AEGIS

Developers Integration Lab (DIL)
Certificate Installation Instructions

Version 1.4

July 22, 2013

REVISION HISTORY

REVISION	DATE	DESCRIPTION
0.1	17 September 2011	First Draft Release – DIL Certificate Installation Instructions
0.2	17 September 2011	Updated certificate download link examples
1.0	13 November 2012	First Publication Release – DIL Certificate Installation Instructions
1.1	3 January 2013	Addition of section 5.4.6 describing how to import alternate certificates for use with other environments
1.2	20 January 2013	Added general grammatical changes
1.3	22 May 2013	Included additional steps for Certificate Set Up
1.4	22 July 2013	Added section 5.4.7

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE

This document provides the required steps to download, install, and configure a DIL Certificate.

1.2 SCOPE

The instructions in this document are applicable to all participants, both internal and external, in the DIL environment.

2. DOCUMENT DESCRIPTION

This document includes the following sections:

- Section 1.0 Introduction
- Section 2.0 Document Description
- Section 3.0 Referenced Documents
- Section 4.0 Problem Description & Goals
- Section 5.0 Instructions

3. REFERENCED DOCUMENTS

- N/A

4. PROBLEM DESCRIPTION & GOALS

Communication between gateways requires a secured transport mechanism. This is accomplished by SSL certificates issued to each gateway server AEGIS.net is a Certificate Authority with the ability to issue SSL certificates using the following hierarchy:

AEGISROOTCA → AEGISDILCA → [Issued Server Certificate]

The hierarchy mentioned above is the three-level certificate architecture used within the DIL. All SSL certificates are of the type PKS-12, however you can add your own private certificate under the trust chain as well. If you are planning on using the Private Cert provided by the DIL, please skip over section 5.4.6.

If you change your machine name at any time, you will need to generate a new certificate. This can be done by notifying the development team at DIL_Support@aegis.net.

5. INSTRUCTIONS

These instructions are intended for use by a participant within the DIL environment. The participant must first complete the self-registration of their DIL account.

5.1 REQUIRED INFORMATION

1. The participant must provide the full machine name of the gateway server as part of their Gateway Profile.
    a. Example of machine name – "machine.domain.com"
2. The participant's CA account information is then defined as:
    a. Your account name will be your machine name; e.g. "machine.domain.com".
    b. Your password will be your machine name without the domain extension; e.g. "machine".
    c. If you do not know your password, please contact the DIL Help Desk Support.

5.2 DOWNLOAD YOUR CERTIFICATE

1. Once logged onto the DIL Test Platform application select the "Download Certificate" menu item.
2. Then select the following link on the "Download Certificate" page:

    Please download your DIL private certificate here machine.domain.com.p12

3. You will now be prompted with a browser dialog to either open or save. Note that if your browser is configured to save by default, you may not see this window. Save your certificate file to your local machine.
    a. Your certificate file name will be your gateway machine name with a ".p12" extension; e.g. "machine.domain.com.p12"
    b. If the install fails, please contact DIL Help Desk Support.

5.3 DOWNLOAD THE CA CERTIFICATES

Your certificate is the end of a three-part chain. You need to download the other two certificate parts: AEGISROOTCA and AEGISDILCA.

1. Select the following link on the "Download Certificate" page to download the AEGISROOTCA:

   Please download the DIL Root certificate here AEGISROOTCA.pem

2. Select the following link on the "Download Certificate" page to download the AEGISDILCA:

   Please download the DIL Cross certificate here AEGISDILCA.pem

5.4 NON-FIPS INSTALLATION (Windows / Glassfish)

5.4.1 SETUP YOUR WORK FOLDER

Windows XP/2003 Server 64 bit is the operating system and Glassfish 2.1.1 is the target application server for these instructions.

1. Create a work folder; e.g. C:\Sun\AppServer\certificaterequest
2. Copy all certificates generated and downloaded from the AEGIS.net CA site to your work folder.
3. Copy the cacerts.jks truststore from the Glassfish domain config folder:

   C:\Sun\AppServer\domains\domain1\config\cacerts.jks

4. Open a command prompt window and change directory to your work folder.

5.4.2 KEYSTORE AND TRUSTSTORE

Execute the following commands to generate your keystore and install the certificates to your keystore and truststore. **Replace the text "<*machine*>" with the value of your machine name.**

IMPORT PKCS12 KEYSTORE TO JAVA KEYSTORE

keytool -importkeystore -srckeystore **<*machine*>**.aegis.net.p12 -srcstoretype PKCS12 -deststoretype JKS -destkeystore gateway.jks

** You will be prompted to enter your password three (3) times. After correctly entering your password you should have an output similar to this:*

```
Enter destination keystore password:
Re-enter new password:
```

```
Enter source keystore password:
Entry for alias <machine>.aegis.net successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

***NOTE**: The "destination keystore password" above is the password specific to the machine or IP address registered with the DIL.*

VERIFY JAVA KEYSTORE

keytool -list -v -keystore gateway.jks > gatewayList

** You will be prompted to enter your password. This will list the private key details. Examine the output to insure there are no errors.*

IMPORT CHAIN OF TRUST CERTIFICATES TO THE TRUSTSTORE

keytool -import -v -trustcacerts -alias AEGISROOTCA -file AEGISROOTCA.pem -keystore cacerts.jks -keypass changeit -storepass changeit

** Enter "yes" or "y" to the prompt. You should see the following output:*

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing cacerts.jks]
```

***NOTE**: The "keypass" value is the literal value "changeit". The "storepass" value is the password specific to the machine or IP address registered with the DIL.*

keytool -import -v -trustcacerts -alias AEGISDILCA -file AEGISDILCA.pem -keystore cacerts.jks -keypass changeit -storepass changeit

** No input is required. You should see the following output:*

```
Certificate was added to keystore
[Storing cacerts.jks]
```

***NOTE**: The "keypass" value is the literal value "changeit". The "storepass" value is the password specific to the machine or IP address registered with the DIL.*

keytool -importkeystore -srckeystore ***<machine>***.aegis.net.p12 -srcstoretype PKCS12 -deststoretype JKS -destkeystore cacerts.jks

** You will be prompted to enter the truststore password followed by your password. You should see the following output:*

```
Enter destination keystore password:
Enter source keystore password:
Entry for alias d6ctptl1.aegis.net successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

VERIFY THE TRUSTSTORE CONTENTS

keytool -list -keystore cacerts.jks > cacertsList

** You will be prompted to enter the truststore password. This will list all of the trusted certificates. Examine the output to insure the imported certificates are present – "aegisrootca", "aegisdilca" and "<machine>.domain.com".*

***NOTE**: The truststore password is the password specific to the machine or IP address registered with the DIL.*

IMPORT ALL CERTIFICATES TO YOUR KEYSTORE

keytool -import -v -trustcacerts -alias AEGISROOTCA -file AEGISROOTCA.pem -keystore gateway.jks -keypass ***<machine>*** -storepass ***<machine>***

** Enter "yes" or "y" to the prompt. You should see the following output:*

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing cacerts.jks]
```

keytool -import -v -trustcacerts -alias AEGISDILCA -file AEGISDILCA.pem -keystore gateway.jks -keypass ***<machine>*** -storepass ***<machine>***

** No input is required. You should see the following output:*

```
Certificate was added to keystore
[Storing cacerts.jks]
```

VERIFY KEYSTORE CONTENTS

keytool -list -keystore gateway.jks > gatewayList2

** You will be prompted to enter your password. This will list all of the trusted certificates. Examine the output to insure the imported certificates are present – "aegisrootca", "aegisdilca" and "<machine>.aegis.net".*

5.4.3 INSTALL THE CERTIFICATES (GLASSFISH)

1. Copy the keystore and truststore files from your work folder to the Glassfish domain config folder:

   C:\Sun\AppServer\domains\domain1\config\gateway.jks

   C:\Sun\AppServer\domains\domain1\config\cacerts.jks

5.4.4 UPDATE GLASSFISH DOMAIN CONFIGURATION

Modify the "domain.xml" Glassfish configuration file to now use your new keystore.

1. Locate and update all “key.alias” values to your certificate alias; i.e. “***<machine>***.domain.com”.
2. Update the following <jvm-options> settings related to your keystore:

```
-Djavax.net.ssl.keyStore=${com.sun.aas.instanceRoot}/config/gateway.jks
-Djavax.net.ssl.keyStorePassword=<machine>
-DSERVER_KEY_ALIAS=<machine>.domain.com
-DCLIENT_KEY_ALIAS=<machine>.domain.com
-
Dcom.sun.enterprise.security.httpsOutboundKeyAlias=<machine>.domain.com
```

5.4.5 VERIFY GLASSFISH DOMAIN CONFIGURATION

1. Start your Glassfish server.
2. Examine the server logs after the application server start up is complete and verify that there are no errors.

5.4.6 USE OF ALTERNATIVE CERTIFICATES

You may store and use additional, alternate certificates in your keystore and truststore files if your test system has the need to communicate with other testing environments. An example of this would be if your test system will also be used for onboard testing with the ***eHealth Exchange*** (formerly the NwHIN). The DIL Certificate Architecture mirrors that of the ***eHealth Exchange*** in that it relies on 3 levels, the Root Certificate, Cross Certificate, and finally the Private certificate. This ‘Chain of Trust’, i.e. the Root and Cross certificates validates and trusts the private certificate.

You must first successfully obtain the required ***eHealth Exchange*** Root Certificate, Cross Certificate, and their Private certificate. Please refer to the CONNECT Open Source Wiki page, “Certificate Setup”, for specific instructions. This page is found at:

https://developer.connectopensource.org/display/CONNECTWIKI/Certificate+Setup

The following steps are those that are needed to add these certificates to your existing keystore and truststore files:

C:\Sun\AppServer\domains\domain1\config\gateway.jks

C:\Sun\AppServer\domains\domain1\config\cacerts.jks

IMPORT THE WEB SERVICE [PRIVATE] CERTIFICATE:

keytool -import -v -trustcacerts -alias gateway -file servercert.bin -keystore gateway.jks -keypass changeit -storepass changeit

** The -keypass and -storepass passwords need to match those of the "servercert.bin" and "gateway.jks" respectively.*

IMPORT CHAIN OF TRUST CERTIFICATES TO THE TRUSTSTORE

keytool -import -v -trustcacerts -alias entrust -file cacert.crt -keystore cacerts.jks -keypass changeit -storepass changeit

** The -keypass and -storepass passwords need to match those of the "cacert.crt" and "cacerts.jks" respectively.*

** Enter "yes" or "y" to the prompt. You should see the following output:*

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing cacerts.jks]
```

keytool -import -v -trustcacerts -alias entrust-cross -file cross.crt -keystore cacerts.jks -keypass changeit -storepass changeit

** The -keypass and -storepass passwords need to match those of the "cross.crt" and "cacerts.jks" respectively.*

** No input is required. You should see the following output:*

```
Certificate was added to keystore
[Storing cacerts.jks]
```

5.4.7 Certificate Revocation List (CRL) Checking

Certificate Revocation Lists (CRLs) are lists of certificates that are no longer valid or that have been revoked by a Certification Authority (CA). Each gateway must implement either Online Certificate Status Protocol (OCSP) based certificate revocation checking or use CRLs against an NHIN-governed CA to determine the revocation status of each certificate.

To enable the CRL checking in glassfish application server, add the following two JVM options in the domain.xml file as the two properties would remain false by default. You will need JDK 6 update 18 or later versions for supporting CRL checking.

<jvm-options>-Dcom.sun.net.ssl.checkRevocation=true</jvm-options>
<jvm-options>-Dcom.sun.security.enableCRLDP=true</jvm-options>

For debugging certification issues, add the following jvm option in domain.xml

<jvm-options>-Djava.security.debug=certpath</jvm-options>

For other application servers, please check your server documentation regarding enabling CRL checking.

FOR CRL checking, you need to open port 9345 at firewall so that you can have access to CRL list at http://ca.dil.aegis.net:9345/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=AEGISDILCA,O=AEGISnetInc,C=US.

5.5 FIPS INSTALLATION (Red Hat Linux / JBoss)

The following set of instructions is intended for users utilizing FIPS mode enabled on the participant machine.

5.5.1 SETUP YOUR WORK FOLDER

Red Hat Enterprise Linux is the operating system and Glassfish 2.1.1 or JBoss 5.1.0 are the target application servers for these instructions. The Mozilla NSS 3.12.4 datastore database is installed in the directory "/opt/fipsdb" for these instructions.

1. Create a work folder; e.g. /opt/fipsdb/cert
2. Copy all certificates generated and downloaded from the AEGIS CA site to your work folder.
3. Open a command prompt window and change directory to your work folder.

5.5.2 NSS DATASTORE

Execute the following commands to import your server certificate and the AEGIS DIL and ROOT CA certificates to your NSS datastore. **Replace the text "<*machine*>" with the value of your machine name.**

DISABLE FIPS MODE

modutil -fips false -dbdir /opt/fipsdb

** FIPS Mode must be disabled before making any modifications to prevent corruption of the NSS datastore. You will be prompted to continue. Simply press the Enter key again. You should see the following output:*

```
WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

FIPS mode disabled.
```

IMPORT PKCS12 SERVER CERTIFICATE TO THE NSS DATASTORE

pk12util -i ***<machine>***.domain.com.p12 -n ***<machine>***.domain.com -d /opt/fipsdb

** You will be prompted to enter the NSS password. After correctly entering that password, you will be prompted to enter the password for your server certificate. After correctly entering that password you should have an output similar to this:*

```
Enter Password or Pin for "NSS Certificate DB":
Enter password for PKCS12 file:
pk12util: PKCS12 IMPORT SUCCESSFUL
```

IMPORT THE AEGIS ROOT AND DIL CA CERTIFICATES

certutil -A -n "AEGISROOTCA" -t "TC,," -i AEGISROOTCA.pem -d /opt/fipsdb

certutil -A -n "AEGISDILCA" -t "TC,," -i AEGISDILCA.pem -d /opt/fipsdb

** No input is required.*

CONFIRM THE CONTENTS OF YOUR NSS DATABASE

certutil -L -d /opt/fipsdb

** No input is required. This will list all of the certificates. Examine the output to insure the imported certificates are present – "aegisrootca", "aegisdilca" and "<machine>.domain.com". You should see the following output:*

```
Certificate Nickname                                         Trust Attributes
                                                             SSL,S/MIME,JAR/XPI

<machine>.domain.com                                         u,u,u
AEGISDILCA                                                   TC,,
AEGISROOTCA                                                  TC,,
```

VERIFY THE CERTIFICATE CHAIN IS CORRECT

vfychain -d /opt/fipsdb ***<machine>***.domain.com

** No input is required. This will verify that the certificate chain has been correctly established. You should see the following output:*

```
Chain is good!
```

ENABLE FIPS MODE

modutil -fips true -dbdir /opt/fipsdb

** FIPS Mode must be enabled before (re)starting the application server. You should see the following output:*

```
WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

FIPS mode enabled.
```

5.5.3 UPDATE JBOSS SERVER CONFIGURATION

Follow the FIPS 140-2 Red Hat Linux / JBoss configuration instructions for CONNECT 3.2:

https://developer.connectopensource.org/display/NHINR32/FIPS+Install+%28Linux+and+JBoss%29

5.5.4 VERIFY JBOSS SERVER CONFIGURATION

1. Start your JBoss server.
2. Examine the server logs after the application server start up is complete and verify that there are no certificate errors.