Create a Private Key and Self-Signed Certificate for Testing

1. Run the following command to create a private key:

```
openssl genrsa -out private-key.pem 2048
```

Important: Anyone in possession of your private key could masquerade as your service, so store your key in a secure location.

2. Use a text editor to create a configuration file in the following form and save it as a `.cnf` file (for instance, `configuration.cnf`):

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no

[req_distinguished_name]
C = DE
ST = Provide your two letter state abbreviation
L = Provide the name of the city in which you are located
O = Provide a name for your organization
CN = Provide a name for the skill

[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @subject_alternate_names

[subject_alternate_names]
DNS.1 = Provide your fully qualified domain name
```

3. Replace the following content in the configuration file with your own values:

```
ST: Provide your two letter state abbreviation
L: Provide the name of the city in which you are located
O: Provide a name for your organization
CN: Provide a name for the skill
DNS.1: Provide the fully qualified domain name for your endpoint
```

Note that you must provide the domain name for your endpoint in the `DNS.1` section, so you may want to wait to create the certificate until you have this information.

See below for a completed sample configuration file.

4. Use the following command to generate a certificate. Specify the names you used for your `private-key.pem` and `configuration.cnf` files:

```
openssl req -new -x509 -days 365 \
            -key private-key.pem \
            -config configuration.cnf \
            -out certificate.pem
```

This produces a self-signed certificate in a file called `certificate.pem`.

Save the certificate `.pem`, private key `.pem`, and the configuration `.cnf` files in a safe place.

Create the Certificate for GeoFencing-Module

The name of the file must be `geoFencingSSL.cert` and must be in the **`hsupload`** Directory of the “Gira Expert Project”.

To create this file you concatenate your `private-key.pem` and `certificate.pem` files to `geoFencingSSL.cert`. It should look like:

```
-----BEGIN PRIVATE KEY-----
…
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
…
-----END CERTIFICATE-----
```

If the certificate file could not be read or does not exist the module will use **`http`** instead of **`https`**.

Example for a complete configuration file

It should look similar to the following example:

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no

[req_distinguished_name]
C = DE
ST = BE
L = Berlin
O = My Company Name
CN = GiraHS-GeoFencing

[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @subject_alternate_names

[subject_alternate_names]
DNS.1 = myaddress.dyndns.com
```

Other SSL Resources

See other resources about SSL and self-signed certificates. Note that these links for these tools take you to third-party sites.

- Open SSL
- How to Create A Self Signed Certificate
- How to Create a Self Signed Certificate using Java Keytool
- Java Keytool Reference