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 certificateii. 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 <u>https://cws.philhealth.gov.ph/soap</u>
- 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

Compute	er 🕨 Local Disk (C:) 🕨				• +j
Organize 🔻 Share wit	h 🔻 Burn New folder				
☆ Favorites	Name	Date modified	Туре	Size	
🧮 Desktop	INSTALLERS	6/2/2011 12:53 PM	File folder		
〕 Downloads	퉬 PerfLogs	7/14/2009 10:37 AM	File folder		
🕮 Recent Places	퉬 Program Files	6/2/2011 8:09 AM	File folder		
	퉬 TESTING	6/10/2011 7:30 AM	File folder		
🥽 Libraries	퉬 Users	6/4/2011 8:52 AM	File folder		
Documents	J Windows	6/8/2011 8:35 AM	File folder		
🌙 Music	📜 eClaims Web Service	6/10/2011 7:29 AM	WinRAR archive	2,265 KB	
Pictures					
Videos					
🖳 Computer					
🚢 Local Disk (C:)					

2. Extract the .rar file

	* 53	1-1				-	unce tell	in and	Aa
Compute	er 🕨 Local Disk (C	:) 🕨							▼ ⁴ 7
Organize 👻 📜 Open	▼ Burn	Nev	w folder						
🔆 Favorites	Name		*	Date modi	fied	d	Туре	Size	
Nesktop	INSTALLER	S		6/2/2011 1	2:5	3 PM	File folder		
📕 Downloads	🃗 PerfLogs			7/14/2009	10:	37 AM	File folder		
🖳 Recent Places	鷆 Program Fi	les		6/2/2011 8	:09	AM	File folder		
	퉬 Users			6/4/2011 8	:52	AM	File folder		
词 Libraries	퉬 Windows			6/8/2011 8	:35	AM	File folder		
Documents	📜 eClaims V		Open		2	9 AM	WinRAR archive	2,265 KB	
J Music	鷆 TESTING	•	Extract files		2	9 AM	File folder		
Pictures			Extract Here						
📑 Videos		1	Extract to eClaims Web Ser	vice\					
			Open with						
🖳 Computer			Restore previous versions						
🚢 Local Disk (C:)					-1				
OfficeFiles (E:)			Send to	•	1				
🚗 Removable Disk (F:)			Cut						
			Сору						
📬 Network					-1				
			Create shortcut						
			Delete						
			Rename						
			Properties		1				
	Ц,	_							

3. Input the password provided in the email that was sent by PhilHealth then click "OK".

Enter password	
Enter password for the encrypted file Claims Web Service\Claims Web Service\ClientTest.exe in archive Claims Web Service.rar	
Enter password	
······	
Show password	
Use for all archives	
Organize passwords	
OK Cancel Help	

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



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*.

Compute	r ► Local Disk (C:) ► eClaims We	b Service 🕨		_
Organize 🔻 🛛 Include in	library	urn New folder		
🔆 Favorites	Name	Date modified	Туре	Size
🧮 Desktop	퉬 cert	6/15/2011 6:15 AM	File folder	
🗼 Downloads	퉬 openssl	6/10/2011 7:35 AM	File folder	
🔠 Recent Places	虪 ClientTest	4/19/2011 5:48 PM	Application	1,496 KB
	🚳 libeay32.dll	7/23/2009 5:32 PM	Application extens	1,096 KB
🥽 Libraries	@ ProxyServer	6/14/2011 3:39 PM	Application	3,736 KB
Documents	🚳 ssleay32.dll	7/23/2009 5:32 PM	Application extens	268 KB
🁌 Music				
Pictures				
Videos 🗧				
👰 Computer				
🚢 Local Disk (C:)				

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". <u>Please take note of the PEM</u> pass phrase you will input.

🏧 Administrator: Command Prompt - openssl.exe pkcs12 -nocerts -in "C:\eClaims Web Service\cert\... 📼 💷 🗮 🌉 C:\eClaims Web Service\openssl\bin>openssl.exe pkcs12 -nocerts -in "C:\eClaims Web Service\cert\phichospital.pfx" -out "C:\eClaims Web Service\cert\phichospita lkey.pem" Enter Import Password: MAC verified OK Enter PEM pass phrase: Ξ

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.



Organize ▼ Include ir	er ► Local Disk (C:) ► eClaims Web So n library ▼ Share with ▼ Burn	ervice 🕨 cert New folder			
🔶 Favorites	Name	Date modified	Туре	Size	
E Desktop	phichospital	6/2/2011 12:51 PM	Personal Informati	6 KB	
🗼 Downloads	phichospitalcert.pem	6/15/2011 6:34 AM	PEM File	3 KB	
🖳 Recent Places	phichospitalkey.pem	6/15/2011 6:29 AM	PEM File	2 KB	
	📮 publicrootca	4/18/2011 4:11 PM	Security Certificate	3 KB	
 Music Pictures Videos Computer Local Disk (C:) OfficeFiles (E:) Network 	C:\eClaims Web Service Claims Web Service\cert hospitalcert.pem" Enter Import Password: MAC verified OK C:\eClaims Web Service\	openssl\bin>openssl.exe \phichospital.pfx" -out	₽ pkcs12 -clcert ''C:\eClaims ₩e	:s —nokeys —ir b Service∖ce;	n "C:∖e *t∖phic

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*".

Organize 👻 🖬 Open	Burn New f	older			
☆ Favorites	Name	^		Date modified	Туре
E Desktop	openssl			6/10/2011 7:35 AM	File fo
🐌 Downloads	ClientTest			4/19/2011 5:48 PM	Appli
🔚 Recent Places	🚳 libeay32.dll			7/23/2009 5:32 PM	Appli
	l phichospital			6/2/2011 12:51 PM	Perso
🧊 Libraries	phichospitalce	rt.pen	1	6/3/2011 3:50 PM	PEM
Documents	phichospitalke	y.pem		6/3/2011 3:40 PM	PEMI
👌 Music	ProxyServer			6/7/2011 1.52 DM	Anni
Pictures	🔄 publicrootca	-	Open		r
😸 Videos	🗟 ssleay32.dll		Run as administrator		- i
			I roubleshoot compat	ibility	
Normal Computer			Add to archive		
🏭 Local Disk (C:)			Add to "ProxyServer.ra	ır"	
OfficeFiles (E:)		2	Compress and email		
👝 Removable Disk (F:)			Compress to "ProxySe	rver.rar" and email	
•			Pin to Taskbar		
Network			Pin to start ivienu		
			Restore previous version	ons	
			Send to		- +
			Cut		
			Сору		
					_
			Delete		
			Pename		
			Nellanne		

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:

🙀 eClaims Proxy Serve	er - Version 1.0.0	
Server not running		
Add Server	Add	a a
Philhealth Servers >	https://edaims.philhealth.gov.ph/soap https://edaims1.philhealth.gov.ph/soap	
Security		
Client Certificate (PEM)	C:\eClaims Web Service\cert\phichospitalcert.	→ b
Key File (PEM)	C:\eClaims Web Service\cert\phichospitalkey.p	c
Key Phrase	•••••	→ d
Root Certificate (CER)	C:\eClaims Web Service\cert\publicrootca.pem	e e
Paristand In		
Start Server		

- a. At the "Add Server" portion, input <u>https://eclaims1.philhealth.gov.ph/soap</u> then click "Add", and input <u>https://eclaims.philhealth.gov.ph/soap</u> 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"

Server started List	tening on Port 8098
Add Server Philhealth Servers >>	Ad https://edaims.philhealth.gov.ph/soap https://edaims1.philhealth.gov.ph/soap
Security	
Client Certificate (PEM)	C:\eClaims Web Service\phichospitalcert.pem
Key File (PEM)	C:\eClaims Web Service\phichospitalkey.pem
Kev Phrase	

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 ^{ClientTest} 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.

M Proxy Client Test	
Philhealth Server URL	http://localhost:8098/soap
Server DateTime	Label 1

Rroxy Client Test	
Philhealth Server URL	http://localhost:8098/soap
Server DateTme	06/10/2011 08:14:41 AM

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://epcname.icsabe 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 **<u>PROMPTLY</u>** 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: <u>network@philhealth.gov.ph</u>, and/or <u>helpdesk@philhealth.gov.ph</u>

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.