



Public Health Information Network Messaging System

Implementing New VeriSign G2 Intermediate Certificate on Windows Systems

Version: 1.0.0

Date: September 29, 2009



EXECUTIVE SUMMARY

VeriSign is requiring all new Secure Socket Layer (SSL) certificates (Server Side certificates) issued by VeriSign contain an Intermediate Certificate Authority (CA) certificate. The Intermediate CA enhances the security of the SSL certificate by incorporating a two-tier hierarchy trust chain. For more information on the VeriSign Intermediate certificate, please visit: http://www.verisign.com/support/advisories/page_040611.html.



REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0.0	Dawn Fama	07-14-09	



TABLE OF CONTENTS

1.0	Keytool Update Instructions	5
1.1	PHINMS Windows Version 2.1 thru 2.6.....	5

LIST OF FIGURES

Figure 1.	cacerts File Locations	5
Figure 2.	VeriSign Enrollment.....	5
Figure 3.	Keytool Command.....	6
Figure 4.	cacerts Directory.....	6

ACRONYM LIST

The acronyms listed below are used in this document.

CA	Certificate Authority
CDC	Centers for Disease Control and Prevention
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System
SSL	Secure Socket Layer

1.0 KEYTOOL UPDATE INSTRUCTIONS

1.1 PHINMS Windows Version 2.1 thru 2.6

Complete the following steps to update Windows versions 2.1 thru 2.5 of PHINMS:

Search for the cacerts file locations using Windows Explorer. Make note of the locations, as the updated (by keytool) cacerts file will be copied over the existing cacerts files.

Copy the cacerts file from the *sender folder* (circled in Figure 1) into the folder where the keytool is located. This will make using the keytool command line entries simpler. (e.g. C:\Program Files\Phinms\jdk\bin.)

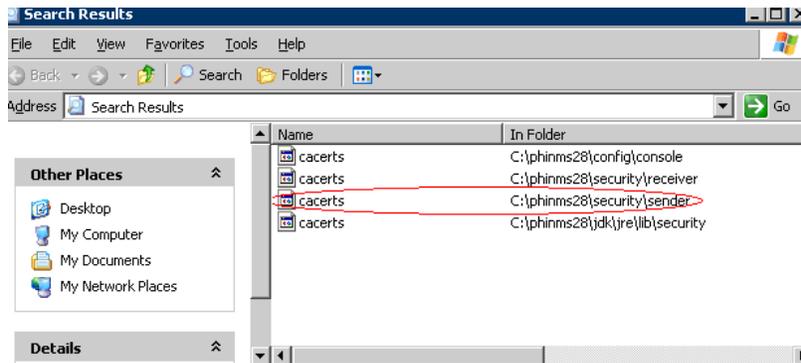


Figure 1. cacerts File Locations

2.0 Request or Download G2 Certificate File Options

Complete the following steps if requesting the certificate from the PHIN Help Desk:

1. Send an email to phintech@cdc.gov requesting a new G2 certificate for PHINMS. The certificate received should be titled “VeriSignCertG2.cer”. ** Please specify your PHINMS version in request.

Copy the file to the keytool folder. (e.g. C:\Program Files\Phinms\jdk\bin.) and continue to step 10.

Complete the following steps if the certificate is downloaded from Verisign:

Navigate to the VeriSign site: <http://www.verisign.com/support/verisign-intermediate-ca/secure-site-intermediate/index.html>.

Locate the certificate denoted with the following text: “If you Enrolled After May 17th, 2009 please use the following” as shown in Figure 2.

If you Enrolled After May 17th, 2009 please use the following:



Figure 2. VeriSign Enrollment

Click the “Select All” button.

Copy the contents by pressing Ctrl-C.

Open a text editor (e.g. Notepad) and paste (Ctrl-V) the text copied from step 4.

Save the file as “VeriSignCertG2.cer” in the keytool location: E.g. C:\Program Files\Phinms\jdk\bin

Open a command prompt.

Navigate to the keytool directory using the following command:

```
cd C:\Program Files\Phinms\jdk\bin
```

Type the keytool command shown in Figure 3. (keytool -v -importcert -file VeriSignCertG2.cer -keystore cacerts -storepass changeit)

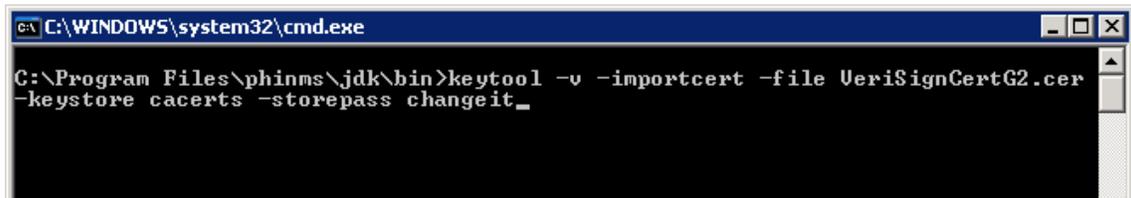


Figure 3. Keytool Command

When the command is successful, the following message in the command window will appear:
Certificate was added to keystore

[Storing cacerts]

Complete the following steps after receiving the *Certificate was added to keystore* message.

Copy the new cacerts file from C:\Program Files\Phinms\jdk\bin\ to the directories shown in Figure 4.

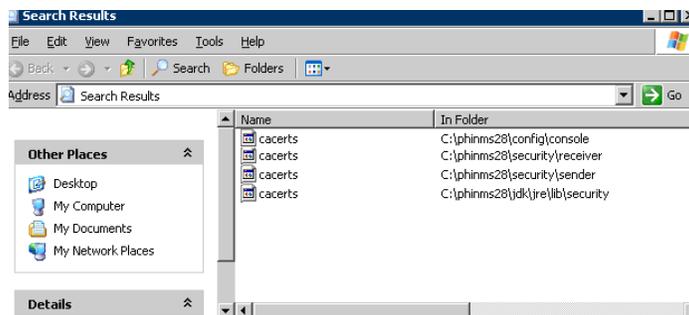


Figure 4. cacerts Directory

Restart PHINMS

Test