Running vREST Enterprise on SSL

To run vREST Enterprise server on SSL, please follow the steps below:

1. **Acquire the private key and certificate file from trusted certificate authority**
    a. For testing purposes, you may generate self signed certificate via openssl. For self signed certificates, browsers will show a warning to end users.
        i. You may execute the following command to generate the self signed certificate using openssl:

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
```

    b. So, for production purposes, it is recommended to acquire the private key and certificate file from trusted certificate authority.
    c. **Note:**
        i. As of now, vREST do not support passphrase for private keys.
        ii. And private key and certificate file must reside in the same directory where config.json file exists.
2. **Enable startOnHTTPS flag in config.json file**
    a. Set true for startOnHTTPS option in config.json file.
3. **Set the appropriate port in config.json file**
    a. Default port for HTTPS is 443, so you may set the port number to 443 in config.json file.
    b. If you are using the well-known port (0 - 1023), then you must execute the vREST Enterprise binary with administrative privileges. Otherwise the server will not start and will result in exception, **bind EACCESS**.
    c. Otherwise you may set any port number of your choice.

That's it.