Secure and Dependable Systems
Jacobs University Bremen
Dragi Kamov

Course: CO21-320203
May 10th, 2019

Homework 5

Problem 5.1

Solution:

a) 1601909768

b) In the unforeseeable future it might happen that we either forget our passphrase to our private key or simply lose the private key itself. In either of those cases we would not be able to revoke our keys if key revocation certificate didn't exist. A key revocation certificate is a revoked copy of our public key, and with it if either of the two mentioned cases happens to us, with the key revocation certificate we are able to "disable" or revoke our keys.

Problem 5.2

Solution:

a) In order to generate a RSA private key I put the following commands into the terminal:

```
$ openssl genrsa -des3 -out private_key.key 4096
```

From the command you could see that I chose the length of the RSA key to be 4096.
Then to make a pair of public/private keys we need to do the following command:

```
$ openssl rsa -pubout -in private_key.key -out public_key.key
```

b) To generate the CSR we type in the command:

```
$ openssl req -new -key private_key.key -out request.csr
```

After inputting all the necessary asked information we have our CSR.

c) To setup a CA we need to do type in the following command:

```
$ openssl req -new -x509 -key private_key.key -out ca.csr -days 365
```

d) In order to sign a CSR we need a CSR from one of our classmates. Let's say that the name of that CSR's name is 'csr_request.csr', then in order to sign that CSR we type the following in the terminal:

```
$ openssl ca -in csr_request.csr -out certificate.crt
```

e) My public key is under the name: "public_key.key".
My CSR can be found under the name: "request.csr".
My CA can be found under the name: "ca.csr".
My signed certificate by Fezile Manana can be found under the name: "cert.crt".

Problem 5.3

Solution:

a) The certificate itself has an expiration date on the 21st of December 2020. There are three certificate chains in the certificate and all of them are valid. This is the data for all three certificate chains:

```
Common name: DFN-Verein Global Issuing CA
Organization: Verein zur Foerderung eines Deutschen Forschungsnetzes e. V. Org. U
Location: DE
Valid from May 24, 2016 to February 22, 2031
Serial Number: 7709478377892925 (0x1b63bad01e2c3d)
Signature Algorithm: sha256WithRSAEncryption
Issuer: DFN-Verein Certification Authority 2
```

```
Common name: DFN-Verein Certification Authority 2
Organization: Verein zur Foerderung eines Deutschen Forschungsnetzes e. V. Org. U
Location: DE
Valid from February 22, 2016 to February 22, 2031
Serial Number: 16360405335420557697 (0xe30bd5f8af25d981)
Signature Algorithm: sha256WithRSAEncryption
Issuer: T-TeleSec GlobalRoot Class 2

Common name: T-TeleSec GlobalRoot Class 2
Organization: T-Systems Enterprise Services GmbH Org. Unit: T-Systems Trust Cente
Location: DE
Valid from October 1, 2008 to October 1, 2033
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: T-TeleSec GlobalRoot Class 2
```

b) OCSP is a way in which the browser assesses the validity of an SSL certificate by verifying with the vendor of the certificate. Online Certificate Status Protocol improves security, but as a disadvantage it causes the website to load slower, since our browser will have to communicate also with the certificate vendor.

https://cnds.jacobs-university.de does not support OCSP stapling, but https://beag.de does. We can test this by typing the following command to the terminal:

```
$ openssl s_client -connect cnds.jacobs-university.de:443 -tls1 -tlsextdebug -sta
$ openssl s_client -connect beadg.de:443 -tls1 -tlsextdebug -status
```