 7607**
> **Email: network@philhealth.gov.ph, and/or helpdesk@philhealth.gov.ph**

Please provide the following details:
- **Hospital Name**
- **Accreditation Number**
- **Authorized Contact Person**
- **Email Address**
- **Contact Number**
- **Reasons/circumstances surrounding its revocation.**

PhilHealth may seek independent confirmation, for example, by making a phone call to the subscriber's employer or other sources, prior to initiating the revocation of a certificate.