БЕЗБЕДНОСТ НА КОМПЈУТЕРСКИ СИСТЕМИ

ЛАБОРАТОРИСКА ВЕЖБА 4

Фисник Лимани, 151027

ДОКУМЕНТАЦИЈА

1. Тековниот директориум: **pwd**
   /home/fisnik/Documents

2. Креираме нов директориум: **mkdir lab4**

3. **cd lab4**

4. Креираме уште еден нов директориум внатре во lab4: **mkdir private**

5. Генерирање на приватниот клуч:
   openssl genrsa -aes256 -out private/151027key.pem 2048

6. Направење read-only само за сопственикот:
   chmod 400 private/151027.key.pem

7. Генерирање барање за сертификат (CSR):
   vim stud_openssl.cnf
   Го ископираме соодветниот текст даден и го зачуваме датотеката.

8. Генерирање на нашето барање:
   openssl req –config stud_openssl.cnf –key private/151027.key.pem –new
   –sha256 –out csr/151027.csr.pem

9. Датотеките вратени од страна на асистентот:
   151027.cert.pem
   ca-chain.cert.pem
   ги ставиме на соодветната папка/именик: **certs**
   која го креираме со: **mkdir certs**

10. Листање на информации за сертификатот:
    openssl x509 -noout -text -in certs/151027.cert.pem

11. Валидација на сертификатот:
    openssl verify -CAfile certs/ca-chain.cert.pem certs/151027.cert.pem

12. Претворање на сертификатот во PKCS #12 формат:
    openssl pkcs12 -export -in certs/151027.cert.pem -inkey private/151027.key.pem -name fisnikl -out 151027.p12 -certfile certs/ca-chain.cert.pem

13. Импортирање на сертификат во Google Chrome
    Settings
    Privacy and Security (More)
    Manage Certificates
    Import (импортирај го соодветната датотека)
    Finish