Implementation Guide

Public Health Information Network Messaging System (PHINMS)

Version 2.6.00

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

August 16, 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 firewalls, 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 using Electronic Business Extensible Markup Language (ebxml) technology.

The PHINMS Implementation Guide provides instructions for installing and configuring the PHINMS software.

REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0	Michele Bowman	Mar 1, 2006	Created version 1.0.0.
2.6.00	Rajeev Seenappa	Aug 1, 2006	Provided input to version 2.6.0.
2.6.00	Travis Mayo	Aug 1, 2006	Provided input to version 2.6.0.
2.6.00	Wendy Fama	Aug 11, 2006	Updated version 2.6.0.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYM LIST

CDC	Centers for Disease Control and Prevention
CPA	Collaboration Protocol Agreement
CPS	Certification Practice Statement
ebxml	Electronic Business Extensible Markup Language
FAQs	Frequently Asked Questions
FTP	File Transfer Protocol
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
PC	Personal Computer
PartyID	Party Identifier
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System
PHINMSG	Public Health Information Network Messaging
RDBMS	Relational Database Management System
SDN	Secure Data Network
SQL	Structured Query Language
TLS	Transport Layer Security
TransportQ	Transport Queue
URL	Uniform Resource Locator
WorkerQ	Worker Queue

1.0 INTRODUCTION

The Public Health Information Network Messaging System (PHINMS) Implementation Guide will assist with the installation, configuration, and upgrade of the software. Documentation is continually updated. Ensure the most recent versions are referenced from the PHINMS website at www.cdc.gov/phin/phinms.

The PHINMS Implementation Guide focuses on using PHINMS to send/receive messages from the CDC. When PHINMS is used to send/receive messages from other organizations, then some of the CDC-specific information may not apply (like how to obtain a Digital certificate and PartyID from the CDC).

1.1 PHINMS Topics

- **Quick How Tos:** A streamlined list and details used to install and run the PHINMS software. Navigate to the PHINMS website, click the PHINMS Installation link, and then click on the Quick How Tos link. The steps are listed in order and should be reviewed prior to using the other topics.
- **Release Notes:** The Release Notes corresponds with the version of software being installed. Proceed to the Release Notes and Installation Guide section on the PHINMS website, click the PHINMS Support link, and then click on the Release Notes and Installation Guide link.
- **Implementation Guide:** The Implementation Guide is continually updated. Ensure the latest copy is referenced by retrieving it from the PHINMS website, click the PHINMS Support link, click on the Release Notes, and Installation Guides link.
- **Online Help:** The PHINMS online help along with the Implementation Guide provides screen shots and step-by-step instructions for configuring and using the PHINMS software. Navigate to PHINMS website, click the PHINMS Support link, and click on the PHINMS Software Online Help link. The online help launches in a new browser. The Contents navigation provides procedures needed.
- **FAQs:** The list of Frequently Asked Questions (FAQs) stored on the PHINMS website answers many questions users have submitted. The PHINMS team welcomes questions, suggestions, and/or comments.

Note: Additional information on all Sections within the PHINMS Implementation Guide can be found on the PHINMS website. The interactive, multimedia online help offers a convenient step-by-step instructions, vivid graphics, and screen captures to speed the training time. Detailed information about PHINMS can be located on the web site in the PHINMS Technical Reference Guide.

1.2 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 home page.

2.0 INSTALL PHINMS 2.6.00

The installation of PHINMS Version 2.6.00 requires the following:

- a Java application server used for all three web-based PHINMS components, the sender, receive, and console,
- one of the following operating systems:
  - Windows 2000,
  - Windows XP,
  - Windows 2003,
  - Linux Red Hat 8.0 or above,
  - or Solaris 8 or above,
- 250M of disk space,
- 512M of memory, and
- local administrator privileges.

Ensure all the correct ports, which may be 5088, 443, and 389 are open on the local host and on the firewall.

Once the requirements above have been met, proceed to Section 2.1. Section 2.1 and Section 2.2 can be accomplished simultaneously.

2.1 Request PartyID

A Party Identifier (PartyID) is required for each organization and every organization sending and receiving messages. A PartyID uniquely identifies a PHINMS installation, also called an instance or node. The PartyID is included with every message informing the recipient of the originator.

Complete the PHINMS software request located at http://www.cdc.gov/phin/software-solutions/phinms/how.html#h-12.2. Information is required about the organization(s) sending and receiving messages. When complete, the Public Health Information Network (PHIN) Deployment Team will email the PartyID to the requestor. Contact the PHIN Help Desk regarding any issues encountered with the PartyID, sending an email to PHINTech@cdc.gov or calling 1-800-532-9929, option 2.

Setting up the PHINMS software requires the PartyID which is permanent and not required to be stored for later use. The PartyID is stored as long as the PHINMS instance for sending messages to partners is being used by the PHINMS application.

Note: If there is a need to install PHINMS at more than one site or to install more than one PHINMS installation at the same site, a PartyID is required for each installation. This is not the case with DPIT where only one instance will be sending to the CDC at a time, but two instances are installed during deployment.

The recommended way to install PHINMS 2.6.00 is to download the application from the File Transport Site (FTP) site. If however, problems are encountered with the download, an install disk may be requested from the PHINMS Deployment Team.

2.2 Request Digital ID Certificate

Administrative privileges are required on the personal computer (PC) before applying for the Digital ID Certificate. Administrative privileges are automatic for Windows 98 users. Determine administrative privileges for Windows XP, 2000, or NT by completing the following steps:

1. select Start > Control Panel > Administrative Tools > Computer Management,
2. expand Local Users and Groups, select Groups,
3. open Administrators Group, and
4. verify the user ID appears in the Members panel under the General tab.

Contact IT Support to provide privileges if the user ID does not appear. Centers for Disease Control and Prevention (CDC) users should contact IT Support at http://itsupport/oaa/login.jsp.

The following system requirements must be met before downloading the Digital ID Certificate:

- Intel-based system with a 486 CPU or greater,
- Windows 98, Windows NT 4.0, or greater,
- internet connectivity,
- Internet Explorer 5.x, Netscape Communicator 6.x, or greater, and
- browser cipher strength - 128 bit or greater.

2.2.1 Apply for Digital ID Certificate

Contact the PHIN helpdesk at 1-800-532-9929, option 6, to obtain a password.

When requesting a Digital ID Certificate, complete the following steps:

5. navigate to http://ca.cdc.gov displaying Figure 2.1,

Figure 2.1. Enter Enrollment Password

6. enter the enrollment password, click **Accept**, displaying system requirements and Digital ID Certificate background information,
7. select the **here** link at the bottom of the screen which provides complete terms for the VeriSign Certification Practice Statement (CPS) and the Digital ID Subscriber Agreement,
8. click on Subscriber Agreements, Digital ID Subscriber Agreement, read the Client ID Subscriber,
9. click the browser's **Back** button three (3) times to return to the CDC Digital ID Enrollment page,
10. click **Enroll** located at the bottom of the screen displaying Figure 2.2,

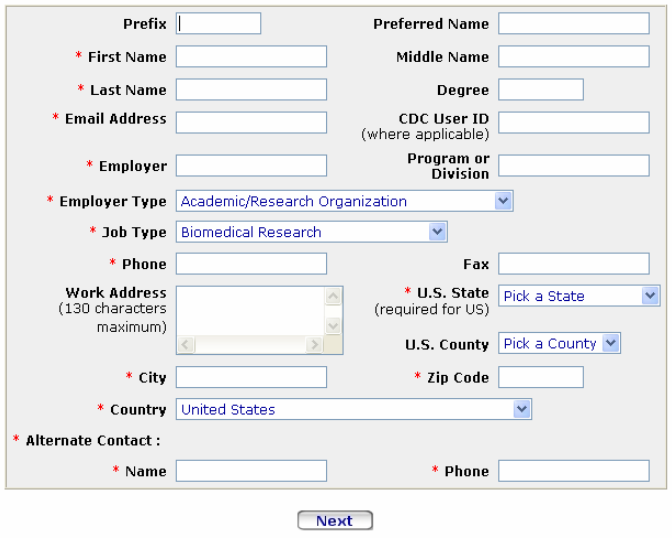

Figure 2.2. Personal Information Screen

11. complete the required fields, click **Next** displaying Figure 2.3,

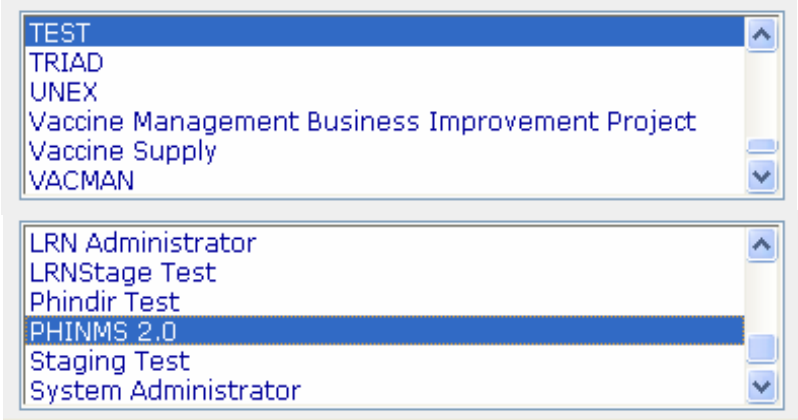

Figure 2.3. Select a Program and Activities

12. select **Test**, **PHINMS 2.0** (linked to Version 2.6.00), click **Next** displaying Figure 2.4, and

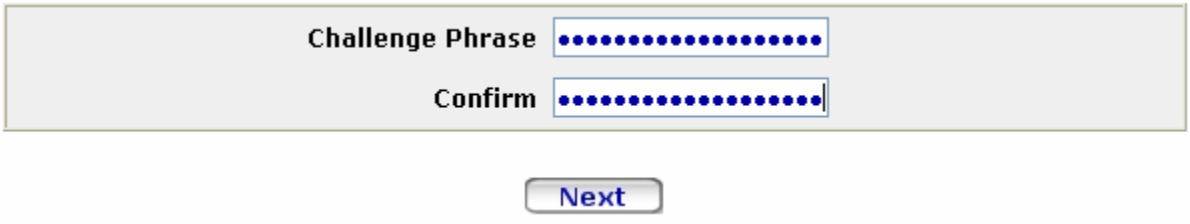

Figure 2.4. Digital ID Certificate Challenge Phrase

13. enter a challenge phrase (guidelines below), click **Next** displaying Figure 2.5.

Note: The Secure Data Network (SDN) environment will indicate special characters are required in the challenge phrase during the enrollment process. However, the PHINMS software requires the user to refrain from using special characters in the challenge phrase.

Create the challenge phrase using the following guidelines:

- contains at least eight (8) characters in length,
- contains only English letters and numbers,
- contains at least four (4) different numbers or letters,
- can not contain any part of the user name or email address,
- can not spell a word unless the word has three (3) or more numbers or symbols before, after, or within the word,
- can not contain more than two consecutive characters, and
- can not contain special characters such as "+, <, &, @, etc" which prevents the user access to the software.

Note: The challenge phrase is case-sensitive. Safely store the challenge phrase for security purposes. The challenge phrase is required each time the SDN is accessed and is different from the password used to log onto the SDN enrollment site. The challenge phrase along with the Digital ID Certificate is used to authenticate a SDN user.

Figure 2.5. Digital ID Certificate Request Received

2.2.2 Approved Digital ID Certificate

Approval notification may take anywhere from 12 to 72 hours via email with instructions similar to those shown in Figure 2.6. Follow the instructions sent in the email before proceeding to Section 2.2.3.

From: CDC SDN Support
Sent: Friday, May 19, 2006 4:36 PM
To: Requestor's Name
Subject: SDN Enrollment Request

The administrator has approved your SDN enrollment request. Please review these instructions with your local IT staff to insure your certificate is installed properly.

1) Check to verify that the version of Internet Explorer is 5.5 or higher (6.0 recommended), or that the version of Netscape is 6.0 or higher and that the cipher strength is 128-bit.

2) For Windows 2000 or XP systems using Internet Explorer, whoever installs the certificate MUST have administrative rights on the computer to which the certificate is being installed. If Netscape is the browser, administrative rights may not be necessary, but the certificate must be downloaded and installed manually using "Import".

3) To retrieve the certificate, you will be asked to enter the challenge phrase set during the most recent application process. If the the phrase cannot be remembered or is not working, you may need to request a new certificate.

4) During installation, a box may pop up asking for permission to install and run Verisign's Import Control. Select Yes, as this is a vital plug-in Verisign needs to install the certificate.

If you do not have local IT support, or a problem occurs during the installation process, reply to this email to contact CDC SDN Support or call 1-800-532-9929, option 1 for assistance and further instructions. If there are any questions about the installation procedure, please contact CDC SDN Support BEFORE attempting the installation.

It is strongly recommended that users make a backup copy of the certificate on a diskette or network drive that is separate from the computer on which the certificate is installed. It is also recommended that this be done while the user or administrator is logged in during the session in which the certificate is installed. For instructions, contact CDC SDN Support before attempting the installation.

To obtain your digital certificate go to the following URL:

https://ca.cdc.gov/sdncode/sdnapp/servlet/CertServlet?usertoken=1ddc0896940b36c2726b95eb619e13dc

Figure 2.6. Digital ID Certificate Approval Email

2.2.3 Download Digital ID Certificate

In order for a successful download of the Digital ID Certificate insure the following:

- Active X is enabled,
- all “Pop-Up blockers are turned off, including blockers similar to Yahoo or Google,

- enable Transport Layer Security (TLS) 1.0, and
- the user downloading the Digital ID Certificate has administrative rights.

Note: Proceed to Section 2.2.3.1 to download the Digital ID Certificate using Internet Explorer and Section 2.2.3.2 using Netscape.

Complete the following steps before proceeding to Section 2.2.3.1 or 2.2.3.2,

14. open **Browser**, select **Tools**, **Internet Options** displaying Figure 2.7,

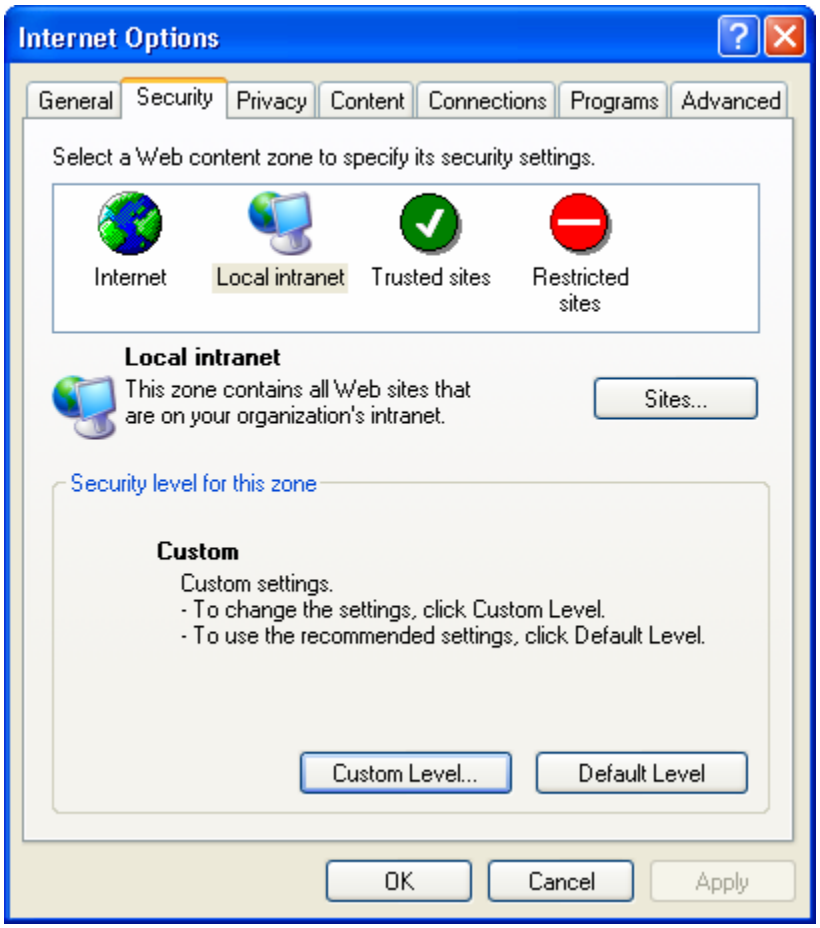

Figure 2.7. Internet Options

15. select the **Security** tab, click **Custom Level**, displaying Figure 2.8,

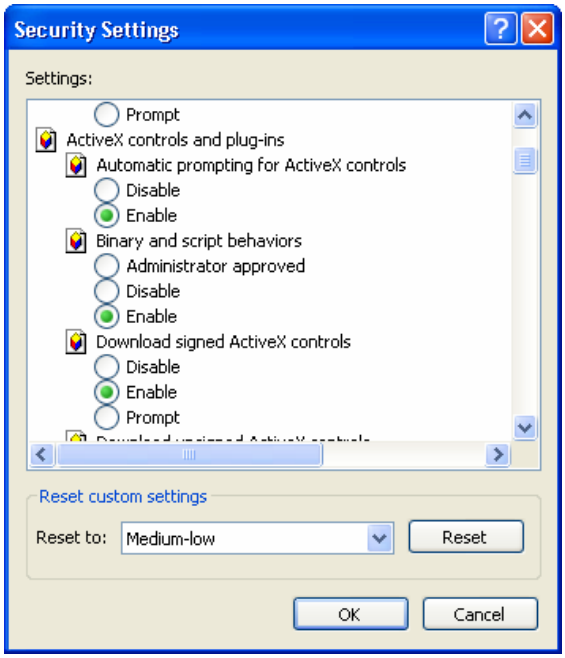

Figure 2.8. Security Settings

16. expand ActiveX controls and plug-ins, select **Enable** Automatic prompting for ActiveX controls, select **Enable** Download signed ActiveX controls, click **OK**, returning to the Browser,
17. select the Advanced tab, displaying Figure 2.9,

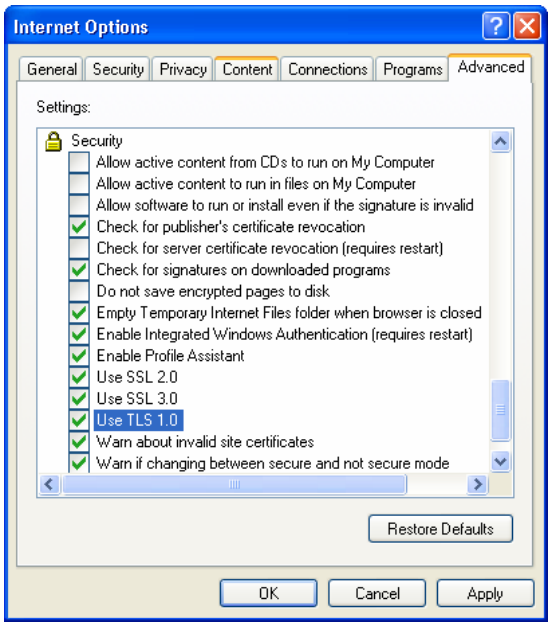

Figure 2.9. Advanced Internet Options

18. scroll down to Security, select **Use TLS 1.0**, click **Apply**, click **OK**, returning to the Browser, and
19. select Tools, Pop-up Blocker, Turn Off Pop-up Blocker,

2.2.3.1 Internet Explorer Download

When the Digital ID Certificate approved has been given, complete the following steps:

Note: The steps below have been documented using Internet Explorer version 6.0.

20. navigate to the link provided in the email displaying Figure 2.10,

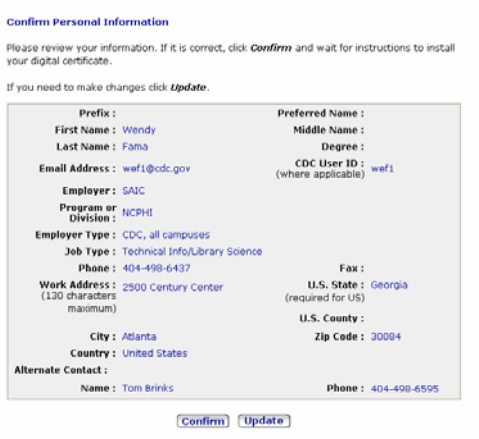

Figure 2.10. Internet Explorer Confirm Personal Information

21. confirm personal information is correct. If correct, click **Confirm**, if not click **Update** displaying Figure 2.11,

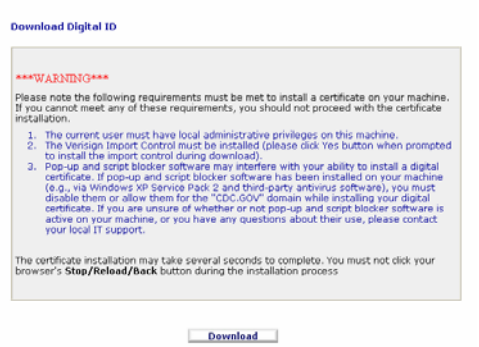

Figure 2.11. Internet Explorer Download Digital ID

22. click **Download** displaying Figure 2.12,

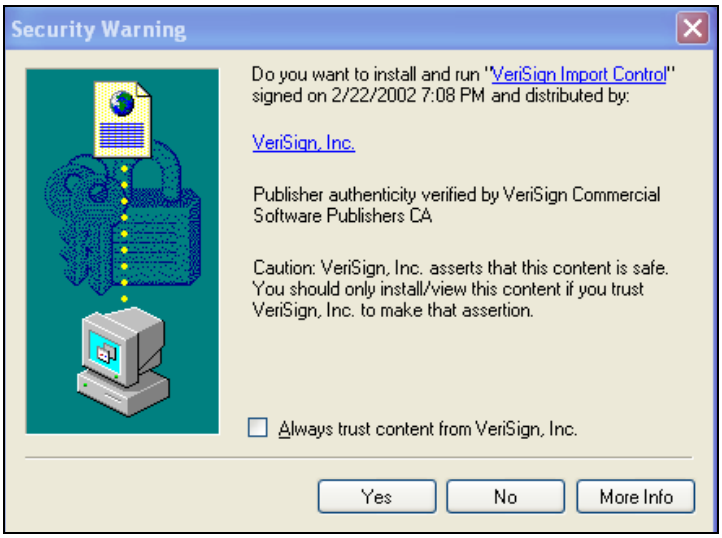

Figure 2.12. Internet Explorer Security Warning

23. click **Yes** displaying Figure 2.13, and

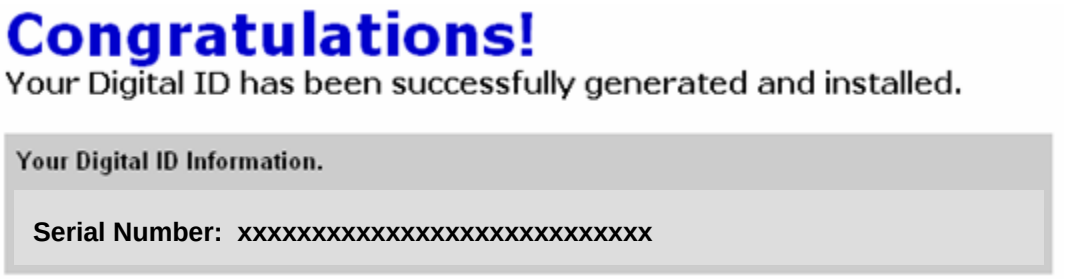

Figure 2.13. Internet Explorer Successful Digital ID Certification Download

24. proceed to Section 2.3.

2.2.3.2 Netscape Download

The Netscape Digital ID Certificate master password needs to be changed before the installation can occur. It is recommended to change the master password to be exactly the same as the challenge phrase. Complete the steps listed below to change the master password.

25. select **Tools**, **Options** from the Netscape browser, select **Advanced** displaying Figure 2.14,

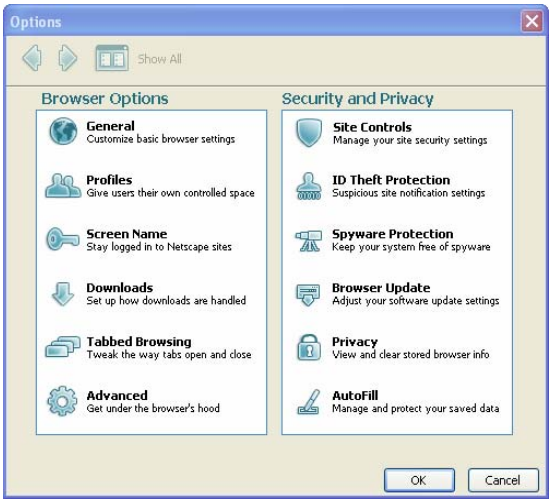

Figure 2.14. Netscape Options

26. select **Advanced** displaying Figure 2.15,

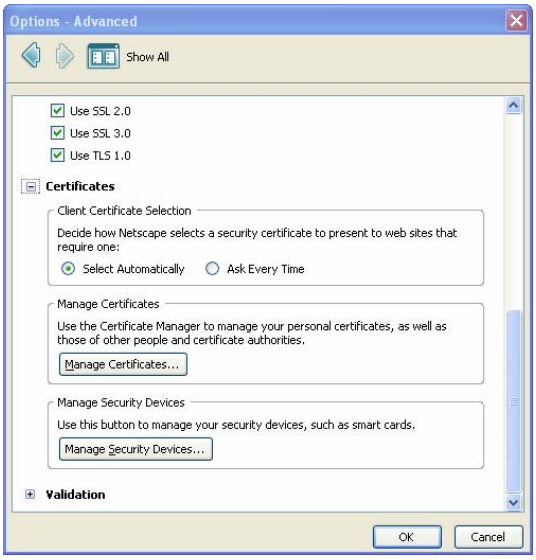

Figure 2.15. Netscape Options - Advanced

27. scroll down and click **Manage Certificates…**displaying Figure 2.16,

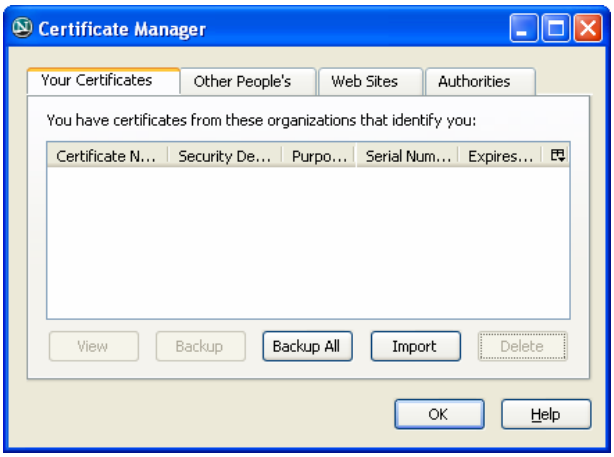

Figure 2.16. Netscape Certificate Manager

28. click **Import** from the **Your Certificates** tab displaying Figure 2.17,

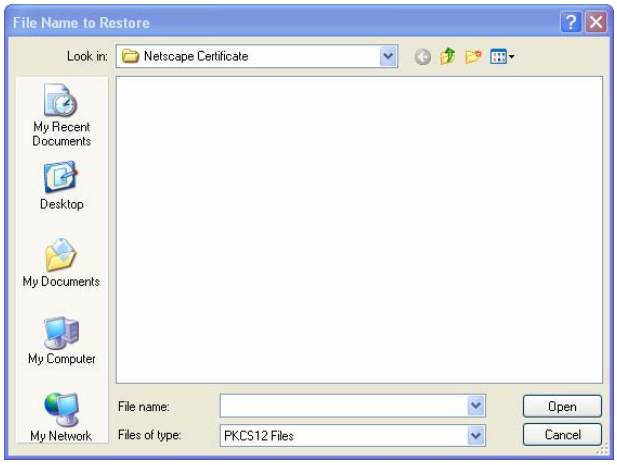

Figure 2.17. Netscape File Name to Restore

29. navigate to the file through **Look in**, select **sdncert**, click **Open** displaying Prompt, enter the **master password** (the challenge phrase is recommended) displaying Figure 2.18,

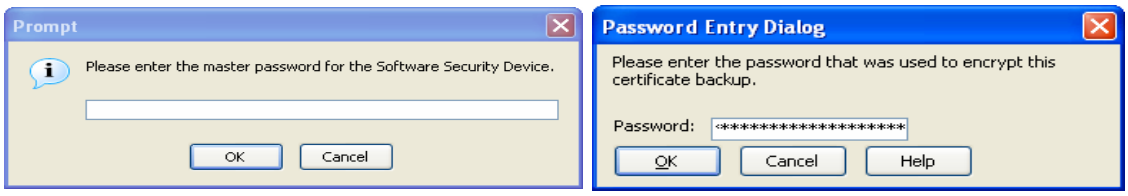

Figure 2.18. Netscape Prompt and Password Entry Dialog

30. enter the **master password**, click **OK** displaying Figure 2.19, and

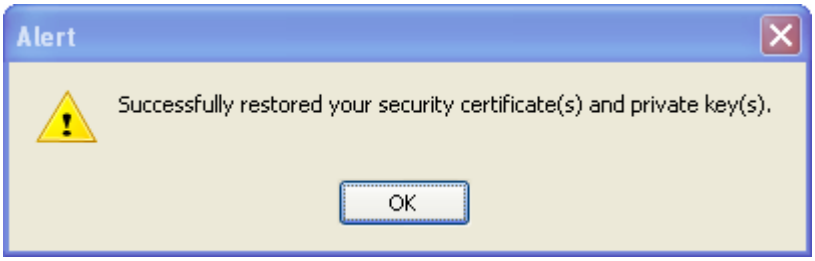

Figure 2.19. Netscape Alert

31. select **OK**, **OK**, close the browser.

When the Digital ID Certificate approved has been given, complete the following steps:

Note: The steps below have been documented using Netscape version 8.1.

32. navigate to the link provided in the email displaying Figure 2.20,

Figure 2.20. Netscape Confirm Personal Information

33. click **Confirm** if correct displaying Figure 2.21, **Update** if not,

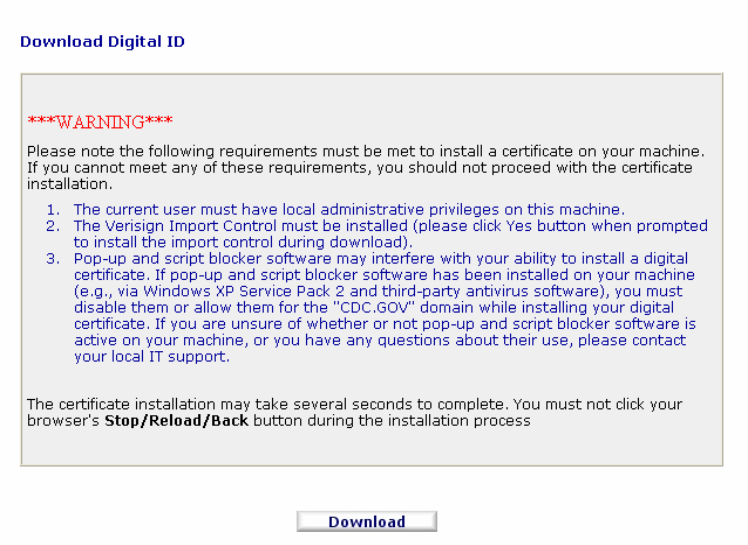

Figure 2.21. Netscape Download Digital ID

34. click **Download** displaying Figure 2.22,

Note: Store the Digital ID Certificate information which will be used for installation. It is extremely important to verify the information captured is correct, remembering the password is lengthy and case sensitive.

35. capture the following information:
    - Located in this directory,
    - In the file named, and
    - The password is.

Figure 2.22. Netscape Install the Encryption Digital ID

36. click **Download P12 File** displaying Figure 2.23,

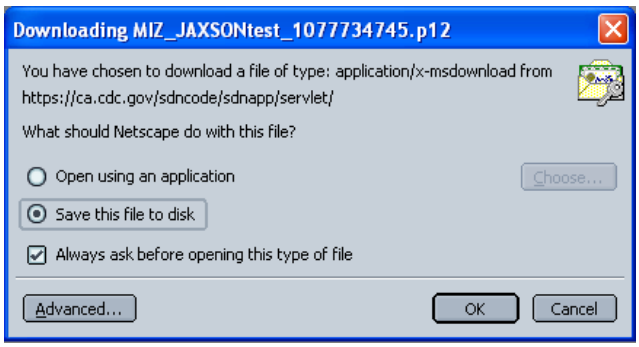

Figure 2.23. Netscape Downloading MIZ_JAXSONtest_1077734745.p12

37. select Save this file to disk, Always ask before opening this type of file, click OK displaying Figure 2.24, and

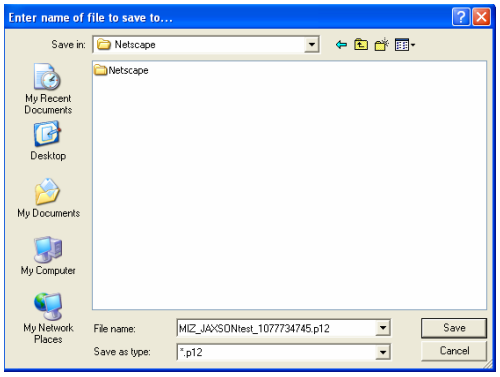

Figure 2.24. Netscape Enter Name of File to Save

38. click **Save**, successfully downloading the Digital ID Certificate on the PC.

2.3 Backup Digital ID Certification

Digital ID Certificates are expensive are paid with federal tax dollars. Minimize the cost of replacing certificates by creating a copy of the Digital ID Certificate also referred to as backing up or exporting.

The procedure to make a copy of the Digital ID Certificate depends on the type of browser used. If Internet Explorer version 6.0 is used, follow the steps in Section 2.3.1, and if Netscape version 8.1 is used, follow the steps in Section 2.3.2.

2.3.1 Backup Internet Explorer Digital ID Certificate

Open an Internet Explorer browser and do the following:

39. select Start > All Programs > Internet Explorer,
40. select **Tools**, **Internet Options**, **Content** tab displaying Figure 2.25,

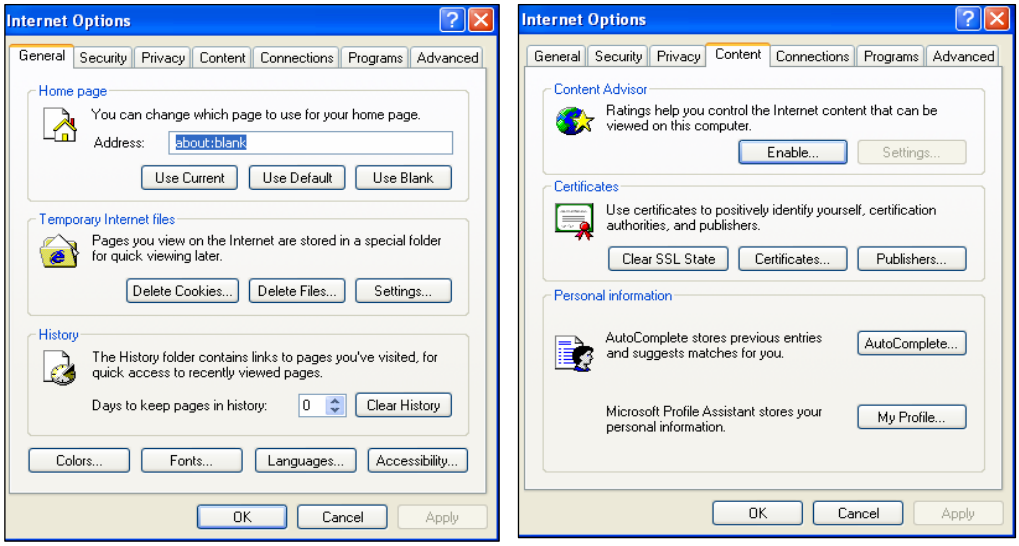

Figure 2.25. Internet Explorer Internet Options

41. click **Certificates** displaying Figure 2.26,

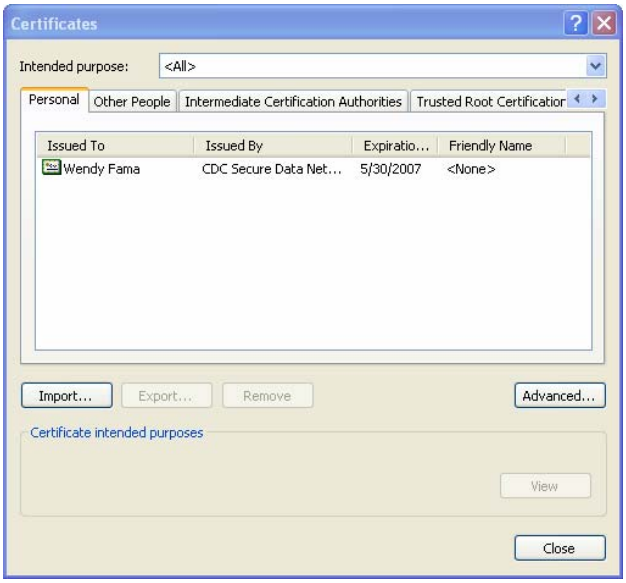

Figure 2.26. Internet Explorer Certificates Dialog Box

42. select the certificate with the appropriate date and issuer, click **Export** displaying Figure 2.27,

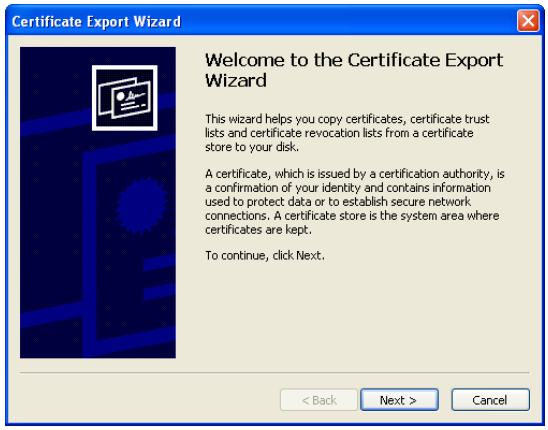

Figure 2.27. Internet Explorer Certificate Export Wizard

43. click **Next** displaying Figure 2.28,

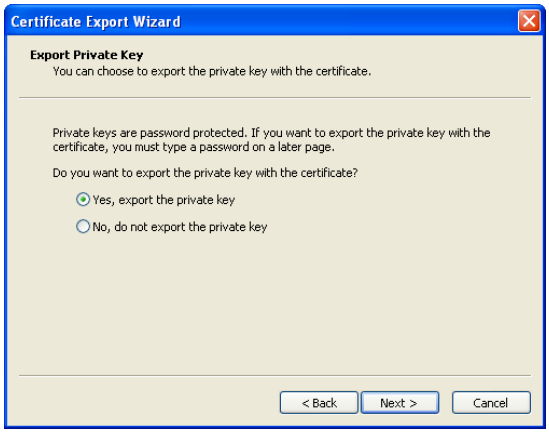

Figure 2.28. Internet Explorer Export Private Key

44. select the **Yes, export the private key**, click **Next** displaying Figure 2.29,

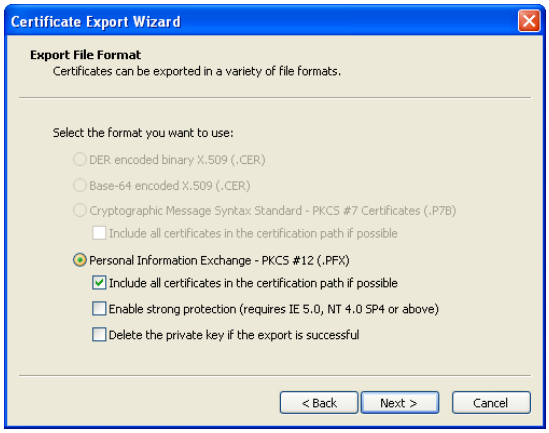

Figure 2.29. Internet Explorer Export File Format

45. select Personal Information Exchange - PKCS #12 (.PFX), check Include all certificates in the certification path if possible, uncheck Enable strong protection, uncheck Delete the private key if the export is successful, click Next displaying Figure 2.30,

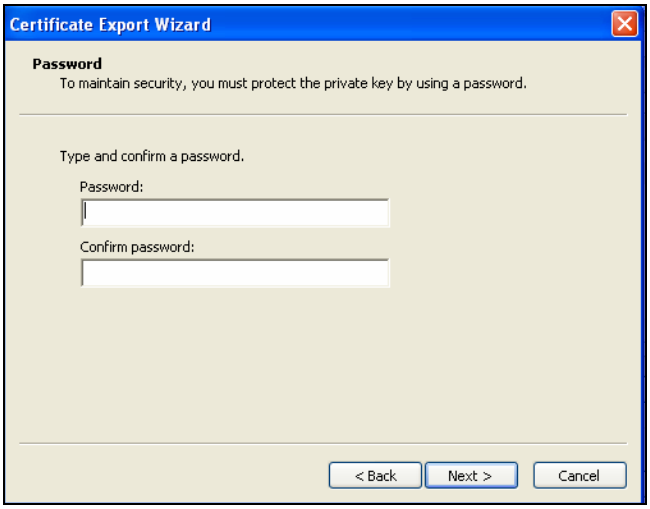

Figure 2.30. Internet Explorer Password

46. create a password, confirm the password (the challenge phrase used earlier is recommended), safely store the password, click **Next** displaying Figure 2.31,

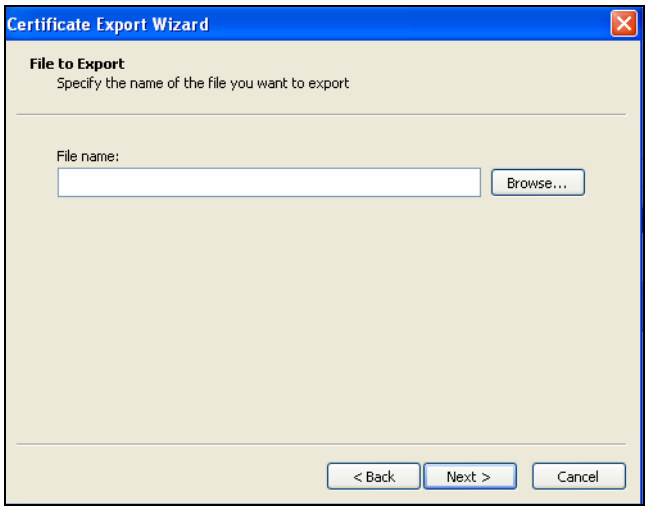

Figure 2.31. Internet Explorer File to Export

47. click **Browse** displaying Figure 2.32,

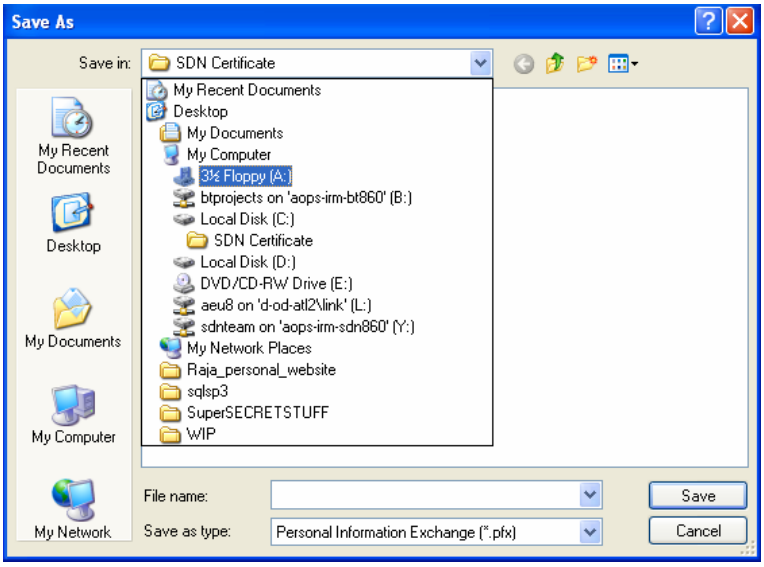

Figure 2.32. Internet Explorer Save As

48. navigate to a floppy, CD, or shared drive, type **sdncert** in the File name field at the bottom of the Save As dialog box, click **Save** displaying Figure 2.33,

Note: Do not store the copy of the Digital ID Certificate on a local drive.

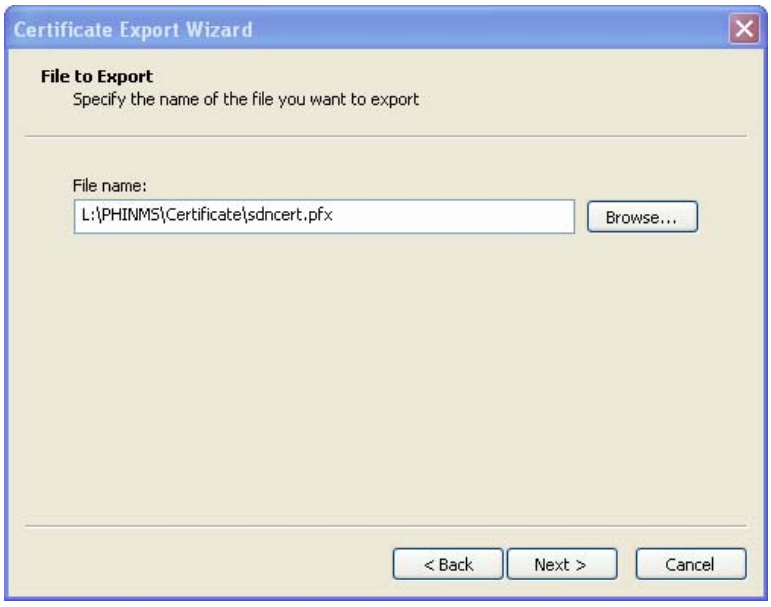

Figure 2.33. Internet Explorer Location of Digital ID Certification

49. the path of the cert is displayed, click **Next**, click **Finish** displaying Figure 2.34, and

Figure 2.34. Internet Explorer Successful Export

50. click **OK**, **Close**, **OK**.

If the Digital ID Certificate was copied to an external drive, label it SDN Digital ID Certificate and store it in a safe and secure place, keeping the passwords and the Digital ID Certificate separate.

2.3.2 Backup Netscape Digital ID Certificate

Open a Netscape browser and do the following:

51. select Start > All Programs > Netscape,
52. select **Menu** displaying Figure 2.35,

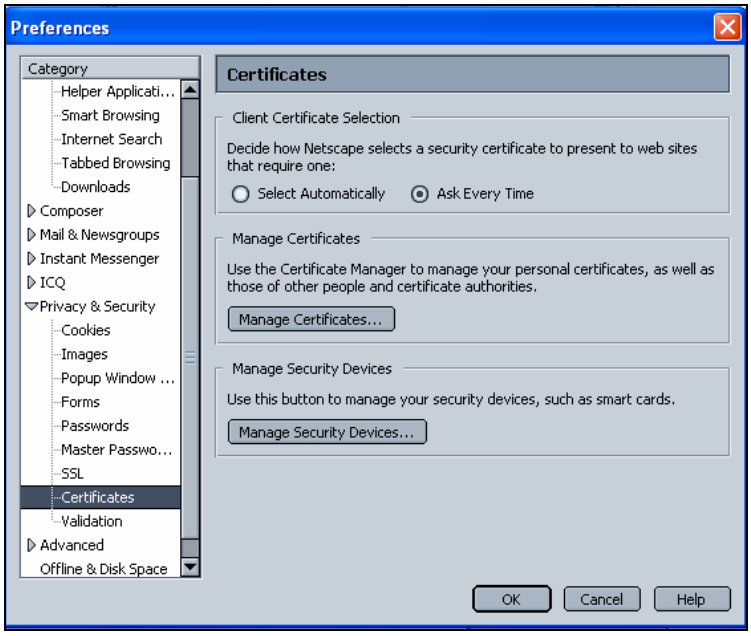

Figure 2.35. Netscape Preferences

53. click **Privacy & Security**, select **Certificates** under the Category heading, click **Manage Certificates** displaying Figure 2.36,

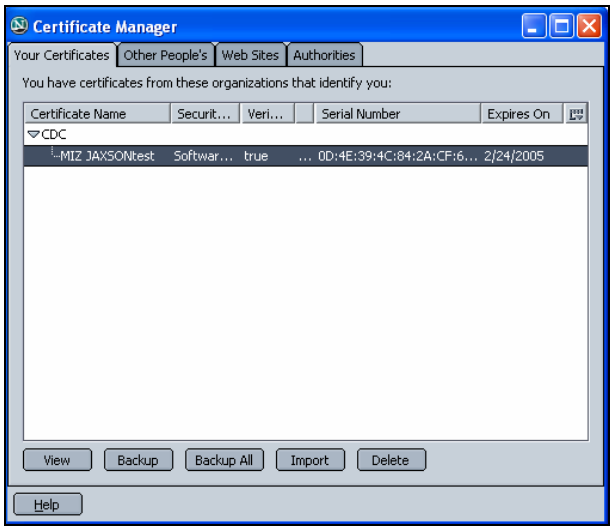

Figure 2.36. Netscape Certificate Manager

54. select the certificate, click **Backup** displaying Figure 2.37,

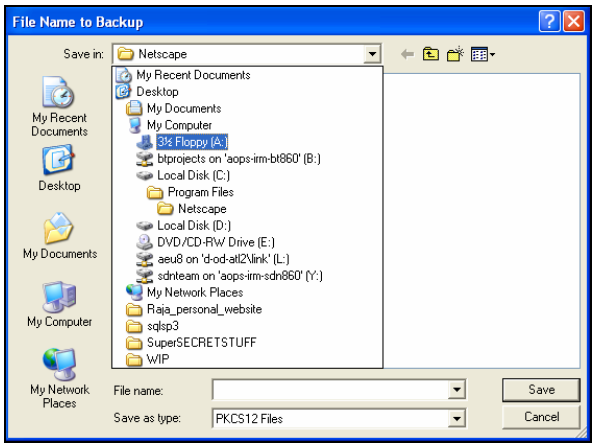

Figure 2.37. Netscape File Name to Backup

55. navigate to a floppy, CD, or shared drive, type **sdncert** in the File name field at the bottom of the Save As dialog box, click **Save** displaying Figure 2.38,

Note: Do not store the copy of the Digital ID Certificate on a local drive.

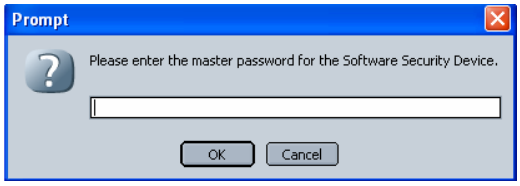

Figure 2.38. Netscape Prompt

56. enter the **master password** (recommendation is to use the challenge phrase) for the Software Security Device, click **OK** displaying Figure 2.39,

Figure 2.39. Netscape Choose a Certificate Backup Password

57. enter the **certificate backup password** in both fields (recommendation is to use the challenge phrase) keeping it in a safe, secure place, click **OK** displaying Figure 2.40,

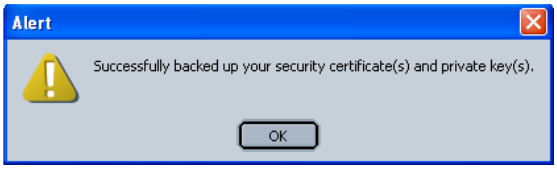

Figure 2.40. Netscape Alert

58. click **OK**, if the certificate has been stored on a floppy or CD, remove from the PC, store in a safe, secure place, and
59. proceed to the CDC program and activities, https://sdn.cdc.gov.

2.4 Download PHINMS via Internet Explorer

Install the PHINMS version 2.6.00 application using Internet Explorer following the steps below:

Note: If an email was not received with the PartyID information, refer to Section 2.1.

60. navigate to FTP site ftp://sftp.cdc.gov displaying Figure 2.41,

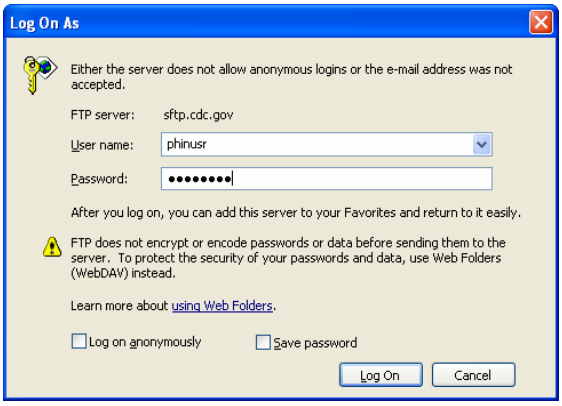

Figure 2.41. Internet Explorer Log On As

61. enter **User name**, **Password**, click **LogOn** displaying first of three (3) folders shown in Figure 2.42,

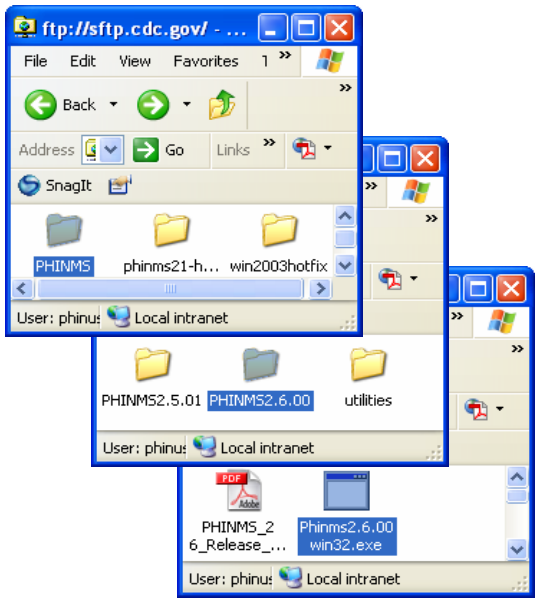

Figure 2.42. Internet Explorer Phinms2.6.00win32.exe

62. open **PHINMS**, **PHINMS2.6.00**, **Phinms2.6.00win32.exe** from screens (Figure 2.39) screens one (1) through three (3) respectively displaying Figure 2.43,

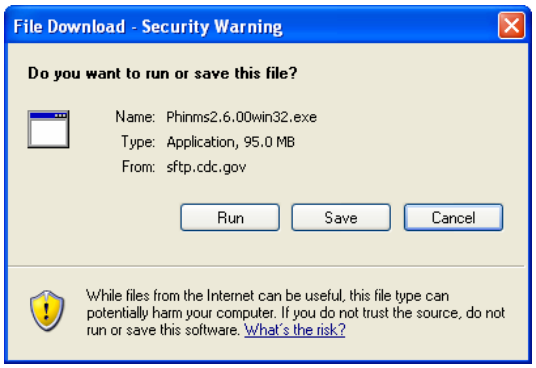

Figure 2.43. Internet Explorer File Download - Security Warning

63. click **Run**, Phinms2.6.00win32.exe will download displaying Figure 2.44,

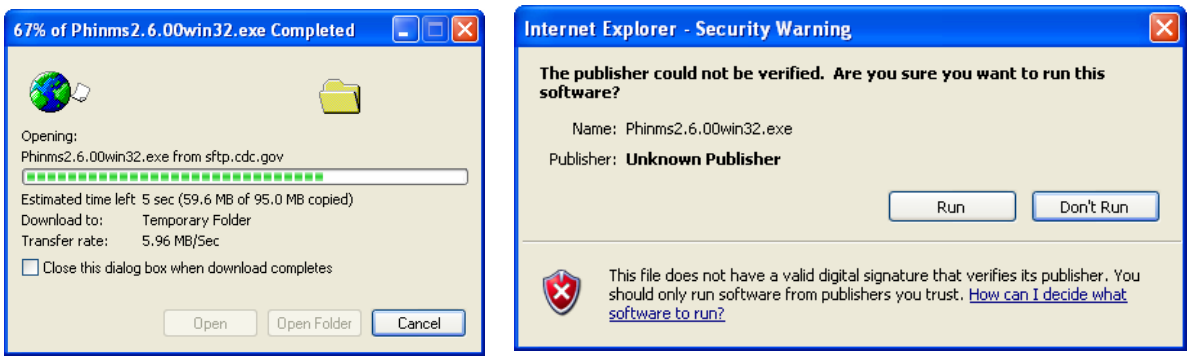

Figure 2.44. Internet Explorer PHINMS Download and Security - Warning

64. select **Run** the InstallShield screen prepares the InstallShield Wizard (taking a few moments) shown in Figure 2.42,

Figure 2.45. Internet Explorer InstallShield Wizard Preparation

65. select **Next** displaying Figure 2.46,

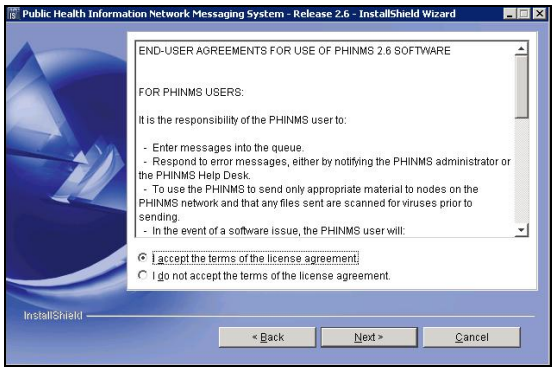

Figure 2.46. Internet Explorer End User Agreement

66. select I accept the terms of the license agreement, click Next displaying Figure 2.47,

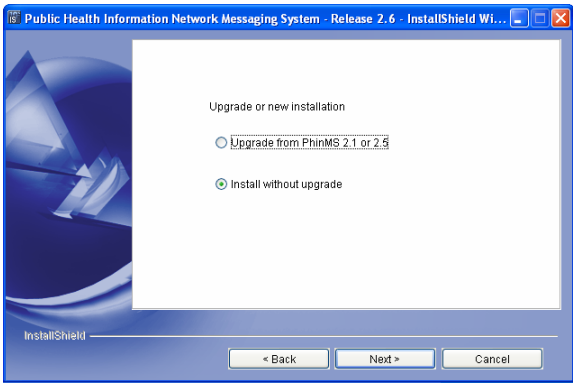

Figure 2.47. Internet Explorer Upgrade or New Installation Screen

67. select **Install without upgrade**, click **Next** displaying Figure 2.48,

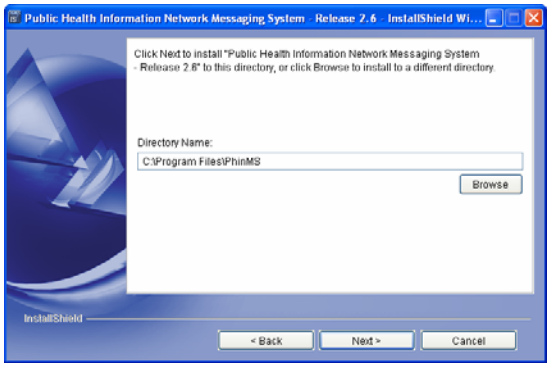

Figure 2.48. Internet Explorer Directory Name

68. select **Browse** to install a different directory or **Next** displaying Figure 2.49,

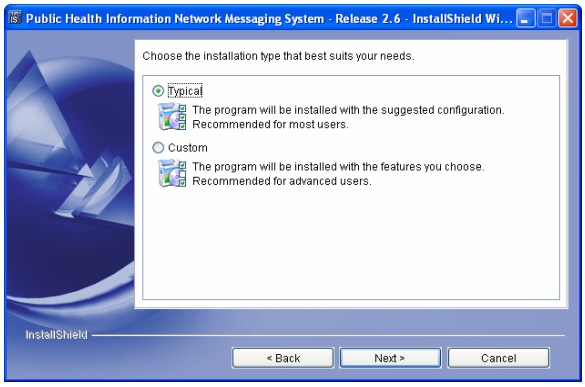

Figure 2.49. Internet Explorer Installation Type

69. select **Typical**, click **Next** displaying Figure 2.50,

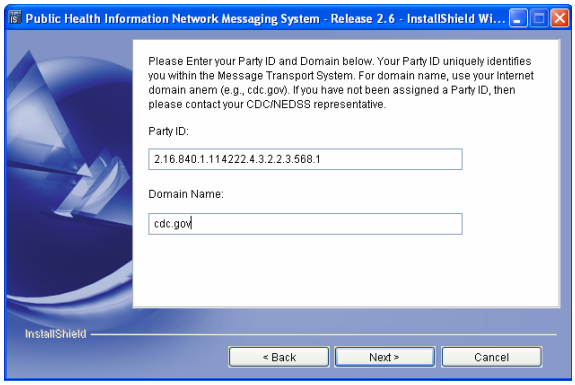

Figure 2.50. Internet Explorer PartyID and Domain Name

70. enter the **PartyID**, **Domain Name**, click **Next** displaying Figure 2.51,

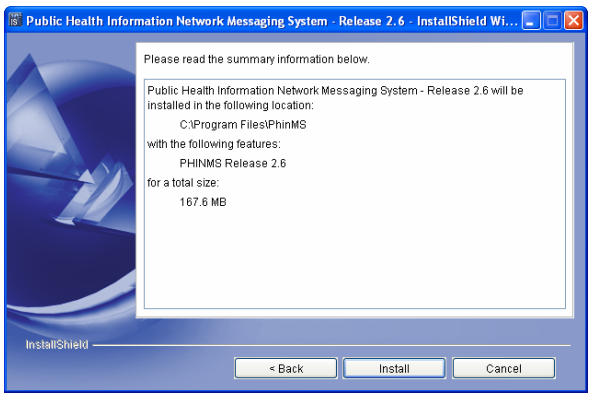

Figure 2.51. Internet Explorer Installation Location

71. click **Install** displaying Figure 2.52,

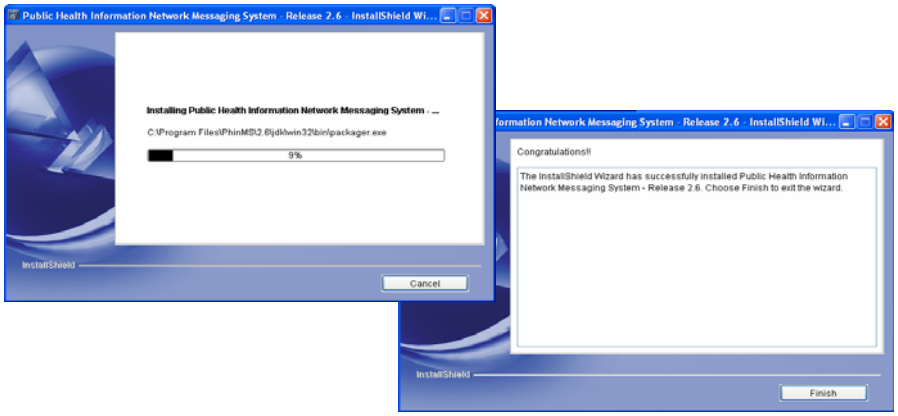

Figure 2.52. Internet Explorer Installing and Congratulations PHINMS

72. click **Finish**, displaying Figure 2.53,

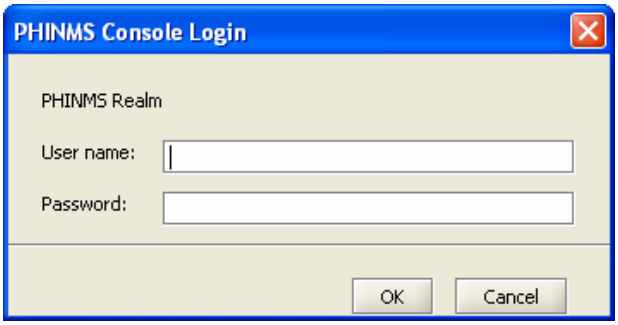

Figure 2.53. Internet Explorer PHINMS Console Login

73. enter **User name**, **Password**, click **OK** displaying Figure 2.54, and

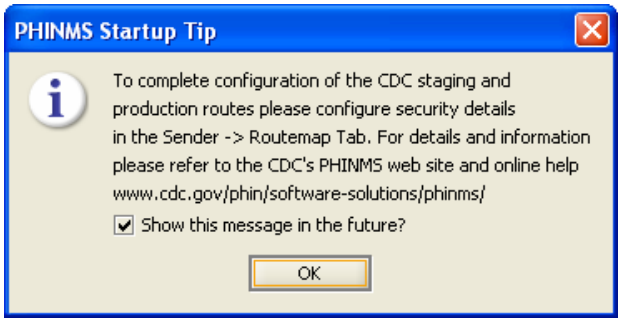

Figure 2.54. Internet Explorer PHINMS Startup Tip

74. click **OK**.

Proceed to Section 4.0 to configure the PHINMS 2.6.00 Console.

2.5 Download PHINMS via Netscape

The Netscape instructions for installing the PHINMS version 2.6.00 are as follows:

Note: If an email was not received with the PartyID information, refer to Section 2.1.

75. navigate to ftp://phinusr:MsSys4U*@sftp.cdc.gov displaying Figure 2.55,

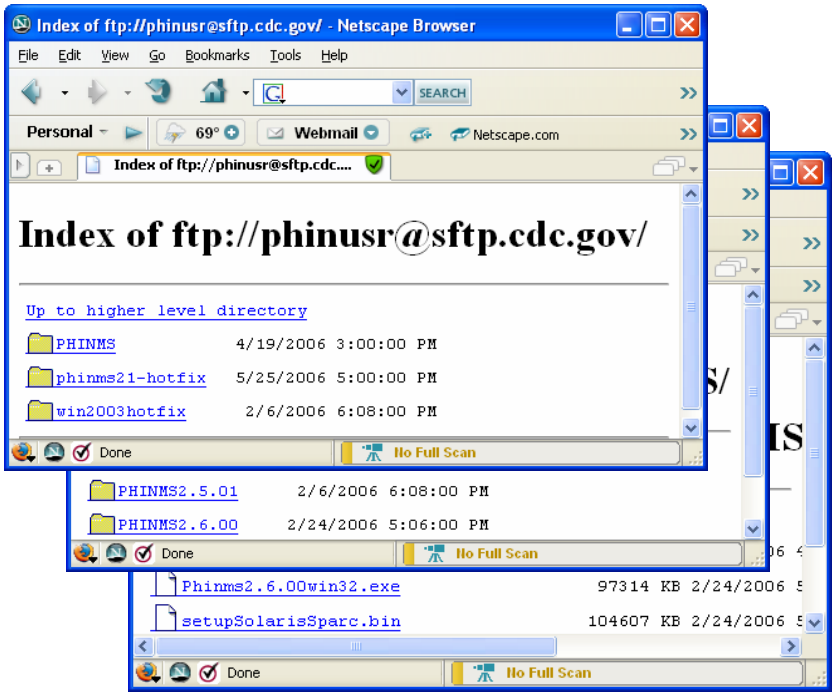

Figure 2.55. Netscape PHINMS Directory

76. open **PHINMS**, **PHINMS2.6.00**, click **Phinms2.6.00win32.exe** displaying Figure 2.56,

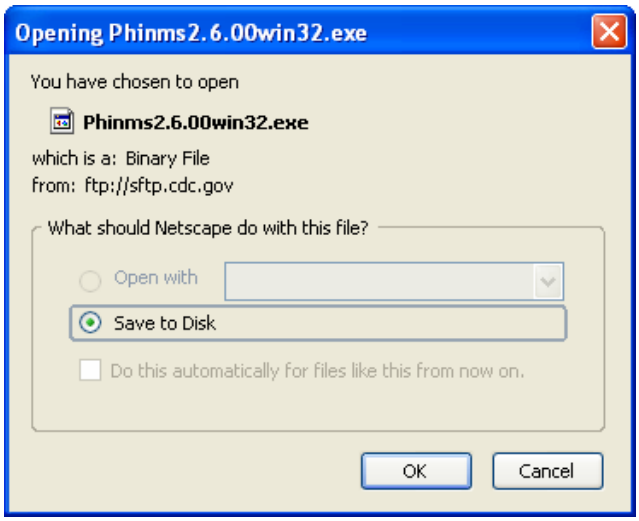

Figure 2.56. Netscape Opening Phinms2.6.00win32.exe

77. select **Save to Disk**, click **OK** displaying Figure 2.57,

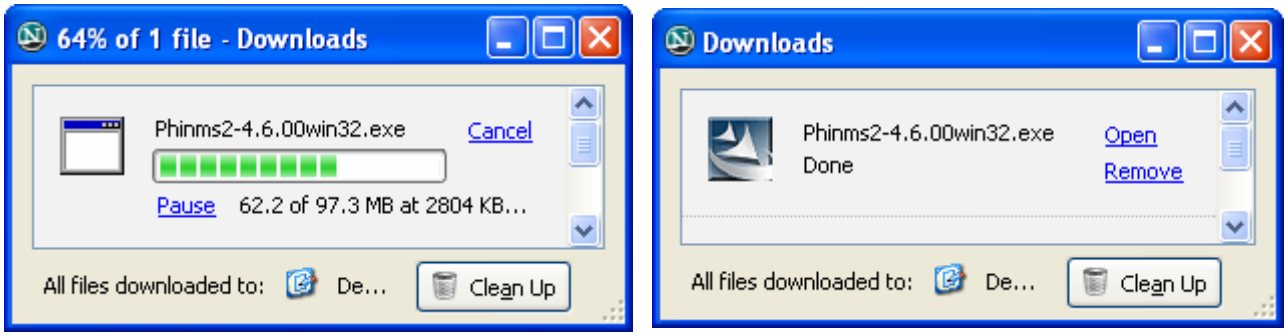

Figure 2.57. Netscape Downloads

78. when the download is successful, click the **Open** link displaying Figure 2.58,

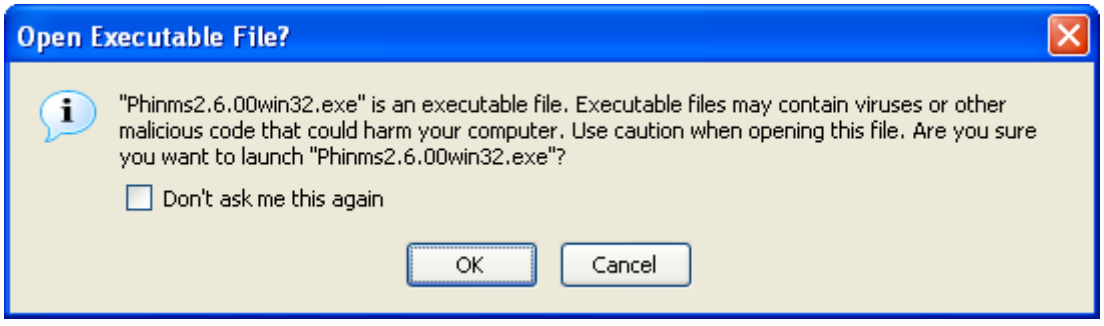

Figure 2.58. Netscape Open Executable File

79. click **OK**, the InstallShield screen prepares the InstallShield Wizard (which takes a few moments) shown in Figure 2.59,

Figure 2.59. Netscape InstallShield Wizard Preparation

80. select **Next** displaying Figure 2.60,

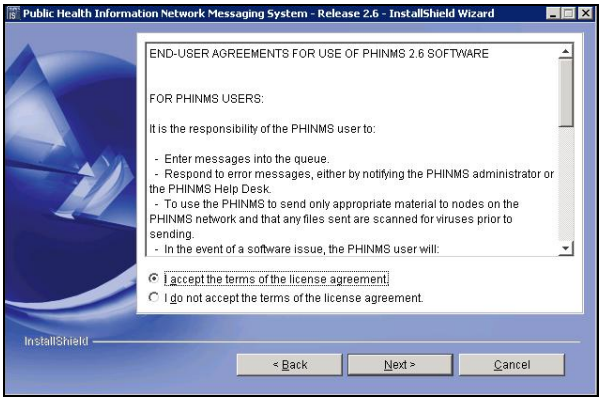

Figure 2.61. Netscape End User Agreement

81. select I accept the terms of the license agreement, click Next displaying Figure 2.62,

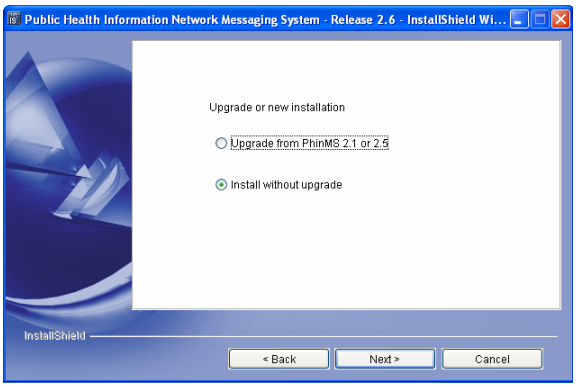

Figure 2.62. Netscape Upgrade or New Installation Screen

82. select **Install without upgrade**, click **Next** displaying Figure 2.63,

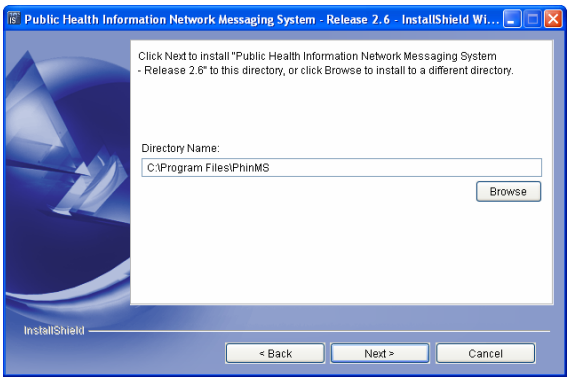

Figure 2.63. Netscape Directory Name

83. select **Browse** to install a different directory or **Next** displaying Figure 2.64,

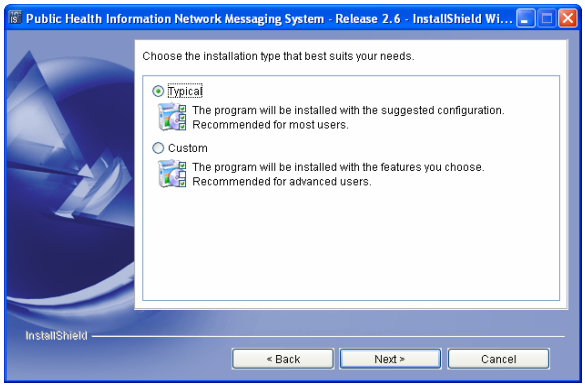

Figure 2.64. Netscape Installation Type

84. select **Typical**, click **Next** displaying Figure 2.65,

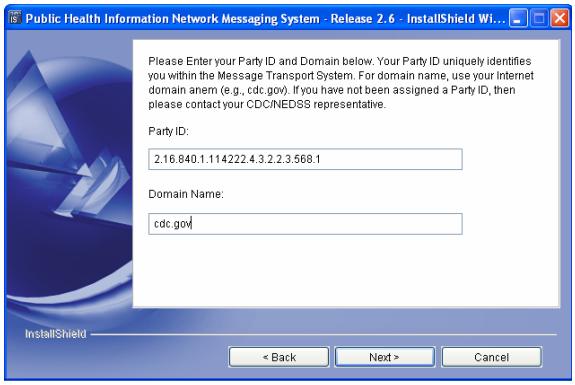

Figure 2.65. Netscape PartyID and Domain Name

85. enter the **PartyID**, **Domain Name**, click **Next** displaying Figure 2.66,

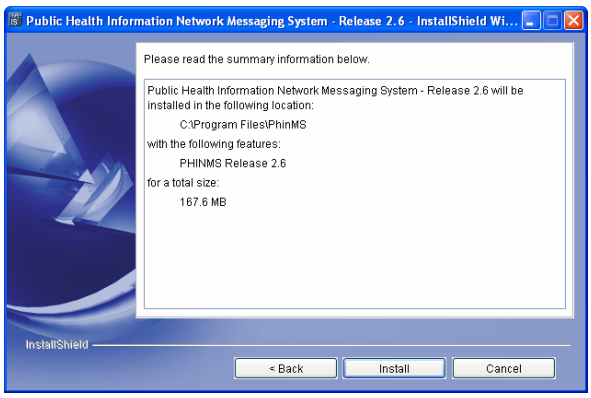

Figure 2.66. Netscape Installation Location

86. the installation location is displayed, click **Install** displaying Figure 2.67,

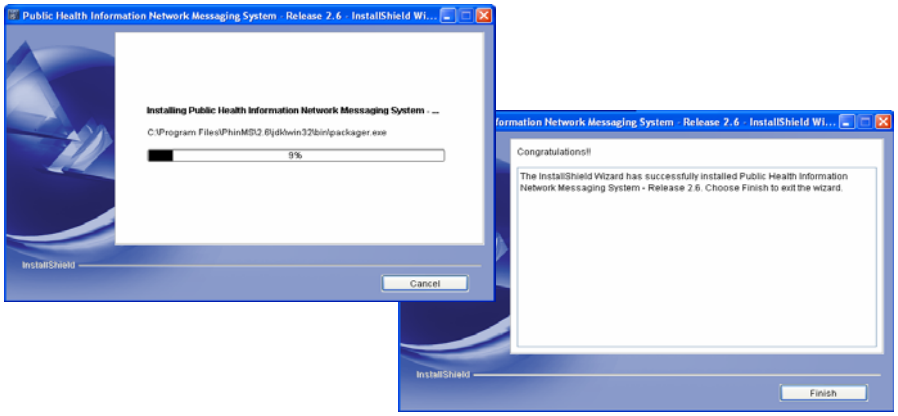

Figure 2.67. Netscape Installing and Congratulations PHINMS

87. click **Finish**, displaying Figure 2.68,

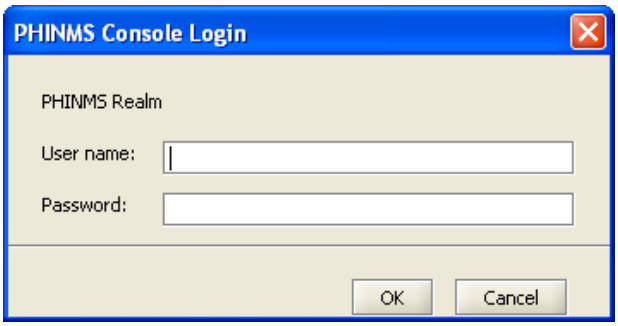

Figure 2.68. Netscape PHINMS Console Login

88. enter the **User name**, **Password**, click **OK** displaying Figure 2.69, and

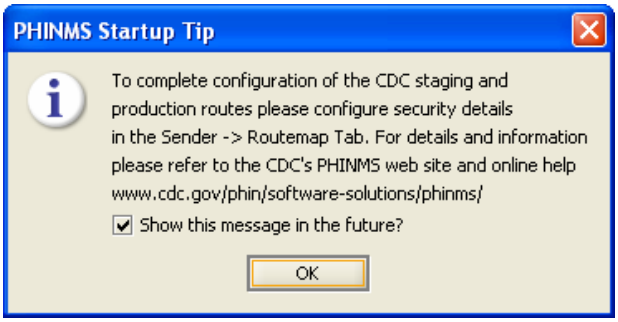

Figure 2.69. Netscape PHINMS Startup Tip

89. click **OK**.

Proceed to Section 4.0 to configure the PHINMS 2.6.00 Console.

2.6 Export SDN Private Key

Once the PHINMS 2.6.00 application and the Digital ID Certificate have successfully been downloaded onto the user's computer complete the following steps to prepare the .pfx file for Keystore entry:

90. open Internet Explorer browser,
91. select **Tools** > **Internet Options** > **Content** displaying Figure 2.70,

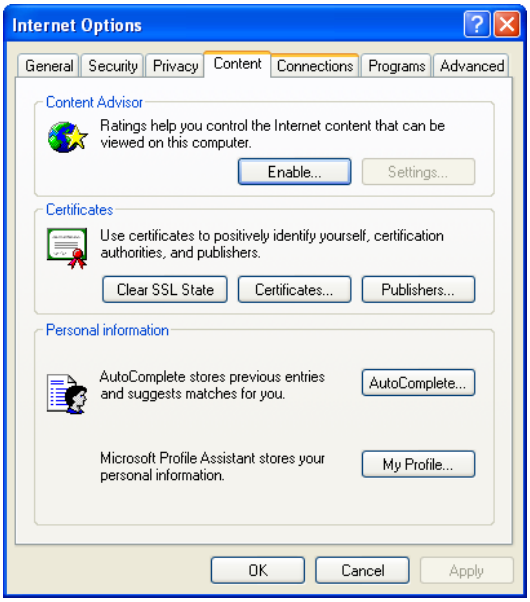

Figure 2.70. Internet Options

92. click **Certificates**, displaying the certificates shown in Figure 2.71,

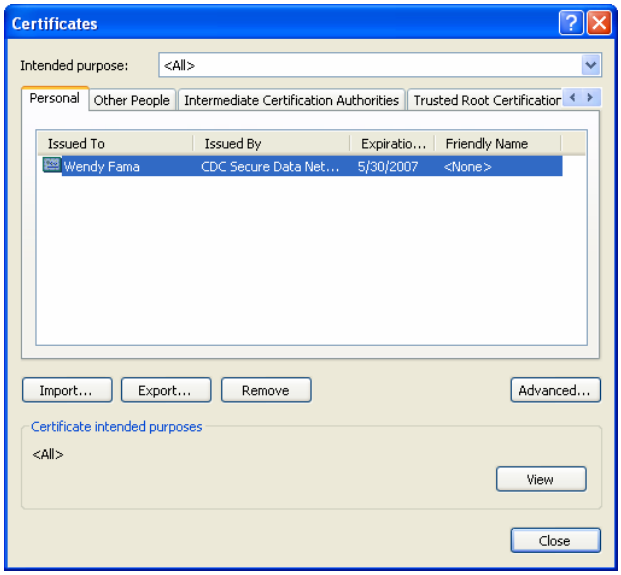

Figure 2.71. Certificates

93. select the certificate to export, click Export displaying Figure 2.72,

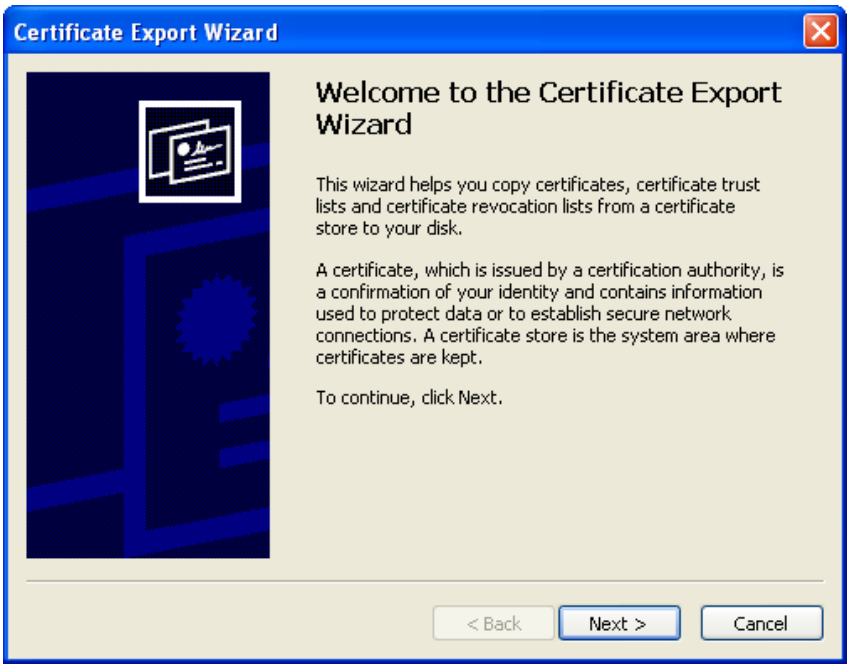

Figure 2.72. Certificate Export Wizard

94. click **Next** displaying Figure 2.73,

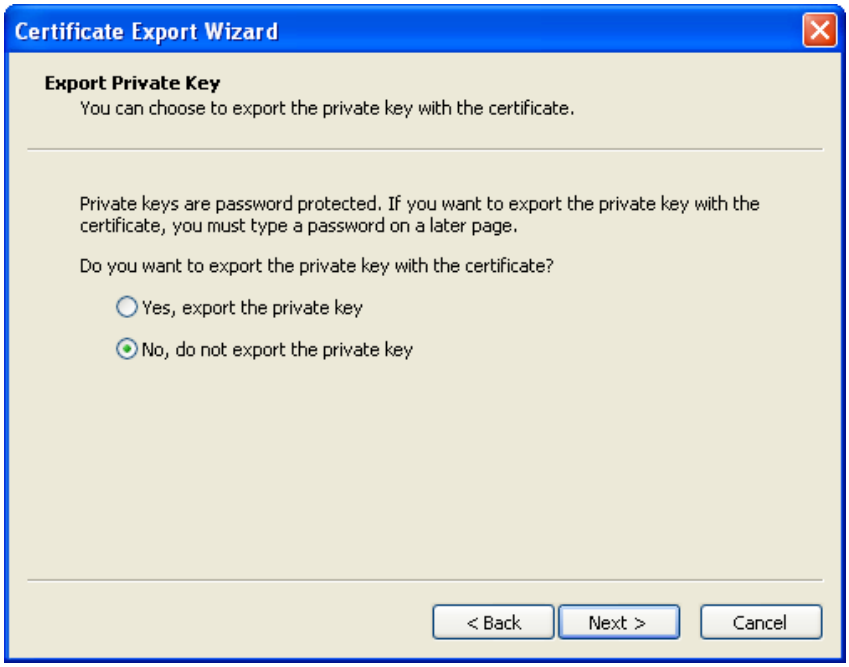

Figure 2.73. Export Private Key

95. select **Yes, export the private key**, click Next Figure 2.74,

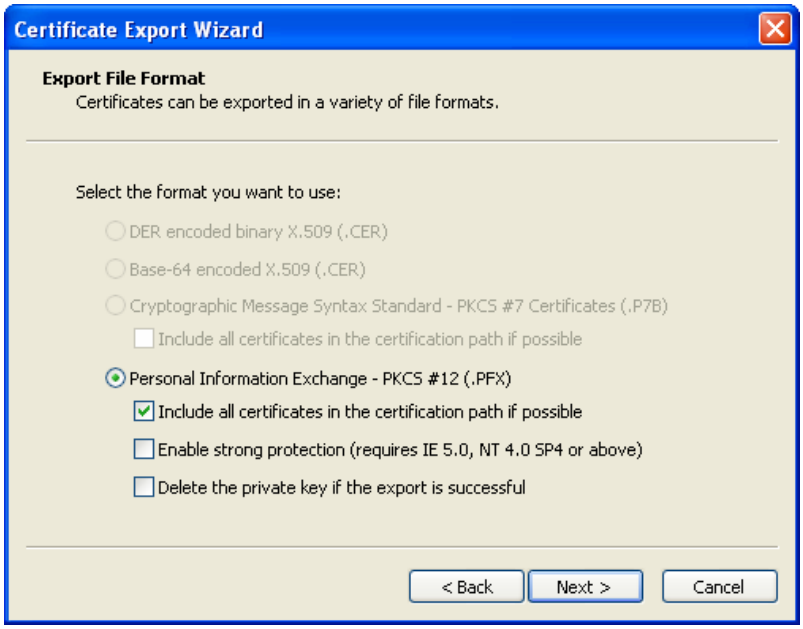

Figure 2.74. Export File Format

96. select Personal information Exchange, check Include all certificates in the certification path if possible, uncheck Enable Strong Protection, uncheck Delete the private key if the export is successful, click Next displaying Figure 2.75,

Figure 2.75. Password

97. enter and confirm the Password (SDN Challenge Phrase is recommended), click **Next** displaying Figure 2.76,

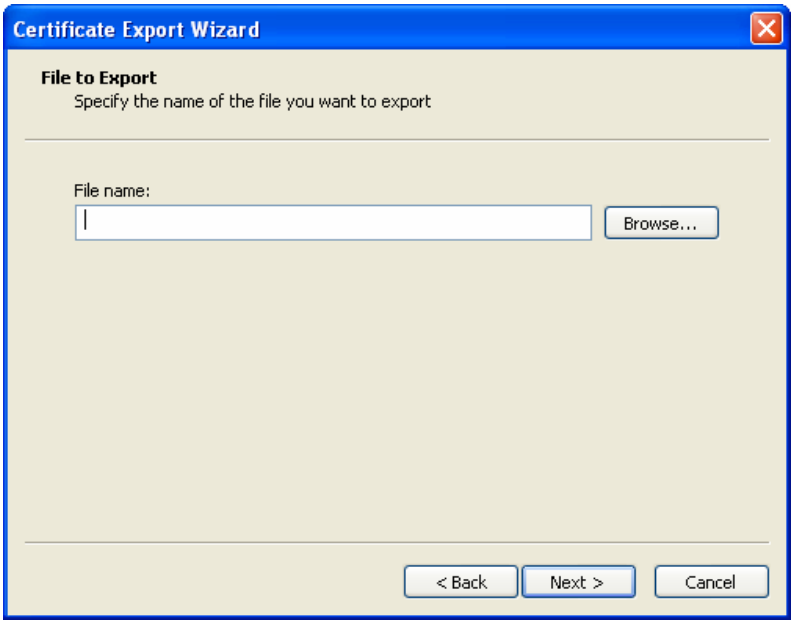

Figure 2.76. File to Export

98. select **Browse** displaying Figure 2.77,

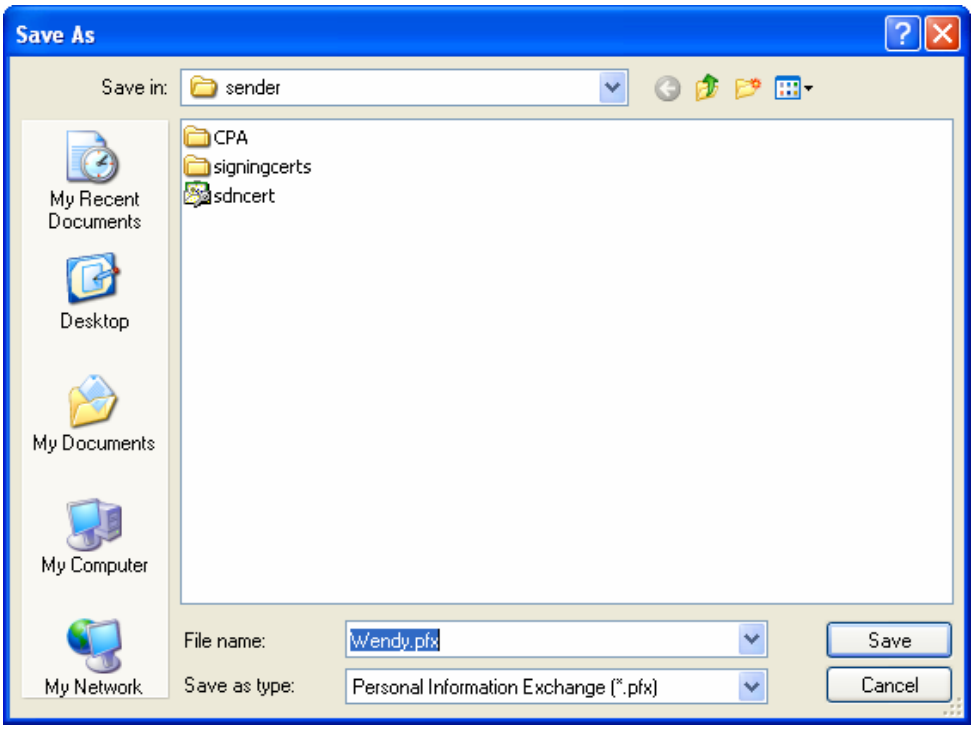

Figure 2.77. Save As

99. navigate to **C:\Program Files\PhinMS\2.6\tomcat-5.0.19\phinms\config\sender**, name the **.pfx file**, click **Save**, displaying the File name on the File to Export screen, click **Next**,

100. click **Finish**, displaying Figure 2.78, and

Figure 2.78. Export was Successful

101. close the browser.

3.0 UPGRADE PHINMS SOFTWARE

PHINMS version 2.6.00 allows upgrading from the following:

- 2.1 sender to 2.6.00 sender,
- 2.1 receiver to 2.6.00 receiver on Tomcat server,
- 2.5.00 or 2.5.01 on Tomcat server, or
- upgrade pre-2.6.00 receivers to 2.6.00 on non-Tomcat application server.

Complete the following steps to upgrade to 2.6.00:

102. open the executable file **Phinms2.6Win32.exe** from the 2.6.00 folder displaying Figure 3.1,

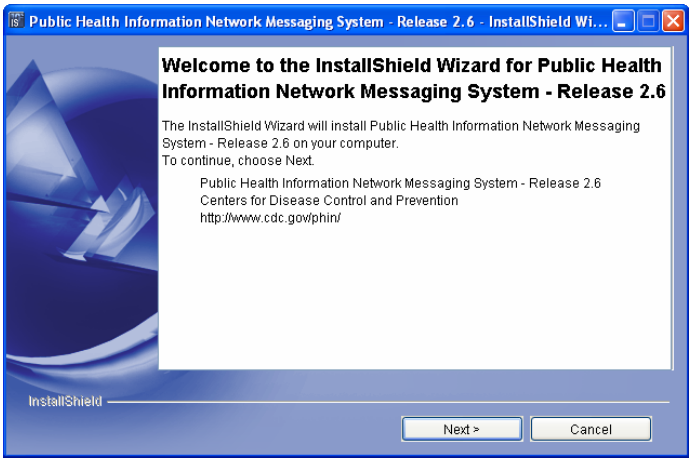

Figure 3.1. Upgrade Welcome

103. select **Next** displaying Figure 3.2,

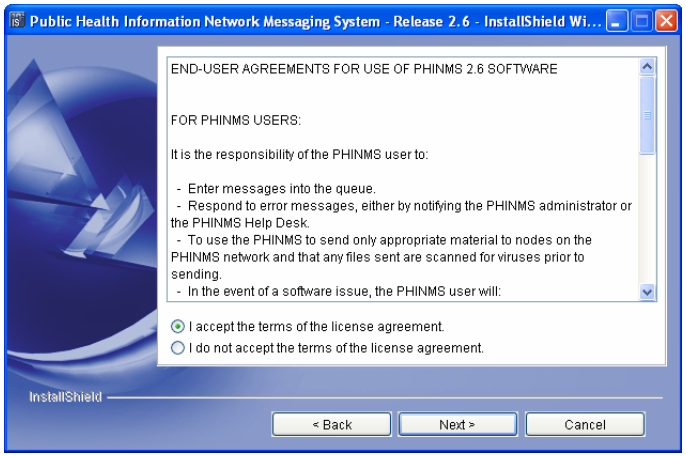

Figure 3.2. End User Agreement

104. select I accept the terms of the license agreement, click Next displaying Figure 3.3,

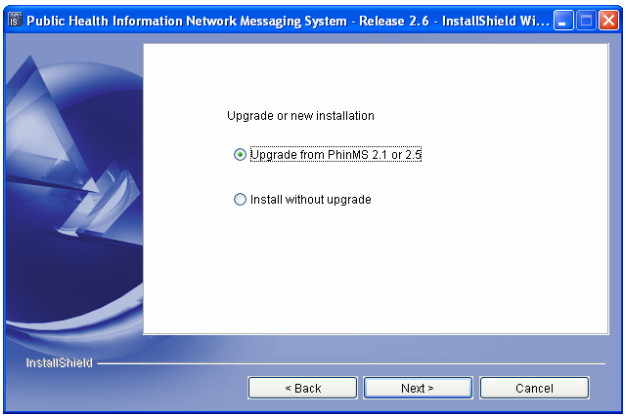

Figure 3.3. Upgrade or New Installation

105. select **Upgrade from PhinMS 2.1 or 2.5**, click **Next** displaying Figure 3.4, and

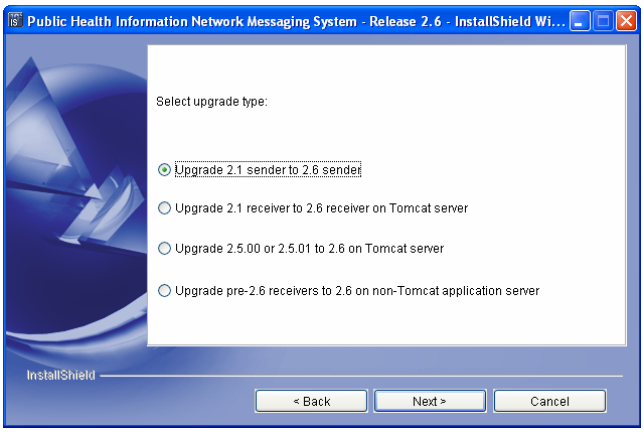

Figure 3.4. Upgrade Type

106. select the upgrade type, click **Next**, continue the upgrade by picking up step 9 in Section 2.4.

4.0 CONFIGURE SQL DATABASE

A Microsoft Access database containing a Transport Queue (TransportQ) is automatically installed with the PHINMS 2.6.00 application. An external database can be created for the purpose of hosting the messaging queue tables. PHINMS 2.6.00 will support the following databases for hosting messaging queues:

- Microsoft Access,
- Microsoft Structured Query Language (SQL) Server,
- Oracle 9i,
- MySQL 4.1, and
- HSQLDB 1.8.0.

A Microsoft Access database is provided with the PHINMS installation on the Windows platform as a default database and facilitates testing installation. Evaluation of the tradeoffs between Microsoft Access and a high transaction volume Relational Database Management System (RDBMS) such as others listed above is recommended.

This section explains the procedures for creating and configuring a Microsoft SQL database.

4.1 Create SQL Database

Complete the following steps to connect to an external PHINMS SQL database such as Microsoft SQL Server:

107. navigate to http://www.microsoft.com/downloads/details.aspx?FamilyID=07287b11-0502-461a-b138-2aa54bfdc03a&DisplayLang=en displaying Figure 4.1,

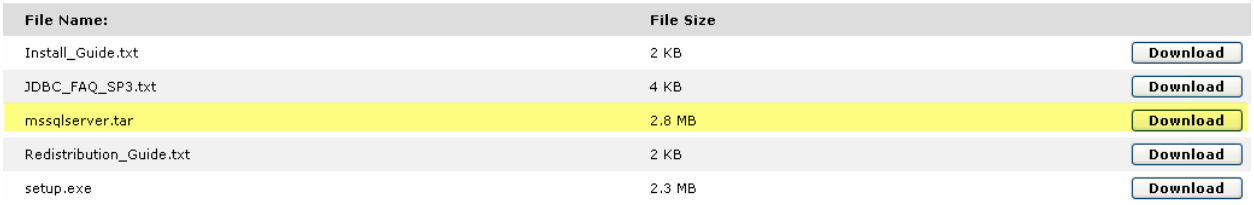

Figure 4.1. Download mssqlserver.tar

108. select **mssqlserver.tar download** which are the Java Database Connectivity (JDBC) drivers from Microsoft displaying Figure 4.2,

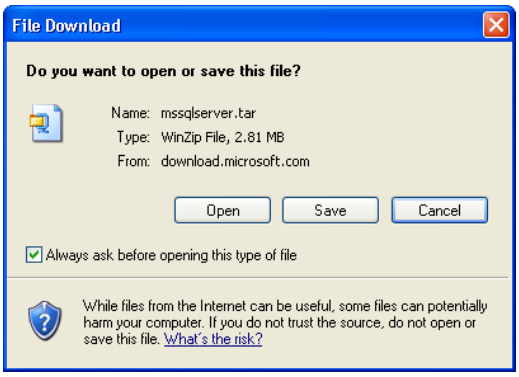

Figure 4.2. File Download

109. select **Open** displaying Figure 4.3,

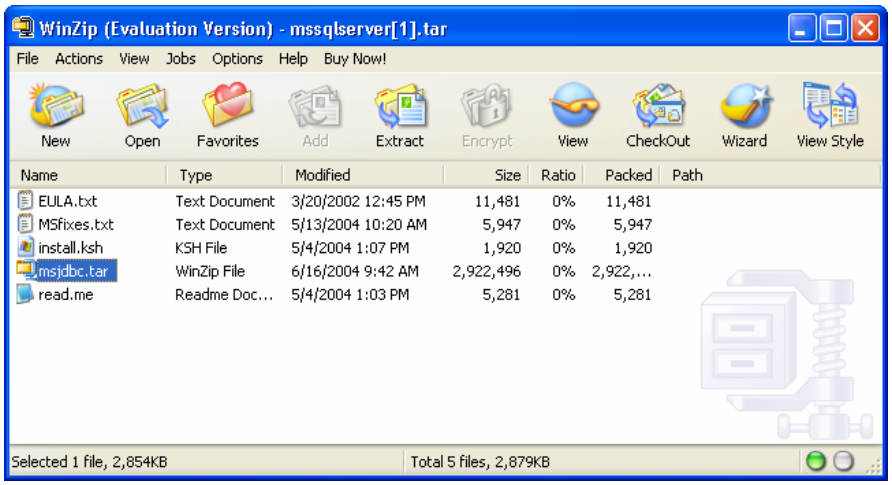

Figure 4.3. Save As

110. open **msjdbc.tar** displaying Figure 4.4,

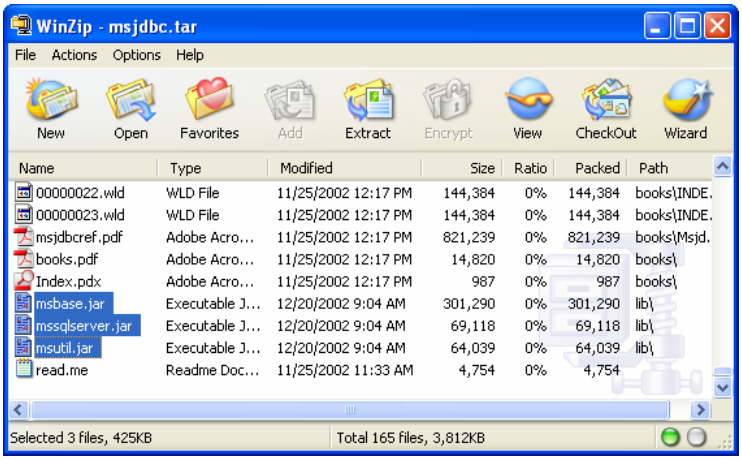

Figure 4.4. WinZip - msjbdc.tar

111. scroll down and select **msbase.jar**, **mssqlserver.jar**, **msutil.jar**, click **Extract** displaying Figure 4.5,

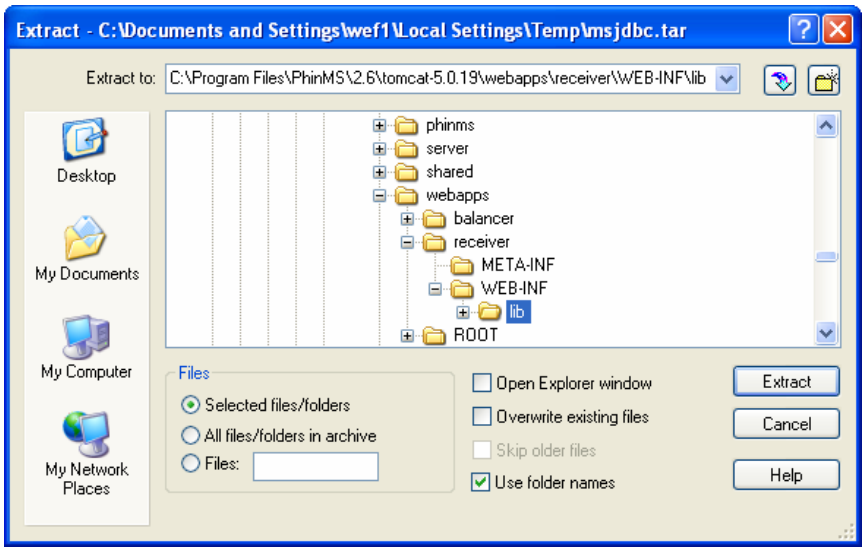

Figure 4.5. Extract Files

112. extract to C:\Program Files\PhinMS\2.6\tomcat-5.0.19\webapps\receiver\WEB-INF\lib, click Extract, close WinZip window,

113. open Microsoft SQL Server Enterprise Manager shown in Figure 4.6,

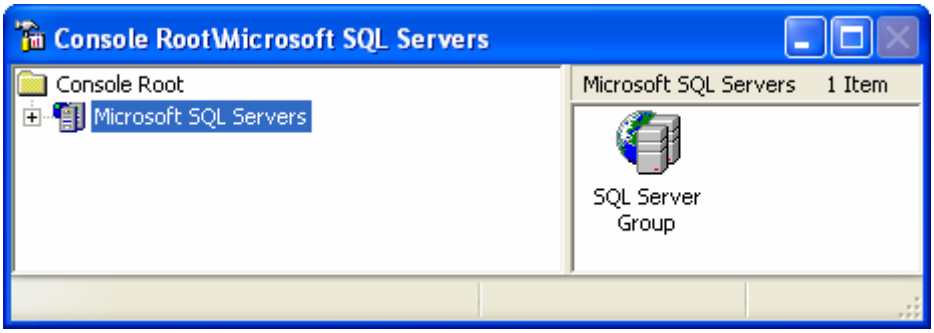

Figure 4.6. Microsoft SQL Server Enterprise Manager

114. click **Microsoft SQL Servers**, **SQL Server Group**, **Local** server, right click on **Database**, select **New Database** displaying Figure 4.7,

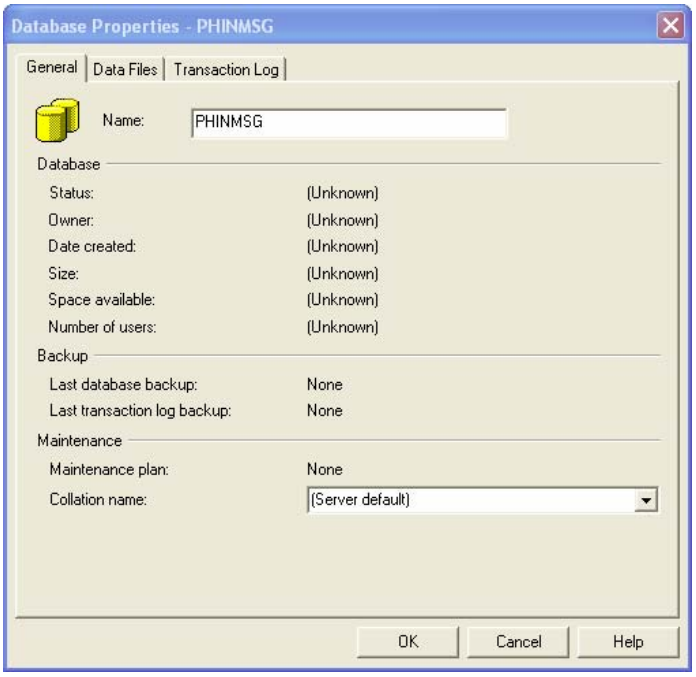

Figure 4.7. Database Properties

115. type **PHINMSG** in the Name field, click **OK** database,

116. open **PHINMSG** database, right click **Users**, select **New Database User**, check **public** and **db_owner**, select **New** for the login name from the dropdown list displaying Figure 4.8, and

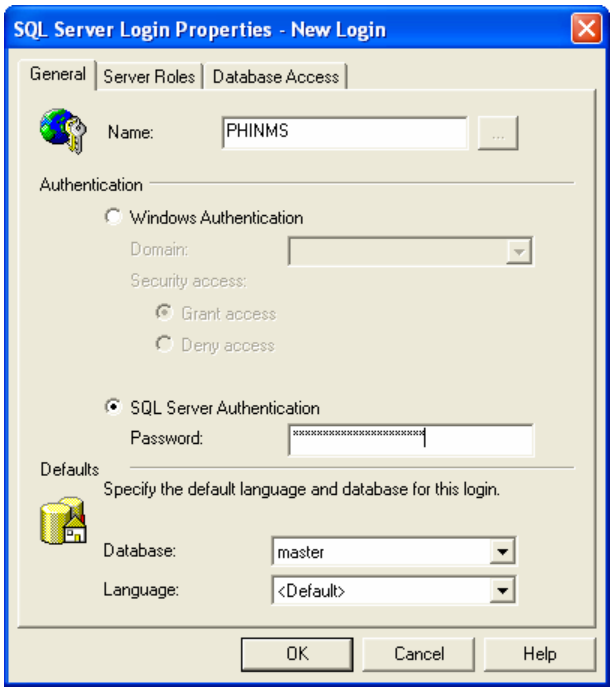

Figure 4.8. SQL Server Login Properties - New Login

117. type **PHINMSG** in the Name field, enter a password (challenge phrase is recommended), click **OK**, **OK**, successfully creating the PHINMS user if the access reads Permit.

4.2 Create TransportQ_out Table

To create the **TransportQ_out** table in the Public Health Information Network Messaging (PHINMSG) database using the Microsoft TransportQ script, complete the following steps:

118. copy SQL script listed below

```
CREATE TABLE [dbo].[TransportQ_out] (
[recordId] [bigint] IDENTITY (1, 1) NOT NULL ,
[messageId] [char] (255) NULL,
[payloadFile] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
[payloadContent] [IMAGE] NULL ,
[destinationFilename] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[routeInfo] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
[service] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
[action] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
[arguments] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
[messageRecipient] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL
,
[messageCreationTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[encryption] [char] (10) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
[signature] [char] (10) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
[publicKeyLdapAddress] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[publicKeyLdapBaseDN] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[publicKeyLdapDN] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
[certificateURL] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL,
[processingStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL
,
[transportStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
[transportErrorCode] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[applicationStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL
,
[applicationErrorCode] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[applicationResponse] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[messageSentTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
[messageReceivedTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
[responseMessageId] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL
,
[responseArguments] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL,
[responseLocalFile] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL
,
[responseFilename] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL
,
[responseContent] [IMAGE] NULL ,
[responseMessageOrigin] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
```

```
[responseMessageSignature] [char] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
[priority] [int] NULL
) ON [PRIMARY]
GO
```

119. open the SQL Server Enterprise Manager, select PHINMS, Tools, SQL Query Analyzer, displaying Figure 4.9,

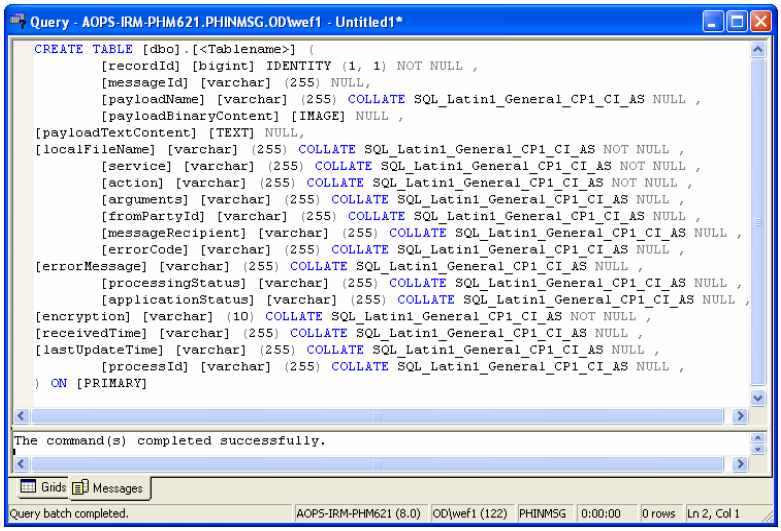

Figure 4.9. Query Analyzer

120. paste the SQL script from step one (1) into the query analyzer, select **Execute Query** (F5),

121. close the Query Analyzer window displaying Figure 4.10,

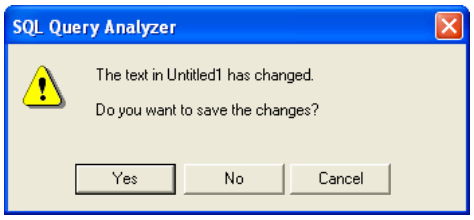

Figure 4.10. Query Analyzer Prompt

122. click **Yes** navigate to **C:\Program Files\PhinMS\2.6\tomcat-5.0.19\phinms**, save as **TransportQ_out**, close window, verify the table was successfully created in the Tables folder shown in Figure 4.11,

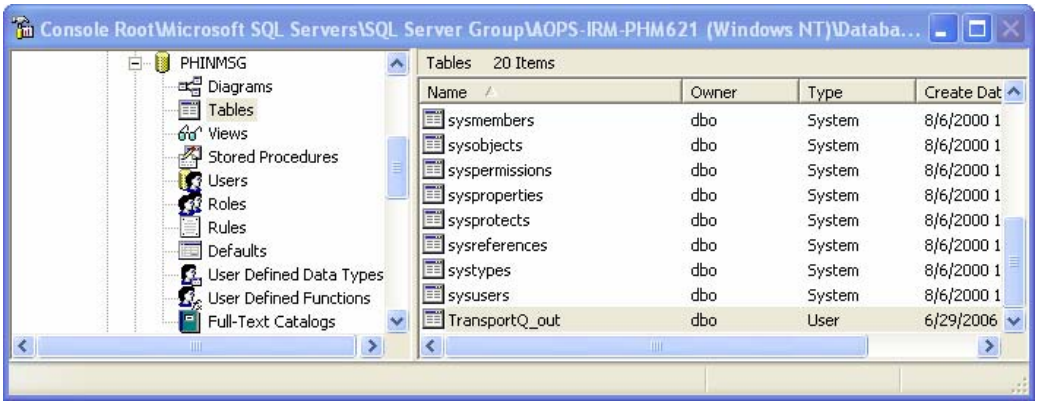

Figure 4.11. TransportQ_out Table

123. select **Control Panel** from Microsoft Start, **Administrative Tools**, **Services** displaying Figure 4.12,

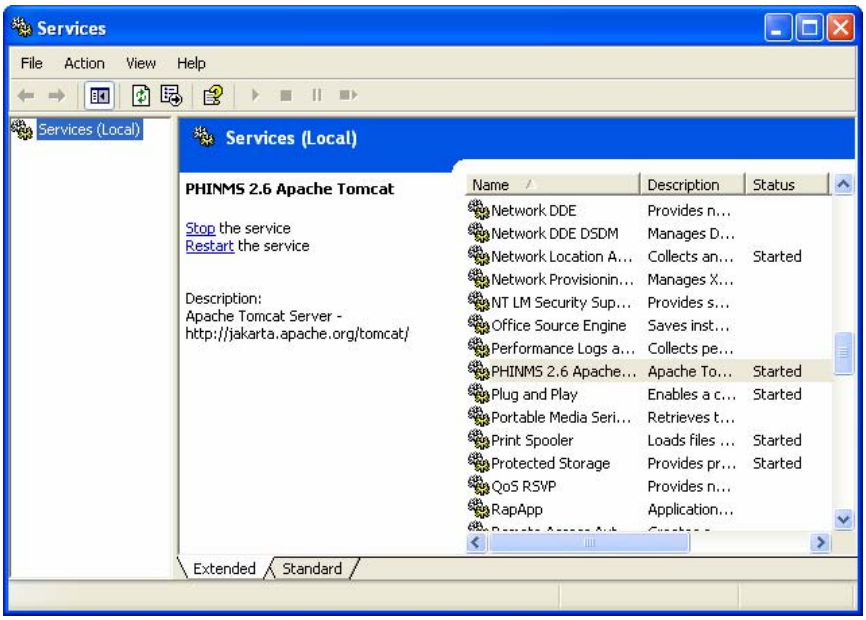

Figure 4.12. Services

124. select PHINMS 2.6 Apache Tomcat,

125. click **Restart the service** displaying Figure 4.13, and

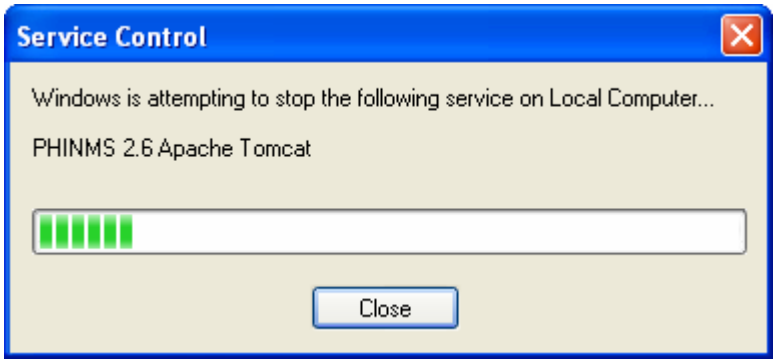

Figure 4.13. Service Control

126. close the windows.

Note: During configuration if problems are encountered, open the log file from Window Explorer **C:\Program Files\PhinMS\2.6\tomcat-5.0.19\phinms\logs\sender** which will document the error.

5.0 SENDER INFORMATION

PHINMS Version 2.6.00 installation has two components - the Sender and the Receiver. Sending a test message allows the PHINMS Sender to send messages to the TransportQ and to the CDC. Testing the PHINMS installation is a three-part procedure which includes the following:

- ping the PHINMS Sender loopback route,
- ping the PHINMS CDC Ping Server (phinmsping.cdc.gov), and
- ping the PHINMS CDC Staging Receiver. (Requires CPA files be emailed to Phintech@cdc.gov. Refer to Section 5.3.1.

Figure 5.1 displays a diagram to assist with understanding the PHINMS authentication process.

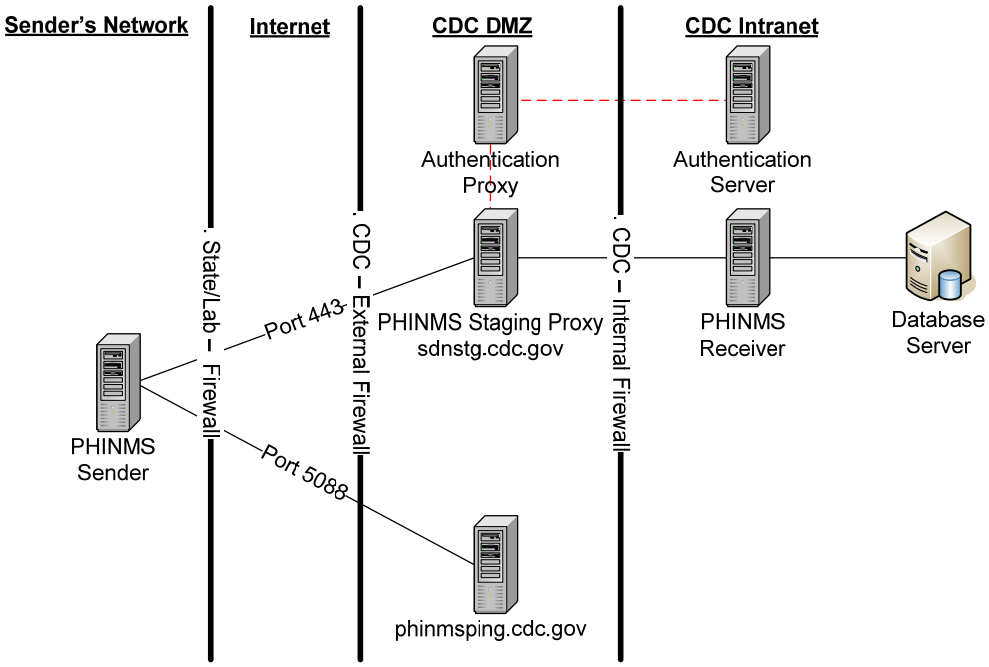

Figure 5.1. CDC PHINMS Topology

5.1 Ping Loopback

The Ping Loopback validates the PHINMS installation was downloaded and installed successfully on the Sender's system. This is not a test to verify messages can be sent outside of a firewall if one is present.

Verify the generated ping loopback is successfully sent to the loopback message processor by completing the following steps:

127.open PHINMS 2.6.00 displaying Figure 5.2,

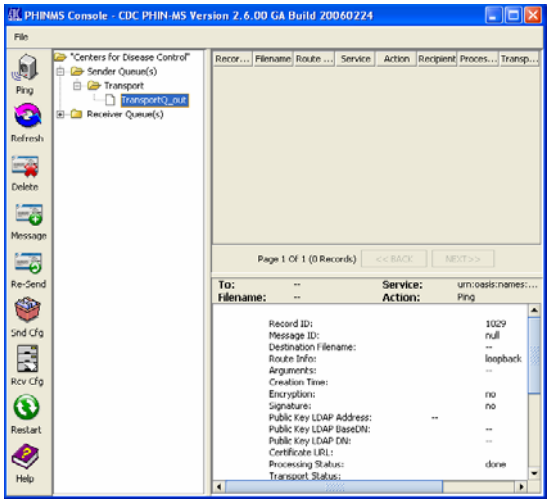

Figure 5.2. PHINMS Console

128. expand **Sender Queue(s)**, expand **Transport**, select **TransportQ_out**, select **Ping** displaying Figure 5.3,

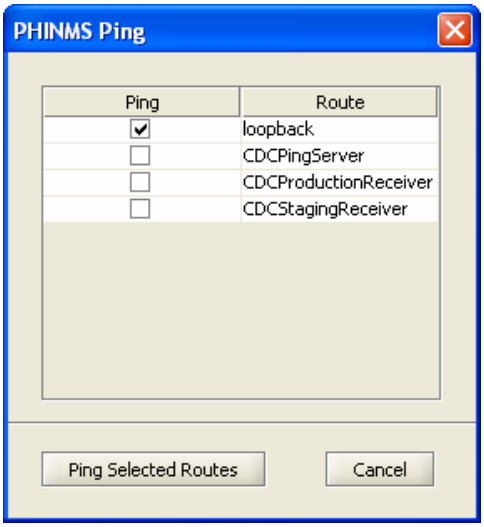

Figure 5.3. PHINMS Ping

129. check **loopback**, click **Ping Selected Routes** displaying Figure 5.4,

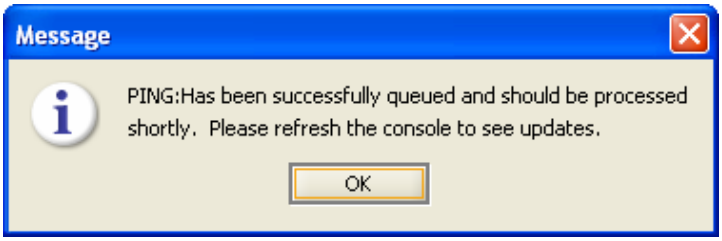

Figure 5.4. Message

130. click **OK**, a Record ID has been created indicating a queued process status shown in Figure 5.5, and

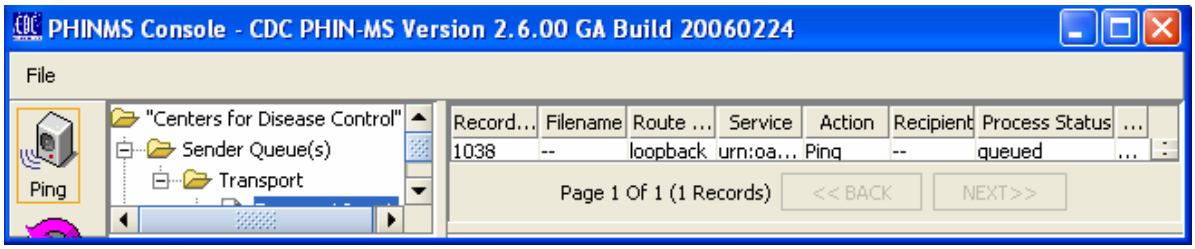

Figure 5.5. Queued Record ID

131. click **Refresh** changing the status to attempted, click **Refresh** again changing the status to done indicating success.

5.2 Ping CDC Ping Server

The ping CDCPingServer validates the sender can connect to the internet and to the CDC without the need for authentication (security credentials). The CDC Ping Server is dedicated to answering Ping requests and will not receive any real messages. Port 5088 needs to be open on the firewall at the sender's location to generate a ping to the CDCPingServer.

Verify the message ping to the CDC Ping Server is successful by completing the following steps:

Verify the ping is successful by completing the following steps:

132. open PHINMS 2.6.00 displaying Figure 5.6,

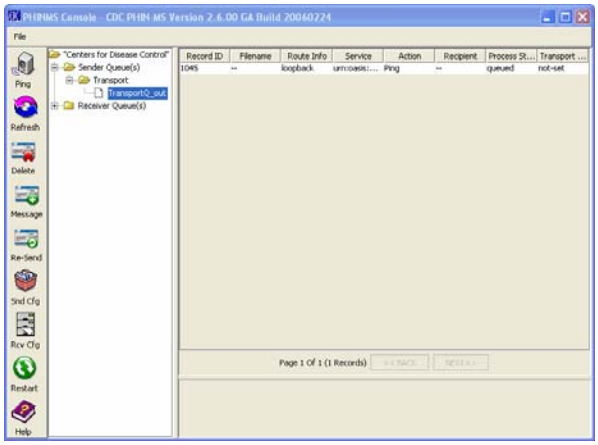

Figure 5.6. PHINMS Console

133. select **Ping** displaying Figure 5.7,

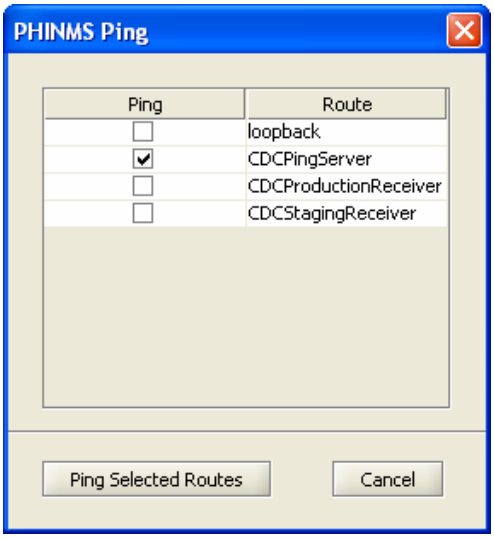

Figure 5.7. PHINMS CDC Ping

134. check **CDCPingServer**, click **Ping Selected Routes** displaying Figure 5.8, and

Figure 5.8. Message

135. click **OK**, a Record ID has been created indicating a queued, click **Refresh** changing the status to attempted, click **Refresh** again changing the status to done indicating success.

5.3 Configure CDC Staging Receiver

The CDC Staging Receiver requires to be configured before sending a Ping. Configure the CDCStagingReceiver using the following steps:

136. select **Snd Cfg** displaying Figure 5.9,

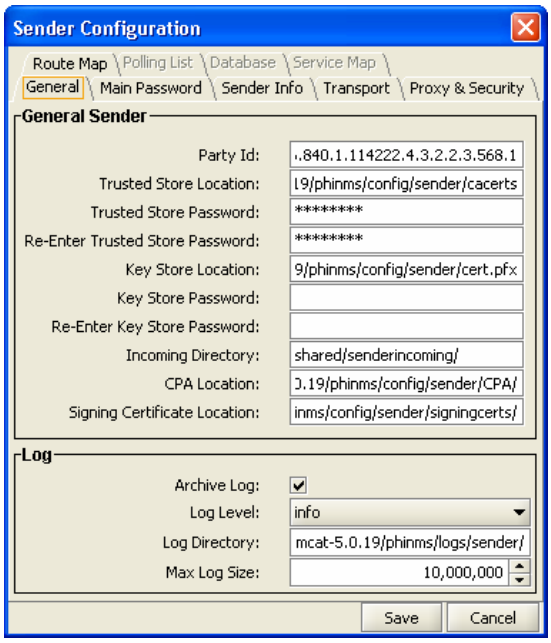

Figure 5.9. Sender Configuration

137.select the **Route Map**, **CDCStagingReceiver**, click **Update** displaying Figure 5.10,

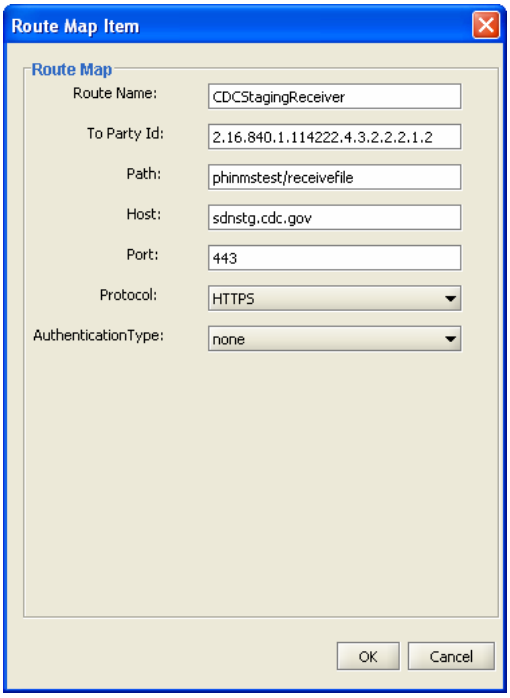

Figure 5.10. Route Map Item

138.select **Netegrity** as the AuthenticationType displaying Figure 5.11,

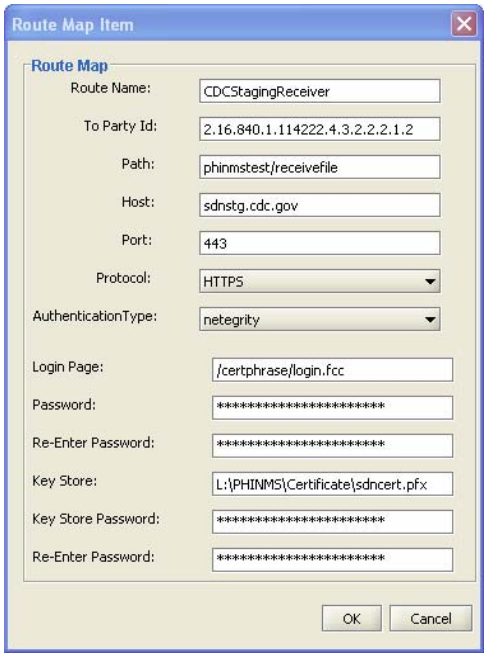

Figure 5.11. CDC Route Map Configuration

139. type **/certphrase/login.fcc** in the Login Page field, enter the **SDN Challenge Phrase**, confirm **SDN Challenge Phrase**, enter the path to the stored certificate keystore (.pfx file), enter the **Key Store Password**, confirm the **Key Store Password**, click **OK**, displaying Figure 5.12,

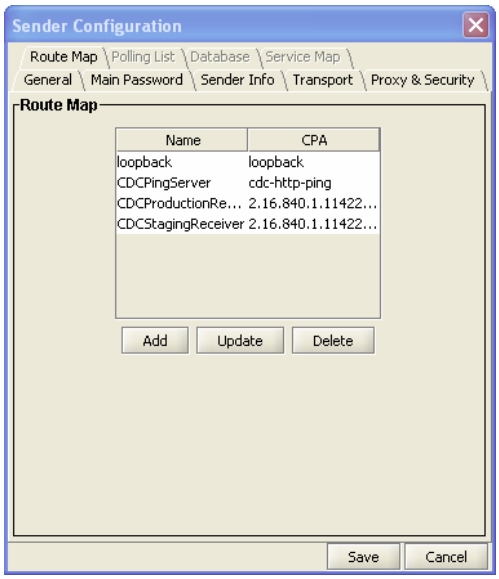

Figure 5.12. CDC Route Map

140. click **Save**, displaying Figure 5.13,

Figure 5.13. CDC Route Configuration Successful

141. click **OK**, restart the PHINMS application displaying Figure 5.14, and

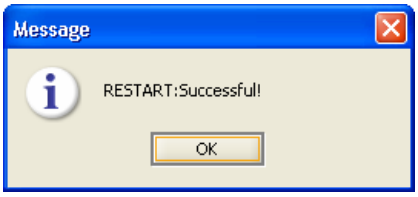

Figure 5.14. Restart Successful

142. click OK.

5.3.1 Email CPA File

PHINMS creates a Collaboration Protocol Agreement (CPA) file for each route listed on the Route Map tab of the Sender Configuration panel.

The PHINMS Administrator must send the PHINMS Helpdesk (Phintech@cdc.gov) the CPA files for each route specifying either the CDC Production Receiver or the CDC Staging Receiver. Only after the PHINMS helpdesk has received the CPA file and applied it to the PHINMS receiver can there be a successful transmission of messages from the sender to the receiver.

The CPA files required to be sent are located in directory x:\install dir\2.6\tomcat-5.0.19\phinms\config\sender\CPA.

Note: More information on CPA can be found in the PHINMS Technical Reference Guide.

5.4 Ping CDC Staging Receiver

The ping PHINMS Staging Receiver validates end-to-end success of the Sender's ability to connect to the CDC over the internet, authenticate with the CDC's Authentication Server, and communicate with the Staging Receiver.

Verify the generated ping message is successfully sent to the CDC Staging Receiver message processor by completing the following steps:

143. open PHINMS 2.6.00 displaying Figure 5.15,

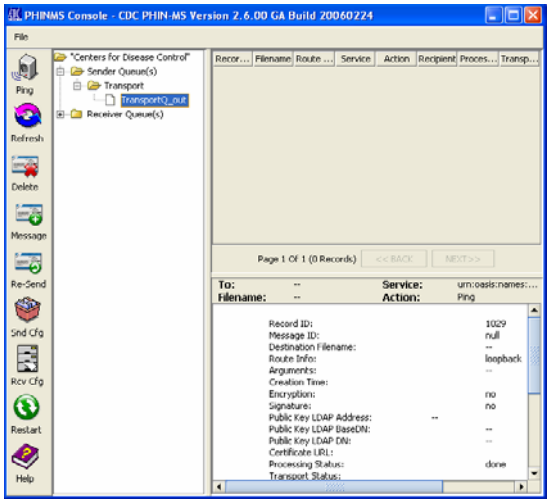

Figure 5.15. PHINMS Console

144. expand **Sender Queue(s)**, expand **Transport**, select **TransportQ_out**, select **Ping** displaying Figure 5.16,

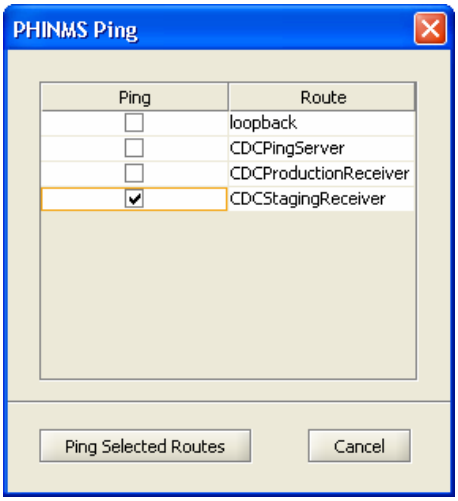

Figure 5.16. PHINMS Ping

145. check CDCStagingReceiver, click **Ping Selected Routes** displaying Figure 5.17,

Figure 5.17. Message

146. click **OK**, a Record ID has been created indicating a queued process status shown in Figure 5.18,

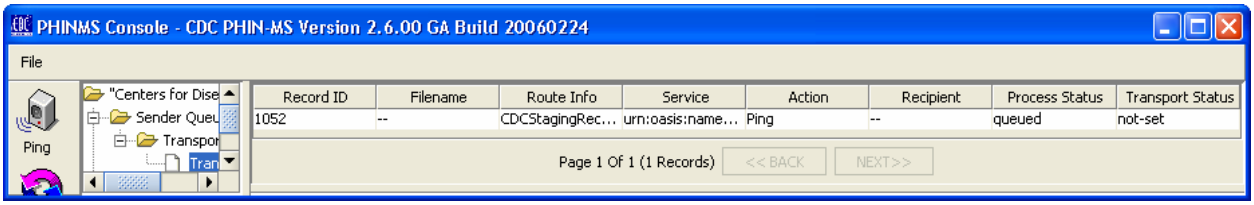

Figure 5.18. Queued Record ID

147. click **Refresh** changing the status to attempted, and

148. click **Refresh** again changing the status to done indicating success.

5.5 Send Test Payload Message

The send payload message verifies the capability to send an outbound message with an attached file to a Receiver.

Note: Ensure the CPA files have been sent to the PHIN Help desk before attempting to send a payload message. Refer to Section 5.3.1 for CPA information.

Send the payload message test to the PHINMS Staging Receiver by completing the following steps:

149. open PHINMS 2.6.00 displaying Figure 5.19,

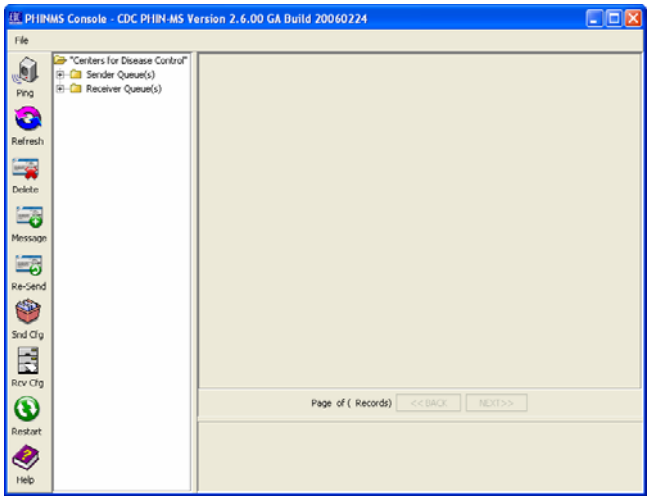

Figure 5.19. PHINMS Console

150. expand **Sender Queue(s)**, expand **Transport**, select **TransportQ_out**, select **Message** displaying Figure 5.20,

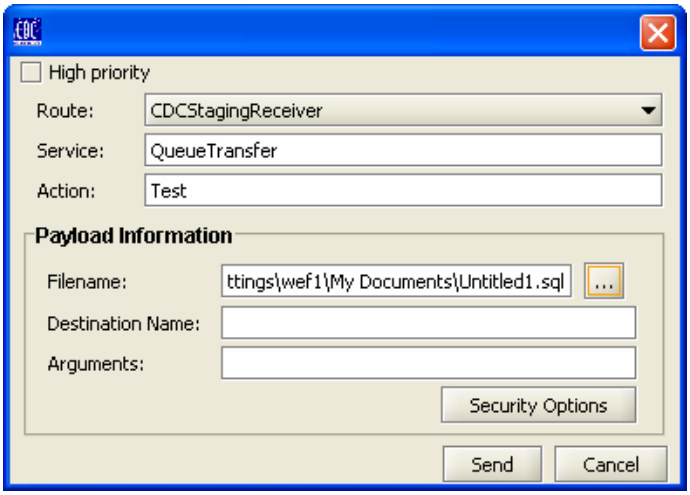

Figure 5.20. PHINMS Ping

151. enter the following parameters:
    - Route: CDC Staging Receiver,
    - Service: QueueTransfer,
    - Action: **Test**,
    - Filename: browse for a file to attach,
    - Destination Name: optional - can be left blank,
    - Arguments: optional - can be left blank,
152. proceed to **Step 5** if using Security Options and to **Step 8** if not,

Note: Security Options are optional for encrypting or signing messages.

153. click **Security Options** displaying Figure 5.21,

Figure 5.21. Security Options

154. enter the following parameters:
    - check Encrypt Message,
    - select Use LDAP lookup to find encryption certificate,
    - Address: directory.verisign.com:389,
    - BaseDN: o=Centers for Disease Control and Prevention,
    - Common Name: **cn=cdc phinms**,
155. click **OK**,
156. click **Send** displaying Figure 5.22, and

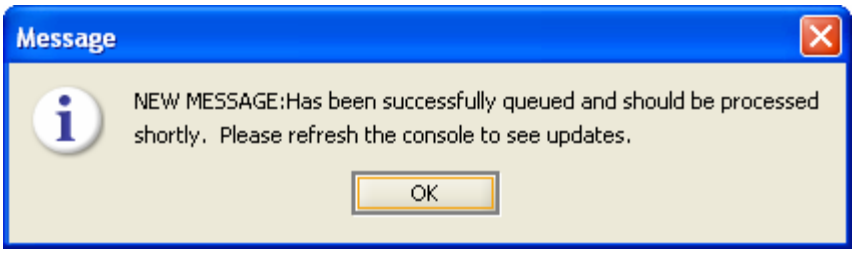

Figure 5.22. Message Notification

157. click **OK**.

5.6 Create Route Map

Messages sent using PHINMS need to address a specific recipient in the PHINMS Console. Each Route is mapped to the recipient's attributes, such as the URL, transport protocol, and authentication type.

Obtain the partner's PartyID, the authentication type, and the security credentials.

Create a Route by completing the following steps:

158. open PHINMS 2.6.00 displaying Figure 5.23,

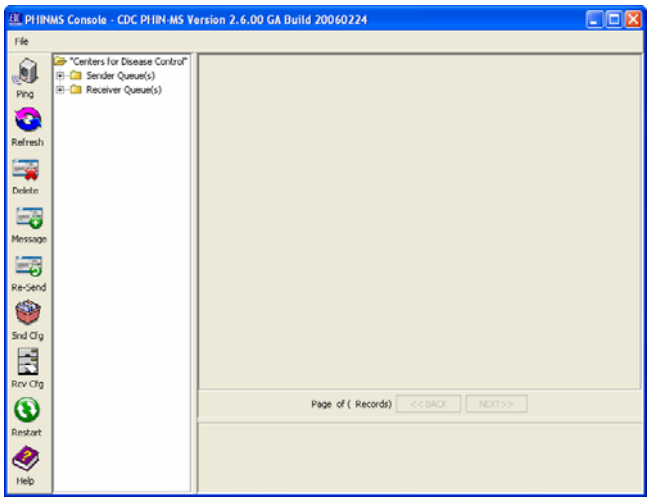

Figure 5.23. PHINMS Console

159. double click **Snd Cfg** displaying Figure 5.24,

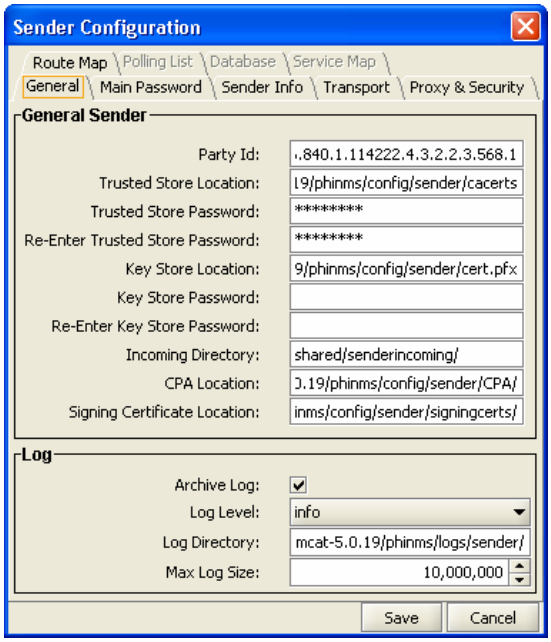

Figure 5.24. Sender Configuration

160. select **Route Map** tab displaying Figure 5.25,

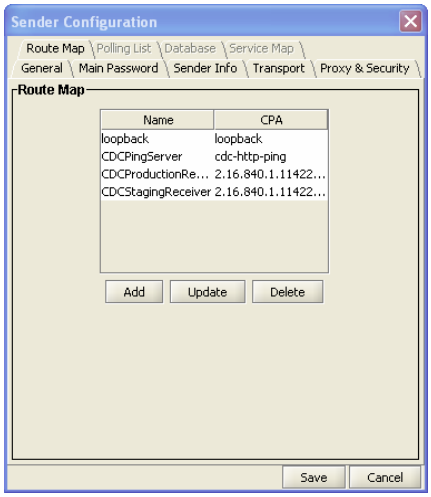

Figure 5.25. Route Map

161. select **Add** displaying Figure 5.26,

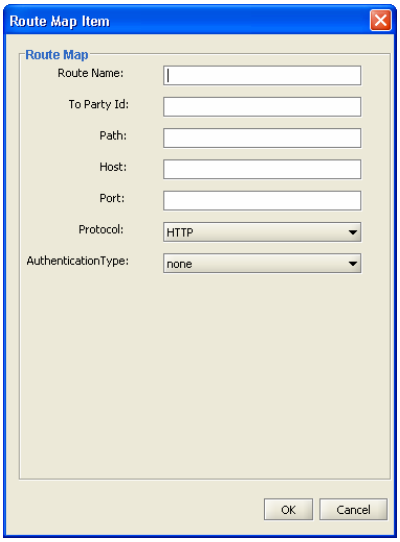

Figure 5.26. Route Map Item

162. enter Route Name, To Party Id, Path, Host, Port, Protocol, AuthenticationType, click OK, click Save, and

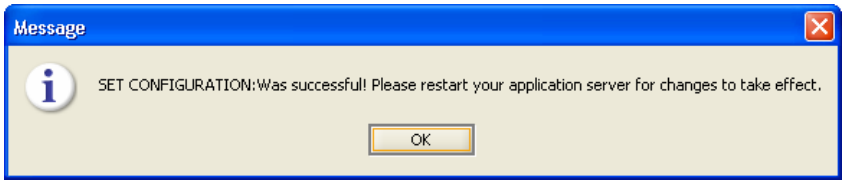

Figure 5.27. Set Configuration

163. click **OK**.

6.0 RECEIVER INFORMATION

6.1 Configure WorkerQ

The Worker Queue (WorkerQ) is the database table used for storing inbound messages. When configured from the Receiver configuration screen in the Console, it is used to drop incoming messages sent to the Receiver. The database configuration needs to be completed before creating WorkerQ table. The instructions to configure a database connection to the external database are in Section 4.0.

If configured from the Sender configuration screen in the Console, it is used to write the responses to polling requests (route-not-read configuration). More information on Sender configuration can be located in the PHINMS Technical Reference Guide.

Create an external database WorkerQ table by following steps below:

164. select **Rcv Cfg** displaying Figure 6.1,

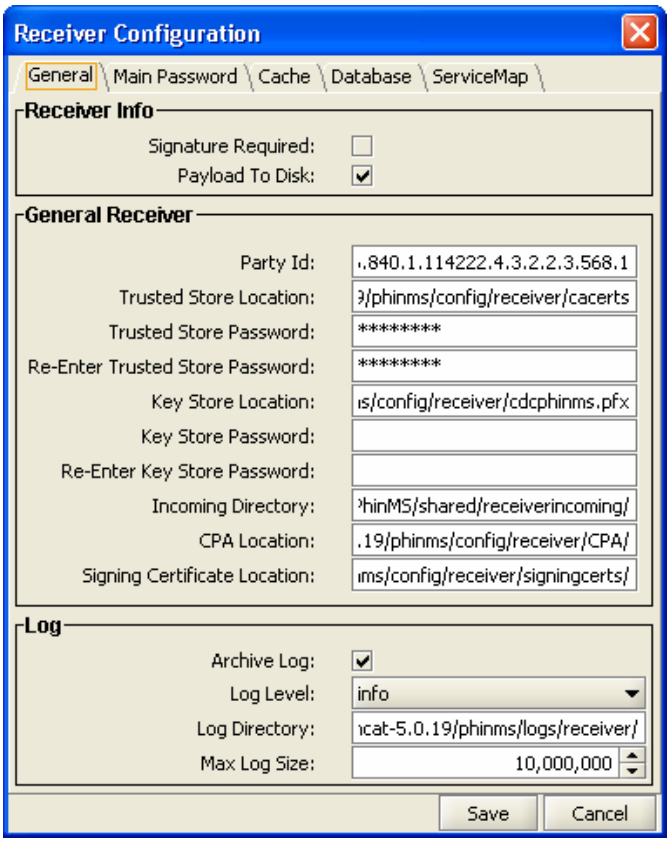

Figure 6.1. Receiver Configuration

165. select the **Database** tab displaying Figure 6.2,

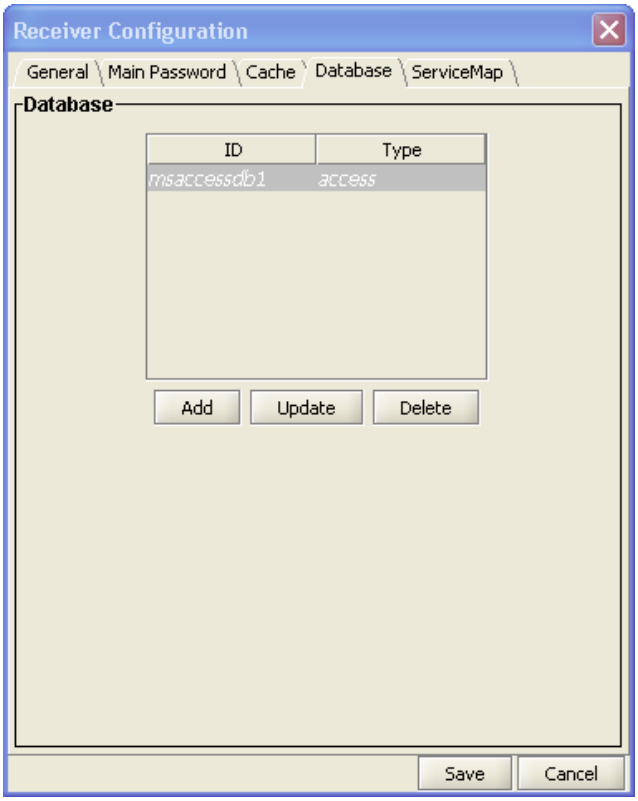

Figure 6.2. Database Configuration

166.click **Add** displaying Figure 6.3,

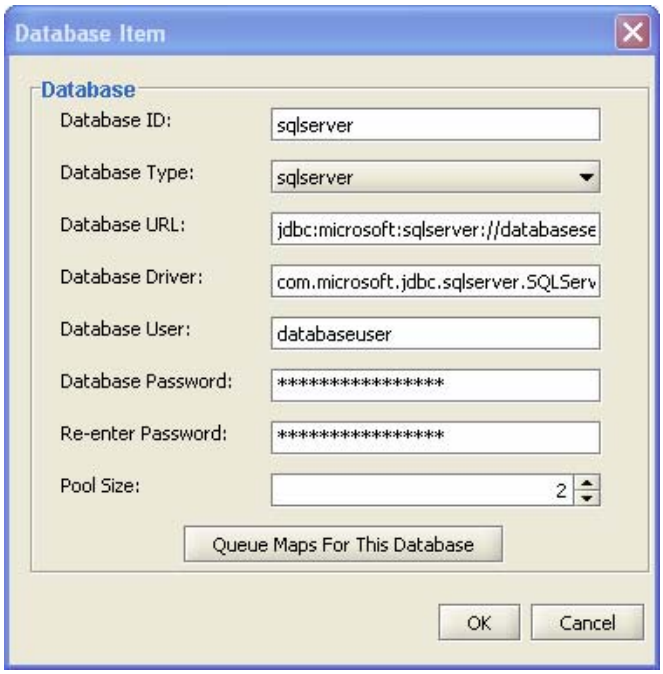

Figure 6.3. Database Item

167. enter the database items using Table 2 for an explanation of the values,

Tag Value	Description
Database ID	The unique name for the database connection pool, referenced in the queue map. The service map uses the **databaseId** to map the queue to a specific database.
Database Type	Designates the type of database.
Database URL	The URL to the database. The URL depends on the type of database and driver used such as **jdbc:microsoft:sqlserver://host:portnumber;DatabaseName=database** for Microsoft SQL Server and **jdbc:oracle://host:port:sid** for Oracle.
Database Driver	The type of JDBC driver. The JDBC driver should be appropriate for the type of database such as **com.microsoft.jdbc.sqlserver.SQLServerDriver** for Microsoft SQL Server and **oracle.jdbc.OracleDriver** for Oracle.
Database User	A pointer to the database user entry in the Message Receiver's encrypted password store. The value is not the database user but the name of the tag within the password file. The value of the tag contains the actual database user name.
Database Password	A pointer to the database password entry in the Message Receiver's encrypted password store. The value is not the database password but the tag within the password file. The value of the tag contains the actual database password.
Pool Size	The number of database connections to open. When setting the pool size ensure the system can handle the maximum client load while keeping enough memory available.

Table 2. WorkerQ Database Tag Values

168. click **Queue maps For This Database** displaying Figure 6.4,

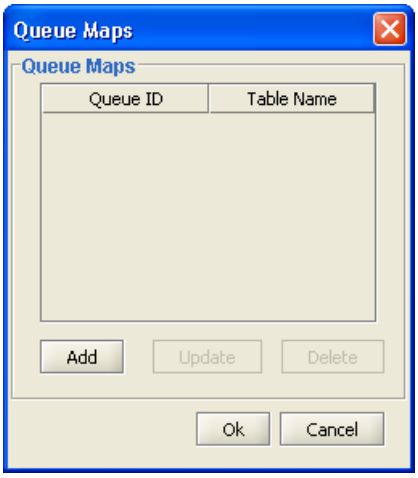

Figure 6.4. Queue Maps

169. click Add displaying Figure 6.5,

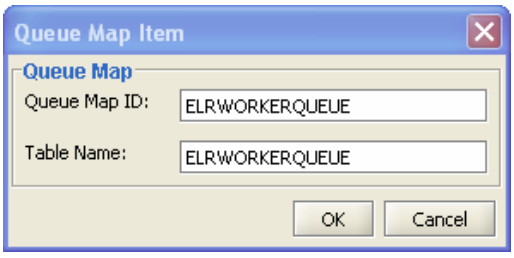

Figure 6.5. Queue Map Item

170. enter Queue Map ID and Table Name,
171. click **OK**, **OK**, **OK**, **OK**, **Save**, and
172. select **Restart**.

6.2 Create Service and Action Pair

Each message sent using PHINMS 2.6.00 has a message envelope. The envelope has addressing information tags called Service and Action known as character strings. Character strings are logically mapped to an application queue on the receiving side. The Service and Action tags determine the message type.

Create a Service and Action pair by completing the following steps:

173. select **Rcv Cfg** displaying Figure 6.6,

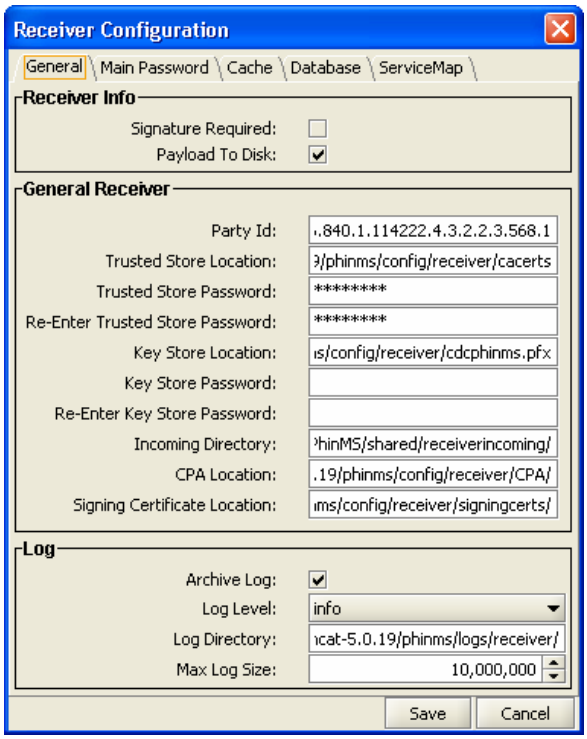

Figure 6.6. Receiver Configuration

174. select the **Service Map** tab displaying Figure 6.7,

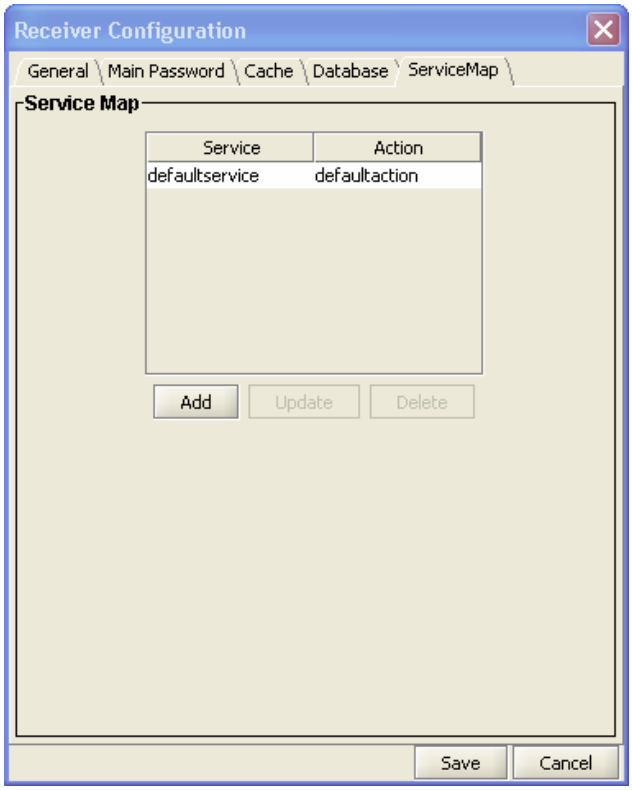

Figure 6.7. Service Map

175.click **Add** displaying Figure 6.8,

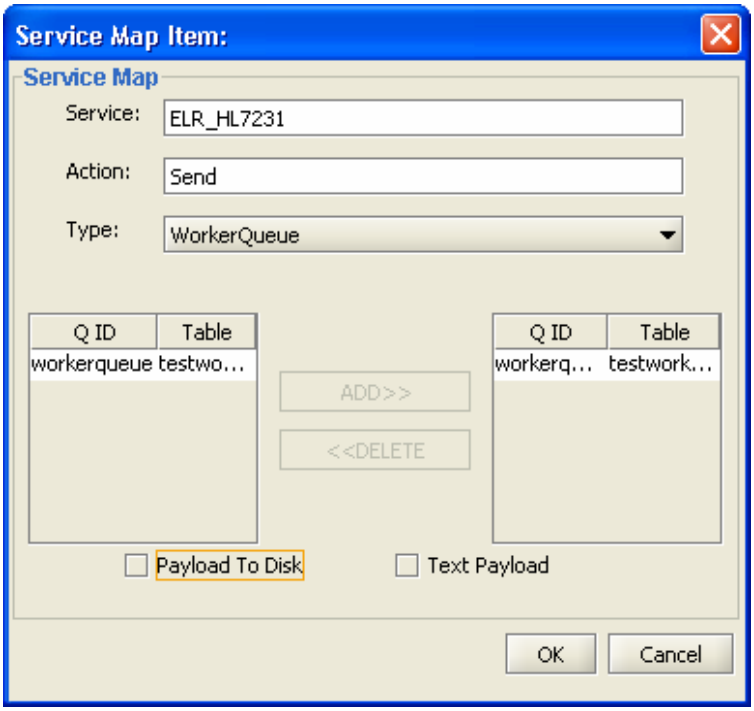

Figure 6.8. Service Map Item

176. enter **Service**, **Action**, select **WorkerQueue** from the dropdown list, highlight **workerqueue** located under Q ID in the left table, click **Add**, click **OK** displaying Figure 6.9,

Figure 6.9. Service and Action Added

177. select **Save** displaying Figure 6.10, and

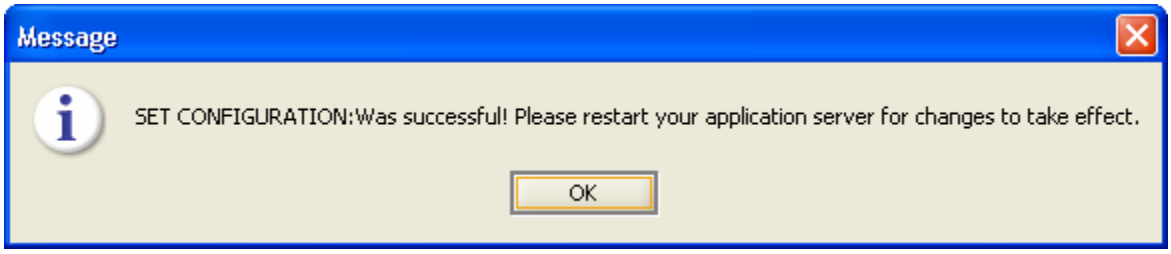

Figure 6.10. Successful Configuration

178. select **Restart**.

6.3 Configure Service Map

179. select **Rcv Cfg** displaying Figure 6.11,

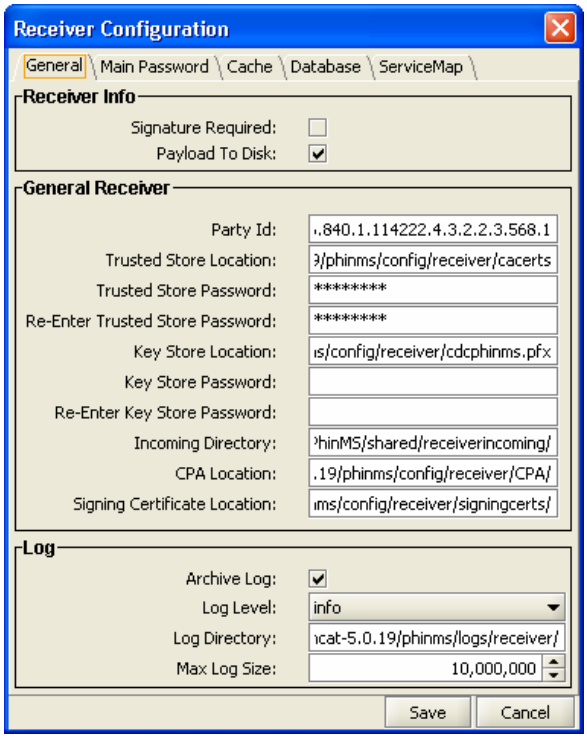

Figure 6.11. Receiver Configuration

180.select **Service Map** displaying Figure 6.12,

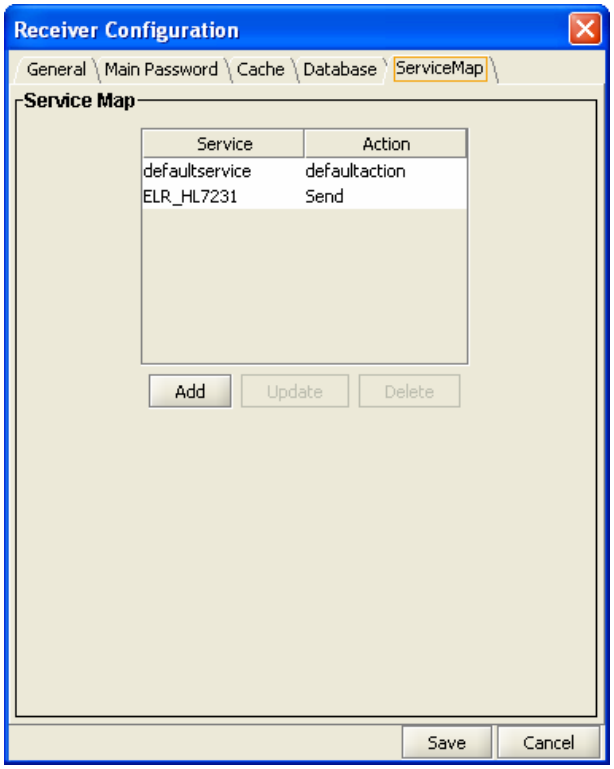

Figure 6.12. Service Map Receiver Configuration

181. click **Add**, displaying Figure 6.13,

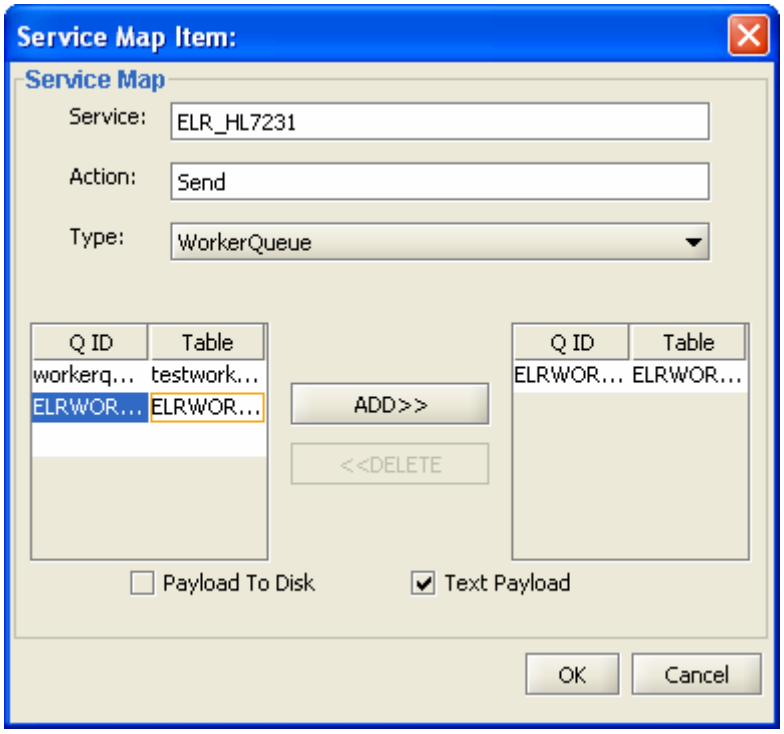

Figure 6.13. Service Map Item

182. enter the following parameters:

- Service: **ELR_HL7231**,
- Action: **Send**,
- Type: **WorkerQueue** opening the service map item,

Note: The Service and Type displayed in Figure 6.13 could use different terms depending on the program used.

183. highlight **ELRWORKERQUEUE QID**, click **Add** moving the Q ID to the right,

184. check Text Payload,

Note: When Payload to Disk is checked the incoming payload is written to disk instead of to the database field. In this case the name of the local file on disk is stored in the WorkerQ table. When Text Payload is checked, the payload is written to the **payloadTextContent** field. When Text Payload is not checked, the payload is written to the **payloadBinaryContent** field in the WorkerQ.

185. click **OK**, and

186. click **Save** returning to the PHINMS console.

Send a dummy message to test the setup. Verify the TransportQ and WorkerQ data fields are correct.

7.0 UNINSTALL PHINMS 2.6.00

Uninstalling PHINMS 2.6.00 requires completing the steps listed below:

187. select **Start** > **Programs** > **PHINMS** > **Uninstall PHINMS** displaying Figure 7.1,

Figure 7.1. Uninstall Welcome

188. click **Next** displaying Figure 7.2,

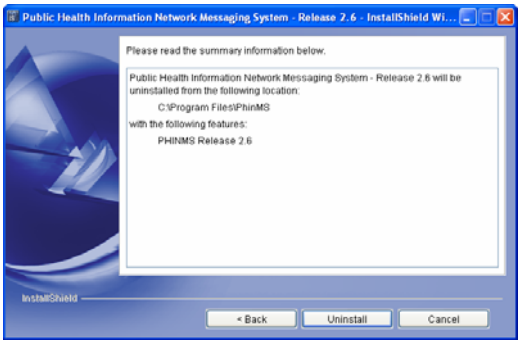

Figure 7.2. Uninstalled Summary

189. click **Uninstall** displaying Figure 7.3, and

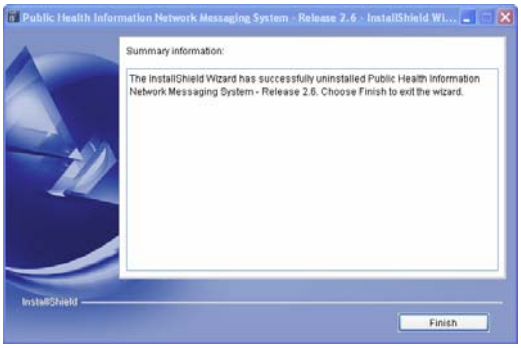

Figure 7.3. Successful Uninstall

190. click **Finish**.