

Безбедност на компјутерски системи-2019/2020/L

[Home](#) / [My courses](#) / [Бнкс-2019/2020/L-35_13298](#) / [Лабораториски](#) / [Лабораториска вежба 4](#)

Лабораториска вежба 4

Целта на оваа лабораториска задача е да се запознаеме со начинот на генерирање на барање за сертификат (certificate signing request - CSR).

Начинот на добивање на потпишан серитикат би бил потполно исто кога и би барале сертификат од глобално признат Certificate Authority.

Следете го следниот линк за повеќе детали на како тоа да ги генерираме барањата:

<https://jamielinux.com/docs/openssl-certificate-authority/index.html>

(1) Генерирање на клуч

Најпрво, креирајте папка што ќе ги содржи сите информации во врска со овој сертификат, и креирајте под папки како што ќе има потреба.

Треба да го изгенерираме нашиот **приватен клуч**. Тоа може да го направиме со следната команда:

```
openssl genrsa -aes256 -out private/INDEX.key.pem 2048 # генерирај го клучот (заменете го INDEX со вашиот индекс)
chmod 400 private/INDEX.key.pem # заштити го со read-only привилегии само за сопственикот
```

ВАЖНО: Осигурајте се дека клучот ви е на сигурно место, и неможе да биде пристапен од никој друг!

(2) Генерирање на барање за сертификат

Следно, треба да изгенерираме барање (CSR) со нашиот приватен клуч. За таа цел, ни треба уште една информација, конфигурацијата за барање на сертификатите:

```
[ req ]
# Options for the `req` tool (`man req`).
default_bits          = 2048
distinguished_name    = req_distinguished_name
string_mask            = utf8only

[ req_distinguished_name ]
# See <https://en.wikipedia.org/wiki/Certificate_signing_request>.
countryName           = Country Name (2 letter code)
stateOrProvinceName   = State or Province Name
localityName          = Locality Name
0.organizationName    = Organization Name
organizationalUnitName = Organizational Unit Name
commonName            = Common Name (student e-mail or group name)
emailAddress          = Email Address

# Optionally, specify some defaults.
countryName_default   = MK
stateOrProvinceName_default = Macedonia
localityName_default  =
0.organizationName_default = FINKI
organizationalUnitName_default =
emailAddress_default  =
```

Зачувајте ја конфигурацијата во папката што ја креиравте, под името: **stud_openssl.cnf**

Сега може да го генерираме нашето барање со:

```
openssl req -config stud_openssl.cnf -key private/INDEX.key.pem -new -sha256 -out csr/INDEX.csr.pem # заменете го INDEX со вашиот индекс
```

Со ова имаме две клучни инфомации:

- Приватниот клуч: **private/INDEX.key.pem**
- Барањето (CSR): **csr/INDEX.csr.pem**

(3) Праќање на барањето

Пратете го вашето барање (**INDEX.csr.pem**) по мејл на: **sasho.najdov@finki.ukim.mk**

Со ова ќе се изгенерира сертификатот, потпишан со Certificate Authority-то што го креиравме за време на вежбите.

(4) Добивање на сертификатот

По мејл, ќе ви биде вратен изгенериранот **сертификат** и **ланецот на сертификати** за проверка. Врз истиот треба да ги направите следните проверки:

- Листање на информации за сертификатот

```
openssl x509 -noout -text -in certs/INDEX.cert.pem
```

- Валидација на сертификатот

```
openssl verify -CAfile certs/ca-chain.cert.pem certs/INDEX.cert.pem
```

(5) Импортирање на сертификат во Веб Пребарувач

Откако ќе го валидирате вашиот сертификат, треба да го импортирате во вашиот веб пребарувач.

За оваа цел, треба сертификатот да го претвориме во **PKCS #12** формат.


Тоа може да го направиме со следната команда:

```
openssl pkcs12 -export -in certs/INDEX.cert.pem -inkey private/INDEX.key.pem -name your_username -out INDEX.p12 -certfile certs/ca-chain.cert.pem
```

Потоа за соодвениот импорт, следете ги инструкциите на овие линкови:

- Firefox: <https://support.globalsign.com/digital-certificates/digital-certificate-installation/install-client-digital-certificate-firefox-windows>
- Chrome: <https://support.globalsign.com/digital-certificates/digital-certificate-installation/install-client-digital-certificate-windows-using-chrome>

Submission status

Submission status	Submitted for grading	
Grading status	Not graded	
Due date	Sunday, 24 May 2020, 11:59 PM	
Time remaining	Assignment was submitted 1 hour 45 mins early	
Last modified	Sunday, 24 May 2020, 10:13 PM	
File submissions	<div><div>-  BnKS LAB4 151027.pdf</div><div>24 May 2020, 10:13 PM</div></div>	
Submission comments	<div><div>► Comments (0)</div></div>	