# On-premises: creating a certificate

If you are using MyTimetable managed hosting, Eveoh will provide you with a certificate to upload. If you are an on-premises customer you will need to create this certificate yourself by performing the following steps:

1. We need to create a self-signed certificate. This can be done using the minimal openssl install found at https://files.eveoh.nl/openssl_min.zip (for Windows) or an OpenSSL install included in the OS (Linux). From the command line, create a self-signed certificate and enter a password (make sure to remember this), the university name, country and domain name of your MyTimetable instance (common name):

   ```
   openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 3650 -config openssl.cnf
   ```

2. MyTimetable requires the generated X.509 certificate and the corresponding private key to be available in a PFX file. Save the X.509 certificate and the private key into the PKCS12 format using OpenSSL:

   ```
   openssl pkcs12 -export -in cert.pem -inkey key.pem -out cert.pfx
   ```

You will require the `cert.pem` file when configuring the Azure AD application and the `cert.pfx` file when configuring MyTimetable.