**1. Sukurti paprastą svetainę vardu** [**http://open.lab**](http://open.lab)

1.2. Konfigūruoti svetainę serveryje.

1.2.1.Kataloge **~/my\_conf** sukurti svetainės konfigūracinį failą **open.conf**

|  |
| --- |
| <VirtualHost \*:80>    ServerName open.lab  DocumentRoot /home/stud/ssllab/my\_www/open  ServerAdmin stud@if.ktu.lt  # suteikti serveriui teises svetainės failu naudojimui atitinkame kataloge  <Directory /home/stud/ssllab/my\_www/open>  Options Indexes FollowSymLinks  AllowOverride None  Require all granted  </Directory>  ErrorLog ${APACHE\_LOG\_DIR}/error.log  CustomLog ${APACHE\_LOG\_DIR}/access.log combined  </VirtualHost> |

1.2.2. Kopijuoti šį failą į Apache konfigūracijų katalogą ir aktyvuoti šią svetainę:

***sudo cp ./my\_conf/open.conf /etc/apache2/sites-available***

***sudo a2ensite open.conf***

1.2.3. Perstartuoti Apache:

***sudo service apache2 restart***

1.2.4. Pakoreguokite atitinkamą index.html įrašydami svetainės duomenis.

1.2.5. Patikrinti svetainės veikimą iš naršyklės [http://open.lab](http://open.lab/).Kaip ieškoti klaidų, aprašyta lab. darbo medžiagoje.

**2. Sukurti lokalų sertifikatą turinčią svetainę** [**https://local.ssl.lab**](https://local.ssl.lab)

2.2. Sukurti privatų raktą ir lokalų sertifikatą šiai svetainei.

2.2.1. Sugeneruoti 2048 bitų ilgio raktą **local.key**:

***openssl genrsa -out ./my\_keys/local.key 2048***

* + 1. Sukurti sertifikato prašymą **local.csr:**

***openssl req -new -extensions v3\_req -key ./my\_keys/local.key -out ./my\_requests/local.csr***

|  |  |
| --- | --- |
| Country Name (2 letter code) [AU]:**LT**  State or Province Name (full name) [Some-State]:**Kaunas**  Locality Name (eg, city) []:**Kaunas**  Organization Name (eg, company) [Internet Widgits Pty Ltd]:**KTU**  Organizational Unit Name (eg, section) []:**IF**  Common Name (e.g. server FQDN or YOUR name) []:**local.ssl.lab**  Email Address []:**stud@if.ktu.lt**  Please enter the following 'extra' attributes  to be sent with your certificate request  A challenge password []:  An optional company name []: | Šie duomenys bus įrašyti į sertifikatą |

Kataloge my\_requests turėjo atsirasti failas su sertifikato prašymu. Pažiūrėkite.

2.2.3. Pačiam pasirašyti sertifikatą **local.crt**

***openssl x509 -req -days 365 -in ./my\_requests/local.csr -signkey ./my\_keys/local.key -out ./my\_certs/local.crt***

Pasitikrinkite atitinkamuose kataloguose failus local.key ir local.crt.

2.3. Konfigūruoti svetainę serveryje.

2.3.1.Kataloge **~/my\_conf** sukurti svetainės konfigūracinį failą **localssl.conf:**

|  |
| --- |
| <VirtualHost \*:443>    ServerName local.ssl.lab  DocumentRoot /home/stud/ssllab/my\_www/localssl  ServerAdmin [stud@if.ktu.lt](mailto:stud@if.ktu.lt)  # nurodyti ssl parametrus  SSLEngine ON  SSLCertificateFile /home/stud/ssllab/my\_certs/local.crt  SSLCertificateKeyFile /home/stud/ssllab/my\_keys/local.key  # suteikti serveriui teises svetaines failu publikavimui  <Directory /home/stud/ssllab/my\_www/localssl>  Options Indexes FollowSymLinks  AllowOverride None  Require all granted  </Directory>  ErrorLog ${APACHE\_LOG\_DIR}/error.log  CustomLog ${APACHE\_LOG\_DIR}/access.log combined  </VirtualHost> |

2.3.2. Aktyvuoti SSL:

**sudo a2enmod ssl**

2.3.3. Kopijuoti šį failą į Apache konfigūracijų katalogą ir aktyvuoti šią svetainę:

***sudo cp ./my\_conf/open.conf /etc/apache2/sites-available***

***sudo a2ensite open.conf***

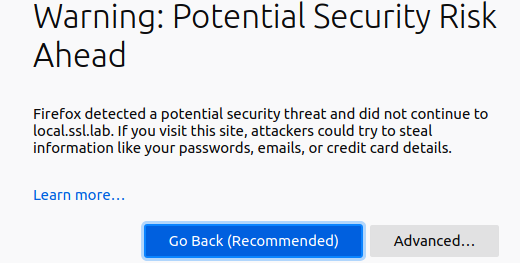
Perstartuoti Apache:

***sudo service apache2 restart***

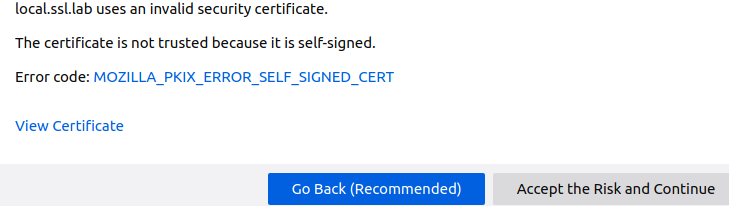
Pakoreguokite atitinkamą index.html įrašydami svetainės duomenis.

2.3.4. Papildykite index.html failą svetainės atributais.

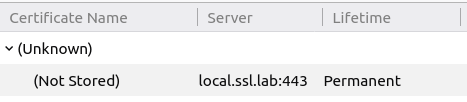
2.3.5. Patikrinti svetainės veikimą iš naršyklės [https://local.ssl.lab](https://local.ssl.lab/) . Lokalaus sertifikato tikrumo naršyklė negali patikrinti, vartotojas turi sukurti išimtį:



Eiti į Advanced > Accept



Patvirtinus išimtį Preferences > Privacy & Security > View Certificates > Servers matome jį irašytą naršyklėje:



1. **Sukurti CA išduotą sertifikatą turinčią svetainę** [**https://ca.ssl.lab**](https://ca.ssl.lab)

3.2. Analogiškai kaip 2.2.1-2.2.2 sukurti privatų raktą **manosvetaine.key** ir sertifikato prašymą  **manosvetaine.csr** šiai svetainei. Common Name: **ca.ssl.lab**.

OpenSSL gali išduoti sertifikatus tik organizacijos viduje, taigi visi atributai sertifikato prašyme prieš Organizational Unit Name turi sutapti:

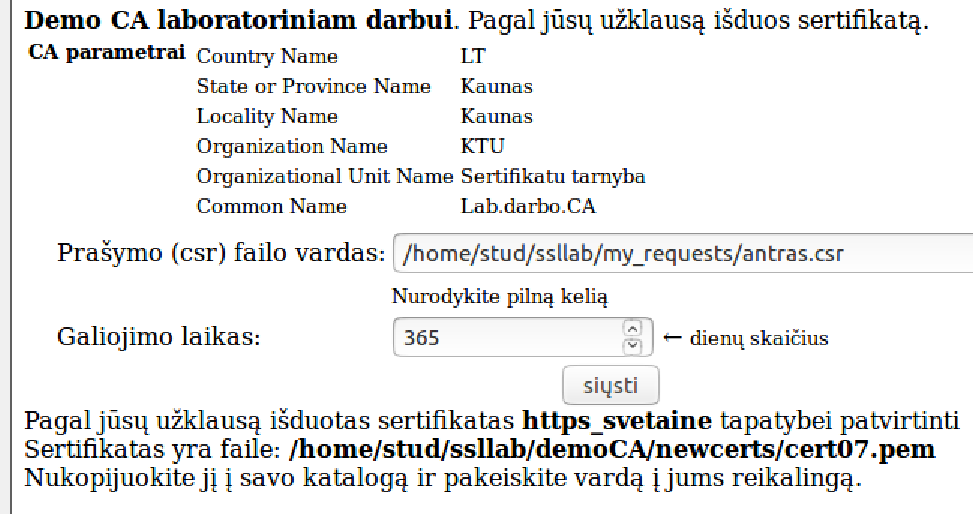
Country Name (2 letter code) [AU]:**LT**

State or Province Name (full name) [Some-State]:**Kaunas**

Locality Name (eg, city) []:**Kaunas**

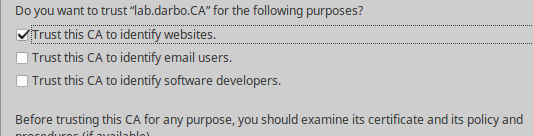
Organization Name (eg, company) [Internet Widgits Pty Ltd]:**KTU**

3.3. Prisijungti prie CA imituojančios svetainės <http://lab.ca> ir gauti sertifikatą:



3.4.Nukopijuokite sertifikatą į ***~/my\_certs***  ir pakeiskite vardą į **manosvetaine.crt.**

3.5. Kad patvirtinti pasitikėjimą Lab.darbo.CA, įrašykite ją Firefox naršyklėje tarp patikimų CA : Preferences > Privacy & Security > View Certificates > Authorities >Import įtraukti **CA\_cert.pem**:



Uždarykite Preferences.

3.6. Konfigūruoti svetainę serveryje.

3.6.1.Kataloge **~/my\_conf** sukurti svetainės konfigūracinį failą **cassl.conf**

|  |
| --- |
| <VirtualHost \*:443>    ServerName ca.ssl.lab  DocumentRoot /home/stud/ssllab/my\_www/cassl  ServerAdmin [stud@if.ktu.lt](mailto:stud@if.ktu.lt)  # nurodyti ssl parametrus  SSLEngine ON  SSLCertificateFile /home/stud/ssllab/my\_certs/manosvetaine.crt  SSLCertificateKeyFile /home/stud/ssllab/my\_keys/manosvetaine.key  SSLCACertificateFile /home/stud/ssllab/demoCA/CA\_cert.pem  # suteikti serveriui teises svetaines failu publikavimui  <Directory /home/stud/ssllab/my\_www/cassl>  Options Indexes FollowSymLinks  AllowOverride None  Require all granted  </Directory>  ErrorLog ${APACHE\_LOG\_DIR}/error.log  CustomLog ${APACHE\_LOG\_DIR}/access.log combined  </VirtualHost> |

3.6.2. Kopijuoti šį failą į Apache konfigūracijų katalogą ir aktyvuoti šią svetainę:

***sudo cp ./my\_conf/open.conf /etc/apache2/sites-available***

***sudo a2ensite open.conf***

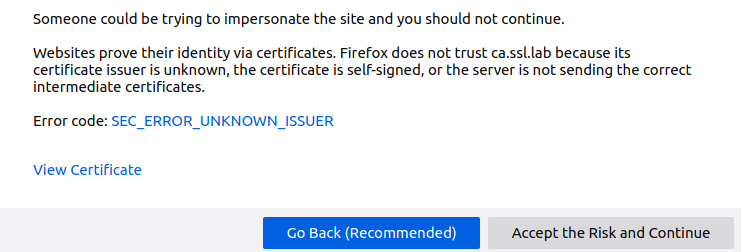
Perstartuoti Apache:

***sudo service apache2 restart***

Pakoreguokite atitinkamą index.html įrašydami svetainės duomenis.

3.6.3. Papildykite index.html failą svetainės atributais.

3.6.4. Patikrinti svetainės veikimą iš naršyklės [https://ca.ssl.lab](https://ca.ssl.lab/) . Atsidaro su juoda spynele, arba jei neuždarėte Preferences ir pan. - nepatikimas sertifikato išdavėjas. Patvirtinkite jį.



Kaip ieškoti klaidų, aprašyta lab. darbo medžiagoje.

**4. Sukurti sertifikatą vartotojui ir įdiegti Firefox naršyklėje**

4.1. Analogiškai kaip 2.2.1-2.2.2 sukurti privatų raktą **mano.key** ir sertifikato prašymą  **mano.csr.** Common Name: **mano.asmeninis.**

4.2. Analogiškai kaip 3.3-3.4 gauti sertifikatą **mano.crt.**

4.3. Sertifikatą **mano.crt** konvertuoti į daugumai naršyklių suprantamą formatą **p12**.

***openssl pkcs12 -export -clcerts -in ./my\_certs/mano.crt -inkey ./my\_keys/mano.key -out ./my\_certs/mano.p12***

Export password: **stud**:

4.4. Į svetainę **ca.ssl.lab** leisime kreiptis tik vartotojams turintiems asmeninius sertifikatus. Papildyti **cassl.conf** failą ir kopijuoti jį į Apache konfigūracijų katalogą:

**SSLVerifyClient require**

**SSLVerifyDepth 1**

Restartuoti Apache2. Įsitikinti, kad svetainė nebeatsidaro.

4.5. Įkelti vartotojo sertifikatą į naršyklę:

Firefox: ***Menu > Preferences > Privacy&Security >Certificates > View Certificates > Your Certificates > Import.*** Uždarykite preferences.

4.6. Patikrinti vartotojo sertifikato veikimą iš Firefox: [https://ca.ssl.lab](https://ca.ssl.lab/). Pabandykite jungtis į local.ssl.lab ir ca.ssl.lab su Crome naršykle be įkeltų CA ir vartotojo sertifikatų.

1. Suarchyvuoti atliktus nustatymus: iš **/home/stud/conf-kopijos** paleisti **./save-ssl.sh** ir įkelti į moodle aplinką gautą failą *vardas.****tar*** (vardo paklaus). Gynimo metu pirmiausia reiks atstatyti būseną, jei virtualioje mašinoje jos nebus ar ji bus sugadinta: atsisiųsti iš moodle, patalpinti į /home/stud/conf-kopijos ir atstatyti: **./load-ssl.sh** (atstatymas neapima Firefox nustatymų: juos atlikti iš naujo).