Stunnel Implementation Guide

Public Health Information Network Messaging System (PHINMS)

Version 1.1

Prepared by:
U.S. Department of Health & Human Services

September 20, 2006
EXECUTIVE SUMMARY

Public health involves many organizations throughout the PHIN (Public Health Information Network), working together to protect and advance the public’s health. These organizations need to use the internet to securely exchange sensitive data between varieties of different public health information systems. The exchange of data, also known as “messaging” is enabled through messages created using special file formats and a standard vocabulary. The exchange uses a common approach to security and encryption, methods for dealing with a variety of firewall, and internet protection schemes. The system provides a standard way for addressing and routing content, a standard and consistent way for information systems to confirm an exchange.

The PHINMS (Public Health Information Network Messaging System) is the software which makes this work. The system securely sends and receives sensitive data over the internet to the public health information systems.

The following document provides instructions for installing and configuring Stunnel to secure and encrypt the route between the IIS Server/Jakarta Internet Server Application Programming Interface (ISAPI) redirect connector and the PHINMS Receiver/Tomcat server.
<table>
<thead>
<tr>
<th>VERSION #</th>
<th>IMPLEMENTER</th>
<th>DATE</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Lawrence Loftley</td>
<td>Aug 11, 2006</td>
<td>Create S-Tunnel Implementation Guide.</td>
</tr>
<tr>
<td>1.0</td>
<td>Wendy Fama</td>
<td>Aug 11, 2006</td>
<td>Update S-Tunnel Implementation Guide.</td>
</tr>
<tr>
<td>1.1</td>
<td>Wendy Fama</td>
<td>Sep 6, 2006</td>
<td>Add One to One Mapping.</td>
</tr>
<tr>
<td>1.1</td>
<td>Wendy Fama</td>
<td>Sep 19, 2006</td>
<td>Add Architecture section.</td>
</tr>
<tr>
<td>1.1</td>
<td>Wendy Fama</td>
<td>Sep 20, 2006</td>
<td>Update based on training feedback.</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1.0 Introduction ............................................................................................................... 8  
1.1 Architecture ........................................................................................................... 8  
1.2 Stunnel .................................................................................................................. 9  
1.3 Communiqués ....................................................................................................... 9  

2.0 Stunnel Configuration ............................................................................................. 10  
2.1 Install Stunnel .................................................................................................... 10  
2.2 Configure IIS Server .......................................................................................... 12  
2.3 Configure PHINMS Receiver Service Mode ..................................................... 13  

3.0 Jakarta ...................................................................................................................... 15  
3.1 Pre-Jakarta Install ............................................................................................. 15  
3.2 Install Jakarta .................................................................................................... 16  
3.3 Configure Jakarta .............................................................................................. 19  
3.4 Test Jakarta IIS Filter ....................................................................................... 28  

4.0 Configure One to One Mapping ............................................................................. 30  
4.1 Create Account ................................................................................................. 30  
4.2 Configure Jakarta Isapi ..................................................................................... 35  
4.3 Test One to One Mapping ............................................................................... 48  

5.0 Secure Socket Layers ............................................................................................. 51  
5.1 Download Openssl ............................................................................................ 51  
5.2 Create Self-Signed Certificates ......................................................................... 53  
5.3 Configure Servers .............................................................................................. 55
LIST OF FIGURES

Figure 1.1. Stunnel Architecture Diagram ................................................................. 9
Figure 2.1. Stunnel-4.15-installer.exe ........................................................................ 10
Figure 2.2. Stunnel Security Warning ........................................................................ 10
Figure 2.3. Stunnel License Agreement ..................................................................... 11
Figure 2.4. Stunnel Installation Options ..................................................................... 11
Figure 2.5. Stunnel Installation Folder ....................................................................... 12
Figure 2.6. Stunnel Installation Complete ................................................................. 12
Figure 2.7. IIS Server Configuration ......................................................................... 13
Figure 2.8. PHINMS Receiver Service Mode Configuration ...................................... 14
Figure 3.1. server.xml File ..................................................................................... 15
Figure 3.2. server.xml Notepad .............................................................................. 15
Figure 3.3. isapi_redirect.msi ................................................................................ 16
Figure 3.4. File Download ..................................................................................... 16
Figure 3.5. Jakarta ISAPI Redirector ....................................................................... 17
Figure 3.6. License Agreement ............................................................................... 17
Figure 3.7. Destination Folder ............................................................................... 18
Figure 3.8. Install the Program ............................................................................... 18
Figure 3.9. Install Complete ................................................................................... 19
Figure 3.10. Jakarta Program Files .......................................................................... 19
Figure 3.11. Open File ......................................................................................... 20
Figure 3.12. Open With ......................................................................................... 20
Figure 3.13. urirworkermap.properties Notepad ...................................................... 21
Figure 3.14. Jakarta Program Files .......................................................................... 21
Figure 3.15. Open File ......................................................................................... 21
Figure 3.17. Open With ......................................................................................... 22
Figure 3.18. workers.properties.minimal Notepad ............................................... 22
Figure 3.19. Administrative Tools .......................................................................... 23
Figure 3.20. IIS Manager ....................................................................................... 23
Figure 3.21. New Web Service Extension .............................................................. 24
Figure 3.22. Add File ............................................................................................ 24
Figure 3.23. Internet Information Services ............................................................. 25
Figure 3.24. Default Web Site ............................................................................... 25
Figure 3.25. Default Web Site Properties ............................................................... 26
Figure 3.26. Add/Edit Filter Properties .................................................................. 26
Figure 3.27. Directory Security ............................................................................. 27
Figure 3.28. Secure Communications ..................................................................... 27
Figure 3.29. Administrative Tools .......................................................................... 28
Figure 3.30. Security Alert .................................................................................... 28
Figure 3.31. PHINMS Receiver Notification ........................................................... 29
Figure 4.1. Jakarta Bin Folder ............................................................................... 30
Figure 4.2. Bin Properties ..................................................................................... 31
Figure 4.3. Advanced Security Setting for Bin ....................................................... 31
Figure 4.4. isapi_redirect.dll .............................................................................. 32
Figure 4.5. isapi_redirect.dll Properties ................................................................. 33
Figure 4.6. Select Users, Computers, or Groups .................................................... 33
### ACRONYM LIST

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDC</td>
<td>Centers for Disease Control and Prevention</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Server</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISAPI</td>
<td>Internet Server Application Programming Interface</td>
</tr>
<tr>
<td>JSP</td>
<td>Java Server Pages</td>
</tr>
<tr>
<td>PHIN</td>
<td>Public Health Information Network</td>
</tr>
<tr>
<td>PHINMS</td>
<td>Public Health Information Network Messaging System</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layers</td>
</tr>
</tbody>
</table>
1.0 INTRODUCTION

The Centers for Disease Control and Prevention (CDC) Public Health Information Network Messaging System (PHINMS) Stunnel Implementation Guide will assist with the installation and configuration of the Stunnel program on a Windows platform. Documentation is continually updated. Ensure the most recent versions are referenced from the PHINMS website at www.cdc.gov/phin/phinms.

1.1 Architecture

Redirecting messages from a Microsoft Integrated Information Server (IIS) as a proxy over an SSL connection to a PHINMS receiver requires the following multiple products:

- IIS Server,
- Jakarta ISAPI plug-in,
- Stunnel,
- Tomcat application server, and
- PHINMS Receiver.

Each component requires proper configuration for PHINMS messages only needed if IIS is being used as a web server, and BEA Web Logic is not being used as an application server.

Stunnel is setup between the IIS and the PHINMS Receiver servers. The Jakarta ISAPI redirector is pointed directly to the AJP13 port on the PHINMS Receiver server. When a firewall exists between the IIS proxy and the PHINMS Receiver, the firewall’s UDP Port 500 must be open as shown in Figure 1.1. More information on self-signed certificates can be found at www.stunnel.org.
This Stunnel Implementation Guide is intended for those responsible for installing and configuring Stunnel and the Jakarta ISAPI to work with a PHINMS 2.6 receiver. It does not address installing or configuring the Tomcat application server nor PHINMS.

The information in this document has only been tested with the Tomcat application server. These settings may or may not work with other application servers such as JBOSS.

### 1.2 Stunnel

The Stunnel program is designed to work as a Secure Socket Layers (SSL) encryption wrapper between remote client and local or remote server. Stunnel can be used to add SSL functionality to commonly used servers without any changes in the programs' code.

### 1.3 Communiqués

The PHINMS team responds to user’s communiqués. Send questions, suggestions, and/or comments concerning PHINMS support or documentation to the PHINMS website using the Contact PHINMS email link located at the top of the website.
2.0 STUNNEL CONFIGURATION

Implementing Stunnel based network communications between the Internet Information Server (IIS) Server and the PHINMS Receiver ensures all network communications between the two servers are encrypted and secure. Network traffic between the servers and other computers will not be affected by the installation of the Stunnel. Figure 2.1 shows the Stunnel architect.

2.1 Install Stunnel

Complete the following steps on both the IIS Server and the PHINMS Receiver to establish Stunnel between IIS and PHINMS Receiver:

1. navigate to http://www.stunnel.org/download/binaries.html displaying Figure 2.1,

![Figure 2.1. Stunnel-4.15-installer.exe](image1)

2. click stunnel-4.15-installer.exe link displaying the left screen of Figure 2.2, click Run displaying the right screen,

![Figure 2.2. Stunnel Security Warning](image2)
3. click **Run** displaying Figure 2.3,

   ![Figure 2.3. Stunnel License Agreement](image)

4. read the **License Agreement**, select **I Agree** displaying Figure 2.4,

   ![Figure 2.4. Stunnel Installation Options](image)

5. check **Start Menu Shortcuts** (optional), select **Next** displaying Figure 2.5,
6. Select **Browse** to choose a Destination Folder (optional), select **Install** displaying Figure 2.6, and

7. Click **Close**.

### 2.2 Configure IIS Server

Complete the following steps to configure Stunnel on the IIS server in client mode:

8. Select **Start > Programs > Stunnel, Edit Stunnel.conf** displaying the left screen in Figure 2.7,
9. add semicolons (;) to the designated lines highlighted yellow, remove the semicolons (;) from the designated lines highlighted green, change accept and connect highlighted blue to 8009 and local host:7002 respectively, select File, Save, close window, and

**Note:** Ensure accept is configured to use port 8009 for ajp13 traffic. The local host should be the PHINMS Receiver Internet Protocol (IP) address.

10. select Start > All Programs > Stunnel > Service Start.

### 2.3 Configure PHINMS Receiver Service Mode

1. select Start > All Programs > Stunnel > Edit Stunnel.conf displaying the left screen in Figure 2.8,
2. add semicolons (;) to the designated lines highlighted yellow, remove the semicolons (;) from the designated lines highlighted green, change accept and connect highlighted blue to **7002 and connect to 8009** respectively, select **File**, **Save**, close window, and

3. select **Start > All Programs > Stunnel > Service start**.

Configure both Stunnel installations to use Self-Signed Certificates which encrypt and decrypt data between the two servers. Verify data traffic session and SSL are established. Test end-to-end from the user browser to PHINMS Sender on PHINMS Receiver.
3.0 JAKARTA

Normally the IIS can not execute servlets and Java Server Pages (JSP). Configuring IIS to use the Jakarta Internet Server Application Programming Interface (ISAPI) redirector plug-in will allow IIS to send servlet and JSP requests to Tomcat and serve them to clients. Further information on Jakarta can be located at http://tomcat.apache.org/connectors-doc/.

3.1 Pre-Jakarta Install

Complete the following steps before installing Jakarta:

1. navigate to C:\Program Files\PhinMS\2.6\tomcat-5.0.19\conf, select server.xml file,

![Figure 3.1. server.xml File](image)

2. right click server.xml file, open with notepad displaying Figure 3.2, and

![Figure 3.2. server.xml Notepad](image)

3. search for 8009, delete the comments highlighted in yellow shown in Figure 3.2, save the server.xml file, close window.
3.2 Install Jakarta

Complete the following steps to configure the Tomcat Jakarta ISAPI redirect connector on the IIS Server:

1. navigate to http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2.15/ displaying Figure 3.3,

2. double click the isapi_redirect.msi link displaying the left screen of Figure 3.4, click Run displaying the right screen,

3. click Run displaying Figure 3.5,
4. click Next, displaying Figure 3.6,

**Figure 3.6. License Agreement**

5. read the License Agreement, select I accept the terms in the license agreement, click Next displaying Figure 3.7,
6. click **Next** displaying Figure 3.8,

![Figure 3.7. Destination Folder](image)

7. click **Install** displaying Figure 3.9, and
8. click **Finish**.

### 3.3 Configure Jakarta

Complete the following steps to configure Jakarta:

1. navigate to `C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\conf` displaying Figure 3.10,

   ![Figure 3.10. Jakarta Program Files](image)

2. right click on `uriworkermap.properties`, select **Open** displaying Figure 3.11,
3. select **Select the program from a list**, click **OK** displaying Figure 3.12,

4. select **Notepad**, click **OK** displaying Figure 3.13,
5. delete `/admin/*=wlb`, `/manager/*=wlb`, `/jsp-examples/*=wlb`, `/servlets-examples/*=wlb`, replace with `/receiver/*=wlb`, select File, Save, close Notepad,

6. navigate to `C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\conf` displaying Figure 3.14,

7. right click on `workers.properties.minimal`, select Open, displaying Figure 3.15,
8. select **Select the program from a list**, click **OK** displaying Figure 3.17,

![Figure 3.17. Open With](image)

9. select **Notepad**, click **OK** displaying Figure 3.18,

![Figure 3.18. workers.properties.minimal Notepad](image)
10. delete localhost, replace with the localhost (IP) address (127.0.0.1), select File, Save, close Notepad,

11. select Start > Settings > Control Panel > Administrator Tools displaying Figure 3.19,

![Figure 3.19. Administrative Tools](image)

12. double click Internet Information Services Manager (IIS), navigate to Web Service Extensions displaying Figure 3.20,

![Figure 3.20. IIS Manager](image)

13. right click on Web Service Extensions, select Add a new Web service extension displaying Figure 3.21,
14. enter an **Extension name**, check **Set extension status to allowed**, select **Add** displaying Figure 3.22,

15. select **Browse**, navigate to `C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\bin\isapi_redirect.dll`, click **OK, OK, OK** displaying Figure 3.23,
16. verify ISAPI Web Extension has been added, expand Web Sites, click on Default Web Site, displaying Figure 3.24,

17. right click on Default Web Site, select Properties displaying Figure 3.25,
18. select ISAPI Filters tab, select Add displaying Figure 3.26,

![Add/Edit Filter Properties](image)

**Figure 3.26. Add/Edit Filter Properties**

19. enter Filter Name, browse to `C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\bin\isapi_redirect.dll`, click OK, select Directory Security tab displaying Figure 3.27,
20. select **Edit** in the Secure communications section displaying Figure 3.28,

![Figure 3.28. Secure Communications](image)

21. check **Require secure channel (SSL)**, click **OK**, **OK** displaying Figure 3.29, and
22. Click on the menu bar to stop and to restart the IIS services.

3.4 Test Jakarta IIS Filter

Complete the following steps to test the Jakarta IIS filter:

1. Open Internet Browser, type the local host of the IIS Web Server, select Enter displaying Figure 3.30,

Note: Ensure https is used for the secure site and not http otherwise an error will occur.

2. Select Yes displaying Figure 3.31, and
3. close window.
4.0 CONFIGURE ONE TO ONE MAPPING

One-to-one mapping maps individual client certificates to local user accounts. The server compares the copy of the client certificate it stores with the client certificate sent by the browser. The two must be absolutely identical for the mapping to proceed. When a client gets another certificate containing all of the same user information, it must be mapped again.

4.1 Create Account

The system administrator must first create a local user account on the IIS server before completing the following steps used to configure one to one mapping:

1. locate the Jakarta Isapi Redirector folder using windows explorer, displaying Figure 4.1,

![Figure 4.1. Jakarta Bin Folder](image)

2. right click Bin, select Sharing and Security displaying Figure 4.2,
3. click the **Advance** tab displaying Figure 4.3,

![Figure 4.2. Bin Properties](image)

Figure 4.2. Bin Properties

4. ensure all of the following **Permission Entries** are listed:

![Figure 4.3. Advanced Security Setting for Bin](image)

Figure 4.3. Advanced Security Setting for Bin
– Network Service,
– Creator Owner,
– Interactive,
– System,
– Administrator,
– User Account,
– the local account the system administrator has created for one to one mapping authentication,

5. check **Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.**, click **OK**, **OK** displaying Figure 4.4,

![Figure 4.4. isapi_redirect.dll](image)

6. right click **isapi_redirect.dll**, select **Properties**, select the **Security** tab displaying Figure 4.5,
7. **click Add** displaying Figure 4.6,

![Select Users, Computers, or Groups](image)

**Figure 4.6. Select Users, Computers, or Groups**

8. **click the Advance tab**, displaying Figure 4.7,
9. Select **Find Now** populating all user account which exist on the machine, select the **User Account**, click **OK**, **OK** displaying Figure 4.8, and

10. Click **Full Control**, click **OK**.
4.2 Configure Jakarta Isapi

The purpose of one to one mapping is to secure individual communications between the source and the destination. One to one mapping uses the individual user account mapped to a client certificate to add additional security. One to one mapping is configured on the IIS server.

1. select **Start > Settings > Control Panel > Administrator Tools** displaying Figure 4.9,

![Figure 4.9. Administrative Tools](image)

2. double click on **Internet Information Service (IIS) Manager** displaying Figure 4.10,

![Figure 4.10. Internet Information Services (IIS) Manager](image)

3. right click the **Default Web Site**, select **Properties** displaying Figure 4.11,
4. select the **Directory Security** tab displaying Figure 4.12,
5. select **Edit** under the **Authentication and access control** displaying Figure 4.13,

![Authentication Methods](image)

Figure 4.13. Authentication Methods

6. uncheck all **check boxes**, click **OK** returning to the Default Web Site Properties screen, click **Edit** under **Secure communications** displaying Figure 4.14,
7. click **Add** to map the user account with the certificate for authentication in the one to one mapping configuration displaying Figure 4.15,
8. ensure ***Require secure channel (SSL), Required client certificates, Enable client certificate mapping*** is selected, click **Edit** on the far right-hand side of the screen displaying Figure 4.16,

![Figure 4.16. Account Mappings](image)

9. select **Add** displaying Figure 4.17,

![Figure 4.17. Open](image)
10. select the **Certificate** used to secure this communication method, click **Open** displaying Figure 4.18,

![Map to Account dialog box](image)

**Figure 4.18. Map To Account**

11. place a check in the box next to **Enable this mapping**, enter the **Map Name**, select **Browse**, search for **account** to map, enter the **Password**, click **OK**, displaying Figure 4.19,

![Confirm Password dialog box](image)

**Figure 4.19. Confirm Password**

12. enter **Password** for confirmation, click **OK**, **OK** displaying Figure 4.20,
13. check **Enable client certificate trust list**, select **New IIS CTL** from the drop-down list, click **OK** displaying Figure 4.21,

![Certificate Trust List Wizard](image)

**Figure 4.21. Certificate Trust List Wizard**

14. click **Next** displaying Figure 4.22,
15. select **Add from Store** or **Add from File** displaying Figure 4.23,

![Select Certificate](image)

**Figure 4.23. Select Certificate**

16. select **Certificate**, click **OK** displaying Figure 4.24,
Figure 4.24. Certificate Trust List Wizard

17. select **Next** displaying Figure 4.25,

Figure 4.25. Certificate Description

18. enter **Description** for the certificate trust list, click **Next** displaying Figure 4.26,
19. click **Finish** displaying Figure 4.27,

![Figure 4.27. Wizard Success](image)

20. click **OK** displaying Figure 4.28,
21. click OK displaying Figure 4.29,

22. click OK displaying Figure 4.30,
23. Click **Select All**, then click **OK** displaying Figure 4.31,

![Figure 4.30. Inheritance Overrides](image)

24. Right-click **Jakarta**, select **Properties**, select the **Directory Security** tab displaying Figure 4.32,
Figure 4.32. Authentication and Access Control

25. select **Edit** under **Authentication and access control** displaying Figure 4.33,

Figure 4.33. Authentication Methods
26. deselect all **Check Boxes**, click **OK** displaying Figure 4.34, and

![Jakarta Properties](image)

**Figure 4.34. Jakarta Properties**

27. click **OK**.

### 4.3 Test One to One Mapping

1. open **Internet Browser**, type URL [https://localhost/receiver/receivefile](https://localhost/receiver/receivefile), select **Go** displaying Figure 4.35,

![Security Alert](image)

**Figure 4.35. Security Alert**

2. select **Yes** displaying Figure 4.36,
3. select the **Digital Certificate**, click **OK** displaying Figure 4.37,

![Choose a digital certificate](image)

**Figure 4.36. Choose a Digital Certificate**

![Test Successful Notification](image)

**Figure 4.37. Test Successful Notification**

**Note:** An error will occur when an invalid Digital Certificate is used on the receiver displaying Figure 4.38.
The page requires a valid SSL client certificate

Your client certificate is untrusted or invalid. A Secure Sockets Layer (SSL) client certificate is used for identifying you as a valid user of the resource.

Please try the following:

- Contact the site administrator to establish client certificate permissions.
- If you already have a valid client certificate, use your Web browser’s security features to ensure that your client certificate is installed properly. (Some Web browsers refer to client certificates as browser or personal certificates.)
- Change your client certificate and click the Refresh button, if appropriate.

HTTP Error 403.16 - Forbidden: Client certificate is ill-formed or is not trusted by the Web server.
Internet Information Services (IIS)

Figure 4.38. Valid SSL Client Certificate Required
5.0 SECURE SOCKET LAYERS

5.1 Download Openssl

The Openssl application should be installed on a single workstation. Complete the following steps to download Openssl:

1. create a folder on the root directory C:\Openssl,

2. navigate to http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7/,
   displaying Figure 5.1,

![Figure 5.1. Openssl.exe](image)

3. click openssl.zip, displaying Figure 5.2,
4. select **Open**, displaying Figure 5.3,

![Figure 5.3. WinZip Openssl](image)

5. select **Extract** displaying Figure 5.4, and
6. navigate to the **Openssl** folder, click **Extract**, close window.

**Note:** The following four files are needed to run Openssl shown in Figure 5.5:

- libeay32.dll,
- libssl32.dll,
- openssl.exe, and
- openssl.conf.

The first three files libeay32.dll, libssl.dll, and open.exe are automatically extracted from the WinZip file. The fourth, openssl needs to be downloaded from PHINMS FTP site. Contact the PHIN Help Desk for assistance [phintech@cdc.gov](mailto:phintech@cdc.gov).

### 5.2 Create Self-Signed Certificates

Complete the following steps to create a Self-Signed Certificates:
1. navigate to C:\openssl, double click on openssl.exe displaying Figure 5.6,

![Figure 5.6. Openssl](image)

2. type req -new -x509 -days 365 -nodes -config openssl.cnf -out c:\openssl\renamecsr.pem -keyout c:\openssl\renamekey.pem, select Enter displaying Figure 5.7,

Note: Replace both “rename” in step two with a unique file name. An example would be phinmscsr.pem and phinmskey.pem. Do not replace csr.pem or key.pem.

![Figure 5.7. Distinguished Name Prompts](image)

3. assign the Distinguished Name (DN) Fields command prompts with information uniquely identifying the Self-Signed Certificates using the examples in Table 1 as a guideline displaying Figure 5.8, and

Note: The DN fields will be incorporated into the Self-Signed Certificates request. The prompts allow blank fields but it is highly recommended to complete all the fields. This will uniquely identify the Self-Signed Certificates.

<table>
<thead>
<tr>
<th>FIELDS</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name:</td>
<td>PL, UK, US, CA</td>
</tr>
<tr>
<td>State or Province Name:</td>
<td>Illinois, Ontario</td>
</tr>
<tr>
<td>Locality:</td>
<td>Chicago, Toronto</td>
</tr>
<tr>
<td>Organization Name:</td>
<td>Bill's Meats, Acme Anvils</td>
</tr>
<tr>
<td>Organizational Unit Name:</td>
<td>Ecommerce Division</td>
</tr>
<tr>
<td>Common Name (FQDN)</td>
<td><a href="http://www.example.com">www.example.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:test@yahoo.com">test@yahoo.com</a></td>
</tr>
</tbody>
</table>
4. close the window.

The new Self-Signed Certificates should be in the C:\openssl folder as shown in Figure 5.9.

5.3 Configure Servers

Complete the following steps to configure secure communications between the two servers using Stunnel:

1. copy the two (2) Self-Signed Certificates created,

2. select Start > Programs > Stunnel, Edit Stunnel.conf displaying the left screen in Figure 5.10,
3. paste the two (2) **Self-Signed Certificates** into the Stunnel.conf file on the lines highlighted in Figure 5.10,

**Note:** Ensure the Self-Signed Certificates are identified as key or cert in the name which helps in configuring Stunnel.conf file.

4. close window displaying Figure 5.11,

5. select **Yes**,

6. select **Start > Programs > Stunnel, Service stop**, and

7. select **Start > Programs > Stunnel, Service start** on both servers.