# ДОКУМЕНТАЦИЈА ЗА ЛАБОРАТОРИСКА ВЕЖБА 4 ПО ИНФОРМАЦИСКА БЕЗБЕДНОСТ

## 1. Вовед

Оваа вежба е изработена од Мартина Петковска со индекс број 223313.

Целта на оваа лабораториска е да се запознаеме со концептите на PKI инфраструктура (Public Key Infrastructure) со што ќе се генерира сопствена хиерархија на сертификати и конфигурација на веб сервер со помош на OpenSSL.

Во оваа вежба ќе креираме Root Certificate Authority (FINKI CA), два Intermediate CA (IB CA и Lab CA) и ќе создадеме серверски и клиентски сертификат за проектот од минатите лабораториски.

Интеграцијата со серверот (XAMPP) ќе овозможи веб апликацијата да работи преку HTTPS, овозможувајќи сигурна комуникација меѓу клиентот и серверот.

**ОПШТО ЗА ЛАБОРАТОРИСКАТА ВЕЖБА**

- Сервер: XAMPP Apache (со веќе вклучен OpenSSL)
- Локација:

```
C:\xampp\pki\
|
├── root\                    # FINKI CA (Root)
|   ├── certs\
|   |   ├── finkiCA.pem          # Root CA сертификат
|   |   └── finkiCA.srl
|   ├── private\
|   |   └── finkiCA.key          # Root CA private key
|   ├── crl\
|   ├── newcerts\
|   ├── index.txt
|   └── serial
|
├── intermediate\              # IB CA + Lab CA (Intermediate)
|   ├── certs\
|   |   ├── ibCA.pem           # IB CA сертификат (потпишан од FINKI CA)
|   |   ├── ibCA.srl
|   |   ├── labCA.pem          # Lab CA сертификат (потпишан од IB CA)
|   |   └── labCA.srl
|   ├── private\
|   |   ├── ibCA.key           # IB CA private key (4096-bit)
|   |   └── labCA.key          # Lab CA private key (4096-bit)
|   ├── ibCA.csr               # CSR за IB CA
```

```
|   ├── labCA.csr            # CSR за Lab CA
|   ├── crl\
|   ├── newcerts\
|   ├── index.txt
|   └── serial
|
├── server\                  # Server Certificate
|   ├── certs\
|   |   ├── server.crt       # Server сертификат (потпишан од Lab CA)
|   |   └── chain.crt        # Целосен ланец на сертификати (Server → Lab → IB → Root)
|   ├── private\
|   |   └── server.key       # Server private key (2048-bit)
|   ├── server.csr           # CSR за server
|   └── server.cnf           # Config за SAN extensions
|
└── client\                  # Client Certificate
    ├── certs\
    |   └── client.crt       # Client сертификат (CN=223313, потпишан од Lab CA)
    ├── private\
    |   └── client.key       # Client private key (4096-bit)
    ├── client.csr           # CSR за client
    ├── client.p12           # PKCS#12 фајл за импорт во прелистувач
```

```
ASUS@MARTA MINGW64 /c/xampp/pki
$ ls -R
.:
client/  intermediate/  root/  server/

./client:
certs/  client.csr  client.p12  private/

./client/certs:
client.crt

./client/private:
client.key

./intermediate:
certs/  crl/  ibCA.csr  index.txt  labCA.csr  newcerts/  private/  serial

./intermediate/certs:
ibCA.crt  ibCA.pem  ibCA.srl  labCA.crt  labCA.pem  labCA.srl

./intermediate/crl:

./intermediate/newcerts:

./intermediate/private:
ibCA.key  labCA.key

./root:
certs/  crl/  index.txt  newcerts/  private/  serial

./root/certs:
FINKI-Root-CA.crt  finkiCA.pem  finkiCA.srl

./root/crl:

./root/newcerts:

./root/private:
finkiCA.key

./server:
certs/  chain.crt  private/  server.cnf  server.csr

./server/certs:
server.crt

./server/private:
server.key
```

- Certificate Chain: **Root CA (FINKI CA) → IB CA → Lab CA → Server/Client сертификати**
- Валидност: Root CA (10 години), Intermediate CA (5 години), Server/Client (5 години)

# ЧЕКОР 1: Генерирање Root Certificate Authority (FINKI CA), кој сам себе се потпишува

- **Подготовка на директориум за Root CA (FINKI CA)**

```
cd /c/xampp/pki/root
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
```

- **Генерирање на private key за FINKI CA**

```
openssl genrsa -out private/finkiCA.key 4096
```

- **Генерирање self-signed root certificate**

```
openssl req -x509 -new -nodes -key private/finkiCA.key -sha256 -days 3650 -out certs/finkiCA.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MK
State or Province Name (full name) [Some-State]:Skopje
Locality Name (eg, city) []:Skopje
Organization Name (eg, company) [Internet Widgits Pty Ltd]FINKI
Organizational Unit Name (eg, section) []:PKI Lab
Common Name (e.g. server FQDN or YOUR name) []:FINKI CA
Email Address []:
```

- **За верификација**: `openssl x509 -in certs/finkiCA.pem -text -noout`

Очекуван излез:

- Issuer: CN=FINKI CA, OU=PKI Lab, O=FINKI, L=Skopje, ST=Skopje, C=MK
- Subject: CN=FINKI CA, OU=PKI Lab, O=FINKI, L=Skopje, ST=Skopje, C=MK
- X509v3 Subject Key Identifier: (автоматски генериран)
- X509v3 Authority Key Identifier: (ист како Subject Key Identifier, бидејќи е self-signed)

# ЧЕКОР 2: Генерирање прв Intermediate Certificate Authority (IB CA), кој е потпишан од FINKI CA, а го потпишува Lab CA

**IB CA** е потпишан од **FINKI CA**, а го потпишува **Lab CA**.

- **Подготовка на директориум кој ќе ги содржи и двата intermediate CA (IB CA & Lab CA)**

```
cd /c/xampp/pki/intermediate
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
```

- **Генерирање private key за IB CA**

```
openssl genrsa -out private/ibCA.key 4096
```

- **Креирање Certificate Signing Request (CSR)**

```
$ openssl req -new -key private/ibCA.key -out ibCA.csr
```

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
---
Country Name (2 letter code) [AU]:MK
State or Province Name (full name) [Some-State]:Skopje
Locality Name (eg, city) []:Skopje
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FINKI
Organizational Unit Name (eg, section) []:PKI Lab
Common Name (e.g. server FQDN or YOUR name) []:IB CA
Email Address []:

- **Потпишување на IB CA со Root CA (FINKI CA)**

```
openssl x509 -req -in ibCA.csr -CA /c/xampp/pki/root/certs/finkiCA.pem -CAkey
/c/xampp/pki/root/private/finkiCA.key -CAcreateserial -out certs/ibCA.pem -days 1825 -sha256
```

Certificate request self-signature ok
subject=C=MK, ST=Skopje, L=Skopje, O=FINKI, OU=PKI Lab, CN=IB CA, emailAddress=

**Параметри**:
- finkiCA.pem → Root CA сертификат
- finkiCA.key → Root CA private key
-days 1825 → 5 години
-sha256 → SHA-256

- **За верификација**: `openssl x509 -in certs/ibCA.pem -text -noout`

Очекуван излез:
  - Issuer: CN=FINKI CA, OU=PKI Lab, O=FINKI, L=Skopje, ST=Skopje, C=MK
  - Subject: CN=IB CA, OU=PKI Lab, O=FINKI, L=Skopje, ST=Skopje, C=MK

# ЧЕКОР 3: Генерирање втор Intermediate Certificate Authority (Lab CA), кој е потпишан од IB CA, а ги потпишува клиентските и серверските сертификати

**Lab CA** е потпишан од **IB CA**, а ги потпишува **клиентските и серверските сертификати**.

- **Генерирање private key за Lab CA**

openssl genrsa -out private/labCA.key 4096

- **Креирање Certificate Signing Request (CSR)**

openssl req -new -key private/labCA.key -out labCA.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
---
Country Name (2 letter code) [AU]:MK
State or Province Name (full name) [Some-State]:Skopje
Locality Name (eg, city) []:Skopje
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FINKI
Organizational Unit Name (eg, section) []:PKI Lab
Common Name (e.g. server FQDN or YOUR name) []:Lab CA
Email Address []:

- **Потпишување на IB CA со Root CA (FINKI CA)**

openssl x509 -req -in labCA.csr -CA certs/ibCA.pem -CAkey private/ibCA.key -CAcreateserial -out certs/labCA.pem -days 1825 -sha256

Certificate request self-signature ok
subject=C=MK, ST=Skopje, L=Skopje, O=FINKI, OU=PKI Lab, CN=Lab CA
**Параметри:**

- /ibCA.pem → IB CA сертификат
- ibCA.key → IB CA private key
-out certs/labCA.pem → излезен сертификат

- **За верификација**: openssl x509 -in certs/labCA.pem -text -noout

Очекуван излез:

  - Issuer: CN= IB CA, OU=PKI Lab, O=FINKI, L=Skopje, ST=Skopje, C=MK
  - Subject: CN=Lab CA, OU=PKI Lab, O=FINKI, L=Skopje, ST=Skopje, C=MK

# ЧЕКОР 4: Генерирање на серверски сертификат

**Локација:** C:\xampp\pki\server

**Серверскиот сертификат** е потпишан од **Lab CA**.

- **Подготовка:**

```
cd C:\xampp\pki\server
mkdir certs private
chmod 700 private
```

- **Креирање конфигурациски фајл за SAN (Subject Alternative Name)**

** Тука мораше да се направи нов конфигурациски фајл каде ќе се додадат alternative names, бидејќи новите верзии на прелистувачите не го прифаќаа сертификатот само со CN (Common Name) – бараат SAN extension.**

```
[ req ]
default_bits       = 2048
prompt             = no
default_md         = sha256
distinguished_name = dn
req_extensions     = req_ext

[ dn ]
C  = MK
ST = Skopje
L  = Skopje
O  = FINKI
OU = PKI Lab
CN = localhost

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = localhost
DNS.2 = *.localhost
IP.1  = 127.0.0.1
IP.2  = ::1
```

- **Генерирање private key**

```
openssl genrsa -out private/server.key 4096
```

- **Креирање CSR со SAN**

```
openssl req -new -key private/server.key -out server.csr -config server.cnf
```

- **Потпишување на IB CA со Root CA (FINKI CA)**

```
openssl x509 -req -in server.csr -CA /c/xampp/pki/intermediate/certs/labCA.pem -CAkey
/c/xampp/pki/intermediate/private/labCA.key -CAcreateserial -out certs/server.crt -
days 1825 -sha256 -extfile server.cnf -extensions req_ext

Certificate request self-signature ok
subject=C=MK, ST=Skopje, L=Skopje, O=FINKI, OU=PKI Lab, CN=localhost
```

- **Креирање на целосен сертификатски синџир (chain)**

Редослед на сертификатите:

1. Server Certificate (server.crt)
2. Lab CA (labCA.pem)
3. IB CA (ibCA.pem)
4. Root CA (finkiCA.pem)

cd /c/xampp/pki

cat server/certs/server.crt intermediate/certs/labCA.pem intermediate/certs/ibCA.pem root/certs/finkiCA.pem > server/chain.crt

За верификација: grep -c "BEGIN CERTIFICATE" server/chain.crt

4

# ЧЕКОР 5: Генерирање на клиентски сертификат

**Клиентскиот сертификат** е потпишан од **Lab CA** и го содржи мојот индекс како CN.

- **Подготовка**:

cd C:\xampp\pki\client
mkdir certs private
chmod 700 private

- **Генерирање private key**

openssl genrsa -out private/client.key 4096

- **Креирање CSR за клиент**

```
openssl req -new -key private/client.key -out client.csr -subj
"/C=MK/ST=Skopje/L=Skopje/O=FINKI/OU=PKI Lab/CN=223313"
```

- **Потпишување од Lab CA**

```
openssl x509 -req -in client.csr -CA /c/xampp/pki/intermediate/certs/labCA.pem -CAkey
/c/xampp/pki/intermediate/private/labCA.key -CAcreateserial -out certs/client.crt -
days 1825 -sha256

Certificate request self-signature ok
subject=C=MK, ST=Skopje, L=Skopje, O=FINKI, OU=PKI Lab, CN=223313, emailAddress=
```

- **Креирање PKCS#12 фајл за импортирање во прелистувач**

openssl pkcs12 -export -out client.p12 -inkey private/client.key -in certs/client.crt

Enter Export Password: 1234

Verifying - Enter Export Password:1234

# ЧЕКОР 6: КОНФИГУРАЦИЈА НА APACHE(преку XAMPP) за HTTPS

**Локација:** C:\xampp\apache\conf\extra\

- **Креирање на SSL конфигурациски фајл: C:\xampp\apache\conf\extra\ib_lab4-ssl.conf**

```
<VirtualHost *:443>
   ServerName localhost
   DocumentRoot "C:/xampp/htdocs/Projects/IB-labs/ib_lab4"

   SSLEngine on

   SSLCertificateFile "C:/xampp/pki/server/chain.crt"
   SSLCertificateKeyFile "C:/xampp/pki/server/private/server.key"

   SSLVerifyClient optional
   SSLVerifyDepth  3
   SSLCACertificateFile "C:/xampp/pki/root/certs/FINKI-Root-CA.crt"

   <Directory "C:/xampp/htdocs/Projects/IB-labs/ib_lab4">
      Options Indexes FollowSymLinks
      AllowOverride All
      Require all granted
   </Directory>
</VirtualHost>

<VirtualHost *:80>
   ServerName localhost
   Redirect permanent / https://localhost/
</VirtualHost>
```

**Објаснување на параметри:**

- SSLEngine on → вклучува SSL/TLS
- SSLCertificateFile → сертификатен синџир (chain.crt)
- SSLCertificateKeyFile → server private key
- SSLVerifyClient require → задолжителна клиентска автентификација
- SSLVerifyDepth 4 → длабочина на синџирот (Root → IB → Lab → Client = 4 нивоа)
- SSLCACertificateFile → Root CA за верификација на клиентските сертификати

- **Вклучување на SSL модул во httpd.conf**

**Фајл:** C:\xampp\apache\conf\httpd.conf

Include conf/extra/ib_lab4-ssl.conf

- Од XAMPP Control Panel да се рестартира Apache серверот

# ДОПОЛНИТЕЛЕН ЧЕКОР: ИНСТАЛИРАЊЕ НА КЛИЕНТСКИ СЕРТИФИКАТ ВО ПРЕЛИСТУВАЧ

**Windows (Chrome, Edge) - Од PKCS#12 фајл**

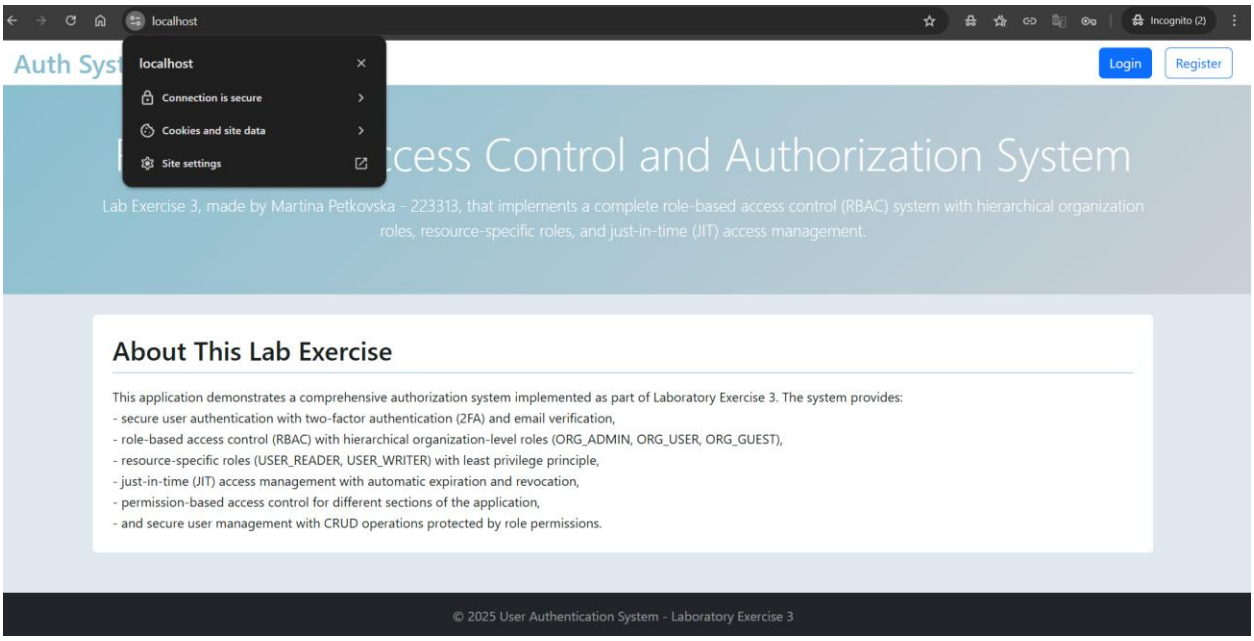
1. Двојно кликни на client.p12
2. Избери "Install Certificate" или "Import"
3. Избери "Current User" или "Local Machine"
4. Избери "Place all certificates in the following store"
5. Кликни "Browse" → избери "Personal" → "Certificates"
6. Внеси лозинка: 1234
7. Кликни "Finish"

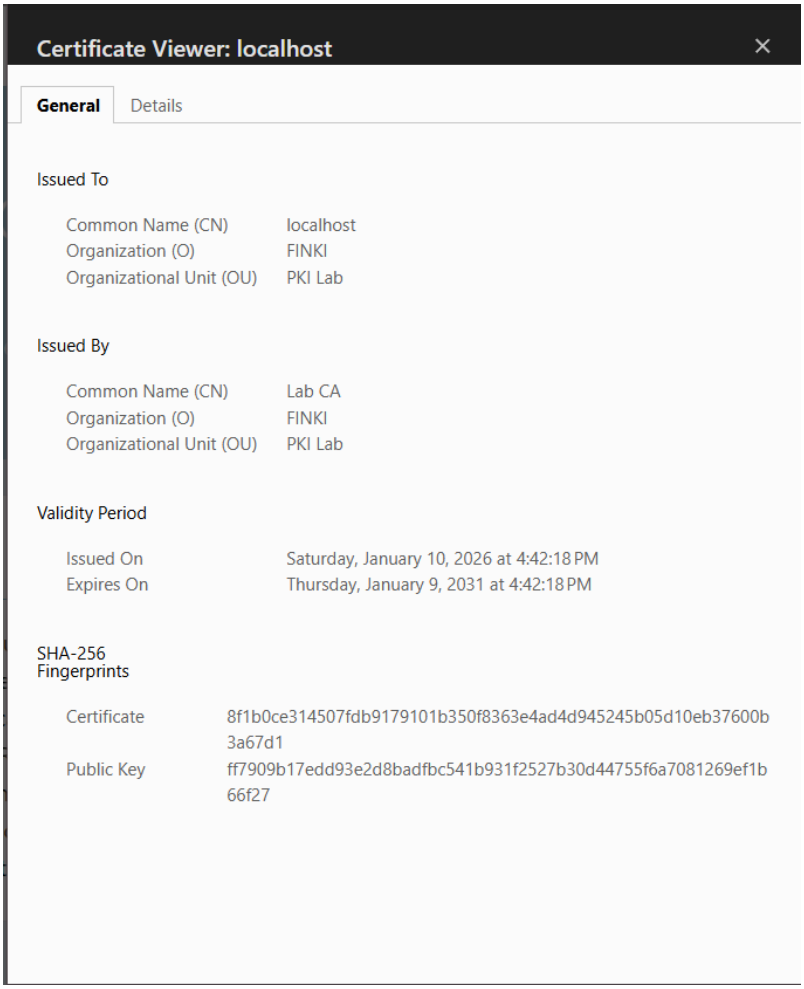
**Важно:** Root CA треба да биде инсталирано во "Trusted Root Certification Authorities" за да прелистувачот го прифати целиот ланец.

1. Отвори certmgr.msc
2. Кликни десен клик на "Trusted Root Certification Authorities" → "Certificates"
3. Action → All Tasks → Import
4. Избери root/certs/finkiCA.pem
5. Избери "Place all certificates in the following store: Trusted Root Certification Authorities"
6. Кликни "Finish"

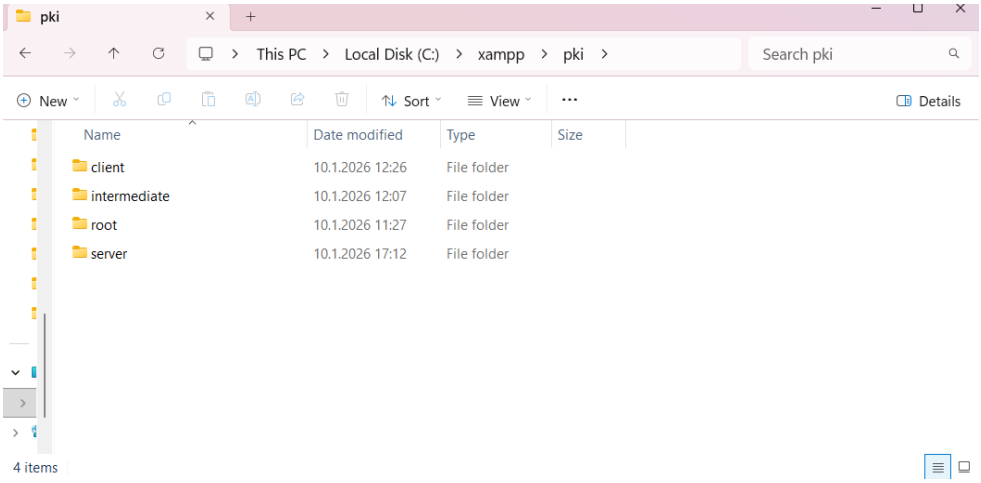
# ТЕСТИРАЊЕ

1. Отвори https://localhost во прелистувач
2. Треба да се прикаже веб-апликацијата со заклучен катанче во адрес-барот
3. Кликни на катанчето → "Certificate" → провери го ланецот


localhost
Incognito (2)
Auth Syst
localhost
Connection is secure
Cookies and site data
Site settings
Login
Register
cess Control and Authorization System
Lab Exercise 3, made by Martina Petkovska - 223313, that implements a complete role-based access control (RBAC) system with hierarchical organization roles, resource-specific roles, and just-in-time (JIT) access management.
About This Lab Exercise
This application demonstrates a comprehensive authorization system implemented as part of Laboratory Exercise 3. The system provides:
- secure user authentication with two-factor authentication (2FA) and email verification,
- role-based access control (RBAC) with hierarchical organization-level roles (ORG_ADMIN, ORG_USER, ORG_GUEST),
- resource-specific roles (USER_READER, USER_WRITER) with least privilege principle,
- just-in-time (JIT) access management with automatic expiration and revocation,
- permission-based access control for different sections of the application,
- and secure user management with CRUD operations protected by role permissions.
© 2025 User Authentication System - Laboratory Exercise 3


Certificate Viewer: localhost
General
Details
Issued To
Common Name (CN) localhost
Organization (O) FINKI
Organizational Unit (OU) PKI Lab
Issued By
Common Name (CN) Lab CA
Organization (O) FINKI
Organizational Unit (OU) PKI Lab
Validity Period
Issued On Saturday, January 10, 2026 at 4:42:18 PM
Expires On Thursday, January 9, 2031 at 4:42:18 PM
SHA-256 Fingerprints
Certificate 8f1b0ce314507fdb9179101b350f8363e4ad4d945245b05d10eb37600b3a67d1
Public Key ff7909b17edd93e2d8badfbc541b931f2527b30d44755f6a7081269ef1b66f27

Структура и изглед на pki директориумот каде што се чуваат сертификатите




Root – директориум. Во certs се наоѓаат фајловите: finkiCA.pem, finkiCA.srl, FINKI-Root-CA.crt, а во private се чува private key: finkiCA.key.