**QA Plan for** 

# **Transmission Security**

## And

## **Client Side Certificate**

Version 2.0

By ViCarePlus Team

Prepared by



ViSolve Inc.,

Contact: 408.666.4320

EMail: vicareplus\_engg@visolve.com

www.visolve.com

February 17, 2010

#### **Revision History**

Version	Date	Author	Reviewed By
1.0	12/16/09	ViCarePlus Team	Team
2.0	02/17/10	ViCarePlus Team	Team

## **Table of Contents**

I. SSL implementation	.4
II. Client side certificate validation Enabled.	.5
III. Client Side Certificate validation Disabled	7

## I. SSL implementation

1. Follow the instructions in Administration -> Other -> Certificates to configure Apache to use HTTPS

2. After enabling HTTPS please type <a href="https://localhost/openemr">https://localhost/openemr</a> (Add security exception of self signed certificate)

Even the user try to access the application (say <u>http://localhost/openemr</u>) via http, it automatically redirects to the https. Application it self enforce to use https.

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.



**Failed Scenario**: If the server is not configured properly with https then it shows the following information.



### II. Client side certificate validation Enabled.

- 1. Follow the instructions in Administration -> Other -> Certificates to configure Apache and Openemr to enable client side SSL certificates.
- 2. In Administration -> Other -> Certificates, Create a client side SSL certificate for the user or host name, download the certificate and import to the browser.
- 3. Type <a href="https://localhost/openemr">https://localhost/openemr</a>

Browser will list the installed certificates. Choose the appropriate certificate and select 'ok'.

ser Identification Request	Þ
This site has requested that you identify yourself with a certifica	ite:
vicare-laptop.kovaiteam.com (:443)	
Organization: "Visolve"	
Issued Under: "Visolve"	
Choose a certificate to present as identification:	
Imported Certificate [00:C2:96:09:86:05:59:85:1C]	*
Details of selected certificate:	
Issued to: E======       E====         laptop.kovaiteam.com,OU=R&       D,O==Visolve,L===         D,O==Visolve,L==       E===         Serial Number: 00:C2:96:09:86:05:59:85:1C         Valid from 11/13/2009 12:00:45 PM to 11/13/2010 12:00:45 PM         Email: ===:@visolve.com         Issued by: E====@visolve.com         Issued by: E====@visolve.com, CN=vicare-laptop.k===:m=m=wisolve.com, CN=vicare-laptop.k==:m=m=wisolve.com, CN=vicare-laptop.k==:m=m=wisolve.com, ST========:C=IN	
Remember this decision	
OK Cance	el

4. Provide user name and password and enjoy playing with Openemr.



**Failed Scenario**: If the client validation failed or the Certificate is not present, it will display the following error.

5	Secure Connection Failed
Þ	An error occurred during a connection to vicare-laptop.kovaiteam.com.
9	SSL peer was unable to negotiate an acceptable set of security parameters.
(	(Error code: ssl_error_handshake_failure_alert)
	<ul> <li>The page you are trying to view can not be shown because the authenticity of the received data could not be verified.</li> </ul>
	<ul> <li>Please contact the web site owners to inform them of this problem.</li> <li>Alternatively, use the command found in the help menu to report this broken site.</li> </ul>
ſ	Try Again

### III. Client Side Certificate validation Disabled.

When Client certificate authentication is disabled by following instructions in Administration -> Other -> Certificates

Test

1. Type <u>https://localhost/openemr</u> hit enter, it should not ask for any client certificate.