



# 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.



VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0	Lawrence Loftley	Aug 11, 2006	Create S-Tunnel Implementation Guide.
1.0	Wendy Fama	Aug 11, 2006	Update S-Tunnel Implementation Guide.
1.1	Wendy Fama	Sep 6, 2006	Add One to One Mapping.
1.1	Wendy Fama	Sep 19, 2006	Add Architecture section.
1.1	Wendy Fama	Sep 20, 2006	Update based on training feedback.

## **REVISION HISTORY**



## TABLE OF CONTENTS

1.0	Introduction	
	1.1 Architecture	
	1.2 Stunnel	9
	1.3 Communiqués	9
2.0	Stunnel Configuration	
	2.1 Install Stunnel	
	2.2 Configure IIS Server	
	2.3 Configure PHINMS Receiver Service Mode	
3.0	Jakarta	
	3.1 Pre-Jakarta Install	
	3.2 Install Jakarta	
	3.3 Configure Jakarta	
	3.4 Test Jakarta IIS Filter	
4.0	Configure One to One Mapping	
	4.1 Create Account	
	4.2 Configure Jakarta Isapi	
	4.3 Test One to One Mapping	
5.0	Secure Socket Lavers	
	5.1 Download Openssi	
	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	uriworkermap.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



Figure 4.7. Advanced Select Users, Computers, or Groups	.34
Figure 4.8. isapi_redirect.dll Properties	.34
Figure 4.9. Administrative Tools	.35
Figure 4.10. Internet Information Services (IIS) Manager	.35
Figure 4.11. Default Web Site Properties	.36
Figure 4.12. Directory Security	.36
Figure 4.13. Authentication Methods	.37
Figure 4.14. Account Mappings	.38
Figure 4.15. Secure Communications	.38
Figure 4.16. Account Mappings	.39
Figure 4.17. Open	.39
Figure 4.18. Map To Account	.40
Figure 4.19. Confirm Password	.40
Figure 4.20. Secure Communications	.41
Figure 4.21. Certificate Trust List Wizard	.41
Figure 4.22. Certificates in the CTL	.42
Figure 4.23. Select Certificate	.42
Figure 4.24. Certificate Trust List Wizard	.43
Figure 4.25. Certificate Description	.43
Figure 4.26. Wizard Complete	.44
Figure 4.27. Wizard Success	.44
Figure 4.28. Secure Communications	.45
Figure 4.29. Default Web Site Properties	.45
Figure 4.30. Inheritance Overrides	.46
Figure 4.31. Internet Information Services (IIS) Manager	.46
Figure 4.32. Authentication and Access Control	.47
Figure 4.33. Authentication Methods	.47
Figure 4.34. Jakarta Properties	.48
Figure 4.35. Security Alert	.48
Figure 4.36. Choose a Digital Certificate	.49
Figure 4.37. Test Successful Notification	.49
Figure 4.38. Valid SSL Client Certificate Required	.50
Figure 5.1. Openssl.exe	.51
Figure 5.2. Openssl File Download	.52
Figure 5.3. WinZip Openssl	.52
Figure 5.4. Extract Files	.53
Figure 5.5. Openssl Files	.53
Figure 5.6. Openssl	.54
Figure 5.7. Distinguished Name Prompts	.54
Figure 5.8. Distinguished Name Fields	.55
Figure 5.9. Self-Signed Certificates	.55
Figure 5.10. Stunnel Configuration File	.56
Figure 5.11. Save Stunnel.conf File	.56



## ACRONYM LIST

CDC	Centers for Disease Control and Prevention

- DN Distinguished Name
- IIS Internet Information Server
- IP Internet Protocol
- ISAPI Internet Server Application Programming Interface
- JSP Java Server Pages
- PHIN Public Health Information Network
- PHINMS Public Health Information Network Messaging System
- SSL Secure Socket Layers



## 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 <u>www.stunnel.org</u>.





Figure 1.1. Stunnel Architecture Diagram

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

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





3. click **Run** displaying Figure 2.3,



Figure 2.3. Stunnel License Agreement

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



Figure 2.4. Stunnel Installation Options

5. check Start Menu Shortcuts (optional), select Next displaying Figure 2.5,



🖶 stunnel 4.15 Se	tup: Installation Folder		_ 🗆 X
Setup will in	stall stunnel 4.15 in the follow Browse and select another fi	wing folder. To insta older.	ll in a different
Destination Folde	r -\stunnel\	B	rowse
Space required: 1.4 Space available: 2.6	MB iGB		
Cancel	Author: Michal Trojnara	< <u>B</u> ack	Install

Figure 2.5. Stunnel Installation Folder

6. select **Browse** to choose a Destination Folder (optional), select **Install** displaying Figure 2.6, and

🔀 stunnel 4.15 S	etup: Completed		
Show <u>d</u> etails			
Cancel	Author: Michal Trojnara	< <u>B</u> ack	⊆lose

## Figure 2.6. Stunnel Installation Complete

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,



🖡 stunnel.conf - Notepad	
File Edit Format View Help	
; Some options used here	may not be adequate for your particular configuration 📶
: Certificate/key is need : The default certificate : be used in a production	ed in server mode and optional in client mode is provided only for testing and should not environment
;key = stunnel.pem	🖻 stunnel.conf - Notepad 📃 🗖 🛛
; Some performance tuning	File Edit Format View Help
socket = 1:TCP_NODELAY=1 socket = r:TCP_NODELAY=1	: Sample stunnel configuration file by Michal Trojnara 2002-2006 ; Some options used here may not be adequate for your particular configuration
<pre>; workaround for Eudora b ;options = DONT_INSERT_EM ; Authentication stuff] ;verify = 2 ; Don't forget to c_rehas ;CApath = certs ; It's often easier to us ;CApith = certs.pem ; Don't forget to c_rehas ;CApith = crls ; Ot torget to c_rehas ;CApith = crls ; Alternatively you can u ;CRLfile = crls.pem ; Some debugging stuff us ;debug = 7 ;output = stunnel.log ; Use it for client mode ;client = yes</pre>	<pre>: Certificate/key is needed in server mode and optional in client mode : The default certificate is provided only for testing and should not : be used in a production environment cert = stunnel.pem :key = stunnel.pem : Some performance tunings socket = 1:TCP_MODELAY=1 socket = 1:TCP_MODELAY=1 socket = r:TCP_MODELAY=1 : workaround for Eudora bug :options = DONT_INSERT_EMPTY_FRAGMENTS : Authentication stuff :verify = 2 : Don't forget to c_rehash CApath :CApath = certs : It's often easier to use CAfile :CAfile = certs.pem : Don't forget to C_rehash CR.path 'CEN anth = celts</pre>
; service-level configura [pop3s]	: Alternatively you can use CRLfile :CRLfile = crls.pem : Some debugging stuff useful for troubleshopting
connect = 110	output = stunnel.log
[imaps] accept = 993 connect = 143	: Use it for client mode client - yes
[ssmtp] accept = 465 connect = 25 :[https] accept = 443	: Service-level configuration :[pop3s] :accept = 995 :connect = 110
connect = 180 TIMEOUTClose = 0	Limaps] accept = 993 :connect = 143
; vim:ft=dosini	:[ssmtp] ;accept = 465 :connect = 25
	[https] accept = 8009 connect = local host:7002 ;TIMEOUTClose = 0
	; vim:ft=dosini

Figure 2.7. IIS Server Configuration

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,





📕 stunnel.conf - Notepad	
File Edit Format View Help	
; Some options used her	e may not be adequate for your particular configuration 🛪
: Certificate/key is ne : The default certifica ; be used in a production cert = stunnel.pem ;key = stunnel.pem	eded in server mode and optional in client mode te is provided only for testing and should not on environment
; Some performance tuni socket = 1:TCP_NODELAY=	Stunnel.conf - Notepad
; workaround for Eudora	File Edit Format Wew Help ; Sample stunnel configuration file by Michal Trojnara 2002-2006 : Some portions used here may not be adequate for your particular configuration
; Authentication stuff ;verify = 2 ; Don't forget to c_reh ;CApath = certs ; It's often easier to ;CAfile = certs.pem ; Don't forget to c_reh ;CALpath = crls ; Alternatively you can ;CALFILE = crls.pem	<pre>: Some options one in the may not be decided to by a particular configuration : Certificate/key is needed in server mode and optional in client mode : The default certificate is provided only for testing and should not : be used in a production environment cert = stunnel.pem ;key = stunnel.pem ; Some performance tunings socket = 1:TCP_NODELAY=1 socket = r:TCP_NODELAY=1</pre>
<pre>Some debugging stuff ;debug = 7 ;output = stunnel.log ; Use it for client mod ;client = yes ; Service-level configu [pop35] accent = 995</pre>	<pre>; workaround for Eudora bug ;options = DONT_INSERT_EMPTY_FRAGMENTS ; Authentication stuff ;verify = 2 ; Don't forget to c_rehash CApath ;CApath = certs ; It's often easier to use CAfile ;CAfile = certs.pem ; Don't forget to c_rehash CRLpath ;CRLpath = crls ; Alternatively you can use CRIfile ; Alternatively you can use CRIfile</pre>
connect = 110 [imaps] accept = 993 connect = 143	<pre>:CRLfile = crls.pem : Some debugging stuff useful for troubleshooting debug = 7 output = stunnel.log</pre>
[ssmtp] accept = 465 connect = 25	; Use it for client mode client = yes
;[https] ;accept = 443 ;connect = 180 ;TIMEOUTclose = 0	:[pop3s] ;compt = 995 ;connect = 110
; vim:ft=dosini	:[imaps] ;accept = 993 ;connect = 143
	:[ssmtp] ;accept = 465 ;connect = 25
	[https] accept = 7002 connect = 8009 ;TIMEOUTClose = 0
	; vim:ft=dosini 🗸

Figure 2.8. PHINMS Receiver Service Mode Configuration

- 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 <a href="http://tomcat.apache.org/connectors-doc/">http://tomcat.apache.org/connectors-doc/</a>.

#### 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

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



Figure 3.2. server.xml Notepad

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 <u>http://www.apache.org/dist/tomcat/tomcat-</u> <u>connectors/jk/binaries/win32/jk-1.2.15/</u> displaying Figure 3.3,

Index of /dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2	.15 - Microsoft Internet E	ixplorer		
File Edit View Favorites Tools Help				<b>1</b>
🔇 Back 👻 🕥 🐇 📓 🏠 🔎 Search 🌟 Favorites 🤗	🗟 • 🍓 💌 • 🗾	<b>11</b> 4	8	
Address 🚳 http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/	jk-1.2.15/		💌 🔁 G	io Links
Google - 🔽 🔽 G Search 🔹 🥥 🚿 🔊 O blocke	d 🛛 🗳 Check 🝷 🌂 AutoL	ink 🔹 🌾	🗍 AutoFill 🛛 🛃 Options 🏾 🖉	
	onnostors/il	l/hi	narios/win32/ik_1 2 1	5 Î
Index of /dist/tomcat/tomcat-c	Last modified	Size	Description	
Index of /dist/tomcat/tomcat-c	Last modified	<u>Size</u>	Description	
Index of /dist/tomcat/tomcat-c	Last modified 08-Nov-2005 07:58	<u>Size</u> - 148K	Description	
Index of /dist/tomcat/tomcat-c	Last modified 08-Nov-2005 07:58 08-Nov-2005 08:55	<u>Size</u> - 148K 194	Description	
Index of /dist/tomcat/tomcat-c	Last modified 08-Nov-2005 07:58 08-Nov-2005 08:55 08-Nov-2005 08:42	<u>Size</u> - 148K 194 630K	Description	
Index of /dist/tomcat/tomcat-co	Last modified 08-Nov-2005 07:58 08-Nov-2005 08:55 08-Nov-2005 08:42 08-Nov-2005 08:55	<u>Size</u> - 148K 194 630K 194	Description	

Figure 3.3. isapi\_redirect.msi

2. double click the **isapi\_redirect.msi** link displaying the left screen of Figure 3.4, click **Run** displaying the right screen,



Figure 3.4. File Download

3. click **Run** displaying Figure 3.5,



🖟 Jakarta Isapi Redirector - InstallShield Wizard 🛛 🔀				
	Welcome to the InstallShield Wizard for Jakarta Isapi Redirector			
	The InstallShield(R) Wizard will install Jakarta Isapi Redirector on your computer. To continue, click Next.			
	WARNING: This program is protected by copyright law and international treaties.			
	< Back Next > Cancel			

Figure 3.5. Jakarta ISAPI Redirector

4. click **Next**, displaying Figure 3.6,

🛃 Jakarta Isapi Redirector - InstallShield Wizard	×
License Agreement Please read the following license agreement carefully.	1
Apache License Version 2.0, January 2004 http://www.apache.org/licenses/	
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTI 1. Definitions. "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.	NO d
I accept the terms in the license agreement I do not accept the terms in the license agreement InstallShield < Back Next >	Print

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,



😼 Jakarta	Isapi Redirector - InstallShield Wizard
<b>Destinati</b> Click Ne>	on Folder At to install to this folder, or click Change to install to a different folder.
	Install Jakarta Isapi Redirector to: C:\Program Files\Apache Software Foundation\Jakarta Isapi Change Redirector\
InstallShield -	< Back Next > Cancel

Figure 3.7. Destination Folder

6. click **Next** displaying Figure 3.8,

🥵 Jakarta Isapi Redirector - InstallShield Wizard	×
Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
Installshield — Cancel Cancel	

Figure 3.8. Install the Program

7. click Install displaying Figure 3.9, and



🛃 Jakarta Isapi Redirector	- InstallShield Wizard 🛛 🔀			
N	InstallShield Wizard Completed			
	The InstallShield Wizard has successfully installed Jakarta Isapi Redirector. Click Finish to exit the wizard.			
	< Back Finish Cancel			

Figure 3.9. Install Complete

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,

🗀 C:\Program Files\Apache	Software Foundat	tion\Jakarta Isapi R	edi 🔳 🗖 🔀
File Edit View Favorites T	ools Help		ali 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 19
🚱 Back 🝷 🕥 🕤 🏂 🍃	🔎 Search 🛛 🍺 Fold	ders 🕼 🎲 ≻	<b>( 19</b>
Address 🛅 C:\Program Files\Apac	he Software Foundatio	on\Jakarta Isapi Redirect	or\conf 🚩 🔁 Go
Name 🔺	Size	Туре	Date Modified
🔤 uriworkermap.properties	1 KB F	PROPERTIES File	4/28/2005 12:03 PM
🔤 workers.properties.minimal	1 KB	MINIMAL File	4/28/2005 11:59 AM
<	Ш		>

Figure 3.10. Jakarta Program Files

2. right click on uriworkermap.properties, select Open displaying Figure 3.11,



Windows ?X			
Windows cannot open this file: File: workers.properties.minimal			
To open this file, Windows needs to know what program created it. Windows can go online to look it up automatically, or you can manually select from a list of programs on your computer.			
What do you want to do?			
◯ Use the Web service to find the appropriate program			
<ul> <li>Select the program from a list</li> </ul>			
OK Cancel			

Figure 3.11. Open File

3. select Select the program from a list, click OK displaying Figure 3.12,

Open With	? 🗙
Choose the program you want to use to open this file:	
File: workers.properties.minimal	
Programs	
Microsoft Office Excel	^
Microsoft Office InfoPath	
Microsoft Office Picture Manager	
🔣 Microsoft Office Visio	=
Microsoft Office Word	
Notepad	
🦉 Paint	
😨 RealPlayer	
🥌 SnaoIt 8	×
Type a description that you want to use for this kind of file:	
Always use the selected program to open this kind of file	
Brows	e
If the program you want is not in the list or on your computer, you for the appropriate program on the Web.	can <u>look</u>
OK Cano	el

Figure 3.12. Open With

4. select Notepad, click OK displaying Figure 3.13,





Figure 3.13. uriworkermap.properties Notepad

- delete /admin/\*=wlb, /manager/\*=wlb, /jsp-examples/\*=wlb, /servletsexamples/\*=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,



Figure 3.14. Jakarta Program Files

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,

Open V	∀ith	<b>?</b>	
$\bigcirc$	Choose the program you want to use to open this file: File: workers.properties.minimal		
Progra	ams		
	Microsoft Office Excel Microsoft Office InfoPath Microsoft Office Picture Manager Microsoft Office Visio Microsoft Office Word Notepad Paint RealPlayer SnaoIt 8		
Тур	e a description that you want to use for this kind of file:		
	Always use the selected program to open this kind of file Browse.		
If the p for the	rogram you want is not in the list or on your computer, you ca appropriate program on the Web.	an <u>look</u>	
	OK Cance		

Figure 3.17. Open With

9. select Notepad, click OK displaying Figure 3.18,



Figure 3.18. workers.properties.minimal Notepad



- 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,

🦏 Administrati <del>v</del> e Tools				x
Eile Edit View Favorites Tools Help				
🚱 Back 👻 🕤 👻 🏂 🔎 Search 🧃	> Folders			
Address 🦏 Administrative Tools			💌 🔁 Go	
	Name 🔺	Size	Туре	
File and Folder Tasks 🛛 🛠	Event Viewer	2 KB	Shortcut	
Departs this file	🗕 厕 Internet Information Services (IIS) Manager	2 KB	Shortcut	
Rename diis nie	Reg Licensing	2 KB	Shortcut	_
Move this file	🕞 Local Security Policy	2 KB	Shortcut	
Copy this file	Manage Your Server	2 KB	Shortcut	-
🚳 Publish this file to the 📃			Þ	· //

Figure 3.19. Administrative Tools

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

internet Information Services\AOPS-IR	M-PHM611 (local computer)\Web Serv	vice Extensions	
Internet Information Services	🃁 Web Service Extensions	-	
Image: Constraint of the state of the s	Allow Prohibit Properties Tasks Add a new Web service extension Allow all Web service extensions for a specific application Prohibit all Web service extensions Open Help Extended Standard	Web Service Extension       Sta         All Unknown CGI Extensions       Pro         All Unknown ISAPI Extensions       Pro         Active Server Pages       Pro         Internet Data Connector       Pro         ISAPI       Allo         Server Side Includes       Allo         Siteminder       Allo         WebDAV       Pro	tus hibited hibited hibited wed wed wed hibited

Figure 3.20. IIS Manager

13. right click on **Web Service Extensions**, select **Add a new Web service extension** displaying Figure 3.21,



New Web Service Extension	×				
Type the name of the new Web service extension, and specify the files that must be enabled for the extension to run.					
Extension name:					
tomcat sample					
R <u>e</u> quired files:					
	A <u>d</u> d				
	Remove				
Set extension status to Allowed					
OK	Help				

Figure 3.21. New Web Service Extension

14. enter an **Extension name**, check **Set extension status to allowed**, select **Add** displaying Figure 3.22,

Add file	×
Enter the file location and name.	
Path to file:	
\Jakarta Isapi Redirector\bin\isapi_redirect.dll	Browse
ОК	Cancel



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,



Thternet Information Services\AOPS-IRM	1-PHM611 (local computer)\Web Serv	vice E	xtensions			_ 🗆 🗵
Internet Information Services	📁 Web Service Extensions	_				
AOPS-IRM-PHM611 (local computer)     Web Sites     Default Web Site     test     Web Service Extensions	Allow Prohibit Properties Tasks Add a new Web service extension Allow all Web service extensions for a specific application Prohibit all Web service extensions Open Help		Web Service Exte All Unknown CISA All Unknown ISAP Active Server Par Internet Data Co ISAPI Server Side Inclu Stervinder tomcat WebDAV	ension Extensions YI Extensions ges nnector des	Status Prohibited Prohibited Prohibited Allowed Allowed Allowed Prohibited	
	Extended / Standard /					

Figure 3.23. Internet Information Services

16. verify **ISAPI Web Extension** has been added, expand **Web Sites**, click on **Default Web Site**, displaying Figure 3.24,

🌆 Administrative Tools				
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help			- <b>1</b>
🔇 Back 🝷 🕤 👻 🏂 🔎 Search 🧜	>> Folders			
Address 🦏 Administrative Tools			-	🔁 Go
	Name 🔺	Size	Туре	<b></b>
File and Folder Tasks 🛛 🛠	Event Viewer	2 KB	Shortcut	
The Design of the Sta	Internet Information Services (IIS) Manager	2 KB	Shortcut	
	A Licensing	2 KB	Shortcut	
😰 Move this file	🕞 Local Security Policy	2 KB	Shortcut	
Copy this file	Manage Your Server	2 KB	Shortcut	-
🚳 Publish this file to the 📃				• <i>[</i> ]

Figure 3.24. Default Web Site

17. right click on Default Web Site, select Properties displaying Figure 3.25,



Documents Web Site	Directory Security Performance	HTTP Headers ISAPI Filters	Custom Errors Home Directory
The following ( listed below, T server,	ilters are active only for his list does not show filt	this Web site and exe ers configured for all t	cuted in the order he Web sites on this
Status	Filter Name	Priority	A <u>d</u> d
			<u>R</u> emove
			Edjt
			Disabl <u>e</u>
			Move <u>up</u>
			Move d <u>o</u> wn

Figure 3.25. Default Web Site Properties

18. select ISAPI Filters tab, select Add displaying Figure 3.26,

Add/Edit Filter P	Properties	×
Eilter name:	jakarta	
Executable:	karta Isapi Redirector\bin\	isapi_redirect.dll
Priority:	High	Browse
ОК	Cancel	Help



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,



Default Web Site	Properties			? ×
Web Site Documents	Performance	ISAPI Filters	Home Jers   Cu	e Directory
- Authentication Ei a	and access control nable anonymous acces: uthentication methods fo	s and edit the or this resource.	<u>E</u> dit	
- IP address and G IF	d domain name restriction irant or deny access to t P addresses or Internet	ns his resource using domain names.	Edįt	
Secure commu	nications equire secure communic nable client certificates ( esource is accessed,	ations and when this	Server Certifi	icate
	ОК	Cancel	Apply	Help



20. select Edit in the Secure communications section displaying Figure 3.28,

Secure Communications	×
Require secure channel (SSL)	7
Require 128-bit encryption	
Client certificates	
Ignore client certificates	
O Accept client certificates	
C Require client certificates	
Enable client certificate mapping     Client certificates can be mapped to Windows user     accounts. This allows access control to resources using     client certificates.     Edit     Edit	
Ne <u>w</u> Ediţ	
OK Cancel <u>H</u> elp	

Figure 3.28. Secure Communications

21. check Require secure channel (SSL), click OK, OK displaying Figure 3.29, and



🐌 Internet Information Services (IIS) Manager		_ 🗆 🗡
🕤 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> elp		_ 8 ×
	■ II	
Carl Internet Information Services	Name	Path
🖻 🚽 AOPS-IRM-PHM611 (local computer)	😍 jakarta	C:\Program Files\
🖻 🍎 Web Sites	😍 Test	D:\Test
🕀 👷 Default Web Site	📄 iisstart.htm	
🕀 💓 test	pagerror.gif	
Web Service Extensions		
		Þ

Figure 3.29. Administrative Tools

22. click I on the menu bar to stop and I 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.



Figure 3.30. Security Alert

2. select **Yes** displaying Figure 3.31, and



🗿 https://158.111.1.250/receiver/receivefile - Microsoft Internet Exp 🔳 🗖 🔀
File Edit View Favorites Tools Help 🥂
🕞 Back 🔹 🕥 👻 📓 🏠 🔎 Search 👷 Favorites 🚱 🔗 - 🌺 🎽
Address 🙆 https://158.111.1.250/receiver/receivefile 💌 🄁 Go 🛛 Links 🧔 SnagIt 🖹 😁
PHIN MS Receiver Centers for Disease Control and Prevention CDC PHIN-MS Version 2.6.00 GA Build 20060224 PartyId = 2.16.840.1.114222.4.3.2.2.3.561.1, Domain=cdc.gov
🕙 Done 🕒 🔮 🕐 Internet 🦪

Figure 3.31. PHINMS Receiver Notification

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

2. right click **Bin**, select **Sharing and Security** displaying Figure 4.2,



bin Properties		? ×
General Sharing Security Cust	omize	
Group or user names:		
Administrators (WEF1-17902) CREATOR OWNER Fama, Wendy (CDC/CCHIS/ Power Users (WEF1-179025)	5\Administrators) NCPHI) (CTR) (we \Power Users)	≤f1@cdc.go
SYSTEM		
	Add	Remove
Permissions for Administrators	Allow	Deny
Full Control Modify Read & Execute List Folder Contents Read Write		
For special permissions or for adva click Advanced.	nced settings,	Advanced
OK	Cancel	Apply

Figure 4.2. Bin Properties

3. click the **Advance** tab displaying Figure 4.3,

Ad	vanced S	ecurity Settings for bir			_	? ×
	Permissions	Auditing Owner Effe	ctive Permissions			
	To view m	ore information about Spec	cial permissions, selec	t a permission entry,	and then click Edit.	
	Permission	n entries:				
	Туре	Name	Permission	Inherited From	Apply To	
	Allow	Users (WEF1-179025	Read & Execute	C:\Program Files\	This folder, subfolders	
	Allow	Power Users (WEF1	Modify	C:\Program Files\	This folder, subfolders	
	Allow	Administrators (WEFT	Full Control	C:\Program Files\	This folder, subfolders	
	Allow	Fama, Wendv (CDC/	Full Control	C:\Program Files\	This folder only	
	Allow	CREATOR OWNER	Full Control	C:\Program Files\	Subfolders and files only	
	Add	d Edit	Remove			
	Inherit define	from parent the permission d here. ce permission entries on all	entries that apply to child objects with en	child objects. Include tries shown here that	these with entries explicit apply to child objects	y
				ОК	Cancel Apply	

Figure 4.3. Advanced Security Setting for Bin

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



- 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

6. right click **Isapi\_redirect.dll**, select **Properties**, select the **Security** tab displaying Figure 4.5,



isapi_redirect.dll Properties		? ×
General Version Security Summ	nary	
Group or user names:		
Administrators (WEF1-179028	5\Administrators)	
🙎 Fama, Wendy (CDC/CCHIS/	NCPHI) (CTR) (w	ef1@cdc.gov)
Power Users (WEF1-179025)	Power Users)	
SYSTEM		
WEFT-T79025/Users		
	Add	Remove
Permissions for Administrators	Allow	Deny
Full Control	$\checkmark$	
Modify	¥	
Read & Execute	~	H
Write	¥.	
Special Permissions		
For special permissions or for adva	nced settings,	Advanced
click Advanced.	_	
	-	
OK	Cancel	Apply

Figure 4.5. isapi\_redirect.dll Properties

7. click Add displaying Figure 4.6,

Select Users, Computers, or Groups	? ×
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
cdc.gov	Locations
Enter the object names to select ( <u>examples</u> ):	
	Check Names
Advanced OK	Cancel

Figure 4.6. Select Users, Computers, or Groups

8. click the **Advance** tab, displaying Figure 4.7,



elect this objec	mputers, or Group : type:	5			<u> </u>
Jsers, Groups, o	or Built-in security princ	ipals		Ot	oject Types
rom this location	1:				
dc.gov				l	ocations
Common Queri	es				
Name:	Starts with 💌			-	Columns
Description	Starts with			-	Find Now
					Ston
Non expir	accounts na password				
	ing parentinena				
		T			$\sim$
Days since la	st logon: 🔽	]			Ś
Days since la	st logon: 📃 💌	]			Ŵ
Days since la	st lagon:	]		OK	Cancel
Days since la	st.logon:	Description	In Folder	OK.	Cancel
Days since la	st logon:	Description	In Folder	OK	Cancel
Days since la	st logon: 💌	Description	In Folder	OK.	Cancel
Days since la	st logon: 💌	Description	In Folder	OK.	Cancel
Days since la	st logon: 💌	Description	In Folder	OK	Cancel
Days since la	st logon: 💌	Description	In Folder	OK	Cancel
Days since la	st logon: 💌	Description	In Folder	OK	Cancel

Figure 4.7. Advanced Select Users, Computers, or Groups

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

isapi_redirect.dll Properties		?
General Version Security Summ	ary	
Group or user names:		
acctOpTemplate (_acctOpTe	emplate@cdc.g	ov)
Administrators (WEF1-179025)	Administrators)	
🔹 🙎 Fama, Wendy (CDC/CCHIS/N	ICPHI) (CTR) (M	vef1@cdc.gov)
Power Users (WEF1-179025\	Power Users)	
SYSTEM		
🕵 Users (WEF1-179025\Users)		
1	ا مده	Bamaua
_	Add	Remove
Permissions for _acct0pTemplate	Allow	Deny
Full Control		
Modify		
Read & Execute		
Read		님
Special Permissions		
Special Fermissions		
J		
For special permissions or for advan	ced settings,	Advanced
click Advancea.	-	
OK	Cancel	Apply

Figure 4.8. isapi\_redirect.dll Properties

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

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

🐌 Internet Information Services (IIS) Mana	ger		
🐚 Eile Action <u>V</u> iew <u>W</u> indow Help			_8×
Contract Information Services	Computer	Local	Version
🖻 🗐 AOPS-IRM-PHM612 (local computer)	AOPS-IRM-PHM612 (local computer)	Yes	IIS V6.0
🕀 🃁 Application Pools			
🖻 🍎 Web Sites			
🖻 😭 Default Web Site			
🦾 🦣 jakarta			
🗄 🍎 Web Service Extensions			
			<u>Ľ</u>

Figure 4.10. Internet Information Services (IIS) Manager

3. right click the Default Web Site, select Properties displaying Figure 4.11,



Default Web Site F	Properties	? ×
Documents Web Site	Directory Security HTTP Headers Custom Errors Performance ISAPI Filters Home Directory	;
Web site identii Description: IP address: ICP port:	ication           Default Web Site         Advanced           (All Unassigned)         Image: Advanced           80         SSL port:         443	
Connections Connection tim Enable HTT	neout: 120 seconds IP <u>K</u> eep-Alives ging	
Acti <u>v</u> e log fo	rmat: ded Log File Format	
	OK Cancel Apply Help	

Figure 4.11. Default Web Site Properties

4. select the **Directory Security** tab displaying Figure 4.12,







5. select **Edit** under the **Authentication and access control** displaying Figure 4.13,

uthentication M	ethods				>
Use the following	/mous acce ) Windows	user accou	int for and	onymo	ous access;
User name:	IUSR_AC	DPS-IRM-PI	HM612		Browse,
Password:					
For the following are required whe - anonym - access Integrated W Digest authen Basic authen	authentic. en: nous acces is restricte /indows au ntication fo tication (pa t authenti	ation meth s is disable d using NT ithenticatio or Windows assword is cation	ods, user ed, or FS access in domain s sent in cle	name ; contr :erver: :ar tex	and password rol lists s (t)
Default domain	ж <u> </u>				Select
<u>R</u> ealm:					Sglect
C	К	Cano		H	elp

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,



to-1 Many-to-1 Edit "one to one" ma nap multiple certifica	appings. Each individual certificate is stes into the same account, but a se	s mapped into a specific Windows account. You can choose to parate mapping entry must exist for each.
Mapping Name test Gina jakarta	e Windows Account AOPS-IRM-PHM612\cqo2 AOPS-IRM-PHM612\cqo2 AOPS-IRM-PHM612\cqo2	Subject
<u>E</u> dit Map	Add Dejete	

Figure 4.14. Account Mappings

7. click **Add** to map the user account with the certificate for authentication in the one to one mapping configuration displaying Figure 4.15,

Secure Communications	×
Require secure channel (SSL)	
Require <u>1</u> 28-bit encryption	
Client certificates	
C Ignore client certificates	
C Accept client certificates	
Require client certificates	
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	
Enable certificate trust list	
Current CTL:	
Ne <u>w</u> Edįt	
OK Cancel <u>H</u> elp	

Figure 4.15. Secure Communications



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,

Account Mappings	×
1-to-1 Many-to-1	
Edit "one to one" mappings. Each individual certificate is mapped into a specific Windows account. You can cl map multiple certificates into the same account, but a separate mapping entry must exist for each.	noose to
Subject	
Mapping Name Windows Account	
O test AUPS-IRM-PHM612\cqo2	
o jakarta ADPS-IRM-PHM612\cqo2	
New Mapping AOPS-IRM-PHM612\cqo2	
- Issuer-	
Edit Map Dejete	
OK Cancel Apply	Help

Figure 4.16. Account Mappings

9. select Add displaying Figure 4.17,

Open		? ×
Look <u>i</u> n	r: 🞯 Desktop 🔽 🕓 🤔 📂 🖽	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer My Network Places lawrenceinterm (1).cer lawrenceinterm.cer swrenceroot.cer newvictorcert4.cer newvictorcert4Interm.cer newvictorcert4Root.cer one.cer phinmsroot.cer root.cer	
My Network Places	File name: lawrenceroot.cer	n
- Haces	Files of type:         Certificate Import Files (".cer,".crt,".spc,".key)         Cancel	:el

Figure 4.17. Open



10. select the **Certificate** used to secure this communication method, click **Open** displaying Figure 4.18,

Map to Account	×
🔽 Enable this m	apping
-Account mappi	ng
When this c automatical	ertificate is presented by a web client and authenticated, the user can y be logged in as a specific Windows user.
Map <u>N</u> ame:	New Mapping
<u>A</u> ccount:	Browse
Password:	
	OK Cancel <u>H</u> elp

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	×
	ОК
Password:	Cancel

Figure 4.19. Confirm Password

12. enter Password for confirmation, click OK, OK displaying Figure 4.20,



ecure Communications
Require secure channel (SSL)
Require <u>1</u> 28-bit encryption
Client certificates
C Ignore client certificates
C Accept client certificates
Require client certificates
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.
Current CTL: New IIS CTL
Ne <u>w</u> Ed <u>i</u> t
OK Cancel <u>H</u> elp

Figure 4.20. Secure Communications

13. check **Enable client certificate trust list**, select **New IIS CTL** from the dropdown list, click **OK** displaying Figure 4.21,



Figure 4.21. Certificate Trust List Wizard

14. click **Next** displaying Figure 4.22,



tificate Trust List Wiza	rd		
Certificates in the CTL			
The certificates listed	in the following table are	currently in t	he CTL.
Current CTL certificate	es:		
Issued To	Issued By		Intended Purposes
		-	
Add from Store	Add from File	Remove	View Certificate
		< Back	Next > Cancel

Figure 4.22. Certificates in the CTL

15. select Add from Store or Add from File displaying Figure 4.23,

Select Certific	ate				? ×
Select the cert	ificates you v	vant to use			
Issued to	Issued by	Intende	Friendly	Expiratio	Location 🔺
root	root	<al ></al >	Certifica	4/16/2016	Personal
root	root	<al ></al >	None	4/16/2016	Trusted
Micros	Microsof	<all></all>	Microsof	5/9/2021	Trusted
Micros	Microsof	<all></all>	Microsof	12/31/2	Trusted
Syma	Symante	<all></all>	None	4/30/2011	Trusted
SDN-CA	SDN-CA	<all></all>	None	7/29/2007	Trusted
MoH o	Mothodz	Control A	Mott ock	2/20/2010	Trusted
	[	ОК	Cancel	<u>⊻</u> iew 0	Certificate

Figure 4.23. Select Certificate

16. select Certificate, click OK displaying Figure 4.24,



ìcate Trust List Wiza	d	
ertificates in the CTL		
The certificates listed	n the following table are curre	ently in the CTL.
<u>C</u> urrent CTL certificate	is:	
Issued To	Issued By	Intended Purposes
root	root	<all></all>
•		
Add from Store	Add from <u>File</u>	nove <u>V</u> iew Certificate
	< Bi	ack Next > Cancel
	<u></u>	

Figure 4.24. Certificate Trust List Wizard

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

lertificate Trust List Wizard 🛛 🔀
Name and Description
The CTL name and description help distinguish it from others CTLs.
Type a friendly name and description for the new CTL. Eriendly name: New IIS CTL Description:
Description: This CTL is to be used as the list of trusted roots for IIS virtual web sites.
< <u>B</u> ack <u>N</u> ext > Cancel

Figure 4.25. Certificate Description

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



Certificate Trust List Wizard		X		
	Completing the Certificate Trust List Wizard			
	You have successfully completed the Certificate Trust List wizard.			
	You selected the following settings:			
Same and	Purpose Client Authentication			
	Identifier {97A7D5BA-71E2-4A6C-9C3F-7BAF86 Validity <none></none>			
	Description This CTL is to be used as the list of tru:			
	< <u>B</u> ack Finish Cano	el		

Figure 4.26. Wizard Complete

19. click Finish displaying Figure 4.27,



Figure 4.27. Wizard Success

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



Secure Communications
Require secure channel (SSL)
Require <u>1</u> 28-bit encryption
Client certificates
C Ignore client certificates
C Accept client certificates
Require client certificates
accounts. This allows access control to resources using Edit
Current CTL: New IIS CTL
Edit
OK Cancel <u>H</u> elp

Figure 4.28. Secure Communications

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

Default Web Site	Properties			? ×	
Web Site Documents	Performance Directory Security	ISAPI Filters	Hom ders   Cu	e Directory	
Authentication	and access control inable anonymous access a uthentication methods for I	nd edit the this resource.	<u> </u>		
□ IP address and	d domain name restrictions irant or deny access to this P addresses or Internet do	; resource using main names,	e Ed <u>i</u> t		
Secure communications Require secure communications and enable client certificates when this resource is accessed.    yiew Certificate  Edit					
	ОК	Cancel	Apply	Help	

Figure 4.29. Default Web Site Properties

22. click **OK** displaying Figure 4.30,



Inheritance Overrides X
The following child nodes also define the value of the "UNCPassword" property, which overrides the value you have just set. Please select from the list below those nodes which should use the new value.
Child Nodes:
iakarta Select All
OK Cancel <u>H</u> elp

Figure 4.30. Inheritance Overrides

23. click Select All, click OK displaying Figure 4.31,



Figure 4.31. Internet Information Services (IIS) Manager

24. right click **Jakarta**, select **Properties**, select the **Directory Security** tab displaying Figure 4.32,



Default Web Site	Properties		? ×				
Web Site Documents	Performance Directory Security	ISAPI Filters HTTP Header	Home Directory s Custom Errors				
Authentication	and access control nable anonymous access ar uthentication methods for t	nd edit the his resource.	Edit				
IP address and G	IP address and domain name restrictions Grant or deny access to this resource using IP addresses or Internet domain names. Edįt						
Secure communications Require secure communications and enable client certificates when this resource is accessed.  Server Certificate  Edit  Edit							
	ок	Cancel	Apply Help				

Figure 4.32. Authentication and Access Control

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

Authentication Me	thods				×		
Use the following Windows user account for anonymous access:							
User name:	User name: IUSR_AOPS-IRM-PHM612 Browse						
Password:	•••••						
Authenticated ac	cess						
For the following are required whe - anonyn - access	For the following authentication methods, user name and password are required when: - anonymous access is disabled, or - access is restricted using NTFS access control lists						
Integrated W	'i <u>n</u> dows au	ithenticatio	n				
Basic authent	ication fo	or Windows assword is :	s domain se sent in clea	rvers ir text)			
.NET Passpor	t au <u>t</u> henti	cation					
Default <u>d</u> omain	: [				Select		
<u>R</u> ealm:					S <u>e</u> lect		
0	к	Canc		Help	>		





26. deselect all Check Boxes, click OK displaying Figure 4.34, and

jakarta Properties	? ×
Virtual Directory   Documents   Directory Security   HTTP	Headers Custom Errors
Authentication and access control	
authentication methods for this resource.	Edit
IP address and domain name restrictions	
Grant or deny access to this resource usin IP addresses or Internet domain names.	g
	Edit
Secure communications	
Require secure communications and enable client certificates when this resource is accessed.	Server Certificate View Certificate Edit
	Арріу Неір

Figure 4.34. Jakarta Properties

27. click **OK**.

## 4.3 Test One to One Mapping

open Internet Browser, type URL <u>https://localhost/receiver/receivefile</u>, select Go displaying Figure 4.35,



Figure 4.35. Security Alert

2. select **Yes** displaying Figure 4.36,



Choose a	digital certificate		?×
	ation The Web site you want t identification. Please cho	o view requests ose a certificate,	
	Name phinms Lawrence Loftley	Issuer root CDC Secure Data Network CA	
	Ma	re Info View Certificate.	

Figure 4.36. Choose a Digital Certificate

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



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.





省 The page requires a valid SSL client certificate - Microsoft Internet 🔳 🗖	$\mathbf{X}$			
File Edit View Favorites Tools Help				
G Back 🔹 🕥 🔹 😰 🏠 🔎 Search 👷 Favorites 🚱 🔗 - 🌺	»			
Address 🕘 https://158.111.1.251/receiver/receivefile 🔽 🔁 Go 🛛 Links 🧔 SnagIt 🖹 🔮	<b>1</b>			
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:				
<ul> <li>Contact the site administrator to establish client certificate permissions.</li> <li>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.)</li> <li>Change your client certificate and click the <u>Refresh</u> button, if appropriate.</li> </ul>				
the Web server.				
Internet Information Services (IIS)	~			
😂 🔮 Internet				

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:\OpenssI,
- 2. navigate to <u>http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7/</u>, displaying Figure 5.1,

🗈 http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7/ - Microsoft Internet Explorer 📃 🗖 🔀						
File Edit Vi	File Edit View Favorites Tools Help 🥂					
🚱 Back 🔹 🕥 🖌 😰 🏠 🔎 Search 🌟 Favorites 🚱 🔗 - 🌺 🔟 - 🛄 🎇 🖓						
Address ど ht	Address 🔕 http://www.stunnel.org/download/stunnel/win32/openssi-0.9.7/					
Note: The files herein are for archival purposes only. All versions of OpenSSL before 0.9.6k and 0.9.7c contain a number of buffer overflows that can open you up to attack. See <a href="http://www.openssl.org/news/secadv_20020730.txt">http://www.openssl.org/news/secadv_20020730.txt</a> and <a href="http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm">http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm</a> for more information.						
Bytes	Т	imestamp	Filename	Туре	=	
1379459	Jan 12	14:30 2003	libeay32.dll	MS Windows PE Intel 80386 console DLL		
254	Jan 12	14:30 2003	libeay32.dll.asc	PGP armored data		
476329	Jan 12	14:30 2003	<u>libss132.d11</u>	MS Windows PE Intel 80386 console DLL		
254	Jan 12	14:30 2003	libss132.dll.asc	PGP armored data		
1089536	Jan 12	14:30 2003	openssl.exe	MS Windows PE Intel 80386 console executable not relocatab		
254	Jan 12	14:30 2003	openssl.exe.asc	PGP armored data	le	
				for almored adda	le	
1170508	Jan 12	14:30 2003	openssl.zip	Zip archive data, at least v2.0 to extract	1e	
<mark>1170508</mark> 254	<mark>Jan 12</mark> Jan 12	14:30 2003 14:30 2003	openssl.zip openssl.zip.asc	Zip archive data, at least v2.0 to extract PGP armored data	le 🗸	
1170508 254	<mark>Jan 12</mark> Jan 12	14:30 2003 14:30 2003	openssl.zip openssl.zip.asc	Zip archive data, at least v2.0 to extract PGP armored data	le V	

Figure 5.1. Openssl.exe

3. click openssl.zip, displaying Figure 5.2,



File Dov	vnload 🛛 🔀			
Do you	u want to open or save this file?			
Q	Name: openssl.zip Type: WinZip File, 1.11 MB From: www.stunnel.org			
	Open Save Cancel			
Always ask before opening this type of file				
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>				

Figure 5.2. Openssl File Download

4. select **Open**, displaying Figure 5.3,



Figure 5.3. WinZip Openssl

5. select Extract displaying Figure 5.4, and



Extract		? 🛛
Extract to:	Folders/drives:	Extract
C:\Openssl	E-Cal Disk (C:)	Cancel
Selected files     All files     Files:	Documents and S	Help
Overwrite existing files	<mark>- Openssl</mark> ⊕	
<ul> <li>Skip older files</li> <li>Use folder names</li> </ul>	Temp	New Folder

Figure 5.4. Extract Files

6. navigate to the **OpenssI** 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.

🗀 C:\Openssl		
File Edit View Favorites	Tools Help	<b>1</b>
🕝 Back 🔹 🕥 🕤 🏂	🔎 Search 🎼 Folders 🕼 🎲 🗙 🍤	•
Address 🛅 C:\Openssl		💌 🄁 Go
Name	Size Type Date Mod	dified 🔺 🗌 🔼
🔊 libeay32.dll	1,348 KB Application Extension 12/31/200	i2 11:54 AM 🛛 😑
🔊 libssl32.dll	466 KB Application Extension 12/31/200	12 11:54 AM 🗧
📰 openssi.exe	1,064 KB Application 12/31/200	2 11:54 AM
📕 openssl	10 KB SpeedDial 6/1/2006 :	12:12 PM 🛛 💌

Figure 5.5. Openssl Files

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 <u>phintech@cdc.gov</u>.

## 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

 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

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.

FIELDS	EXAMPLES
Country Name:	PL, UK, US, CA
State or Province Name:	Illinois, Ontario
Locality:	Chicago, Toronto
Organization Name:	Bill's Meats, Acme Anvils
Organizational Unit Name:	Ecommerce Division
Common Name (FQDN)	www.example.com
Email address	test@yahoo.com



## Table 1. Distinguished Name Fields Examples



Figure 5.8. Distinguished Name Fields

4. close the window.

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

😂 C: \openssl				
File Edit View Favorites T	ools Help			an 1997
🕞 Back 👻 🅥 👻 🏂	🔎 Search 🛛 🎼 F	olders 🕼 🎲	× 🍤 💷	
Address 🗀 C:\openssl				💌 🄁 Go
Name 🔺	Size	Туре	Date Modified	
🔊 libeay32.dll	1,348 KB	Application Extension	12/31/2002 11:54 AM	
🔊 libssl32.dll	466 KB	Application Extension	12/31/2002 11:54 AM	
📕 openssi	10 KB	SpeedDial	6/1/2006 12:12 PM	
📰 openssi.exe	1,064 KB	Application	12/31/2002 11:54 AM	
🖬 .rnd	1 KB	RND File	8/18/2006 8:11 AM	
🗩 renamekey.pem	1 KB	PEM File	8/18/2006 8:15 AM	
renamecsr.pem	2 KB	PEM File	8/18/2006 8:15 AM	

Figure 5.9. Self-Signed Certificates

## 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,
- select Start > Programs > Stunnel, Edit Stunnel.conf displaying the left screen in Figure 5.10,



🕞 stunnel.conf - Notepad	
Elle Edit Format View Help	
; Sample stunnel configuration file by Michal Trojnara 2002-2006 ; Some options used here may not be adequate for your particular configuration	<b>^</b>
: Certificate/Key is needed in server mode and optional in client mode : The default certificate is provided only for testing and should not ; be used in a production environment cert = phinmscettreq.pem key = phinmspytk.pem	
: Some performance tunings socket = 1:TCP_NOBELAY=1 socket = r:TCP_NOBELAY=1	
; Workaround for Eudora bug ;options = DONT_INSERT_EMPTY_FRAGMENTS	
: Authentication stuff :verify = 2 : Don't forget to c_rehash CApath :CApath = certs : It's often easier to use cAfile :CAfile = certs.pem : Don't forget to c_rehash CRLpath :CRLpath = crls : Alternative]y you can use CRLfile :CRLfile = crls.pem	
: Some debugging stuff useful for troubleshooting debug = 7 output = stunnel.log	
; Use it for client mode client = yes	
; Service-level configuration	
:[pop3s] :accept = 995 :connect = 110	
:[imaps] =accept = 993 : connect = 143	
:[ssmtp] :accept = 465 :connect = 25	
[https] accept = 8009 connect = 158.111.1.249:7002 ;TIMEOUTClose = 0	
; vim:ft=dosini	-
	▶ //.

Figure 5.10. Stunnel Configuration File

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,



Figure 5.11. Save Stunnel.conf File

- 5. select Yes,
- 6. select Start > Programs > Stunnel, Service stop, and
- 7. select Start > Programs > Stunnel, Service start on both servers.