Configuring SSL

And

Certificate Authority for Client Side Certificates

Version 2.0

By ViCarePlus Team

VICARE+

EMR/EHR Customization Redefined

Prepared by

ViSolve Inc.,

Contact: 408.666.4320

EMail: vicareplus_support@visolve.com

www.vicareplus.com

2nd February 2010

Revision History

Version	Date	Author	Reviewed By
1.0	12/16/09	ViCarePlus Team	Team
2.0	02/02/10	ViCarePlus Team	Team

Table of Contents

Configuring SSL and Certificate Authority for Client Side Certificates

1. Prerequisite

1.1 OpenSSl:

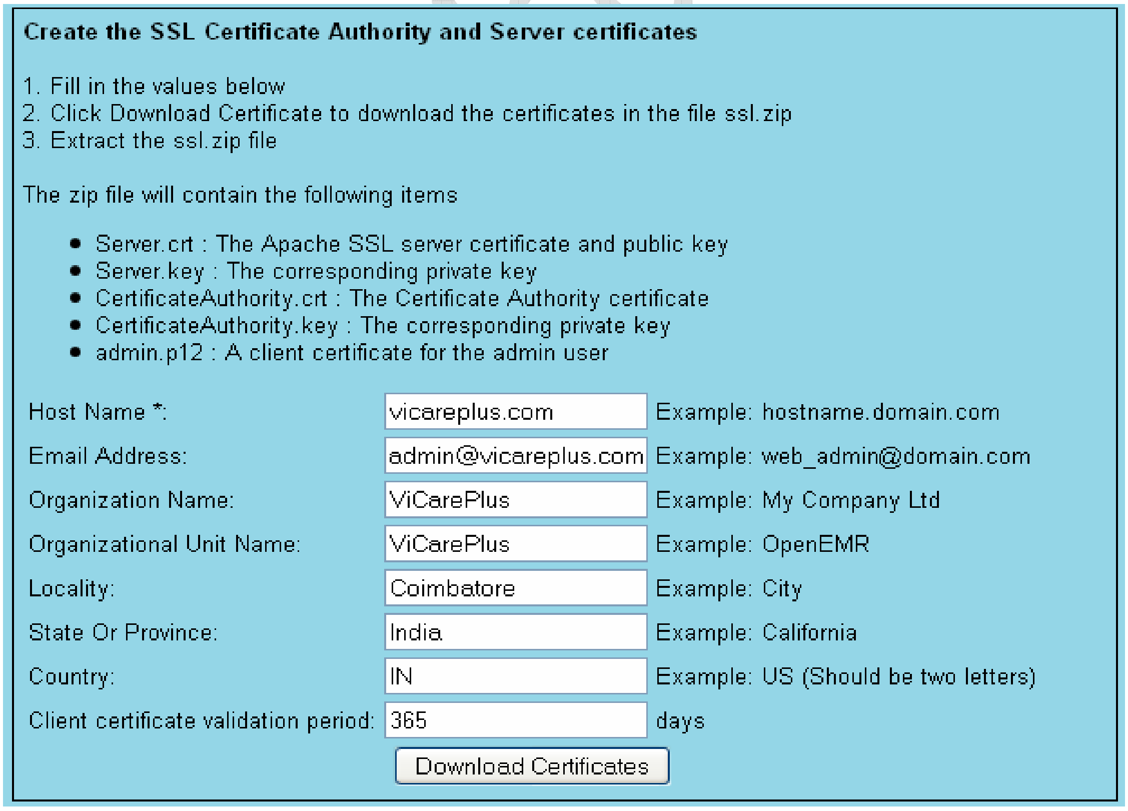
Make sure OpenSSl is installed in your machine. If not, download the package and install it. http://www.openssl.org/source/openssl-0.9.8l.tar.gz

2. Creation of SSL Server and CA Certificates.

Visit screen administration -> other ->certificate

Step 1. Fill the following details and click the “Download Certificate” button

- Host Name
- Email Address
- Organization Name
- Organizational Unit Name
- Locality
- State or Province
- Country



Create the SSL Certificate Authority and Server certificates

1. Fill in the values below
2. Click Download Certificate to download the certificates in the file ssl.zip
3. Extract the ssl.zip file

The zip file will contain the following items

- Server.crt : The Apache SSL server certificate and public key
- Server.key : The corresponding private key
- CertificateAuthority.crt : The Certificate Authority certificate
- CertificateAuthority.key : The corresponding private key
- admin.p12 : A client certificate for the admin user

Host Name *:	vicareplus.com	Example: hostname.domain.com
Email Address:	admin@vicareplus.com	Example: web_admin@domain.com
Organization Name:	ViCarePlus	Example: My Company Ltd
Organizational Unit Name:	ViCarePlus	Example: OpenEMR
Locality:	Coimbatore	Example: City
State Or Province:	India	Example: California
Country:	IN	Example: US (Should be two letters)
Client certificate validation period:	365	days

Note: Once the "Download Certificate" is clicked, the certificates are zipped and available as "ssl.zip" for download

Step 2. Extract the "ssl.zip" file. Do make sure it contains following five files.

1. Server.crt
2. Server.key
3. CertificateAuthority.crt
4. CertificateAuthority.key
5. admin.p12

Move the ssl.zip folder to the machine where openemr is installed. Unzip "ssl.zip"

Step 3. Create a new folder named "ssl" inside the Apache installation directory (say /etc/apache2)

Step 4. Copy the certificates Server.key, Server.crt, CertificateAuthority.crt, CertificateAuthority.key to the newly created "ssl" folder.

Step 4. To Configure Apache to use HTTPS, Add the new certificates to the Apache configuration file

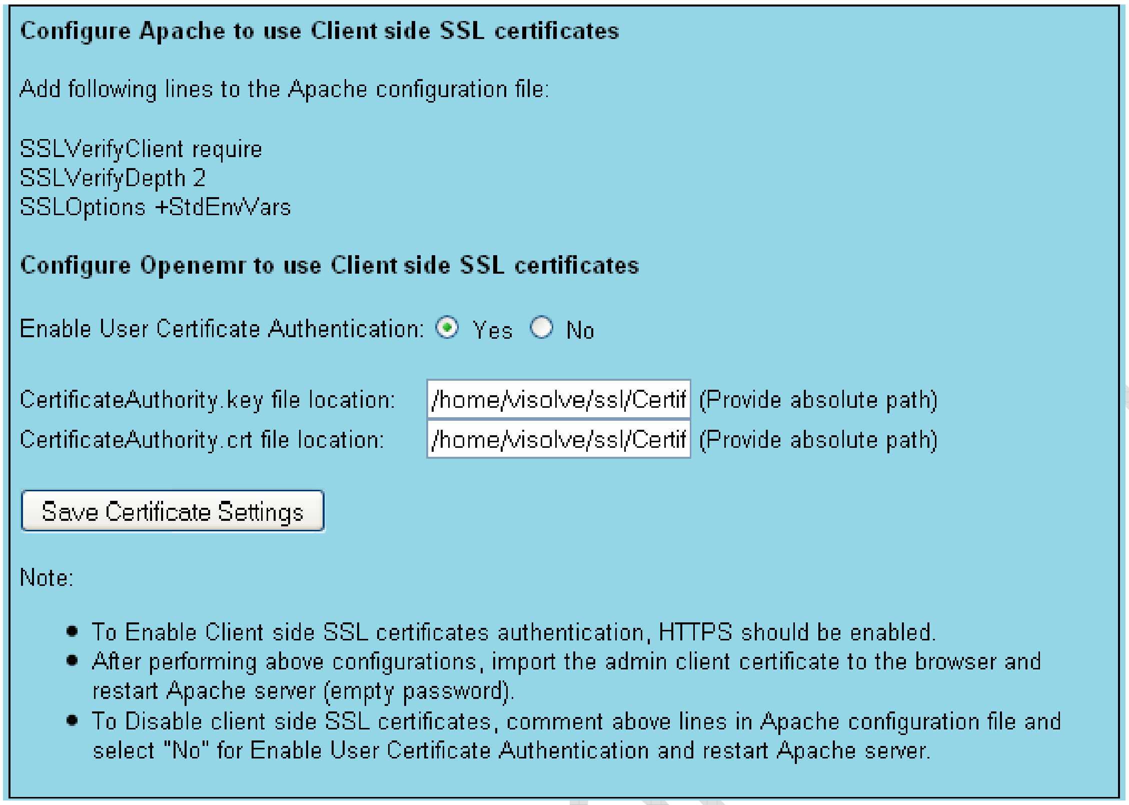
```
SSLEngine on
SSLCertificateFile /path/to/server.crt
SSLCertificateKeyFile /path/to/server.key
SSLCACertificateFile  /path/to/CertificateAuthority.crt
```

Note:

- To Enable only HTTPS, perform the above changes and restart Apache server. If you want to configure client side certificates also, please configure them in the next section.
- To Disable HTTPS, comment the above lines in Apache configuration file and restart Apache server.

Step 5. To Configure Apache to use Client side SSL certificates, Add following lines to the Apache configuration file:

```
SSLVerifyClient require
SSLVerifyDepth 2
SSLOptions +StdEnvVars
```



Configure Apache to use Client side SSL certificates

Add following lines to the Apache configuration file:

```
SSLVerifyClient require
SSLVerifyDepth 2
SSLOptions +StdEnvVars
```

Configure Openemr to use Client side SSL certificates

Enable User Certificate Authentication: ● Yes ○ No

CertificateAuthority.key file location: /home/visolve/ssl/Certif (Provide absolute path)

CertificateAuthority.crt file location: /home/visolve/ssl/Certif (Provide absolute path)

Note:

- To Enable Client side SSL certificates authentication, HTTPS should be enabled.
- After performing above configurations, import the admin client certificate to the browser and restart Apache server (empty password).
- To Disable client side SSL certificates, comment above lines in Apache configuration file and select "No" for Enable User Certificate Authentication and restart Apache server.

Step 6. Fill the absolute paths for the Certificate Authority Key and Certificate files

CertificateAuthority.key file location – Fill full the path of the CertificateAuthority.key location.

In case if it is located in /etc/apache2/ssl/CertificateAuthority.key, fill the path as "/etc/apache2/ssl/CertificateAuthority.key"

CertificateAuthority.crt file location – Fill full the path of the CertificateAuthority.crt location.

In case if it is located in /etc/apache2/ssl/CertificateAuthority.key, fill the path as "/etc/apache2/ssl/CertificateAuthority.crt"

Note:

- To Enable Client side SSL certificates authentication, HTTPS should be enabled.
- After performing above configurations, import the admin client certificate to the browser (empty password) and restart Apache server
- To Disable client side SSL certificates, comment above lines in Apache configuration file and select "No" for Enable User Certificate Authentication [and click 'Save Certificates Settings'] and restart Apache server.

3. Apache – SSL Configurations.

Locate the apache configuration file and edit the VirtualHost part belongs to OpenEMR. The items listed in bold need to be added in apache configurations for SSL.

```
<VirtualHost *:<port>>
DocumentRoot ……………………
….
…
#Configuration needs for https
SSLEngine on
SSLCertificateFile /path/to/server.crt
SSLCertificateKeyFile /path/to/server.key
SSLCACertificateFile  /path/to/CertificateAuthority.crt

#Configuration needs for client side certificates
SSLVerifyClient require
SSLVerifyDepth 10
SSLOptions +StdEnvVars
…
…
</VirtualHost>
```

Optional – Enforce apache to use only https for openemr.

```
# To enforce https

    DocumentRoot "/var/www/html/example/"

    <Directory "/var/www/html/openemr/">
    #The following rewrite just forces everything to https!!!
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
    </Directory>

</VirtualHost>
```

After performing the changes, restart the apache server so that changes can take effect.

```
/etc/init.d/httpd restart
```

In some other cases command will be /etc/init.d/apache2 restart

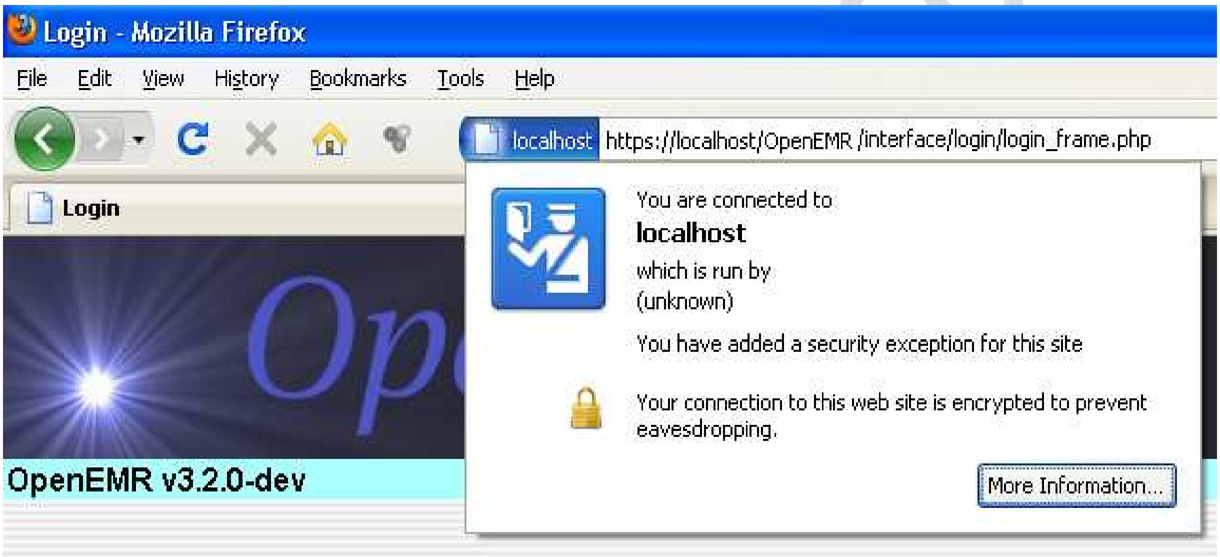
4. Testing:

4.1 Testing Server Certificate Installation.

1. Open web browser (Ex: Mozilla Firefox)

2. Type https://localhost/openemr
(Add security exception of self signed certificate)

In this screenshot you can notice lock icon with comment as "*Your connection to this website is encrypted to prevent eavesdropping*"*;* this ensures that the communication is secured by SSL.



https://localhost/OpenEMR /interface/login/login_frame.php

You are connected to
localhost
which is run by
(unknown)

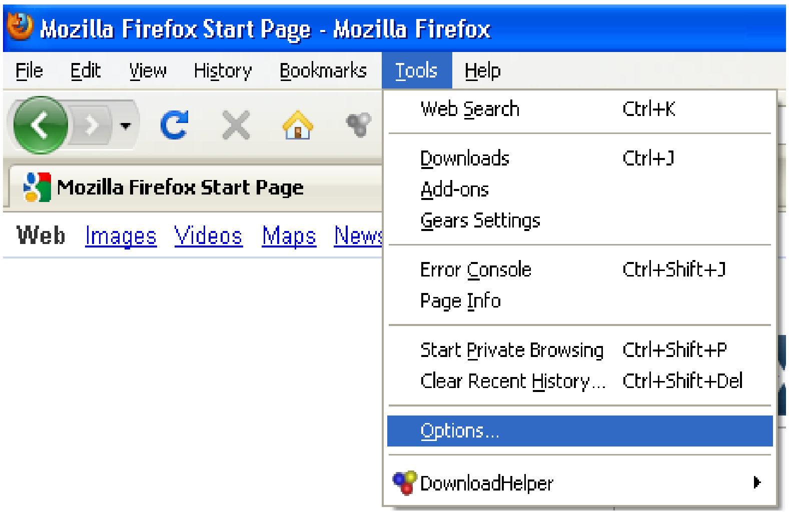
You have added a security exception for this site

Your connection to this web site is encrypted to prevent eavesdropping.

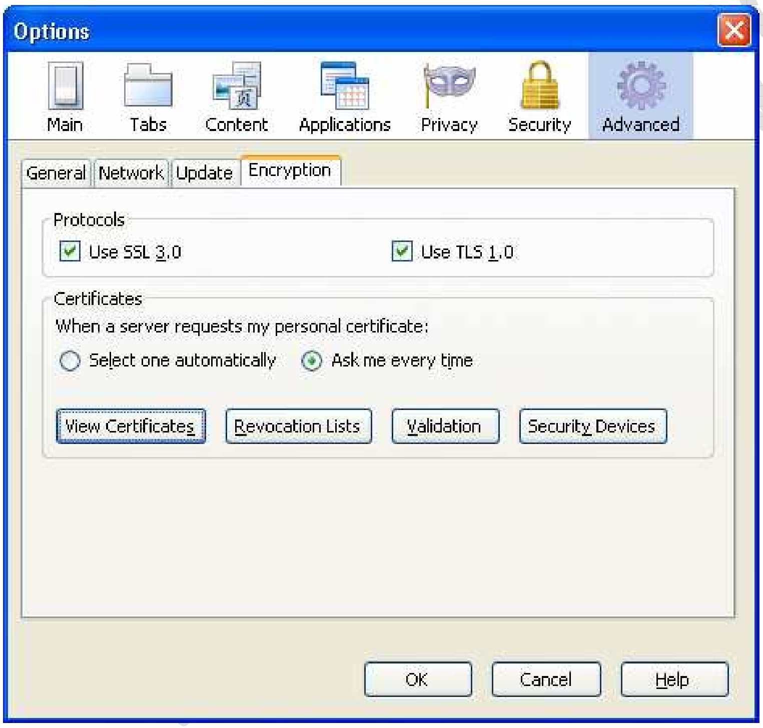
4.2 Exporting Client certificate to the web browser.

Open web Browser (Ex: Mozilla Firefox)

Step 1.
(Windows) Select ***Tools*** in Menu, select ***Options...***.
(Linux) Select ***Edit*** in Menu, select ***Preferences...***.


Mozilla Firefox Start Page - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Mozilla Firefox Start Page
Web
Images
Videos
Maps
News
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Gears Settings
Error Console Ctrl+Shift+J
Page Info
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Options...
DownloadHelper

Step2. In '**Options**' window select '**Advanced'** tab then select '**Encryption**' Tab. Click '***View Certificates'***.



Protocols

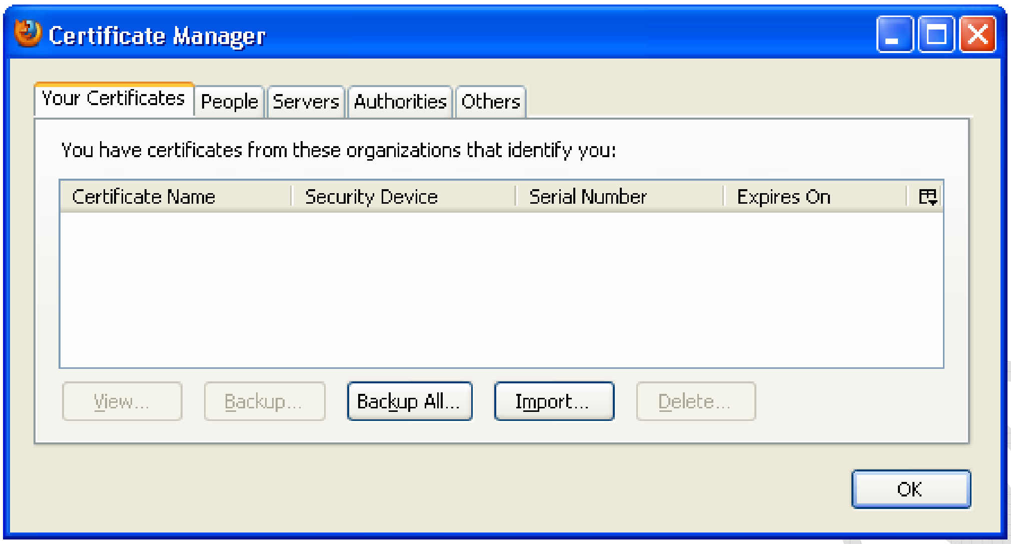
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

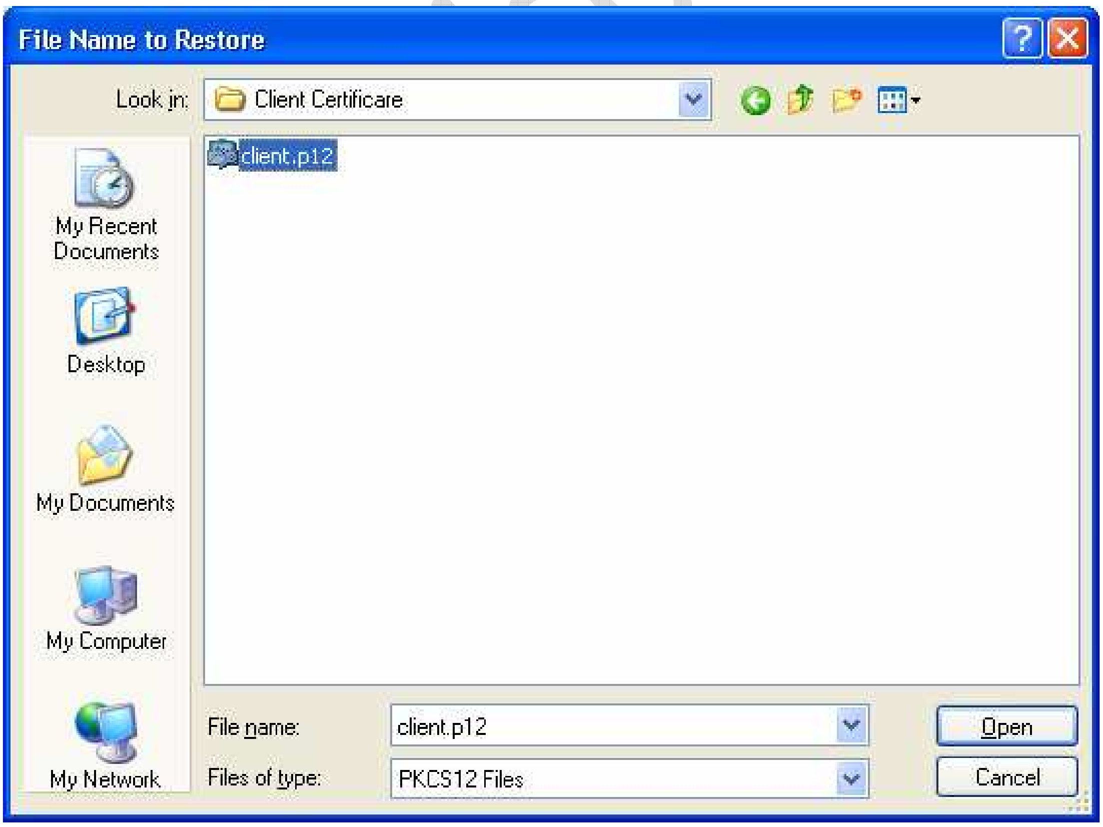
○ Select one automatically ● Ask me every time

Step 3: Certificate manager window will be displayed; here you should select '***Your Certificates'*** *tab* and click ***Import…*** button



You have certificates from these organizations that identify you:

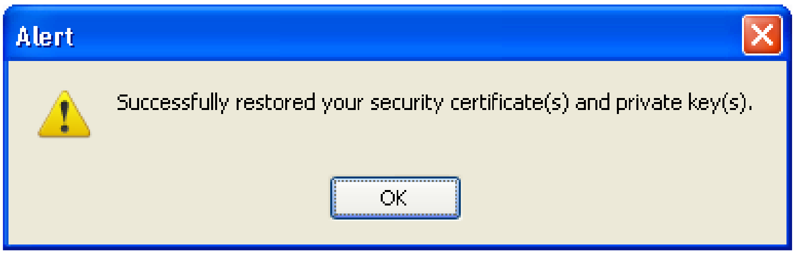
Step 4: It will bring the open dialog. Select the client.p12 file and click open. Then give your password and click ok. This will import your certificate to the browser.



Look in: Client Certificare

File name: client.p12

Files of type: PKCS12 Files



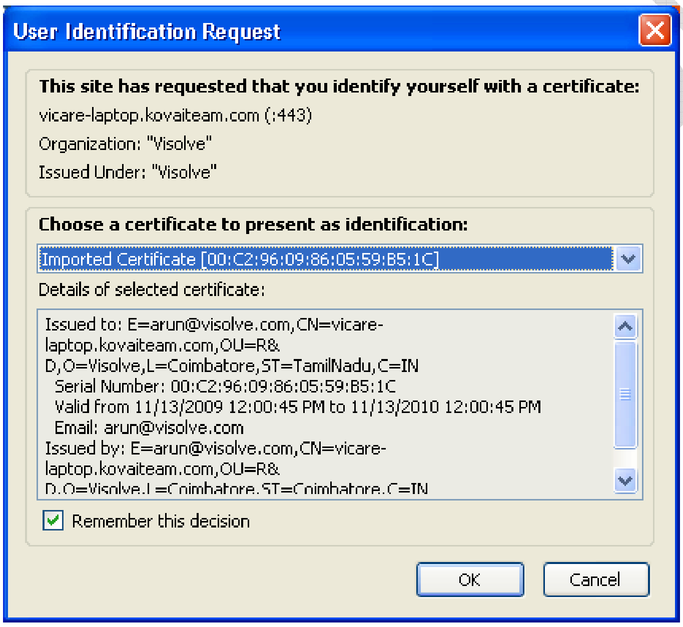
Successfully restored your security certificate(s) and private key(s).

Step 5: Click ok to close the option window. Now the certificate is imported to the browser.

4.3 OpenEMR with client side certificate validation.

Type https://localhost/openemr

Browser (Ex. Mozilla Firefox) will list the installed certificates. Choose the appropriate certificate and select ok



This site has requested that you identify yourself with a certificate:

vicare-laptop.kovaiteam.com (:443)

Organization: "Visolve"

Issued Under: "Visolve"

Choose a certificate to present as identification:

Imported Certificate [00:C2:96:09:86:05:59:B5:1C]

Details of selected certificate:

Issued to: E=arun@visolve.com,CN=vicare-laptop.kovaiteam.com,OU=R&D,O=Visolve,L=Coimbatore,ST=TamilNadu,C=IN
  Serial Number: 00:C2:96:09:86:05:59:B5:1C
  Valid from 11/13/2009 12:00:45 PM to 11/13/2010 12:00:45 PM
  Email: arun@visolve.com
Issued by: E=arun@visolve.com,CN=vicare-laptop.kovaiteam.com,OU=R&D,O=Visolve,L=Coimbatore,ST=Coimbatore,C=IN

☑ Remember this decision

Your Username will be fetched automatically from the provided certificate.

Enjoy playing with OpenEMR!!