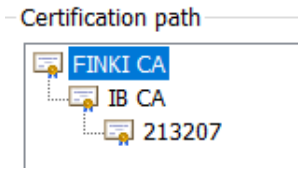
Тамара Георгиева 213207

Документација за лабараториска вежба IV

Слики од кодот и сертификатите

Root Certificate

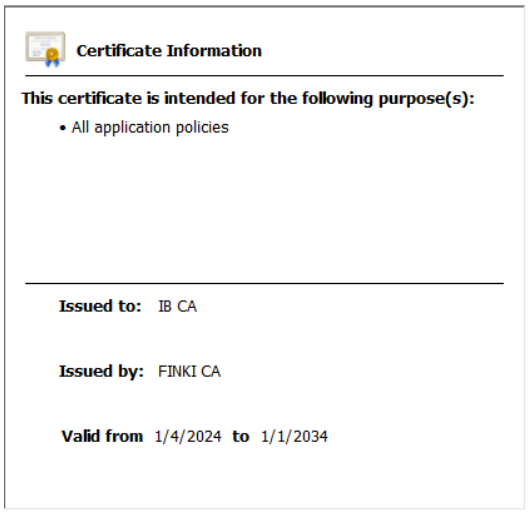


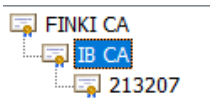

```
C:\Users\User>mkdir C:\root\ca

C:\Users\User>cd C:\root\ca

C:\root\ca>mkdir certs crl newcerts private

C:\root\ca>cd private

C:\root\ca\private>echo. > index.txt

C:\root\ca\private>echo 1000 > serial

C:\root\ca\private>cd C:\root\ca

C:\root\ca>openssl genrsa -aes256 -out private/ca.key.pem 4096
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

C:\root\ca>openssl req -config openssl.cnf ^
More? -key private\ca.key.pem ^
More?       -new -x509 -days 7300 -sha256 -extensions v3_ca ^
More?       -out certs\ca.cert.pem
Enter pass phrase for private\ca.key.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.
-----
MK [MK]:MK
Skopje [Skopje]:Skopje
Skopje [Skopje]:Skopje
FINKI CA [FINKI CA]:FINKI CA
FINKI CA [FINKI CA]:FINKI CA
FINKI CA []:FINKI CA
tamarageorgievag@gmail.com [tamarageorgievag@gmail.com]:tamarageorgievag@gmail.com
```

Тамара Георгиева 213207

Intermediate Certificate

```
C:\Users\User>mkdir C:\root\ca\intermediate
C:\Users\User>cd C:\root\ca\intermediate
C:\root\ca\intermediate>mkdir certs crl csr newcerts private
C:\root\ca\intermediate>echo. > index.txt
C:\root\ca\intermediate>echo 1000 > serial
C:\root\ca\intermediate>echo 1000 > C:\root\ca\ib\crlnumber
C:\root\ca\intermediate>cd C:\root\ca

c:\root\ca>openssl genrsa -aes256 -out intermediate\private\intermediate.key.pem 4096
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

c:\root\ca>icacls intermediate\private\intermediate.key.pem /inheritance:r /grant:r "%username%:(F)"
processed file: intermediate\private\intermediate.key.pem
Successfully processed 1 files; Failed processing 0 files

c:\root\ca>openssl req -config intermediate\openssl.cnf -new -sha256 -key intermediate\private\intermediate.key.pem -out intermediate\csr\intermediate.csr.pem
Enter pass phrase for intermediate\private\intermediate.key.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) [GB]:MK
State or Province Name [England]:Skopje
Locality Name []:Skopje
Organization Name [Alice Ltd]:FINKI CA
Organizational Unit Name []:FINKI IB
Common Name []:IB CA
Email Address []:tamarageorgievag@gmail.com

c:\root\ca>openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in intermediate\csr\intermediate.csr.pem -out intermediate\certs\intermediate.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /root/ca/private/ca.key.pem:
Check that the request matches the signature
Signature ok

Signature ok
Certificate Details:
        Serial Number: 6 (0x6)
        Validity
            Not Before: Jan  7 22:49:46 2024 GMT
            Not After : Jan  4 22:49:46 2034 GMT
        Subject:
            countryName               = MK
            stateOrProvinceName       = Skopje
            organizationName          = FINKI CA
            organizationalUnitName    = FINKI IB
            commonName                = IB CA
            emailAddress              = tamarageorgievag@gmail.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                0D:7E:B6:45:97:A1:F4:B0:E3:CE:DF:56:CB:7F:29:EA:F3:A0:E8:31
            X509v3 Authority Key Identifier:
                B7:92:DB:94:60:D2:84:C5:39:DB:94:85:D6:0C:D3:DC:06:60:86:A2
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Jan  4 22:49:46 2034 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated

c:\root\ca>icacls intermediate\certs\intermediate.cert.pem /grant Everyone:F
processed file: intermediate\certs\intermediate.cert.pem
Successfully processed 1 files; Failed processing 0 files

c:\root\ca>openssl x509 -noout -text -in intermediate\certs\intermediate.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 6 (0x6)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=MK, ST=Skopje, L=Skopje, O=FINKI CA, OU=FINKI CA, CN=FINKI CA, emailAddress=tamarageorgievag@gmail.com
        Validity
            Not Before: Jan  7 22:49:46 2024 GMT
            Not After : Jan  4 22:49:46 2034 GMT
        Subject: C=MK, ST=Skopje, O=FINKI CA, OU=FINKI IB, CN=IB CA, emailAddress=tamarageorgievag@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
c:\root\ca>openssl verify -CAfile certs\ca.cert.pem intermediate\certs\intermediate.cert.pem
intermediate\certs\intermediate.cert.pem: OK
```





Тамара Георгиева 213207

Client Certificate

```
C:\Users\User>cd C:\root\ca

C:\root\ca>

C:\root\ca>openssl genrsa -aes256 -out intermediate\private\www.213207.key.pem 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

c:\root\ca>icacls C:\root\ca\intermediate\private\www.213207.com.key.pem /grant Everyone:F
processed file: C:\root\ca\intermediate\private\www.213207.com.key.pem
Successfully processed 1 files; Failed processing 0 files

c:\root\ca>openssl req -config C:\root\ca\intermediate\openssl.cnf -key C:\root\ca\intermediate\private\www.213207.com.key.pem -new -sha256 -out C:\root\ca\intermediate\csr\www.213207.com.c
Enter pass phrase for C:\root\ca\intermediate\private\www.213207.com.key.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) [GB]:MK
State or Province Name [England]:Skopje
Locality Name []:Skopje
Organization Name [Alice Ltd]:FINKI
Organizational Unit Name []:IB CA
Common Name []:213207
Email Address []:tamarageorgievag@gmail.com


C:\root\ca>openssl ca -config C:\root\ca\lab\openssl.cnf -extensions usr_cert -days 365 -notext -md sha256 -in C:\root\ca\lab\csr\www.klient213207.com.csr.pem -out C:\root\ca\lab\certs\www.
Using configuration from C:\root\ca\lab\openssl.cnf
Enter pass phrase for /root/ca/private/ca.key.pem:
Check that the request matches the signature
Signature ok

Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Jan  4 22:06:17 2024 GMT
            Not After : Jan  3 22:06:17 2025 GMT
        Subject:
            countryName               = MK
            stateOrProvinceName       = Skopje
            organizationName          = FINKI CA
            organizationalUnitName    = IB CA
            commonName                = 213207
            emailAddress              = tamarageorgievag@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Comment:
                OpenSSL Generated Client Certificate
            X509v3 Subject Key Identifier:
                1D:0E:55:D1:AA:35:E5:26:79:9B:B0:09:FE:44:3B:61:19:45:91:9F
            X509v3 Authority Key Identifier:
                B7:92:DB:94:60:D2:84:C5:39:DB:94:85:D6:0C:D3:DC:06:60:86:A2
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
Certificate is to be certified until Jan  3 22:06:17 2025 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
```