**Steps to make connection secure (HTTP to HTTPS) between**

**Client and Server**

1. We need to create a self-signed certificate at the IIS manager.
   1. Login in to EC2 instance and open IIS. From left panel, click on the server name and navigate to “Server Certificates”:

A screenshot of a cell phone

Description automatically generated

1.2 From the right panel, click on “Create Self-Signed Certificate”:

A screenshot of a social media post

Description automatically generated

1.3 Specify a name for the self-signed certificate:

A screenshot of a cell phone

Description automatically generated

1.4 Now we can see the new created certificate in the Server Certificates list:

A screenshot of a social media post

Description automatically generated

1.5 Bind the server certificate to the application.

From the left panel, click on the Default Web Sites. On the right panel, click on the “Bindings”:

A screenshot of a social media post

Description automatically generated

1.6 In Site Bindings tab, add a new Site binding for HTTPS on port 443. Select the new created self-signed certificate from the SSL Certificate dropdown menu:

A screenshot of a computer

Description automatically generated

1.7 Configure the site to accept SSL certificate.

From the left panel, navigate to Sites 🡪 Default Web Site 🡪 SSL settings.

A screenshot of a computer

Description automatically generated

Do the following changes to the SSL settings and click ‘Apply’ to save the changes:

A screenshot of a social media post

Description automatically generated

1. After configuring IIS to listen HTTPS on port 443, client-side source code needs to be updated to accept the self-signed certificates.

2.1 A new class ***UnsafeOkHttpClient*** ​should be created to support **OkHttpClient** ​with self-signed certificate.

In *Api.java* file comment line “okHttpClient client = new okHttpClient.Builder().addInterceptor(interceptor).build();” and add new line

“okHttpClient client = UnsafeOkHttpClient.getLoginUnsafeOkHttpClient();”

Below is the code snippet of updated Api.java file:

A screenshot of a social media post

Description automatically generated

2.2 Use the contents of below file, to copy into UnsafeOkHttpClient.java file.



2.3 In *CommonUtils.java* file, the **MlaBaseURL** needs to be updated from http to https as shown in below screenshot.



1. At Postman, since this certificate is self-signed and cannot be verified. Therefore, we need to switch off the SSL certificate verification.

Navigate to Settings 🡪 General, switch off SSL certificate verification option. Below is the screenshot of the changes made to Postman settings:

A screenshot of a computer

Description automatically generated

1. To verify if the connection is secure, test a GET or POST method with HTTPS protocol.

Below is the POSTMAN snippet where I can access application using HTTPS:

A screenshot of a social media post

Description automatically generated