


```
eb:53:8b:8e:80:be:1e:f8:bc:f2:6c:45:ab:50:63:
5a:ca:8c:e9:17:15:10:9a:49:0a:8f:40:7d:31:28:
35:9f:e8:ab:3b:aa:9a:bc:cd:b4:88:45:4f:96:07:
57:51:fc:2c:a7:63:69:dc:72:3a:70:b7:1e:58:8c:
46:d1
Exponent: 65537 (0x10001)
Attributes:
challengePassword      :Q@wertyuiop
Requested Extensions:
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
b3:fc:3c:bc:eb:a1:95:c8:b6:9e:c5:a3:01:af:a6:d2:3e:b6:
c7:26:74:c2:4d:a8:11:39:fd:4f:69:c6:9c:20:cf:a1:2c:af:
47:67:64:87:ed:73:1f:aa:20:69:0b:9e:4f:7f:81:ec:fb:bf:
c9:c1:f9:8e:3d:a3:24:25:52:7d:51:58:cb:bd:46:63:ea:d1:
46:13:a5:42:aa:3c:19:4a:d3:54:01:d5:1a:1b:14:fe:64:d9:
45:1b:d4:cf:76:e3:94:3f:fc:a7:1c:50:9a:af:7e:5a:43:83:
2b:ed:f3:b0:9d:ce:e2:52:f9:cf:d1:6a:7b:de:f9:85:32:1f:
64:17:fe:33:68:b2:52:5d:bf:75:7e:20:4d:89:4c:2d:b4:77:
0e:dc:1b:cd:63:c6:0f:f2:26:12:3c:a1:03:c3:03:17:29:c7:
a3:49:1a:d2:3e:e0:1b:88:16:af:d1:67:37:62:2b:5e:72:77:
51:5a:32:d1:c6:41:d2:88:53:59:5f:b3:03:df:36:1e:1c:18:
a5:bb:00:a9:e1:45:57:28:74:4d:48:cb:db:c3:71:f9:69:1d:
a5:42:08:fa:45:2a:ca:c6:aa:b1:38:10:e6:8e:1a:30:26:61:
f1:a8:33:f1:f6:fa:56:1f:da:fc:7c:16:15:c7:86:7c:51:65:
9c:8e:2c:4e
# nie miałem dwóch maszyn żeby zrobić test natomiast widać że sygnatury są
poprawne
root@WSL:misc> openssl ca -in a_certreq.pem -out a_cert.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/akey.pem:
Check that the request matches the signature
Signature ok
ERROR:There is already a certificate for
/C=PL/ST=Mazowsze/O=ostrowski.net.pl/OU=self
employed/CN=Kacper/emailAddress=kacper@ostrowski.net.pl
The matching entry has the following details
Type          :Valid
Expires on    :280607114242Z
Serial Number :08C91A9FB4B4CC7F795D526E21DF72351FF56611
File name     :unknown
Subject Name  :/C=PL/ST=Mazowsze/O=ostrowski.net.pl/OU=self
employed/CN=Kacper/emailAddress=kacper@ostrowski.net.pl
root@WSL:misc>
```

Questions

Question 1: Which files were modified in the "Test CA" database on user C's machine?

When a certificate is issued by a Certification Authority (CA), the following files in the directory are modified demoCA:

- `index.txt` - CA database file containing information on issued certificates.
- `serial` - file storing the serial number of the next certificate.
- `newcerts/<number>.pem` - the newly generated user certificate.

These files are automatically updated by the command `openssl ca`.

Command to verify the digital certificate (on machine A)

The user of machine A can verify the certificate using the following command:

```
openssl verify -CAfile cacert.pem a_cert.pem
```

where:

- `cacert.pem` - certificate of the Certification Authority (CA),
- `a_cert.pem` - certificate of user A to be verified.

Question 2: Which data is needed to perform the digital certificate verification operation?

To perform a digital certificate verification operation, the following data is needed:

- The user certificate to be verified (e.g. `a_cert.pem`).
- Certificate of the Certification Authority (e.g. `cacert.pem`) that issued the signed certificate.
- (Optional) Revoked Certificate List (CRL) if the verification is to include revocations.