

## Лабораториска вежба бр.2

### Инфраструктура на јавен клуч

Марко Бунтески 129/2021

#### 1. zadaca

```
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzs_last
File Edit View Search Terminal Help
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~$ cd seed
bash: cd: seed: No such file or directory
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~$ pwd
~/home/bunte
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~$ cd ..
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/home$ cd seed
bash: cd: seed: No such file or directory
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/home$ cd lab2bzs_last
bash: cd: lab2bzs_last: No such file or directory
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/home$ cd bunte
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ mkdir certs
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Can't open 'openssl.cnf' for reading. No such file or directory
40C19FF237F0000:error:10000002:system library:BIO_new_file:No such file or directory:../crypto/bio/bss_file.c:67:calling fopen(openssl.cnf, r)
40C19FF237F0000:error:10000008:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:75:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ mkdir demoCA
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ mkdir certs
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ mkdir crl
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ mkdir newcerts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ touch index.txt
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ touch serial
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ ls -l
total 28
drwxr-xr-x 2 bunte bunte 4096 Apr 29 15:06 certs
drwxr-xr-x 2 bunte bunte 4096 Apr 29 15:06 crl
-rw-r--r-- 1 bunte bunte 0 Apr 29 15:06 index.txt
drwxr-xr-x 2 bunte bunte 4096 Apr 29 15:06 newcerts
-rw-r--r-- 1 bunte bunte 12419 Apr 29 14:28 openssl.cnf
-rw-r--r-- 1 bunte bunte 0 Apr 29 15:06 serial
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
---
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]:SK
Locality Name (eg, city) []:Kisela voda
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Bunte inc
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:bunte
Email Address []:buntekisl@gmail.com
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ openssl genrsa -aes128 -out server.key 1024
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ openssl rsa -in server.key -text
Enter pass phrase for server key:
```

#### 2. zadaca

```
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzs_last
File Edit View Search Terminal Help
Locality Name (eg, city) []:Kisela voda
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Bunte inc
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:bunte
Email Address []:buntekisl@gmail.com
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzs_last$ openssl genrsa -aes128 -out server.key 1024
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Enter pass phrase for server key:
Private-Key: (1024 bit, 2 primes)
modulus:
  00:c9:dc:4c:54:32:0a:42:c2:60:b3:af:1a:73:f1:
  44:c7:87:b7:a4:9a:03:8d:ec:2d:b4:06:51:e6:b4:
  c1:51:7d:04:89:10:5f:0b:24:64:f7:c1:7a:45:56:
  a6:51:fd:c2:98:3b:0d:96:52:45:67:9f:c2:14:ac:
  19:ab:1a:62:73:04:b7:96:b4:91:38:b7:0a:bb:87:
  d9:83:22:69:3b:98:59:3d:8c:d8:a6:3f:b5:04:e8:
  29:97:0b:ca:1e:54:b5:fa:e9:49:f9:0b:0f:e9:15:
  16:57:e9:0f:44:29:19:35:fa:9f:0b:a5:c4:15:ca:
  24:ee:2f:2b:79:0e:8e:56:49
publicExponent: 65537 (0x10001)
privateExponent:
  00:b3:a8:b7:c2:9c:d6:d3:f8:1e:8b:2e:08:b4:32:
  83:4d:b7:2c:2a:72:ed:48:ee:78:ca:e6:69:14:95:
  c2:0d:5e:99:c0:17:15:be:d3:15:8d:51:05:1b:1b:
  80:d2:2e:b1:78:3e:a7:fc:77:62:d0:54:af:2f:28:
  f1:7b:08:f3:1f:a0:97:07:1e:53:ba:4e:67:af:04:
  52:e9:ed:a8:9d:1c:52:f6:2b:4b:06:c1:21:4b:0b:
  e4:a8:7d:1e:29:54:ff:3b:7f:b5:55:ef:a8:65:10:
  2f:d1:ad:2d:0b:68:74:0a:3d:05:69:45:14:a6:f6:
  74:e9:e1:06:06:3a:d1:93:01
primes:
  00:f7:88:f7:15:83:8a:ca:54:f2:46:66:86:96:3b:
  69:7b:01:f0:06:a1:ea:47:16:c2:13:ae:f7:1c:00:
  11:c3:0a:61:97:0f:43:cd:60:d2:54:28:7d:08:e1:
  0e:4b:b9:74:7b:98:e7:06:49:69:68:66:f6:cf:df:
  96:33:0b:84:69
prime2:
  00:d0:c3:7a:49:ac:28:ea:27:a4:1d:e5:1f:87:73:
  29:82:72:1a:09:2f:43:c1:89:f7:f0:ce:54:a0:f4:
  d1:22:4d:f2:8a:84:8c:8f:05:31:95:b5:30:46:75:
  5a:1a:66:df:20:4d:e8:ec:4b:44:c9:29:9e:91:44:
  a9:3b:a8:86:e1
exponent1:
  2a:b9:c9:6c:3d:38:47:94:41:fd:44:d5:16:39:4b:
  0b:1b:ca:06:41:6c:5e:b8:d6:ec:13:15:cf:ad:73:
  63:66:f7:51:01:b9:22:4a:04:03:e2:b9:08:57:10:
  51:26:51:a4:c3:cf:9c:96:2f:4b:05:fa:3b:cb:9b:
  f1:69:b3:01
exponent2:
  40:85:59:e3:11:29:48:0d:4e:64:ca:ee:aef:42:
  12:05:f0:14:55:ce:4b:f8:27:c0:2e:14:eb:d6:1e:
  58:ca:dc:56:b1:af:04:90:f6:0d:3d:2d:99:69:25:
  9a:e9:56:06:a8:0d:a9:92:26:c3:3a:6e:be:99:08:
  ef:ee:75:21
coefficient:
  00:fa:c5:d8:2c:1e:64:72:fa:06:2c:e7:73:42:b0:
```

```
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bks_last
File Edit View Search Terminal Help
8c:62:4d:2e:5e:b7:f1:f4:b7:4e:af:c3:ab:aa:31:
w6:63:53:df:c8
writing RSA key
-----BEGIN PRIVATE KEY-----
MIIECAIBAAQgBgkqhkiG9w0BAQgFAASCAQAwggMAGAgEAgGBmUCTFQyIABLYVlvb
gnPwPwht6SAA431LD0G0ca0vF911K0X9AKZP1BckWgUHQvg73Z2SRwchvH5S
GasaYnPUv5a8kT1/CruK2YMIaTuYMT2H2K4/tYtOKZdryhSUvfrpSfigd-kvFlfp
D8pGT06mwlLdXKJ04vK3A0/121AgBBAECQYEAS6/vpxs8/ge1y410K0T0bcs
Knl1Q04y4vZp3XK2Q324frzrP1j3f8wub18v6d6w/het8F5v1ye4j2wCK
Bx5tUK5nrW56eig8x5911L1sEhS8vkqH8ekVT/03+1ve+o2RAV8dtC280Cj3V
aAUUpv286eEABjPRAECQ0031PcvgdKVPJ02oaW0214AFDwoepHf1xpv848HD
Cdx3j9wV02W0124000u87Nedc0a1cz833Yz48pA4AMW55aw618ekHut
h3Mpgn1a259bW0n38W5UpTR1K3yc0QMD4ux1blMhVnVaGbF1E307E1EysnekUsp
OKCG4QJAKrn3b084R5R8/UTVFjLLCvkgpFxfRj78WVz61z72bJUMG31sEaH4S
5fC0512pPPPH3jv54K68ub8w6g0J021ZAEpSA10ZDnrur8KcpwFFA05/gn
wC4U9y6WmCvrgv8J023T0t8mK1mUWZqMq21x1puvPK17+51IO3BAPS18Cw
ZHL0B1zn10Kazu+ICf8cFP7W9C9XNML+Zpt+akqCH9HvFwH0XJGJNL1638T5H
Tq/Dq6ox0NT38e
-----END PRIVATE KEY-----
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
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]:SK
Locality Name (eg, city) []:karposh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:dragan inc
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:dragan
Email Address []:dragan@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:bunteskl
An optional company name []:..
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key \
-config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
ca: ./demoCA/newcerts is not a directory
./demoCA/newcerts: No such file or directory
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The organizationName field is different between
CA certificate (Bunte inc) and the request (dragan inc)
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number: 4096 (0x1000)
Validity
Not Before: Apr 29 13:19:46 2024 GMT
Not After : Apr 29 13:19:46 2025 GMT
Subject:
countryName = MK
stateOrProvinceName = SK
localityName = karposh
organizationName = dragan inc
organizationalUnitName = IT
commonName = dragan
emailAddress = dragan@gmail.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
72:18:8A:2C:6B:59:BE:BA:0F:AA:19:50:93:6D:7A:17:09:4F:08:7C
X509v3 Authority Key Identifier:
14:06:27:CC:37:5F:DE:34:FD:15:E1:5A:27:56:74:AB:74:0C:7F:6F
Certificate is to be certified until Apr 29 13:19:46 2025 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Date Base Updated
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$
```

```
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bks_last
File Edit View Search Terminal Help
State or Province Name (full name) [Some-State]:SK
Locality Name (eg, city) []:karposh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:dragan inc
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:dragan
Email Address []:dragan@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:bunteskl
An optional company name []:..
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key \
-config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
ca: ./demoCA/newcerts is not a directory
./demoCA/newcerts: No such file or directory
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The organizationName field is different between
CA certificate (Bunte inc) and the request (dragan inc)
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number: 4096 (0x1000)
Validity
Not Before: Apr 29 13:19:46 2024 GMT
Not After : Apr 29 13:19:46 2025 GMT
Subject:
countryName = MK
stateOrProvinceName = SK
localityName = karposh
organizationName = dragan inc
organizationalUnitName = IT
commonName = dragan
emailAddress = dragan@gmail.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
72:18:8A:2C:6B:59:BE:BA:0F:AA:19:50:93:6D:7A:17:09:4F:08:7C
X509v3 Authority Key Identifier:
14:06:27:CC:37:5F:DE:34:FD:15:E1:5A:27:56:74:AB:74:0C:7F:6F
Certificate is to be certified until Apr 29 13:19:46 2025 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Date Base Updated
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bks_last$
```

3.

```
hosts [Read-Only] (/etc)
File Edit View Search Tools Documents Help
127.0.0.1 localhost
127.0.0.1 lab2bzks.com
127.0.1.1 bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Plain Text Spaces: 4 Ln 11, Col 23 INS

```
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last
File Edit View Search Terminal Help

1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ sudo nano /etc/hosts
[sudo] password for bunte:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ sudo nano /etc/hosts

Use "fg" to return to nano.

[!]+ Stopped sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ cp server.key server.pem
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ cat server.crt >> server.pem
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
4057C8FB07F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Could not read server certificate private key from server.pem
40F7F69937F0000:error:1000010C:STORE routines:ossl_store_handle_load_result:unsupported:../crypto/store/store_result.c:151:
40F7F69937F0000:error:1C000064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/implementations/ciphers/ciphercommon_block.c:124:
40F7F69937F0000:error:11000074:PKCS12 routines:PKCS12_pbe_crypt_ex:pkcs12 cipherfinal error:../crypto/pkcs12/p12_decr.c:86:maybe wrong password
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
4097EB3977F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Could not read server certificate private key from server.pem
40C740E377F0000:error:1000010C:STORE routines:ossl_store_handle_load_result:unsupported:../crypto/store/store_result.c:151:
40C740E377F0000:error:1C000064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/implementations/ciphers/ciphercommon_block.c:124:
40C740E377F0000:error:11000074:PKCS12 routines:PKCS12_pbe_crypt_ex:pkcs12 cipherfinal error:../crypto/pkcs12/p12_decr.c:86:maybe wrong password
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
40C739AC47F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
4097CDBF0E7F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$ sudo nano /etc/hosts
[sudo] password for bunte:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last$
```

```
hosts [Read-Only] (/etc)
File Edit View Search Tools Documents Help
127.0.0.1 localhost
127.0.0.1 SEEDPKILab2018.com
127.0.1.1 bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

