IIB Certificates

REF; <http://www.davidbolton.com/?p=74>

1. Open a command prompt and navigate to C:\Program Files (x86)\IBM\WebSphere MQ\java\jre\bin

Execute the following command:keytool -genkey -alias tomcat -keyalg RSA -keystore iibdev.keystore

1. Enter a keystore password (fghdev) . Instead of “your name”, use the FQDN of the server that it runs on.( Iibdev.ottouk.com) Add the OU and other questions. If a typo is entered just hit CTRL+C to kill the process and the keystore will not be created (until the very end). If at the end and the keystore is fubar’d just delete and start over.
2. Execute the following command:  
   keytool -certreq -keyalg RSA -alias tomcat -file certkey.txt -keystore iibdev.keystore

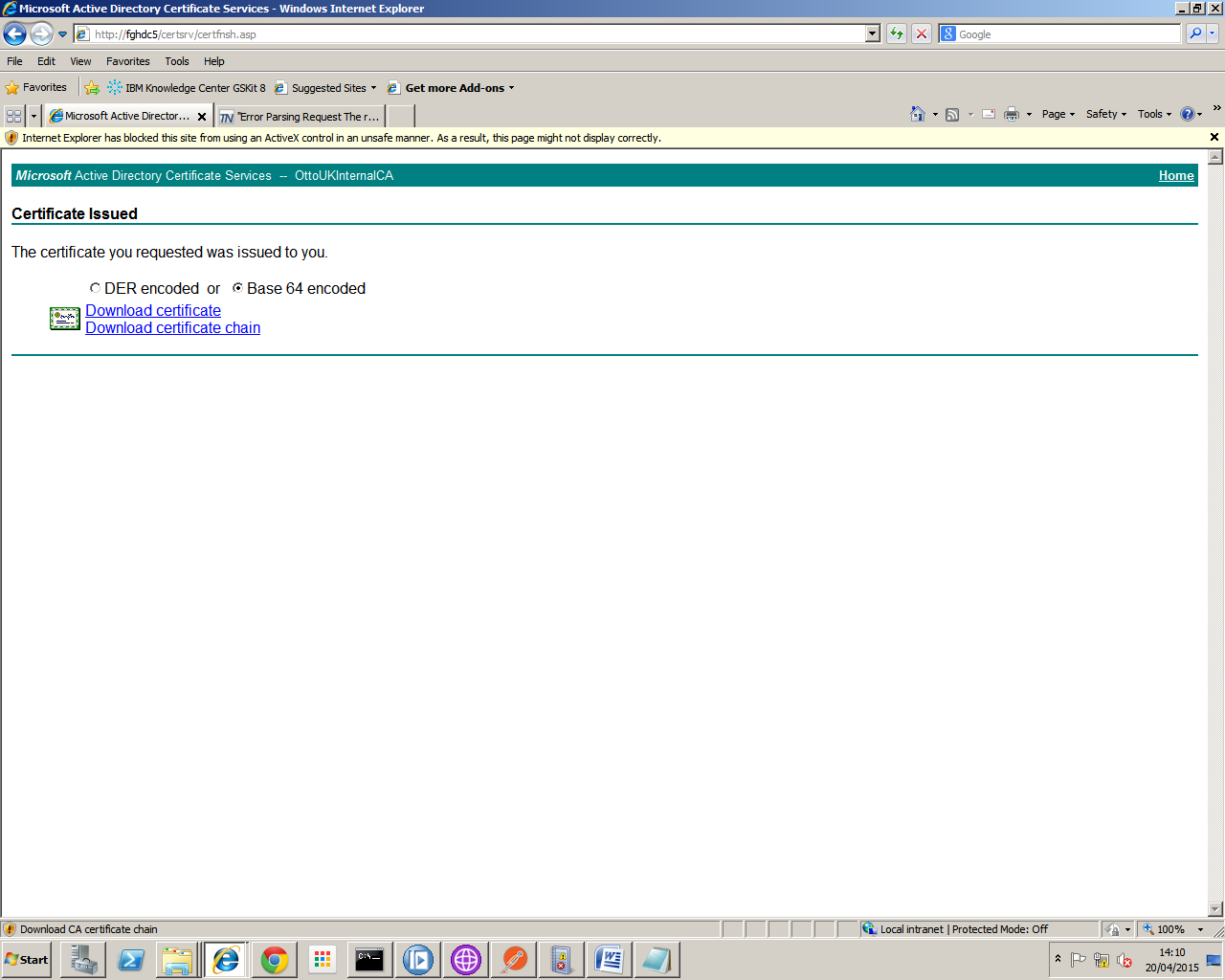
This creates a txt file cert request in C:\Program Files (x86)\IBM\WebSphere MQ\java\jre\bin

1. Enter the keystore password from step 4.
2. In steps 8-13, access the private CA with domain admin credentials or higher in order to view server-based certificates, otherwise only user based certificates will be available (user, basic EFS).
3. Open Internet Explorer (using domain admin privileges) and select the private CA address (http://fghdc5/certsrv).

Next, get a copy of the Root CA and save it to the same path as seen in the command prompt: Select the link “Download a CA certificate, certificate chain, or CRL” then select “Download CA certificate” and save it (certnew.cer) to C:\Program Files (x86)\IBM\WebSphere MQ\java\jre\bin

.

1. Next, request a certificate from the CA. The easiest way to do this is to just hit the “back” button in Internet Explorer. Select “Request a certificate” and then “advanced certificate request”.
2. Now select “ Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.”
3. Now open the certkey.txt file (from step 5) and copy and paste the contents into the first text box. Next, under ” Certificate Template” select “Web Server” and then click the Submit button at the bottom.
4. Go to fghdc5, open certfifcation authority and issue the certificate.
5. The page will now present download links to the certificate. Select the “Download certificate chain” link and save the file (certnew.p7b) to C:\Program Files (x86)\IBM\WebSphere MQ\java\jre\bin.



1. Now go back to the command prompt and execute the following command:keytool -import -alias tomcat -keystore iibdev.keystore -trustcacerts -file certnew.p7b

Install reply = yes

1. \*\*\* Don’t think this is needed\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*It is requisite that the private CA’s root certificate is added to the list of trusted CAs in the Java cacerts file. The Java cacerts file uses the standard *changeit* password for access. Type the following command (selecting any desired alias name):keytool -import -alias iibdevcacert -keystore ..libsecuritycacerts -file certnew.cer

Trust this certificate = yes

1. Verify the certificate signing by entering the following command:

keytool -list -v -keystore iibdev.keystore -storepass fghdev (password from step 4)

Two certificates should be listed, the first being the iibdev web server certificate and the second being the Root CA certificate. Syntax will be as follows:

Entry type: keyEntry

Certificate chain length: 2

Certificate[1]:

Certificate[2]:

Open IBM Integration Console.

* 1. Enable SSL on the Integration Node.

mqsichangeproperties IB9NODE –b httplistener –o HTTPListener –n enableSSLConnector –v true

* 1. Configure the integration node with keystore information

Mqsichangeproperties IB9NODE –b httplistener –o HTTPSConnector –n keystoreFile –v “C:\Program Files (x86)\IBM\WebSphere MQ\java\jre\bin\iibdev.keystore”

* 1. Set the Keystore password

Mqsichangeproperties IB9NODE –b httplistener –o HTTPSConnector –n keystorePass –v fghdev

* 1. Set the Port for HTTPS SSL connections.

Mqsichangeproperties IB9NODE –b httplistener –o HTTPSConnector –n port –v 7083

* 1. Configure truststore information.

mqsichangeproperties IB9NODE –b httplistener –o HTTPSConnector –n truststoreFile –v“C:\Program Files (x86)\IBM\WebSphere MQ\java\jre\bin\iibdev.keystore”

* 1. Configure the truststore password.

mqsichangeproperties IB9NODE –b httplistener –o HTTPSConnector –n truststorePass –v fghdev

* 1. Disable Client Authentication.

mqsichangeproperties IB9NODE –b httplistener –o HTTPSConnector –n clientAuth –v false

mqsichangeproperties IB9NODE –o BrokerRegistery –n brokerTruststoreFile –v “C:\Program Files (x86)\IBM\WebSphere MQ\java\jre\bin\iibdev.keystore”

mqsisetdbparms IB9NODE –n brokerTruststore::password –u temp –p fghdev

mqsistop IB9NODE

mqsistart IB9NODE

In IBM Broker Explorer

On the properties of the HTTPInput Node tick the https box.