Lab1 – Certificates

You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

The labs use the following topology:

All VMs in this lab are in VirtualBox ***Bridged*** network. The machines that have static IP need to have an offset, check the topology image for reference. USE YOUR WIN7 WORKSTATION IP ADDRESS AS **x**.

All templates for VMs can be found in \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\

- **Install subCA**

Using the Centos7_k2019 template from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\, clone another VM with the name CA. Remember to set “Reinitialize the MAC address…” tickbox in the import wizard. Set VM interface as *Bridged.*

Boot up the VMs shown in the topology and login to the new subCA VM (**root/root66**). Check that it has got an IP. First, lets create the CA certificate and other required files:

```
mkdir /root/ca
cd /root/ca
wget https://student.labranet.jamk.fi/~jojuh/ttks/ca.cnf
wget https://student.labranet.jamk.fi/~jojuh/ttks/usr.cnf
echo 01 > serial
touch index.txt
touch index.txt.attr
openssl req -new -newkey rsa:4096 -keyout ca.key -config ca.cnf -days 365
   -extensions v3_ca -x509 -out ca.pem
```

When asked for a passphrase for the key, use **root66**. Fill in the information, set both CN (Common Name) as *your-student-id*-CA and O (Organisation) as *your-student-id*. (Example: CN=e6210-ca and O=e6210).

Check the content of the new CA certificate:

```
openssl x509 -text -noout -in ca.pem
```

You should see the info you typed, public key is 4096bits and the most important part: CA:TRUE in Basic constraints. Without this, your CA cert will not be trusted by the clients.

```
[root@elek-424-ws-01.labranet.jamk.fi ca]# ls
ca.cnf  index.txt  index.txt.attr  serial  usr.cnf
[root@elek-424-ws-01.labranet.jamk.fi ca]# openssl req -new -newkey rsa:4096 -ke
yout ca.key -config ca.cnf -days 365 -extensions v3_ca -x509 -out ca.pem
Generating a 4096 bit RSA private key
........++
.....................................++
writing new private key to 'ca.key'
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 (C) [FI]:
Locality Name (L) [JKL]:
Organization Name (O) [Default Company Ltd]:m3227
Organizational Unit Name (OU) []:m3227
Common Name (CN) []:m3227-ca
Email Address []:
[root@elek-424-ws-01.labranet.jamk.fi ca]# openssl x509 -text -noout -in ca.pem
```

```
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
    Public-Key: (4096 bit)re Algorithm: sha256WithRSAEncryption
```

- **Creating a CSR for the web server**

Clone and boot up the Webserver VM. Create a new RSA key and CSR for the webserver. To use subjectAltNames correctly, we need a local copy of the openssl.conf:

```
cp /etc/pki/tls/openssl.cnf /root/openssl_san.cnf
```

Now modify this new file and add the following lines to the bottom of the config:

```
[alt_names]
DNS.1 = www.your-student-id.zz
DNS.2 = your-student-id.zz
IP.1 = your-webserver-ip-here
```

```
[alt_names]

DNS.1 = www.m3227.zz
DNS.2 = m3227.zz
IP.1 = 192.168.44.135
```

Then find the [v3_req] section and add:

```
subjectAltName = @alt_names
```

```
[ v3_req ]

# Extensions to add to a certificate request

subjectAltName = @alt_names
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

Also uncomment the following under [req] –section:

```
req_extensions = v3_req
```

```
req_extensions = v3_req # The extensions to add to a certificate request
```

BONUS: As there is no way to give these subjectAltNames as parameters to openssl command-line, several different ways of doing this have been engineered. If you want a challenge, find a way to add SANs in a oneliner command.

Now we can use the new config file and correct SANs should appear in the certificate request:

```
openssl req -new -newkey rsa:2048 -nodes -keyout www.key -out www.csr
   -config /root/openssl_san.cnf
```

```
[root@localhost.localdomain ~]# openssl req -new -newkey rsa:2048 -nodes -keyout www.key -out www.csr -config /root/o
penssl_san.cnf
Generating a 2048 bit RSA private key
.............................+++
......+++
writing new private key to 'www.key'
-----
```

Set CN as www.your-student-id.zz, other fields like you did with the CA. **Be very precise with the command-line above to avoid errors! It is only a single line!** Double-check the contents of the CSR, it absolutely should show the Subject Alternative Name fields too:

```
Country Name (2 letter code) [XX]:FI
State or Province Name (full name) []:JKL
Locality Name (eg, city) [Default City]:JKL
Organization Name (eg, company) [Default Company Ltd]:m3227
Organizational Unit Name (eg, section) []:m3227
Common Name (eg, your name or your server's hostname) []:www.m3227.zz
Email Address []:
```

```
openssl req -noout -text -in www.csr
```

On the CA VM, copy the csr from the webserver to the CA machine (Change the IP to point to Web server):

```
cd /root/ca
scp root@webserver-ip-here:www.csr ./
```

```
[root@elek-424-ws-01.labranet.jamk.fi ca]# cd /root/ca
[root@elek-424-ws-01.labranet.jamk.fi ca]# scp root@192.168.44.135:www.csr ./
The authenticity of host '192.168.44.135 (192.168.44.135)' can't be established.
ECDSA key fingerprint is SHA256:I7Titguz9FMvrudOlwFyLLQG9ZXsFxZTvPeOlorSbjc.
ECDSA key fingerprint is MD5:e8:ae:cd:d3:dd:ca:3e:95:a2:89:d4:6a:fb:8d:97:67.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.44.135' (ECDSA) to the list of known hosts.
root@192.168.44.135's password:
www.csr                                       100% 1106   984.4KB/s   00:00
```

If everything seems to be right, sign the CSR with the CA key:

```
openssl ca -config usr.cnf -extensions usr_cert -days 180 -keyfile ca.key
    -cert ca.pem -in www.csr -out www.pem
```

Before answering yes, take time to check that the certificate info is correct. Especially check that Basic Constraints has CA:FALSE as we do not want our webserver to be a CA. Examine the contents of the new CRT file:

```
[root@elek-424-ws-01.labranet.jamk.fi ca]# openssl ca -config usr.cnf -extensions usr_cert -days 180 -keyfile ca.key
-cert ca.pem -in www.csr -out www.pem
Using configuration from usr.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jan  9 11:39:26 2020 GMT
            Not After : Jul  7 11:39:26 2020 GMT
        Subject:
            countryName               = FI
            stateOrProvinceName       = JKL
            localityName              = JKL
            organizationName          = m3227
            organizationalUnitName    = m3227
            commonName                = www.m3227.zz
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                59:C7:E9:B7:DD:20:42:47:F9:A6:6B:7B:00:6F:18:AA:E7:7F:7F:8E
            X509v3 Authority Key Identifier:
                keyid:5F:5B:FC:28:CD:F1:44:92:18:B2:AE:97:F0:CD:71:35:6F:D5:D8:BF

            X509v3 Subject Alternative Name:
                DNS:www.m3227.zz, DNS:m3227.zz, IP Address:192.168.44.135
Certificate is to be certified until Jul  7 11:39:26 2020 GMT (180 days)
Sign the certificate? [y/n]:
```

QUESTIONNAIRE: What are the correct key usage values for a generic Web server?

- Digital Signature, Non Repudiation, Key Encipherment

```
openssl x509 -noout -text -in www.pem
```

And finally, copy it back to the Webserver VM.

```
scp www.pem root@webserver-ip-here:www.pem
```

```
^C[root@elek-424-ws-01.labranet.jamk.fi ca]# scp www.pem root@192.168.44.135:www.pem
root@192.168.44.135's password:
www.pem                                       100% 5966     5.5MB/s   00:00
```

- **Configure SSL**

In the Webserver, you have to do two things. First, install Apache and mod_ssl and add firewall rule:

```
yum install httpd mod_ssl
firewall-cmd --permanent --add-service=http --add-service=https
firewall-cmd --reload
```

Then copy the key and certificate to the correct paths:

```
cp www.key /etc/pki/tls/private/
cp www.pem /etc/pki/tls/certs/
```

```
Complete!
[root@localhost.localdomain ~]# firewall-cmd --permanent --add-service=http --add-service=https
success
[root@localhost.localdomain ~]# firewall-cmd --reload
success
[root@localhost.localdomain ~]# ls
anaconda-ks.cfg  openssl_san.cnf  www.csr  www.key  www.pem
[root@localhost.localdomain ~]# cp www.key /etc/pki/tls/private/
[root@localhost.localdomain ~]# cp www.pem /etc/pki/tls/certs/
[root@localhost.localdomain ~]#
```

In those folders should exist also a default self-signed certificate (localhost.key and localhost.crt). Check their permissions and set the same permissions to the www.key and www.pem.

```
-rw-------. 1 root root 1675 Jan  9 11:52 localhost.key
-rw-------. 1 root root 1704 Jan  9 11:53 www.key
```

```
-rw-------. 1 root root 5966 Jan  9 11:53 www.pem
```

Last thing you need to do is edit /etc/httpd/conf.d/ssl.conf and change Apache to use your certificates. Find the following lines:

```
SSLCertificateFile …
SSLCertificateKeyFile …
~~SSLCertificateChainFile …~~
```

```
SSLCertificateFile /etc/pki/tls/certs/www.pem

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/www.key
```

And set them to point to your files. Reload apache (*systemctl restart httpd*).

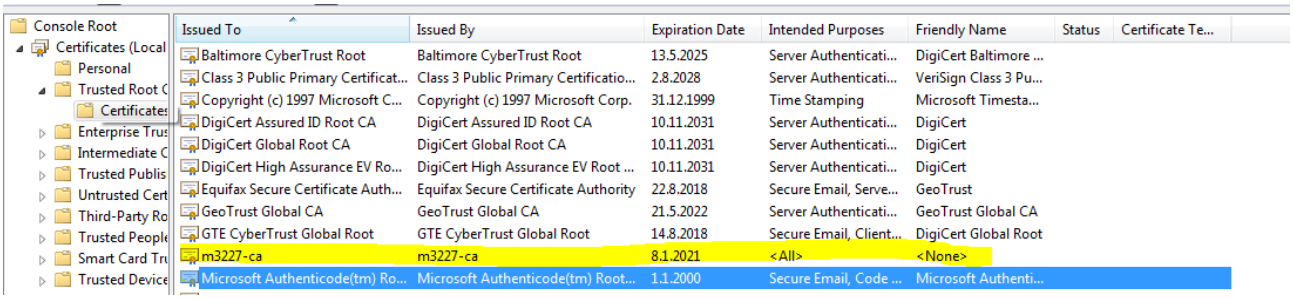
QUESTIONNAIRE: When and how is the SSLCertificateChainFile option used?

```
#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
```

Trusted root

Your Workstation VM needs to trust the **CA certificate**. Copy the ca.pem to the Windows VM. You can use WinSCP or copy/paste via PuTTY. There are several places where the ca.pem needs to be put

In a Windows-based PC, you can add the certificate to trusted roots in MMC console using the Local Computer Certificate tool. Open mmc.exe from Start->Run, and add *Certificates Snap-in* for the *Computer Account*. Import the certificate to *Trusted Root Certification Authorities*.



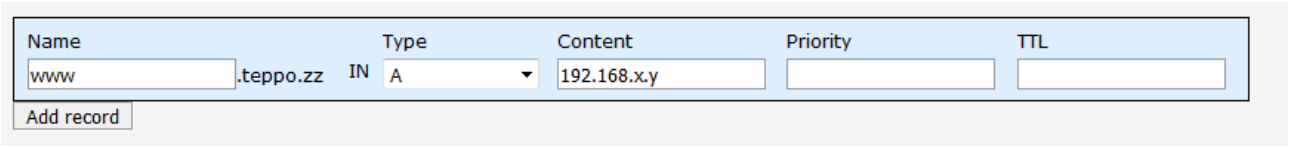
However, Firefox does not use the system certificates so we must add it to your Firefox profile Certificates. Open Firefox, select *Options -> Advanced -> Certificates -> View Certificates*. Select the *Authorities* tab, Click Import and select the certificate file. Add trusts for all purposes.

*BONUS: Copy the ca.pem to the webserver also and add it to the trusted root certificates of the Centos. Test with wget https://localhost/. Check the man page for **update-ca-trust** command for help/more information.*

- ## DNS name and testing

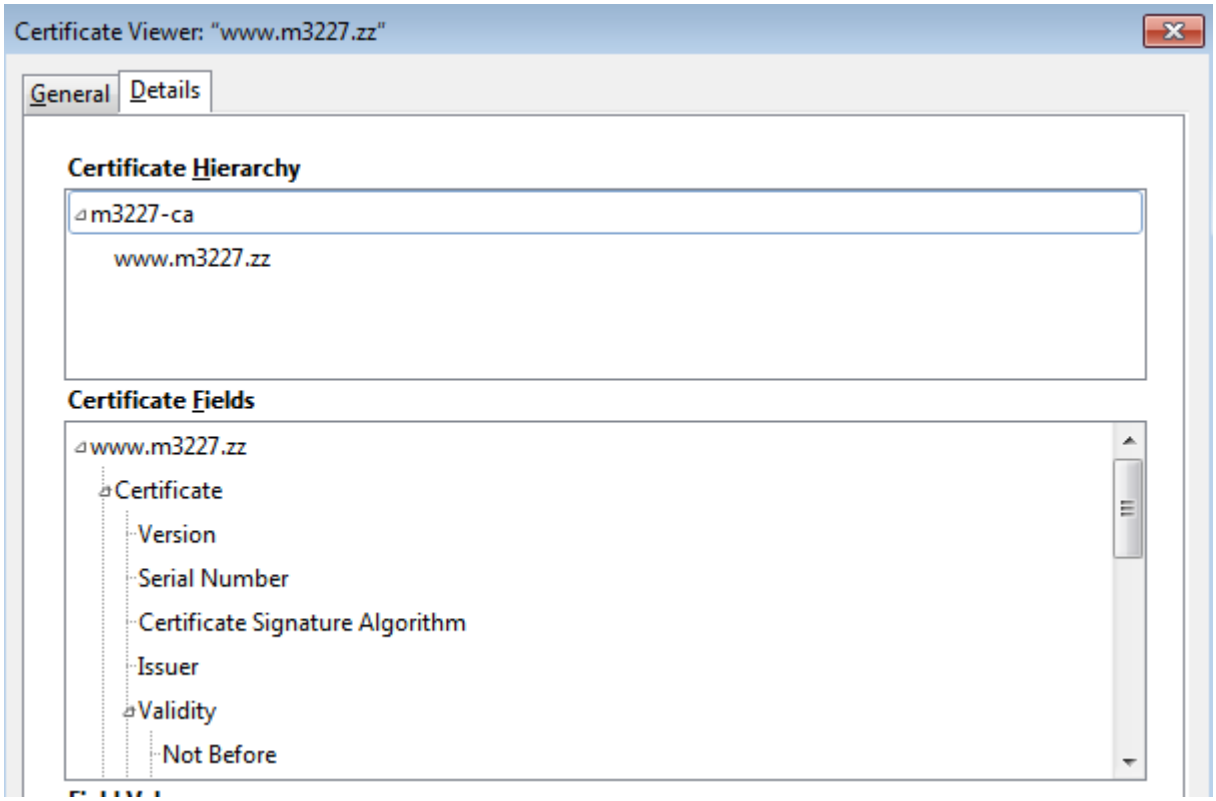
Final step is to add a DNS name for the webserver. If you added the correct IP address to the SubjectAltNames, this is not strictly necessary as browsing with IP works also.

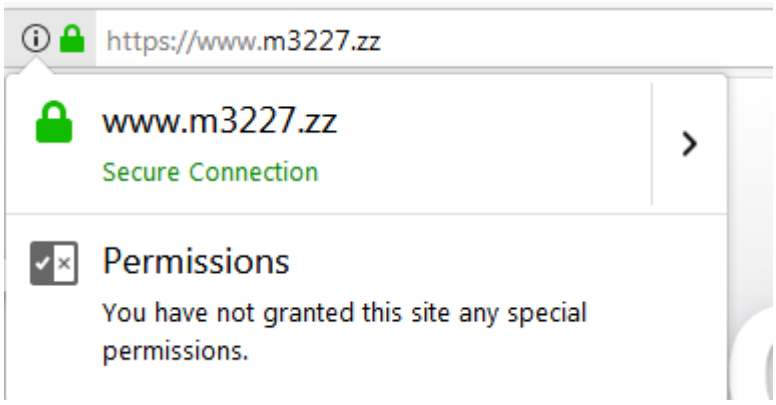
Browse to https://zz.labranet.jamk.fi/ and login with your LabraNet account. You need to add an DNS A record for www.student-id.zz like in the picture. After this, you should be able to access the webserver using the DNS name also.



If you are working at home, find out how to add a hosts-entry to the Workstation VM. The correct path for Windows 7 VM is C:\Windows\System32\drivers\etc\hosts. Point www.student-id.zz in the Windows hosts-file to the correct IP address. This way you can test the server even without a DNS entry.

When you are finished, take a screenshot of the Certificate Hierarchy path (shown in View Certificate - Details)




https://www.m3227.zz
www.m3227.zz
Secure Connection
Permissions
You have not granted this site any special permissions.