LAB1.2 Digital Certificates and IPsec

Saddam Hossen
P.no. 9112301917
Email: sahb16@student.bth.se

Task 1: [v3_ca]

Environment

I have used following commands as instructed for the folder structure
mkdir sahb16_ca
cd sahb16_ca
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
pwd

then copy the openssl.cnf to the directory of sahb16_ca from /etc/ssl/openssl.cnf

Enabled extensions

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
basicConstraints = CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

Descriptions:

subjectKeyIdentifier=hash Identifies certificates which contain a particular public key.

authorityKeyIdentifier=keyid:always,issuer Identifies the public key corresponding to the private key used to sign a certificate.

For the **keyid** option, if it is present an attempt is made to copy the subject key identifier from the parent certificate .
For the issuer option, it copies the issuer and serial number from the issuer certificate. This will only be done if the **keyid** option fails or is not included unless the "always" flag will always include the value.

Indicates whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.

keyUsage = critical, digitalSignature, cRLSign, keyCertSign Key usage is a multi valued extension consisting of a list of names of the permitted key usages.

The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

The cRLSign bit is asserted when the subject public key is used for verifying signatures on certificate revocation lists (for example, CRLs, delta CRLs, or ARLs).

The keyCertSign bit is asserted when the subject public key is used for verifying signatures on public key certificates.

Task 2: [v3_intermediate_ca]

[v3_intermediate_ca]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

subjectKeyIdentifier=hash Identifies certificates which contain a particular public key.

authorityKeyIdentifier=keyid:always,issuer Identifies the public key corresponding to the private key used to sign a certificate.

For the **keyid** option, if it is present an attempt is made to copy the subject key identifier from the parent certificate.

For the issuer option, it copies the issuer and serial number from the issuer certificate. This will only be done if the keyid option fails or is not included unless the "always" flag will always include the value.

basicConstraints = critical, CA:true, pathlen:0

Indicates whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.

If CA is TRUE then an optional pathlen name followed by an non-negative value can be included.

The pathlen parameter indicates the maximum number of CAs that can appear below this one in a chain. So if you have a CA with a pathlen of zero it can only be used to sign end user certificates and not further CAs.

keyUsage = critical, digitalSignature, cRLSign, keyCertSign

Key usage is a multi valued extension consisting of a list of names of the permitted key usages.

The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

The cRLSign bit is asserted when the subject public key is used for verifying signatures on certificate revocation lists (for example, CRLs, delta CRLs, or ARLs).

The keyCertSign bit is asserted when the subject public key is used for verifying signatures on public key certificates.

Compare to the v3_ca section

For v3_ca section

basicConstraints = CA:true

For v3_intermediate_ca section

basicConstraints = critical, CA:true, pathlen:0

Task 3: [usr_cert]

Extensions
basicConstraints=CA:FALSE
nsComment= "OpenSSL Generated Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

Description:

basicConstraints=CA:FALSE

An end user certificate must either set CA to FALSE or exclude the extension entirely. Some software may require the inclusion of basicConstraints with CA set to FALSE for end entity certificates.

nsComment= "OpenSSL Generated Certificate" This will be displayed in Netscape's comment listbox.

subjectKeyIdentifier=hash
Identifies certificates which contain a particular public key.

authorityKeyIdentifier=keyid,issuer
Identifies the public key corresponding to the private key used to sign a certificate.

For the keyid option, if it is present an attempt is made to copy the subject key identifier from the parent certificate.

For the issuer option, it copies the issuer and serial number from the issuer certificate.

This will only be done if the keyid option fails or is not included unless the "always" flag will always include the value.
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment

The nonRepudiation bit is asserted when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non- repudiation service that protects against the signing entity falsely denying some action.

The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

The keyEncipherment bit is asserted when the subject public key is used for enciphering private or secret keys, i.e., for key transport.

extendedKeyUsage = clientAuth, emailProtection

This extensions consists of a list of usages indicating purposes for which the certificate public key can be used for.

The value clientAuth means SSL/TLS Web Client Authentication. The value emailProtection means E-mail Protection (S/MIME).

Task 4: [server_cert]

[server_cert]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

basicConstraints = CA:FALSE
An end user certificate must either set CA to FALSE or exclude the extension entirely.
Some software may require the inclusion of basicConstraints with CA set to FALSE for end entity certificates.
subjectKeyIdentifier = hash
Identifies certificates which contain a particular public key.
authorityKeyIdentifier = keyid,issuer:always
Identifies the public key corresponding to the private key used to sign a certificate.

For the keyid option, if it is present an attempt is made to copy the subject key identifier from the parent certificate For the issuer option, it copies the issuer and serial number from the issuer certificate.
This will only be done if the keyid option fails or is not included unless the "always" flag will always include the value.

keyUsage = critical, digitalSignature, keyEncipherment

The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

The keyEncipherment bit is asserted when the subject public key is used for enciphering private or secret keys, i.e., for key transport.
extendedKeyUsage = serverAuth

This extension consists of a list of usages indicating purposes for which the certificate public key can be used for.
The value serverAuth means SSL/TLS Web Server Authentication.

Then I have created a ca1 directory under the root CA directory - /home/ats/sahb16_ca. Then I have run the following commands.
cd ca1
mkdir certs crl newcerts private csr
chmod 700 private touch index.txt
echo 2000 > serial
echo 2000 > crlnumber
cp ../openssl.cnf .

```
ats@serverA:~/sahb16_ca/ca1$ mkdir certs crl newcerts private csr
ats@serverA:~/sahb16_ca/ca1$ chmod 700 private
ats@serverA:~/sahb16_ca/ca1$ touch index.txt
ats@serverA:~/sahb16_ca/ca1$ echo 2000 > serial
ats@serverA:~/sahb16_ca/ca1$ echo 2000 > crlnumber
ats@serverA:~/sahb16_ca/ca1$ cp ../openssl.cnf .
```

Task 5 Policies:

For the CA policy

[policy_match]

countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional

```
 # For the 'anything' policy
# At this point in time, you must list all acceptable 'object'
# types.
 [ policy_anything ]
countryName  = optional
stateOrProvinceName = optional
localityName  = optional
organizationName = optional
organizationalUnitName = optional
commonName  = supplied
emailAddress  = optional
```

In policy_match section, if the value of an attribute is match, then it should be matched with the CA's DN.
All fields listed as supplied must be present. The fields listed as optional are allowed, but not required to be there.

Compare the policy_match section with the policy_anything section

countryName, stateOrProvinceName, organizationName must be present as the CA for all certificates it signs and commonName will be supplied by the issuer.

Keys and certs for root and ca1

Create the private RSA key for root and ca1, respectively
openssl genrsa -aes256 -out private/root.key.pem 4096
openssl genrsa -aes256 -out ca1/private/ca1.key.pem 4096

Obtain the public key using OpenSSH openssl rsa -in
private/root.key.pem -pubout -out root.pub.pem

For additional protection
chmod 400 private/root.key.pem
chmod 400 ca1/private/ca1.key.pem
Generate the self-signed certificate
openssl req -config openssl.cnf -key private/root.key.pem -new -x509 -days 7300 -sha256 -extensions v3_ca -out certs/root.cert.pem

Task 6:

Used Command:

openssl req -config openssl.cnf -key private/root.key.pem -new -x509 -days 7300 -sha256 -extensions v3_ca -out certs/root.cert.pem

-config filename
this allows an alternative configuration file to be specified, this overrides the compile time filename or any specified in the OPENSSL_CONF environment variable.

-key filename
This specifies the file to read the private key from. It also accepts PKCS#8 format private keys for PEM format files.

-new
this option generates a new certificate request. It will prompt the user for the relevant field values. The actual fields prompted for and their maximum and minimum sizes are specified in the configuration file and any requested extensions.

If the -key option is not used it will generate a new RSA private key using information specified in the configuration file.

-x509
this option outputs a self signed certificate instead of a certificate request. This is typically used to generate a test certificate or a self signed root CA. The extensions added to the certificate (if any) are specified in the configuration file.
Unless specified using the set_serial option, a large random number will be used for the serial number.

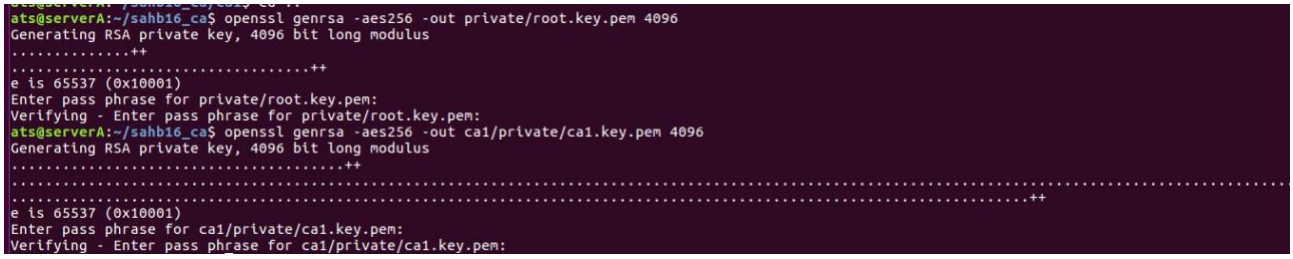
-days
n when the -x509 option is being used this specifies the number of days to certify the certificate for. The default is 30 days.
-extensions
section this option specifies alternative sections to include certificate extensions (if the -x509 option is present) or certificate request extensions.
This allows several different sections to be used in the same configuration file to specify requests for a variety of purposes.
-out filename

This specifies the output filename to write to or standard output by default.

ats@serverA:~/sahb16_ca$ chmod 400 private/root.key.pem
ats@serverA:~/sahb16_ca$ chmod 400 ca1/private/ca1.key.pem
ats@serverA:~/sahb16_ca$ openssl req -config openssl.cnf -key private/root.key.pem -new -x509 -days 7300 -sha256 -extensions v3_ca -out certs/root.cert.pem
Enter pass phrase for private/root.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) [AU]:SE
State or Province Name (full name) [Some-State]:Blekinge

Locality Name (eg, city) []:Karlskrona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ET2540
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:saddam-root
Email Address []:



Task 7:

ats@serverA:~/sahb16_ca$ openssl x509 -noout -text -in certs/root.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 11802078299821680574 (0xa3c967af0037a7be)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Validity
            Not Before: May 25 22:03:25 2018 GMT
            Not After : May 20 22:03:25 2038 GMT
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b6:8f:f2:f0:be:ee:d3:7d:bf:da:fb:c7:7e:b8:
                    ea:19:a0:8f:48:e8:d7:35:5f:83:08:0a:be:1f:cb:
                    be:b6:13:2a:ef:6e:12:e3:d7:07:8d:c4:57:d5:65:
                    b9:db:a2:48:fa:46:24:73:15:da:83:aa:3f:49:05:
                    a9:a6:db:e1:b5:3a:fe:a3:3b:3a:f1:f3:ad:0e:6e:
                    48:76:68:23:f0:02:14:72:0d:6f:14:00:46:02:54:
                    94:d9:4d:fd:5d:fc:9d:52:28:2f:07:58:30:92:8b:
                    b4:30:aa:5a:ac:24:b9:0b:14:c1:11:c0:d5:77:55:
                    98:3e:ae:b8:1d:b6:9f:e0:58:62:df:3d:63:9f:5c:
                    9f:0d:ba:e3:6d:e4:de:4e:16:3f:62:33:f0:2a:90:
                    98:26:58:a3:7f:63:c7:cb:32:0b:17:63:b9:a0:ab:
                    83:5c:65:66:0b:f8:2e:c2:7e:48:9e:da:94:c9:e2:
                    cc:b8:d3:f4:ca:9c:ef:0c:54:f1:c5:2f:53:b6:13:
                    d2:13:f7:33:32:c6:ed:9b:e4:35:47:ad:28:f5:7a:

```
            6c:30:67:cc:a7:70:2a:6e:41:4a:74:c6:b7:79:2f:
            10:22:10:26:3e:ae:0c:0d:13:16:ef:c2:ca:b5:4d:
            bc:e9:43:25:d7:d2:73:a7:29:78:ce:87:dd:01:6a:
            27:99:d3:2b:a9:43:4d:f1:fd:61:d1:23:fa:5d:7d:
            ee:5d:0f:14:37:7d:65:fb:04:9d:c1:18:e3:2d:a1:
            ec:43:ca:45:1c:37:6f:a3:a9:5f:78:20:f9:4f:7b:
            dd:3c:20:e9:f6:c4:65:06:9e:de:cd:a4:08:91:c1:
            dd:df:ba:7e:6f:99:b6:9a:9b:d1:71:9f:32:37:e8:
            5f:ce:94:af:db:c7:47:c4:aa:d1:59:70:6f:55:3d:
            5f:6b:33:ad:24:0e:ad:7a:9f:52:32:a3:0a:4b:27:
            68:57:58:96:c6:23:b3:a9:44:af:bc:05:36:f4:64:
            4d:fe:f4:31:57:a8:c8:be:a1:f2:28:8f:51:91:f6:
            2f:cd:f9:20:4e:ae:0f:4c:5d:02:ab:a9:74:c6:31:
            0a:b8:61:ea:f6:6d:3c:4e:6d:31:29:93:0c:44:43:
            c9:46:b5:af:e1:f8:78:68:da:65:ff:37:6f:b3:4a:
            30:19:32:e0:69:a5:e4:a0:cf:47:3e:bc:e2:d2:99:
            46:5e:0c:2b:c4:60:ec:56:a1:7c:62:b5:de:1c:8a:
            9d:29:24:c9:89:39:96:29:c8:fd:8c:38:38:c8:1a:
            b2:dc:71:11:d9:b6:83:c8:98:e3:2f:91:f8:71:9f:
            d5:45:fe:37:90:fc:cd:84:f6:36:96:33:60:0e:0a:
            30:3e:79
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        F3:2E:FC:AA:C3:B5:E9:B1:29:59:CF:7A:43:5C:78:A7:77:37:38:92
      X509v3 Authority Key Identifier:
        keyid:F3:2E:FC:AA:C3:B5:E9:B1:29:59:CF:7A:43:5C:78:A7:77:37:38:92

      X509v3 Basic Constraints:
        CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
    00:f5:4f:68:ed:31:85:38:f0:db:f3:35:e9:f0:b5:27:4f:29:
    75:74:6e:23:04:26:54:d9:05:5b:a6:bf:f0:a9:e0:aa:96:39:
    67:83:60:63:0a:6b:ae:2a:2c:10:ff:49:b9:e9:6e:75:00:3c:
    78:0e:51:2e:f1:dd:3e:02:1b:4f:e9:1e:95:0d:6a:d7:12:de:
    1b:d7:67:1d:29:97:fc:63:bc:f1:ce:06:9f:0a:56:93:a9:c4:
    fa:0f:92:69:44:04:12:54:f7:43:5c:8f:b6:f2:e2:f4:3a:6a:
    d1:c1:3d:50:02:e8:3b:8e:a0:c9:72:4c:1f:ef:68:b2:6f:22:
    11:6b:08:d5:08:c8:39:74:32:e6:f9:6a:20:df:3c:3a:a6:29:
    c4:95:75:f2:72:b1:92:da:f9:41:4a:fb:6a:b7:e9:5a:8d:80:
    fb:a8:14:e1:a8:0f:a6:82:d1:81:90:94:7a:e8:38:31:8a:c7:
    1d:83:71:3e:32:68:8c:89:33:de:84:72:32:0c:0a:e7:e6:19:
    72:90:cc:5b:7b:71:3f:cd:7e:ef:c3:8a:f1:1c:80:25:f1:cc:
    2d:c5:20:80:7e:af:9a:53:4c:ac:ff:37:ac:33:27:ee:21:7e:
    d9:3c:eb:da:52:44:82:af:3f:eb:b6:12:13:8e:a4:55:f6:41:
    72:8b:78:c4:be:4c:79:f9:54:9b:35:03:90:8a:bb:1a:9d:a9:
    7a:b0:7d:7a:c9:67:f1:56:60:14:4f:a4:5b:21:ad:d0:d0:cc:
    f3:e3:15:90:d5:4c:28:55:12:e3:9e:e2:f5:af:0d:52:94:aa:
    40:cf:86:69:77:2e:1b:fe:05:8b:a3:88:19:39:d6:14:66:4d:
    01:b2:5d:13:25:4a:57:f6:e4:c0:b2:ce:71:fe:87:19:5e:f6:
    4a:27:bb:ff:93:30:76:2b:41:2f:e8:a1:7e:ac:cc:b0:1a:99:
    19:28:b9:e2:f0:c1:85:7a:6d:5c:31:49:f9:6f:e9:3b:c1:86:
```

55:b7:12:ac:51:00:10:29:5b:7a:ca:4e:a8:62:72:9d:ab:ed:
e0:af:5c:7c:28:20:43:bc:47:72:b4:5e:c4:2a:4d:c5:96:a5:
54:3f:59:b0:71:bf:78:7f:1b:d1:63:40:3b:bc:54:4e:ca:81:
79:ad:bd:e3:2b:a1:9c:c7:a8:f4:c2:40:fa:33:55:5e:e2:c3:
91:92:79:4d:c6:a9:f3:aa:23:f7:ff:87:a8:81:e8:cf:2b:5b:
5e:f5:0d:96:b7:6e:9f:00:bf:86:4d:88:a5:d4:56:21:bc:d3:
7a:eb:44:ea:78:0d:60:47:64:a6:c5:27:2c:40:b1:41:10:2e:
7d:07:65:22:0f:4

```
ats@serverA:~/sahb16_ca$ openssl x509 -noout -text -in certs/root.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 11802078299821680574 (0xa3c967af0037a7be)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Validity
            Not Before: May 25 22:03:25 2018 GMT
            Not After : May 20 22:03:25 2038 GMT
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b6:8f:f2:f0:be:ee:d3:7d:bf:da:fb:c7:7e:b8:
                    ea:19:a0:8f:48:e8:d7:35:5f:83:08:0a:be:1f:cb:
                    be:b6:13:2a:ef:6e:12:e3:d7:07:8d:c4:57:d5:65:
                    b9:db:a2:48:fa:46:24:73:15:da:83:aa:3f:49:05:
                    a9:a6:db:e1:b5:3a:fe:a3:3b:3a:f1:f3:ad:0e:6e:
                    48:76:68:23:f0:02:14:72:0d:6f:14:00:46:02:54:
                    94:d9:4d:fd:5d:fc:9d:52:28:2f:07:58:30:92:8b:
                    b4:30:aa:5a:ac:24:b9:0b:14:c1:11:c0:d5:77:55:
                    98:3e:ae:b8:1d:b6:9f:e0:58:62:df:3d:63:9f:5c:
                    9f:0d:ba:e3:6d:e4:de:4e:16:3f:62:33:f0:2a:90:
                    98:26:58:a3:7f:63:c7:cb:32:0b:17:63:b9:a0:ab:
                    83:5c:65:66:0b:f8:2e:c2:7e:48:9e:da:94:c9:e2:
                    cc:b8:d3:f4:ca:9c:ef:0c:54:f1:c5:2f:53:b6:13:
                    d2:13:f7:33:32:c6:ed:9b:e4:35:47:ad:28:f5:7a:
                    6c:30:67:cc:a7:70:2a:6e:41:4a:74:c6:b7:79:2f:
                    10:22:10:26:3e:ae:0c:0d:13:16:ef:c2:ca:b5:4d:
                    bc:e9:43:25:d7:d2:73:a7:29:78:ce:87:dd:01:6a:
                    27:99:d3:2b:a9:43:4d:f1:fd:61:d1:23:fa:5d:7d:
                    ee:5d:0f:14:37:7d:65:fb:04:9d:c1:18:e3:2d:a1:
                    ec:43:ca:45:1c:37:6f:a3:a9:5f:78:20:f9:4f:7b:
                    dd:3c:20:e9:f6:c4:65:06:9e:de:cd:a4:08:91:c1:
                    dd:df:ba:7e:6f:99:b6:9a:9b:d1:71:9f:32:37:e8:
```

```
ats@serverA:~/sahb16_ca$ openssl req -config ca1/openssl.cnf -new -sha256 -key ca1/private/ca1.key.pem
Enter pass phrase for ca1/private/ca1.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) [AU]:SE
State or Province Name (full name) [Some-State]:Blekinge
Locality Name (eg, city) []:Karlskrona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ET2540
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:saddam-ca
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
-----BEGIN CERTIFICATE REQUEST-----
MIIEnzCCAocCAQAwWjELMAkGA1UEBhMCU0UxETAPBgNVBAgMCEJsZWtpbmdlMRMw
EQYDVQQHDApLYXJsc2tyb25hMQ8wDQYDVQQKDAZFVDI1NDAxEjAQBgNVBAMMCXNh
ZGRhbS1jYTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMZNvBTu1z92
kQzVrzWNBkaUknoXZDhMQ4V1jfjcw6xlYyDHcB7V1SSGKjX0W3P/wxhjPIUbuhW3
zx8V4HS48uayPXFXpB2aP1rMYjczwoQeSAqjeIx0s263NzXoBMbliQzQNdWC4Rty
qNsyshJIxy67/h2HYTvFM4vP5/uGTGKokNxCgyMy8uTHO+QNJofOBIG2fh8LbUNW
ad8ix/sI0GrsQtm4c/3aGCESUiOu5il6vWozpkm3ZCbvC42aCJUgg5kn6LIugnrm
SdtS5Q4O8xNJF5Fj1Ho7Qqq/LMCjKKjBKbnnd8K2z1vHE1/XRx+/9Hoyz2/U4tuz
AwDCi8rM3G/ewET57GoDXV6BQuYxWV3dBmup9/wixwhwp8SobT/qZGT7UJ1M/lLm
QnuuYdps0Poy3Tgk1S8MBWvRfAq7XkB/F44m023FJB8jkAEEaFV3LwBa9l+umf8L
mjjONe8G5ifeppInHQtfK5HOTPKXDP/0DcT6KvksSgwjwrtF0qttqNBWGMav4up7
oHWzh8hPHXfi+pH8hGFIEaHHLqRbFP1e4O7R0jaRGXGLjNfOIqJy9rqhcK9OIxkJ
URPZDRMxDrdIluHcq3JCBGw/xXqLp2YjiNeEOt4f37hNy23mxYlxrUKRjy+tikKM
3EMekTNwpnzA0d/N/FeOB8akQre9ruyrAgMBAAGgADANBgkqhkiG9w0BAQsFAAOC
AgEAY58QSMkNCWVf1rMf6kBUjfCYzo481PaASF+T/mmf9PetHzW6oHLPXassx8Qs
eyxu/js0H3MthaprnyihBbjJ4CTwtMV7zBxVjxmbdUbSc/NdXvPaZsYl9NjUNLN4
Pcew3Hvt8fv+Pkz8ddf4QUlmnPCpDnRUN0mpnq6IaHoVjnjRZMO3D5QLSJkD/xwz
```

Create the CSR

openssl req -config ca1/openssl.cnf -new -sha256 -key ca1/private/ca1.key.pem -out ca1/csr/ca1.csr.pem

Task 8: Verify the CSR

```
ats@serverA:~/sahb16_ca$ openssl req -text -noout -verify -in ca1/csr/ca1.csr.pem
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:c6:4d:bc:14:ee:d7:3f:76:91:0c:d5:af:35:8d:
                    06:46:94:92:7a:17:64:38:4c:43:85:75:8d:f8:dc:
                    c3:ac:65:63:20:c7:70:1e:d5:d5:24:86:2a:35:f4:
                    5b:73:ff:c3:18:63:3c:85:1b:ba:15:b7:cf:1f:15:
                    e0:74:b8:f2:e6:b2:3d:71:57:a4:1d:9a:3f:5a:cc:
                    62:37:33:c2:84:1e:48:0a:a3:78:8c:74:b3:6e:b7:
                    37:35:e8:04:c6:e5:89:0c:d0:35:d5:82:e1:1b:72:
                    a8:db:32:b2:12:48:c7:2e:bb:fe:1d:87:61:3b:c5:
                    33:8b:cf:e7:fb:86:4c:62:a8:90:dc:42:83:23:32:
                    f2:e4:c7:3b:e4:0d:26:87:ce:04:81:b6:7e:1f:0b:
                    6d:43:56:69:df:22:c7:fb:08:d0:6a:ec:42:d9:b8:
                    73:fd:da:18:21:12:52:23:ae:e6:29:7a:bd:6a:33:
                    a6:49:b7:64:26:ef:0b:8d:9a:08:95:20:83:99:27:
                    e8:b2:2e:82:7a:e6:49:db:52:e5:0e:0e:f3:13:49:
                    17:91:63:d4:7a:3b:42:aa:bf:2c:c0:a3:28:a8:c1:
                    29:b9:e7:77:c2:b6:cf:5b:c7:13:5f:d7:47:1f:bf:
                    f4:7a:32:cf:6f:d4:e2:db:b3:03:00:c2:8b:ca:cc:
                    dc:6f:de:c0:44:f9:ec:6a:03:5d:5e:81:42:e6:31:
                    59:5d:dd:06:6b:a9:f7:fc:22:c7:08:70:a7:c4:a8:
                    6d:3f:ea:64:64:fb:50:9d:4c:fe:52:e6:42:7b:ae:
                    61:da:6c:d0:fa:32:dd:38:24:d5:2f:0c:05:6b:d1:
                    7c:0a:bb:5e:40:7f:17:8e:26:d3:6d:c5:24:1f:23:
                    90:01:04:68:55:77:2f:00:5a:f6:5f:ae:99:ff:0b:
                    9a:38:ce:35:ef:06:e6:27:de:a6:92:27:1d:0b:5f:
                    2b:91:ce:4c:f2:97:0c:ff:f4:0d:c4:fa:2a:f9:2c:
                    4a:0c:23:c2:bb:45:d2:ab:6d:a8:d0:56:18:c6:af:
                    e2:ea:7b:a0:75:b3:87:c8:4f:1d:77:e2:fa:91:fc:
                    84:61:48:11:a1:c7:2e:a4:5b:14:fd:5e:e0:ee:d1:
                    d2:36:91:19:71:8b:8c:d7:ce:22:a2:72:f6:ba:a1:
                    70:af:4e:23:19:09:51:13:d9:0d:13:31:0e:b7:48:
                    96:e1:dc:ab:72:42:04:6c:3f:c5:7a:8b:a7:66:23:
                    88:d7:84:3a:de:1f:df:b8:4d:cb:6d:e6:c5:89:71:
                    ad:42:91:8f:2f:ad:8a:42:8c:dc:43:1e:91:33:70:
```

```
                a6:7c:c0:d1:df:cd:fc:57:8e:07:c6:a4:42:b7:bd:
                ae:ec:ab
            Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         63:9f:10:48:c9:0d:09:65:5f:d6:b3:1f:ea:40:54:8d:f0:98:
         ce:8e:3c:d4:f6:80:48:5f:93:fe:69:9f:f4:f7:ad:1f:35:ba:
         a0:72:cf:5d:ab:2c:c7:c4:2c:7b:2c:6e:fe:3b:34:1f:73:2d:
         85:aa:6b:9f:28:a1:05:b8:c9:e0:24:f0:b4:c5:7b:cc:1c:55:
         8f:19:9b:75:46:d2:73:f3:5d:5e:f3:da:66:c6:25:f4:d8:d4:
         34:b3:78:3d:c7:b0:dc:7b:ed:f1:fb:fe:3e:4c:fc:75:d7:f8:
         41:49:66:9c:f0:a9:0e:74:54:37:49:a9:9e:ae:88:68:7a:15:
         8e:78:d1:64:c3:b7:0f:94:0b:48:99:03:ff:1c:33:39:ab:01:
         71:ed:29:ff:58:1a:ce:fd:e9:2a:57:aa:04:54:97:c7:63:2b:
         63:a1:1e:44:4f:95:ec:bf:68:87:6a:60:61:6a:b0:3f:12:45:
         64:19:46:2b:2f:66:9f:e9:f3:56:ee:4c:d6:1d:0f:e6:8e:2d:
         6e:a7:fd:7d:ca:60:d2:61:48:9a:2c:a3:8c:f6:47:14:12:63:
         97:54:c8:e4:29:1f:9a:b8:8c:79:e2:0f:9a:a7:aa:d0:1a:26:
         5f:4c:58:1d:29:dc:44:2d:24:a2:76:72:08:0c:b4:95:ba:44:
         8e:8e:13:47:a0:b3:71:49:fa:7b:36:74:78:8d:95:0d:14:83:
         3b:75:e6:fd:6f:34:ba:88:11:5d:09:0f:f8:c8:16:0b:be:db:
         cf:62:d6:f9:34:bf:0b:e1:78:ac:aa:4f:a4:a9:1a:df:b7:dc:
         05:5b:24:51:6e:76:fe:f3:bc:57:f2:25:da:64:80:ef:88:33:
         03:d3:1a:b2:d9:09:b8:cb:dd:02:2a:45:bd:61:4c:e2:10:1b:
         c2:30:ef:ab:92:76:e2:8f:00:89:44:12:62:96:b6:33:65:3e:
         e7:43:b8:38:58:1b:2a:a7:30:97:e2:28:1f:40:03:f8:0d:29:
         93:0c:80:67:6d:62:c7:f7:98:db:35:07:a5:b2:3a:38:1b:e8:
         f2:46:13:29:9d:ba:5b:9b:e2:3a:61:c1:0c:09:82:81:97:e2:
         96:2c:c2:36:ab:91:68:bf:6f:a5:c3:70:02:7c:9f:42:78:d4:
         d8:89:46:a8:96:a7:cf:c8:f3:07:00:d6:1c:0c:54:19:66:55:
         f6:9b:bf:a6:7d:16:82:29:12:39:dd:23:d6:c9:41:96:8c:f4:
         4c:a5:0f:3d:14:77:20:e5:3c:bd:c3:5f:e1:c6:9b:f5:23:a4:
         56:9d:97:05:5b:ca:81:2d:3c:ff:4f:b4:91:9e:76:5b:85:21:
         c2:eb:98:e9:eb:79:d0:82
ats@serverA:~/sahb16_ca$
```

```
ats@serverA:~/sahb16_ca$ openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days
3650 -notext -md sha256 -in ca1/csr/ca1.csr.pem -out ca1/certs/ca1.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/private/root.key.pem:
```

```
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8192 (0x2000)
        Validity
            Not Before: May 25 23:44:12 2018 GMT
            Not After : May 22 23:44:12 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            organizationName          = ET2540
            commonName                = saddam-ca
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                C7:C8:67:63:C1:21:73:CC:9E:F7:1D:8C:71:F4:B9:4F:BE:2F:73:5F
            X509v3 Authority Key Identifier:
                keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until May 22 23:44:12 2028 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
Data Base Updated
ats@serverA:~/sahb16_ca$
```

```
ats@serverA:~/sahb16_ca$ openssl req -text -noout -verify -in ca1/csr/ca1.csr.pem
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:c6:4d:bc:14:ee:d7:3f:76:91:0c:d5:af:35:8d:
                    06:46:94:92:7a:17:64:38:4c:43:85:75:8d:f8:dc:
                    c3:ac:65:63:20:c7:70:1e:d5:d5:24:86:2a:35:f4:
                    5b:73:ff:c3:18:63:3c:85:1b:ba:15:b7:cf:1f:15:
                    e0:74:b8:f2:e6:b2:3d:71:57:a4:1d:9a:3f:5a:cc:
                    62:37:33:c2:84:1e:48:0a:a3:78:8c:74:b3:6e:b7:
                    37:35:e8:04:c6:e5:89:0c:d0:35:d5:82:e1:1b:72:
                    a8:db:32:b2:12:48:c7:2e:bb:fe:1d:87:61:3b:c5:
                    33:8b:cf:e7:fb:86:4c:62:a8:90:dc:42:83:23:32:
                    f2:e4:c7:3b:e4:0d:26:87:ce:04:81:b6:7e:1f:0b:
                    6d:43:56:69:df:22:c7:fb:08:d0:6a:ec:42:d9:b8:
                    73:fd:da:18:21:12:52:23:ae:e6:29:7a:bd:6a:33:
                    a6:49:b7:64:26:ef:0b:8d:9a:08:95:20:83:99:27:
                    e8:b2:2e:82:7a:e6:49:db:52:e5:0e:0e:f3:13:49:
                    17:91:63:d4:7a:3b:42:aa:bf:2c:c0:a3:28:a8:c1:
                    29:b9:e7:77:c2:b6:cf:5b:c7:13:5f:d7:47:1f:bf:
                    f4:7a:32:cf:6f:d4:e2:db:b3:03:00:c2:8b:ca:cc:
                    dc:6f:de:c0:44:f9:ec:6a:03:5d:5e:81:42:e6:31:
                    59:5d:dd:06:6b:a9:f7:fc:22:c7:08:70:a7:c4:a8:
                    6d:3f:ea:64:64:fb:50:9d:4c:fe:52:e6:42:7b:ae:
                    61:da:6c:d0:fa:32:dd:38:24:d5:2f:0c:05:6b:d1:
                    7c:0a:bb:5e:40:7f:17:8e:26:d3:6d:c5:24:1f:23:
                    90:01:04:68:55:77:2f:00:5a:f6:5f:ae:99:ff:0b:
                    9a:38:ce:35:ef:06:e6:27:de:a6:92:27:1d:0b:5f:
```

```
ats@serverA:~/sahb16_ca$ openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in ca1/csr/ca1.csr.pem -out ca1/c
erts/ca1.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/private/root.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8192 (0x2000)
        Validity
            Not Before: May 25 23:44:12 2018 GMT
            Not After : May 22 23:44:12 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            organizationName          = ET2540
            commonName                = saddam-ca
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                C7:C8:67:63:C1:21:73:CC:9E:F7:1D:8C:71:F4:B9:4F:BE:2F:73:5F
            X509v3 Authority Key Identifier:
                keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until May 22 23:44:12 2028 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
Data Base Updated
ats@serverA:~/sahb16_ca$
```

Task 9

Command
openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in ca1/csr/ca1.csr.pem -out ca1/certs/ca1.cert.pem

-config openssl.cnf
specifies the configuration file to use.

-extensions v3_intermediate_ca
the section of the configuration file containing certificate extensions to be added when a certificate is issued (defaults to x509_extensions unless the -extfile option is used).

If no extension section is present then, a V1 certificate is created. If the extension section is present (even if it is empty), then a V3 certificate is created.

-days 3650
the number of days to certify the certificate for.

-notext
don't output the text form of a certificate to the output file.

-md sha256
the message digest to use. Possible values include md5, sha1 and mdc2. This option also applies to CRLs.

-in ca1/csr/ca1.csr.pem
an input filename containing a single certificate request to be signed by the CA.

-out ca1/certs/ca1.cert.pem
the output file to output certificates to. The default is standard output. The certificate details will also be printed out to this file in PEM format (except that -spkac outputs DER format).

Task 10: Verify the certificate for CA1

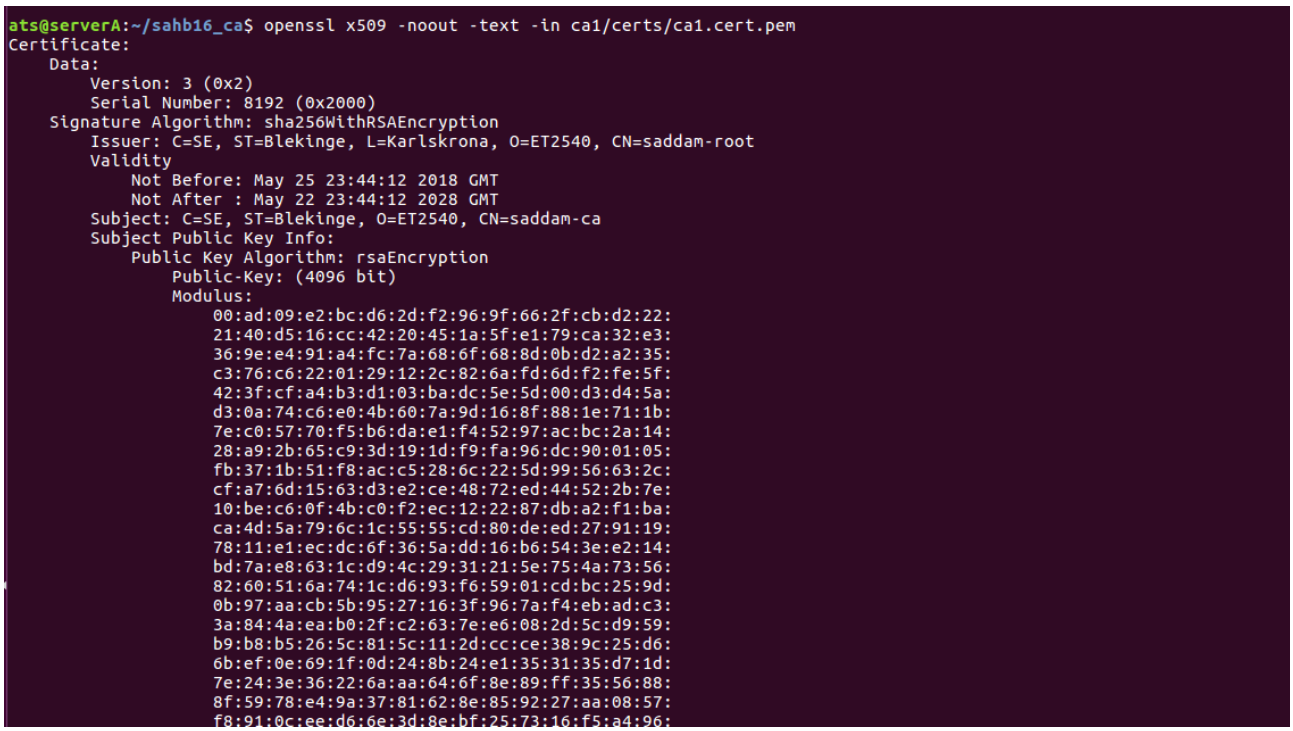
ats@serverA:~/sahb16_ca$ clear

ats@serverA:~/sahb16_ca$ openssl x509 -noout -text -in ca1/certs/ca1.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8192 (0x2000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Validity
            Not Before: May 25 23:44:12 2018 GMT
            Not After : May 22 23:44:12 2028 GMT
        Subject: C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:

```
            00:ad:09:e2:bc:d6:2d:f2:96:9f:66:2f:cb:d2:22:
            21:40:d5:16:cc:42:20:45:1a:5f:e1:79:ca:32:e3:
            36:9e:e4:91:a4:fc:7a:68:6f:68:8d:0b:d2:a2:35:
            c3:76:c6:22:01:29:12:2c:82:6a:fd:6d:f2:fe:5f:
            42:3f:cf:a4:b3:d1:03:ba:dc:5e:5d:00:d3:d4:5a:
            d3:0a:74:c6:e0:4b:60:7a:9d:16:8f:88:1e:71:1b:
            7e:c0:57:70:f5:b6:da:e1:f4:52:97:ac:bc:2a:14:
            28:a9:2b:65:c9:3d:19:1d:f9:fa:96:dc:90:01:05:
            fb:37:1b:51:f8:ac:c5:28:6c:22:5d:99:56:63:2c:
            cf:a7:6d:15:63:d3:e2:ce:48:72:ed:44:52:2b:7e:
            10:be:c6:0f:4b:c0:f2:ec:12:22:87:db:a2:f1:ba:
            ca:4d:5a:79:6c:1c:55:55:cd:80:de:ed:27:91:19:
            78:11:e1:ec:dc:6f:36:5a:dd:16:b6:54:3e:e2:14:
            bd:7a:e8:63:1c:d9:4c:29:31:21:5e:75:4a:73:56:
            82:60:51:6a:74:1c:d6:93:f6:59:01:cd:bc:25:9d:
            0b:97:aa:cb:5b:95:27:16:3f:96:7a:f4:eb:ad:c3:
            3a:84:4a:ea:b0:2f:c2:63:7e:e6:08:2d:5c:d9:59:
            b9:b8:b5:26:5c:81:5c:11:2d:cc:ce:38:9c:25:d6:
            6b:ef:0e:69:1f:0d:24:8b:24:e1:35:31:35:d7:1d:
            7e:24:3e:36:22:6a:aa:64:6f:8e:89:ff:35:56:88:
            8f:59:78:e4:9a:37:81:62:8e:85:92:27:aa:08:57:
            f8:91:0c:ee:d6:6e:3d:8e:bf:25:73:16:f5:a4:96:
            a3:ec:a4:e3:c7:d5:a0:ba:9f:1b:50:2f:d5:0e:2e:
            b4:47:01:22:af:57:fa:8d:d8:62:75:4d:75:bd:48:
            57:c1:8e:0e:68:50:9b:1f:8e:0e:0e:cc:a0:52:87:
            5f:7a:43:41:f2:cf:75:32:8b:f0:05:be:58:59:12:
            e9:20:88:aa:24:7a:59:f1:73:1b:48:28:4f:4c:97:
            c7:51:31:c4:a6:bf:4c:79:e5:d4:0f:bb:64:fb:bf:
            b8:d6:36:2d:9f:41:79:66:04:b1:16:2b:7b:cc:f2:
            53:45:10:ca:a1:ce:2d:59:64:4e:78:70:d6:ed:6a:
            cf:f1:c7:c7:c5:fc:27:99:6d:5e:3b:04:90:0b:11:
            eb:bf:66:64:a4:20:8b:47:50:71:e1:2a:34:6e:84:
            bb:40:71:31:1e:d7:3a:34:4e:8a:cf:23:90:f6:c3:
            51:81:72:24:c1:60:9f:99:18:07:69:0a:96:d0:45:
            84:72:51
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        C7:C8:67:63:C1:21:73:CC:9E:F7:1D:8C:71:F4:B9:4F:BE:2F:73:5F
      X509v3 Authority Key Identifier:
        keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A

      X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:0
      X509v3 Key Usage: critical
        Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
    c6:81:f8:9d:4b:b9:f8:59:7b:d8:89:8f:57:d7:71:63:ea:3b:
    ce:79:66:8a:26:7a:37:12:61:09:e3:2a:91:a6:7b:2f:b5:7c:
    f6:89:a7:32:fd:ab:69:8f:a6:80:c8:77:56:b1:e8:4d:e2:13:
    6c:17:87:52:f4:a7:99:5e:5c:3b:2e:1c:9f:7a:95:fa:6e:81:
    70:26:4b:39:90:02:c3:b2:49:c3:80:2d:e5:7d:c6:dd:5d:f9:
```

```
        54:de:09:45:a1:fb:6f:07:fc:ad:c6:6f:df:bb:b7:23:80:8d:
        01:15:d4:21:06:8f:ca:88:ca:2d:02:df:5e:04:ad:d7:ee:a2:
        36:2d:ae:e4:7c:33:3d:fa:58:e5:49:c2:5c:74:6b:87:94:41:
        af:c6:88:bc:55:3c:38:20:d3:64:8e:e3:56:f6:d2:2c:2a:a8:
        9f:94:a2:3c:02:1e:8e:b4:7c:b1:1a:3e:d0:70:07:1f:02:ee:
        38:01:c0:12:50:03:c0:a5:57:4e:b2:55:83:6a:05:88:9f:08:
        3a:8d:c4:42:af:7f:75:42:64:c1:29:ee:59:4c:97:41:de:38:
        b6:7c:b0:9d:ac:cf:58:a2:0a:9d:8c:d2:4b:6e:4f:79:5f:47:
        49:f0:5a:03:eb:55:1b:60:8e:94:4c:2d:be:6e:cd:ff:0f:ff:
        2a:c0:8e:33:cd:e1:54:29:ff:00:ba:b1:4e:80:a6:32:c7:bb:
        b4:36:0c:dc:ce:37:29:fe:0a:25:7c:d2:d7:4d:51:d0:a0:02:
        4e:70:d3:b6:d8:40:b4:fb:1c:83:45:38:8c:46:79:40:c5:19:
        79:a0:a5:68:5f:81:de:9b:95:8b:fd:e7:23:2a:ac:e4:b3:c5:
        b0:e1:83:6f:df:ee:47:35:5b:1c:ee:2f:59:a6:63:a1:3d:81:
        03:4b:02:ca:b8:5a:f7:55:f2:90:39:f0:c8:52:39:6f:d8:9f:
        e8:5c:33:05:43:bf:30:11:1b:1f:4e:d6:ba:9a:05:22:4f:1a:
        2f:58:74:87:42:3e:bd:ce:d7:40:16:16:e5:bb:01:c3:7a:f9:
        81:b7:82:a3:30:93:46:d2:28:8a:80:e0:90:a4:f4:e7:a2:08:
        d3:20:10:c5:56:e5:9e:d1:11:14:16:4f:bb:24:8f:f2:84:16:
        cf:ce:dd:1f:95:5b:d6:59:b8:b1:16:d2:c0:b9:25:a6:d2:3a:
        08:1e:b9:3b:13:ab:0c:50:6e:ed:0e:51:1d:48:c0:d0:a3:e1:
        de:12:cc:2b:cc:13:31:f4:f2:99:35:46:05:a4:6a:ca:6a:cd:
        b6:3c:61:89:4e:ed:e5:c6:33:63:30:b2:28:a4:6b:55:29:b9:
        17:ca:b1:5e:12:01:25:b1
ats@serverA:~/sahb16_ca$
```

```
ats@serverA:~/sahb16_ca$ openssl verify -CAfile certs/root.cert.pem ca1/certs/ca1.cert.pem
ca1/certs/ca1.cert.pem: OK
ats@serverA:~/sahb16_ca$
```



Task 11:

Create a certificate chain
cat ca1/certs/ca1.cert.pem certs/root.cert.pem > ca1/certs/ca1.cert-chain.pem

Ensure the certificate chain is accessible to all users on Server A

chmod 444 ca1/certs/ca1.cert-chain.pem

ats@serverA:~/sahb16_ca$ openssl genrsa -out ca1/private/serverCa1.key.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

ats@serverA:~/sahb16_ca$ openssl req -config ca1/openssl.cnf -new -sha256 -key ca1/private/serverCa1.key.pem -out ca1/csr/serverCa1.csr.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) [SE]:
State or Province Name (full name) [Blekinge]:

```
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [ET2540]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:serverCa1
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:



ats@serverA:~/sahb16_ca$ openssl req -noout -text -in ca1/csr/serverCa1.csr.pem
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=serverCa1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:28:17:84:33:56:c6:ce:34:8c:a3:ad:8d:05:
                    b7:37:fe:a2:e8:4c:10:c3:99:dc:81:bb:95:76:7e:
                    5b:91:4c:e7:cb:d8:6d:bb:79:ae:08:94:61:10:00:
                    db:0a:8e:78:62:97:d6:dc:64:f6:74:49:cb:78:db:
                    1f:6b:a2:82:a7:df:4f:9f:d3:ca:e7:56:cb:e1:0c:
                    e5:5f:5c:8c:f6:b7:c4:b7:1b:9f:d9:c8:29:24:54:
                    5f:b6:2e:d5:f5:3f:eb:76:d9:d1:29:fc:3d:58:0a:
                    12:23:21:ca:60:8c:52:3a:0c:ae:0e:f3:ed:85:fe:
                    6c:42:09:08:af:f6:69:32:6f:09:88:e4:5a:02:13:
                    f0:74:13:8d:cb:99:f4:06:89:b1:ab:f7:12:f3:1c:
                    39:49:78:fd:04:96:7c:ba:2a:d0:3c:4c:44:14:db:
                    de:1f:02:54:88:cf:b9:23:55:36:85:a8:85:0e:da:
                    f9:de:ba:d5:ea:96:03:9e:13:16:2a:a1:87:45:ee:
                    e1:4d:72:ec:14:ff:b8:a6:4a:17:8e:5e:91:7d:0b:
                    ee:1e:e5:45:a3:3a:b6:ee:5d:fd:54:ce:c9:de:10:
                    ae:ec:45:d0:a2:2d:d1:3b:40:1b:1b:43:e8:55:80:
                    9a:c0:c9:de:76:27:10:91:eb:13:e3:c1:2d:a5:da:
                    76:1f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         99:ae:24:52:af:f9:d3:d6:1a:7e:5f:25:3f:16:02:a9:e0:19:
         53:42:93:26:79:59:d5:2b:ae:62:63:aa:92:bc:6c:49:73:f4:
         25:ea:36:d2:92:6c:c2:bc:61:80:91:90:71:a6:f6:9e:82:a2:
         a2:5f:8e:9b:1e:89:5c:e8:4d:35:2a:72:76:c6:b9:42:c4:c1:
         a1:85:25:14:87:89:cb:93:bf:57:6e:e4:58:a9:73:c7:fa:3d:
         75:ec:1e:1d:83:52:4a:b5:01:0b:4e:5b:98:37:52:be:24:63:
         d1:61:38:9b:83:7a:3a:99:ad:35:6d:da:c9:97:f9:0c:e2:6b:
         26:78:b0:13:7f:21:a7:64:41:ba:27:fd:ca:02:24:6b:44:04:
```

```
        2e:33:1b:3b:2e:61:e5:a3:84:a7:93:10:c6:82:13:dc:55:82:
        00:c1:db:87:9e:89:01:26:be:f3:06:db:79:7a:3c:f5:b6:9f:
        00:8c:d5:5c:33:b1:17:bb:2a:25:61:21:46:ce:48:c7:0a:67:
        f4:ba:40:2d:23:d3:b0:f4:ea:6b:d1:62:9c:66:17:95:2c:a3:
        c3:b0:02:e2:81:bc:fa:c5:a3:74:68:03:0d:5e:d2:5d:3b:3b:
        fb:5f:13:68:a4:ac:28:e7:9a:2b:06:47:7b:10:75:cb:fc:09:
        8a:48:5f:7a
ats@serverA:~/sahb16_ca$

ats@serverA:~/sahb16_ca$ openssl ca -config openssl.cnf -extensions server_cert -days 3650 -
notext  -in ca1/csr/serverCa1.csr.pem -out ca1/certs/serverCa1.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/private/root.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8193 (0x2001)
        Validity
            Not Before: May 26 00:32:25 2018 GMT
            Not After : May 23 00:32:25 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            organizationName          = ET2540
            commonName                = serverCa1
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                77:6C:DC:63:53:01:6B:3C:AE:84:E9:B4:AF:58:28:5C:E6:EB:50:59
            X509v3 Authority Key Identifier:
                keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
                serial:84:DC:0E:85:21:D9:7F:54

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
Certificate is to be certified until May 23 00:32:25 2028 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
Data Base Updated
ats@serverA:~/sahb16_ca$




ats@serverA:~/sahb16_ca$ openssl x509 -noout -text -in ca1/certs/serverCa1.cert.pem
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8193 (0x2001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Validity
            Not Before: May 26 00:32:25 2018 GMT
            Not After : May 23 00:32:25 2028 GMT
        Subject: C=SE, ST=Blekinge, O=ET2540, CN=serverCa1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:28:17:84:33:56:c6:ce:34:8c:a3:ad:8d:05:
                    b7:37:fe:a2:e8:4c:10:c3:99:dc:81:bb:95:76:7e:
                    5b:91:4c:e7:cb:d8:6d:bb:79:ae:08:94:61:10:00:
                    db:0a:8e:78:62:97:d6:dc:64:f6:74:49:cb:78:db:
                    1f:6b:a2:82:a7:df:4f:9f:d3:ca:e7:56:cb:e1:0c:
                    e5:5f:5c:8c:f6:b7:c4:b7:1b:9f:d9:c8:29:24:54:
                    5f:b6:2e:d5:f5:3f:eb:76:d9:d1:29:fc:3d:58:0a:
                    12:23:21:ca:60:8c:52:3a:0c:ae:0e:f3:ed:85:fe:
                    6c:42:09:08:af:f6:69:32:6f:09:88:e4:5a:02:13:
                    f0:74:13:8d:cb:99:f4:06:89:b1:ab:f7:12:f3:1c:
                    39:49:78:fd:04:96:7c:ba:2a:d0:3c:4c:44:14:db:
                    de:1f:02:54:88:cf:b9:23:55:36:85:a8:85:0e:da:
                    f9:de:ba:d5:ea:96:03:9e:13:16:2a:a1:87:45:ee:
                    e1:4d:72:ec:14:ff:b8:a6:4a:17:8e:5e:91:7d:0b:
                    ee:1e:e5:45:a3:3a:b6:ee:5d:fd:54:ce:c9:de:10:
                    ae:ec:45:d0:a2:2d:d1:3b:40:1b:1b:43:e8:55:80:
                    9a:c0:c9:de:76:27:10:91:eb:13:e3:c1:2d:a5:da:
                    76:1f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                77:6C:DC:63:53:01:6B:3C:AE:84:E9:B4:AF:58:28:5C:E6:EB:50:59
            X509v3 Authority Key Identifier:
                keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
                serial:84:DC:0E:85:21:D9:7F:54

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         88:61:72:28:9e:1c:ac:a6:07:25:e2:f3:e0:e4:ba:3d:45:05:
         31:ad:68:20:ca:cc:0e:70:37:85:47:86:e2:5d:1e:d7:6d:80:
         36:6d:54:1c:7c:50:e4:0e:02:d0:c0:f2:be:ac:52:0f:54:75:
         eb:9f:34:b2:cc:28:e2:2a:05:b9:32:3c:07:89:9f:6e:46:95:
```

```
        5c:c9:25:19:27:04:25:06:63:64:6a:f6:75:61:29:04:90:ab:
        ab:07:3c:d9:09:e6:24:f2:6b:26:25:3e:47:a9:d6:72:f0:de:
        c1:31:f6:5c:b0:9f:57:7d:c9:7f:5e:fb:a5:c6:fb:c3:bf:48:
        73:d3:0a:f1:15:3d:79:83:ca:43:d7:86:c6:5b:7a:b5:5d:d7:
        de:4f:05:0d:ca:70:05:03:cc:08:58:b1:1e:e9:cd:cd:e0:84:
        c9:d3:33:09:83:c7:26:f8:4e:90:f9:79:b5:12:9f:b9:b8:45:
        9a:40:f3:64:63:22:dd:d2:10:8b:08:d9:f4:7c:36:94:86:7b:
        3c:c4:67:8e:82:0e:c7:d4:bd:ae:f0:93:46:c4:09:50:c3:25:
        c6:37:83:f8:b0:24:49:96:82:e1:83:80:c8:ce:1b:68:14:56:
        13:67:19:f4:6d:af:27:a8:09:6b:89:66:30:d5:70:b2:ad:4e:
        a2:3b:bf:fa:e0:aa:67:f8:b3:1e:66:e5:11:a3:90:65:6c:6a:
        2d:74:73:64:ae:cb:a6:5c:cb:33:8a:44:8a:8d:7f:8f:55:ec:
        11:a1:e7:28:44:f5:6f:98:a5:a5:72:cb:38:28:a5:ae:a1:bc:
        0e:37:d0:b9:98:31:56:57:ee:30:c7:d3:08:bc:2b:5d:e3:2d:
        3e:2c:8f:c7:f4:66:97:f7:20:30:d9:39:ac:84:d7:df:9b:6b:
        85:e6:b8:5e:8f:01:83:ea:0e:bc:79:0e:e7:bc:2c:76:da:5c:
        43:52:1f:fb:d0:2d:d0:fd:95:e3:b1:e3:dd:f1:1d:05:59:44:
        7d:17:26:95:86:1f:88:90:8b:04:50:43:95:e4:00:a2:f9:df:
        bc:7a:55:ac:63:ba:46:17:61:00:2e:e8:48:65:8d:d1:86:d3:
        e8:d3:cf:09:1b:69:3e:35:f6:61:de:6a:6d:9b:44:60:ae:27:
        38:8f:a1:c3:14:9f:6d:5c:ab:d8:02:b0:bd:03:69:c0:44:82:
        b7:89:ba:8f:3e:83:5f:09:9d:6e:d7:99:7b:78:21:ab:80:45:
        1d:ce:4b:17:84:15:2f:ad:cf:62:bf:a3:ef:02:57:37:03:d8:
        7e:ac:3c:53:66:e8:43:63:5f:81:b5:d0:35:b7:cb:f1:5c:8e:
        95:cf:c1:a3:fd:6f:11:19
ats@serverA:~/sahb16_ca$
```

```
ats@serverA:~/sahb16_ca$ openssl verify -CAfile certs/root.cert.pem ca1/certs/serverCa1.cert.pem
ca1/certs/serverCa1.cert.pem: OK
ats@serverA:~/sahb16_ca$
```

Content of the CSR :

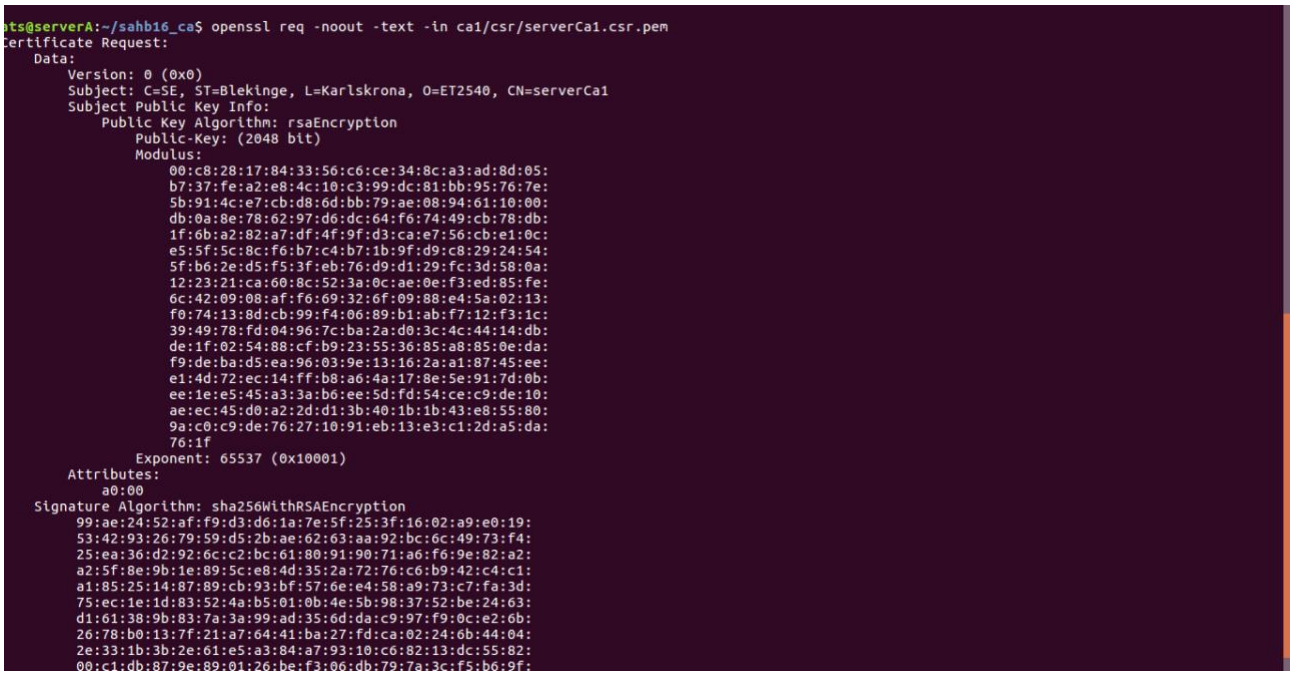
```
ats@serverA:~/sahb16_ca$ openssl req -noout -text -in ca1/csr/serverCa1.csr.pem
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=serverCa1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:28:17:84:33:56:c6:ce:34:8c:a3:ad:8d:05:
                    b7:37:fe:a2:e8:4c:10:c3:99:dc:81:bb:95:76:7e:
```

```
                5b:91:4c:e7:cb:d8:6d:bb:79:ae:08:94:61:10:00:
                db:0a:8e:78:62:97:d6:dc:64:f6:74:49:cb:78:db:
                1f:6b:a2:82:a7:df:4f:9f:d3:ca:e7:56:cb:e1:0c:
                e5:5f:5c:8c:f6:b7:c4:b7:1b:9f:d9:c8:29:24:54:
                5f:b6:2e:d5:f5:3f:eb:76:d9:d1:29:fc:3d:58:0a:
                12:23:21:ca:60:8c:52:3a:0c:ae:0e:f3:ed:85:fe:
                6c:42:09:08:af:f6:69:32:6f:09:88:e4:5a:02:13:
                f0:74:13:8d:cb:99:f4:06:89:b1:ab:f7:12:f3:1c:
                39:49:78:fd:04:96:7c:ba:2a:d0:3c:4c:44:14:db:
                de:1f:02:54:88:cf:b9:23:55:36:85:a8:85:0e:da:
                f9:de:ba:d5:ea:96:03:9e:13:16:2a:a1:87:45:ee:
                e1:4d:72:ec:14:ff:b8:a6:4a:17:8e:5e:91:7d:0b:
                ee:1e:e5:45:a3:3a:b6:ee:5d:fd:54:ce:c9:de:10:
                ae:ec:45:d0:a2:2d:d1:3b:40:1b:1b:43:e8:55:80:
                9a:c0:c9:de:76:27:10:91:eb:13:e3:c1:2d:a5:da:
                76:1f
            Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         99:ae:24:52:af:f9:d3:d6:1a:7e:5f:25:3f:16:02:a9:e0:19:
         53:42:93:26:79:59:d5:2b:ae:62:63:aa:92:bc:6c:49:73:f4:
         25:ea:36:d2:92:6c:c2:bc:61:80:91:90:71:a6:f6:9e:82:a2:
         a2:5f:8e:9b:1e:89:5c:e8:4d:35:2a:72:76:c6:b9:42:c4:c1:
         a1:85:25:14:87:89:cb:93:bf:57:6e:e4:58:a9:73:c7:fa:3d:
         75:ec:1e:1d:83:52:4a:b5:01:0b:4e:5b:98:37:52:be:24:63:
         d1:61:38:9b:83:7a:3a:99:ad:35:6d:da:c9:97:f9:0c:e2:6b:
         26:78:b0:13:7f:21:a7:64:41:ba:27:fd:ca:02:24:6b:44:04:
         2e:33:1b:3b:2e:61:e5:a3:84:a7:93:10:c6:82:13:dc:55:82:
         00:c1:db:87:9e:89:01:26:be:f3:06:db:79:7a:3c:f5:b6:9f:
         00:8c:d5:5c:33:b1:17:bb:2a:25:61:21:46:ce:48:c7:0a:67:
         f4:ba:40:2d:23:d3:b0:f4:ea:6b:d1:62:9c:66:17:95:2c:a3:
         c3:b0:02:e2:81:bc:fa:c5:a3:74:68:03:0d:5e:d2:5d:3b:3b:
         fb:5f:13:68:a4:ac:28:e7:9a:2b:06:47:7b:10:75:cb:fc:09:
         8a:48:5f:7a
ats@serverA:~/sahb16_ca$
```

```
ats@serverA:~/sahb16_ca$ openssl x509 -noout -text -in ca1/certs/serverCa1.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8193 (0x2001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Validity
            Not Before: May 26 00:32:25 2018 GMT
```

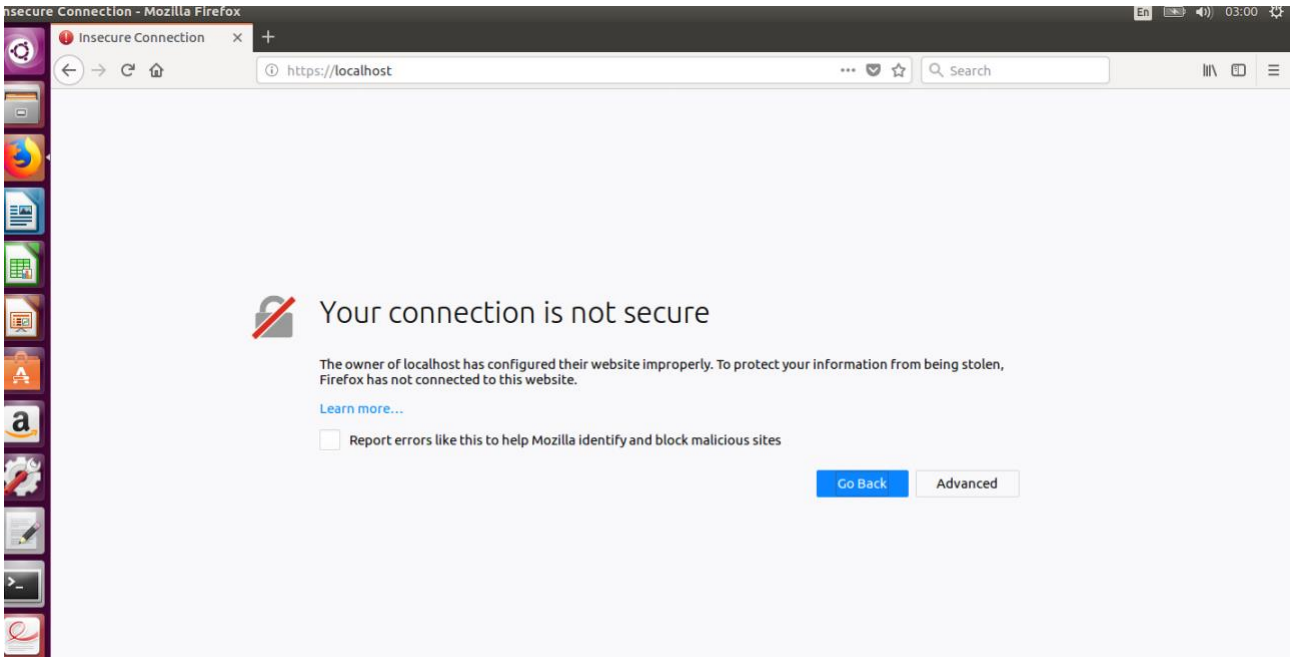
```
        Not After : May 23 00:32:25 2028 GMT
    Subject: C=SE, ST=Blekinge, O=ET2540, CN=serverCa1
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:c8:28:17:84:33:56:c6:ce:34:8c:a3:ad:8d:05:
                b7:37:fe:a2:e8:4c:10:c3:99:dc:81:bb:95:76:7e:
                5b:91:4c:e7:cb:d8:6d:bb:79:ae:08:94:61:10:00:
                db:0a:8e:78:62:97:d6:dc:64:f6:74:49:cb:78:db:
                1f:6b:a2:82:a7:df:4f:9f:d3:ca:e7:56:cb:e1:0c:
                e5:5f:5c:8c:f6:b7:c4:b7:1b:9f:d9:c8:29:24:54:
                5f:b6:2e:d5:f5:3f:eb:76:d9:d1:29:fc:3d:58:0a:
                12:23:21:ca:60:8c:52:3a:0c:ae:0e:f3:ed:85:fe:
                6c:42:09:08:af:f6:69:32:6f:09:88:e4:5a:02:13:
                f0:74:13:8d:cb:99:f4:06:89:b1:ab:f7:12:f3:1c:
                39:49:78:fd:04:96:7c:ba:2a:d0:3c:4c:44:14:db:
                de:1f:02:54:88:cf:b9:23:55:36:85:a8:85:0e:da:
                f9:de:ba:d5:ea:96:03:9e:13:16:2a:a1:87:45:ee:
                e1:4d:72:ec:14:ff:b8:a6:4a:17:8e:5e:91:7d:0b:
                ee:1e:e5:45:a3:3a:b6:ee:5d:fd:54:ce:c9:de:10:
                ae:ec:45:d0:a2:2d:d1:3b:40:1b:1b:43:e8:55:80:
                9a:c0:c9:de:76:27:10:91:eb:13:e3:c1:2d:a5:da:
                76:1f
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Subject Key Identifier:
            77:6C:DC:63:53:01:6B:3C:AE:84:E9:B4:AF:58:28:5C:E6:EB:50:59
        X509v3 Authority Key Identifier:
            keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A
            DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
            serial:84:DC:0E:85:21:D9:7F:54

        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
Signature Algorithm: sha256WithRSAEncryption
    88:61:72:28:9e:1c:ac:a6:07:25:e2:f3:e0:e4:ba:3d:45:05:
    31:ad:68:20:ca:cc:0e:70:37:85:47:86:e2:5d:1e:d7:6d:80:
    36:6d:54:1c:7c:50:e4:0e:02:d0:c0:f2:be:ac:52:0f:54:75:
    eb:9f:34:b2:cc:28:e2:2a:05:b9:32:3c:07:89:9f:6e:46:95:
    5c:c9:25:19:27:04:25:06:63:64:6a:f6:75:61:29:04:90:ab:
    ab:07:3c:d9:09:e6:24:f2:6b:26:25:3e:47:a9:d6:72:f0:de:
    c1:31:f6:5c:b0:9f:57:7d:c9:7f:5e:fb:a5:c6:fb:c3:bf:48:
    73:d3:0a:f1:15:3d:79:83:ca:43:d7:86:c6:5b:7a:b5:5d:d7:
    de:4f:05:0d:ca:70:05:03:cc:08:58:b1:1e:e9:cd:cd:e0:84:
    c9:d3:33:09:83:c7:26:f8:4e:90:f9:79:b5:12:9f:b9:b8:45:
    9a:40:f3:64:63:22:dd:d2:10:8b:08:d9:f4:7c:36:94:86:7b:
    3c:c4:67:8e:82:0e:c7:d4:bd:ae:f0:93:46:c4:09:50:c3:25:
```

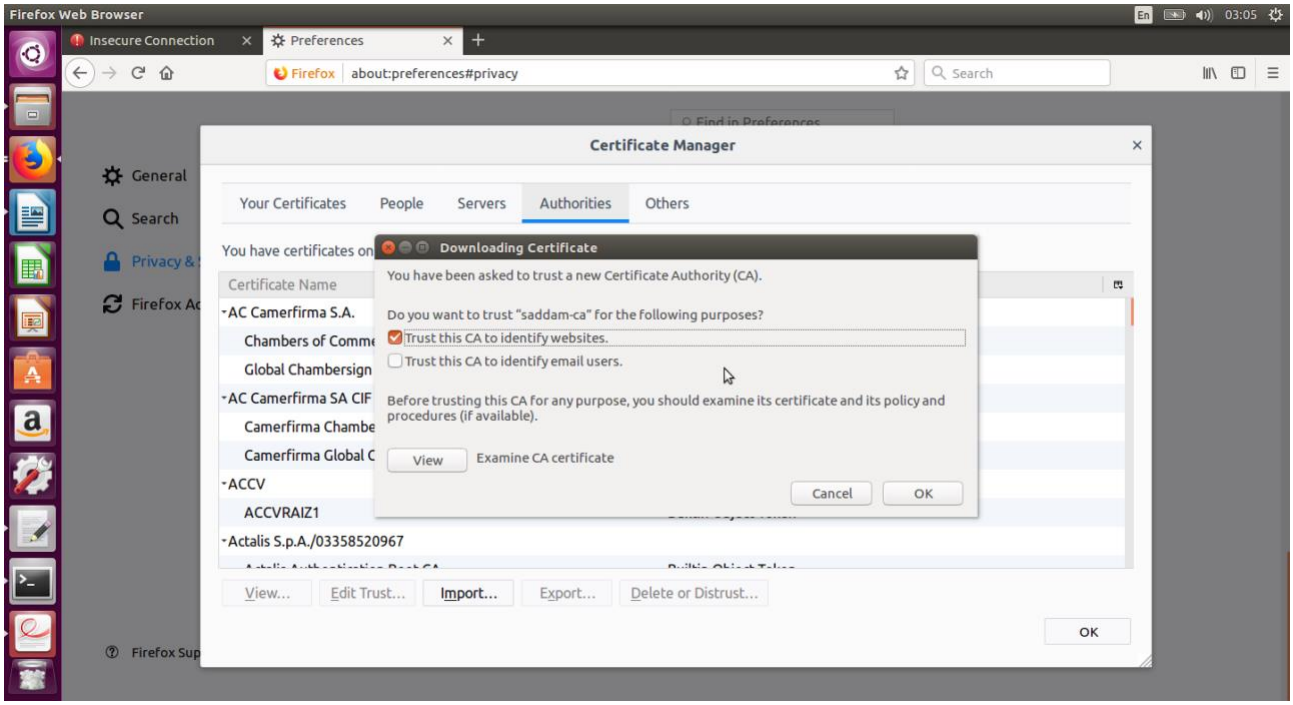
c6:37:83:f8:b0:24:49:96:82:e1:83:80:c8:ce:1b:68:14:56:
13:67:19:f4:6d:af:27:a8:09:6b:89:66:30:d5:70:b2:ad:4e:
a2:3b:bf:fa:e0:aa:67:f8:b3:1e:66:e5:11:a3:90:65:6c:6a:
2d:74:73:64:ae:cb:a6:5c:cb:33:8a:44:8a:8d:7f:8f:55:ec:
11:a1:e7:28:44:f5:6f:98:a5:a5:72:cb:38:28:a5:ae:a1:bc:
0e:37:d0:b9:98:31:56:57:ee:30:c7:d3:08:bc:2b:5d:e3:2d:
3e:2c:8f:c7:f4:66:97:f7:20:30:d9:39:ac:84:d7:df:9b:6b:
85:e6:b8:5e:8f:01:83:ea:0e:bc:79:0e:e7:bc:2c:76:da:5c:
43:52:1f:fb:d0:2d:d0:fd:95:e3:b1:e3:dd:f1:1d:05:59:44:
7d:17:26:95:86:1f:88:90:8b:04:50:43:95:e4:00:a2:f9:df:
bc:7a:55:ac:63:ba:46:17:61:00:2e:e8:48:65:8d:d1:86:d3:
e8:d3:cf:09:1b:69:3e:35:f6:61:de:6a:6d:9b:44:60:ae:27:
38:8f:a1:c3:14:9f:6d:5c:ab:d8:02:b0:bd:03:69:c0:44:82:
b7:89:ba:8f:3e:83:5f:09:9d:6e:d7:99:7b:78:21:ab:80:45:
1d:ce:4b:17:84:15:2f:ad:cf:62:bf:a3:ef:02:57:37:03:d8:
7e:ac:3c:53:66:e8:43:63:5f:81:b5:d0:35:b7:cb:f1:5c:8e:
95:cf:c1:a3:fd:6f:11:19
ats@serverA:~/sahb16_ca$

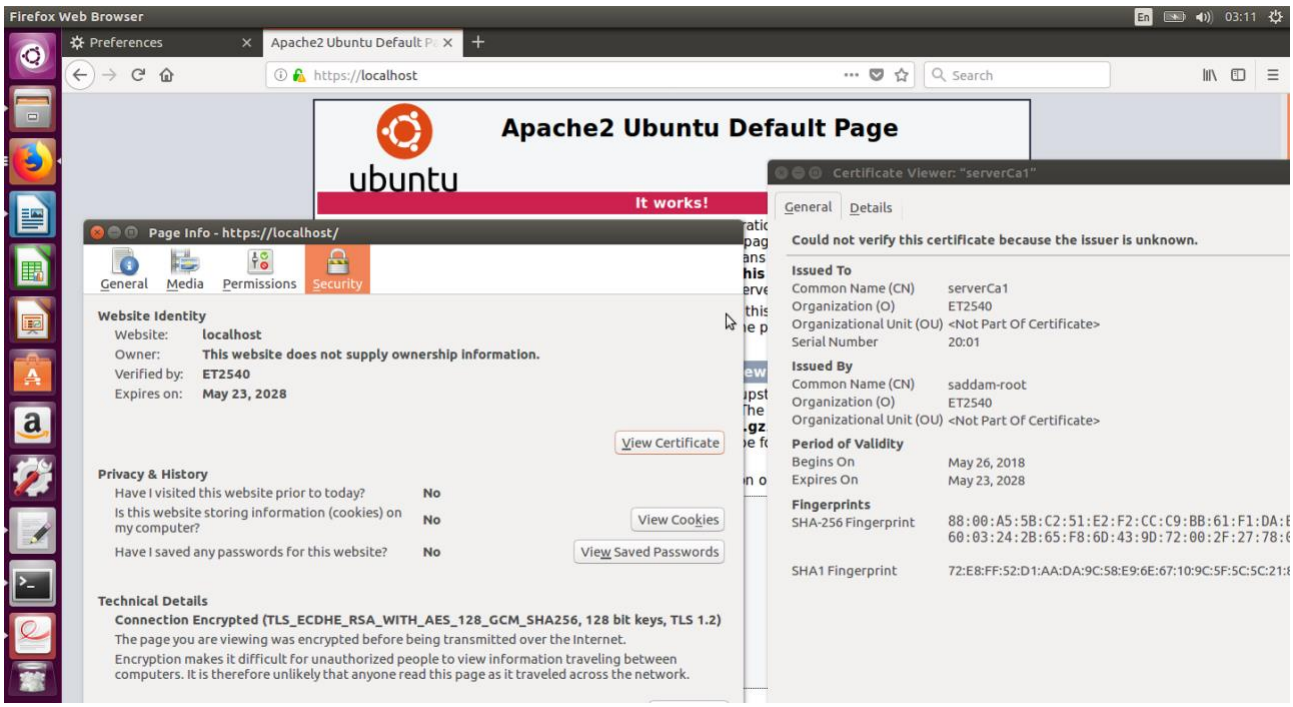


Task 12: Apache2 Server

Add certificate chain to Firefox web browser


Insecure Connection - Mozilla Firefox
Insecure Connection
https://localhost
Search
Your connection is not secure
The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced


Firefox Web Browser
Insecure Connection
Preferences
Firefox
about:preferences#privacy
Search
General
Search
Privacy &
Firefox Ac
Certificate Manager
Your Certificates
People
Servers
Authorities
Others
You have certificates on
Certificate Name
AC Camerfirma S.A.
Chambers of Comme
Global Chambersign
AC Camerfirma SA CIF
Camerfirma Chambe
Camerfirma Global C
ACCV
ACCVRAIZ1
Actalis S.p.A./03358520967
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "saddam-ca" for the following purposes?
Trust this CA to identify websites.
Trust this CA to identify email users.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
Cancel
OK
Firefox Sup



Show your certificate in Firefox

Revoke the certificate

Edit the CA1 OpenSSL configuration file and add the following parameter to the server_cert section:
crlDistributionPoints = URI:https://localhost/ca1.crl.pem

Task 13:

ats@serverA:~/sahb16_ca$ openssl ca -config ca1/openssl.cnf -gencrl -out ca1/crl/ca1.crl.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/ca1/private/ca1.key.pem:

ats@serverA:~/sahb16_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=SE/ST=Blekinge/O=ET2540/CN=saddam-ca
        Last Update: May 26 01:15:33 2018 GMT
        Next Update: Jun 25 01:15:33 2018 GMT
        CRL extensions:
            X509v3 CRL Number:
                8192
No Revoked Certificates.
    Signature Algorithm: sha256WithRSAEncryption
         93:71:09:7f:eb:54:67:1c:4d:c5:39:79:9d:24:4e:7c:5c:7a:
         93:1e:d2:12:a9:91:a6:52:40:1d:b2:55:34:6e:96:5a:67:17:
         4e:ff:19:3c:81:e9:81:eb:95:54:33:51:b3:a3:8f:11:c2:b2:
         dc:d5:73:cb:cb:7a:8c:9c:92:30:7a:5a:f5:90:a1:d2:67:bb:
         c4:c4:13:85:af:d4:16:c0:4e:b8:b3:63:c7:bf:fe:7d:e4:dc:

a3:6d:59:bf:4e:c3:23:35:fb:5c:5f:3f:3e:be:6a:42:50:06:
94:ba:5c:5c:f0:31:0f:58:e4:0f:28:a5:2a:a5:3f:dc:fc:4c:
06:ec:6e:aa:2e:61:09:37:05:0e:43:4d:1b:a8:88:f3:50:6e:
8c:8e:bf:30:f7:c2:f3:72:b4:a9:97:2e:94:c6:ca:03:2e:27:
1f:0d:1b:4e:a3:71:69:10:e8:5b:23:e8:8c:00:9c:fc:64:0f:
7c:37:97:10:65:01:09:62:3e:64:dc:da:f2:51:f0:d8:fc:f1:
d9:10:f4:08:8e:f2:1a:2f:80:dd:3f:c8:9f:bb:ff:c9:04:96:
4d:e7:45:cd:17:e2:4e:f8:6a:e0:18:3c:d7:97:17:83:14:a0:
f0:47:d0:c5:db:bd:4c:58:4a:7e:71:d6:b2:25:03:81:f1:0a:
d7:c0:45:ef:a8:5f:46:d5:74:51:7a:40:f0:8f:20:0f:bd:37:
b5:94:31:16:06:df:b2:70:ed:29:b8:d8:41:05:51:b7:dc:fe:
21:4b:17:9d:0a:91:38:9c:a7:96:84:2b:0d:80:8b:d5:1a:09:
71:16:0e:35:31:2a:96:0f:e7:e6:b6:b7:5c:81:39:53:b2:80:
87:30:18:aa:5a:4f:3d:4c:56:66:41:62:b4:88:33:7a:ad:41:
57:52:7d:84:4f:80:ac:65:01:36:56:54:5a:d1:d7:ce:38:e5:
89:bc:7e:29:0e:4d:59:ed:4c:27:c0:e0:1d:9a:0c:64:44:79:
f3:f3:29:0f:4f:40:29:a2:6a:ba:ea:8a:80:24:a4:e7:e6:b5:
0f:96:2e:c8:19:91:fe:24:10:c3:01:9b:dd:04:92:06:b6:9f:
9f:60:7f:a8:d1:e4:e5:9e:26:fc:b5:cc:75:1a:61:ee:45:13:
c0:ce:7b:0b:06:ac:0a:fc:5d:ac:3b:69:2f:ec:57:94:43:e6:
c2:77:50:77:35:ea:76:4d:5f:4f:a3:3d:9b:35:1b:c5:ac:98:
7b:4a:8c:e9:32:5c:f6:e6:15:3b:ec:56:bd:4d:e0:fc:5c:ae:
9d:94:e9:ce:a3:dc:4c:af:ff:5a:65:81:b2:1e:f0:38:b4:35:
8b:1c:84:82:3a:6b:8d:ef
ats@serverA:~/sahb16_ca$

```
ats@serverA:~/sahb16_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=SE/ST=Blekinge/O=ET2540/CN=saddam-ca
        Last Update: May 26 01:15:33 2018 GMT
        Next Update: Jun 25 01:15:33 2018 GMT
        CRL extensions:
            X509v3 CRL Number:
                8192
No Revoked Certificates.
    Signature Algorithm: sha256WithRSAEncryption
         93:71:09:7f:eb:54:67:1c:4d:c5:39:79:9d:24:4e:7c:5c:7a:
         93:1e:d2:12:a9:91:a6:52:40:1d:b2:55:34:6e:96:5a:67:17:
         4e:ff:19:3c:81:e9:81:eb:95:54:33:51:b3:a3:8f:11:c2:b2:
         dc:d5:73:cb:cb:7a:8c:9c:92:30:7a:5a:f5:90:a1:d2:67:bb:
         c4:c4:13:85:af:d4:16:c0:4e:b8:b3:63:c7:bf:fe:7d:e4:dc:
         a3:6d:59:bf:4e:c3:23:35:fb:5c:5f:3f:3e:be:6a:42:50:06:
         94:ba:5c:5c:f0:31:0f:58:e4:0f:28:a5:2a:a5:3f:dc:fc:4c:
         06:ec:6e:aa:2e:61:09:37:05:0e:43:4d:1b:a8:88:f3:50:6e:
         8c:8e:bf:30:f7:c2:f3:72:b4:a9:97:2e:94:c6:ca:03:2e:27:
         1f:0d:1b:4e:a3:71:69:10:e8:5b:23:e8:8c:00:9c:fc:64:0f:
         7c:37:97:10:65:01:09:62:3e:64:dc:da:f2:51:f0:d8:fc:f1:
         d9:10:f4:08:8e:f2:1a:2f:80:dd:3f:c8:9f:bb:ff:c9:04:96:
         4d:e7:45:cd:17:e2:4e:f8:6a:e0:18:3c:d7:97:17:83:14:a0:
         f0:47:d0:c5:db:bd:4c:58:4a:7e:71:d6:b2:25:03:81:f1:0a:
         d7:c0:45:ef:a8:5f:46:d5:74:51:7a:40:f0:8f:20:0f:bd:37:
         b5:94:31:16:06:df:b2:70:ed:29:b8:d8:41:05:51:b7:dc:fe:
         21:4b:17:9d:0a:91:38:9c:a7:96:84:2b:0d:80:8b:d5:1a:09:
         71:16:0e:35:31:2a:96:0f:e7:e6:b6:b7:5c:81:39:53:b2:80:
         87:30:18:aa:5a:4f:3d:4c:56:66:41:62:b4:88:33:7a:ad:41:
         57:52:7d:84:4f:80:ac:65:01:36:56:54:5a:d1:d7:ce:38:e5:
         89:bc:7e:29:0e:4d:59:ed:4c:27:c0:e0:1d:9a:0c:64:44:79:
         f3:f3:29:0f:4f:40:29:a2:6a:ba:ea:8a:80:24:a4:e7:e6:b5:
         0f:96:2e:c8:19:91:fe:24:10:c3:01:9b:dd:04:92:06:b6:9f:
         9f:60:7f:a8:d1:e4:e5:9e:26:fc:b5:cc:75:1a:61:ee:45:13:
         c0:ce:7b:0b:06:ac:0a:fc:5d:ac:3b:69:2f:ec:57:94:43:e6:
         c2:77:50:77:35:ea:76:4d:5f:4f:a3:3d:9b:35:1b:c5:ac:98:
         7b:4a:8c:e9:32:5c:f6:e6:15:3b:ec:56:bd:4d:e0:fc:5c:ae:
         9d:94:e9:ce:a3:dc:4c:af:ff:5a:65:81:b2:1e:f0:38:b4:35:
         8b:1c:84:82:3a:6b:8d:ef
ats@serverA:~/sahb16_ca$
```

Task 14 Revoke a certificate:

Creating certificate for dragos illie:

ats@serverA:~/sahb16_ca$ openssl genrsa -out ca1/private/dragos.ilie@bth.se.key.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
ats@serverA:~/sahb16_ca$ openssl req -config ca1/openssl.cnf -new -sha256 -key ca1/private/dragos.ilie@bth.se.key.pem -out ca1/csr/dragos.ilie@bth.se.csr.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) [SE]:

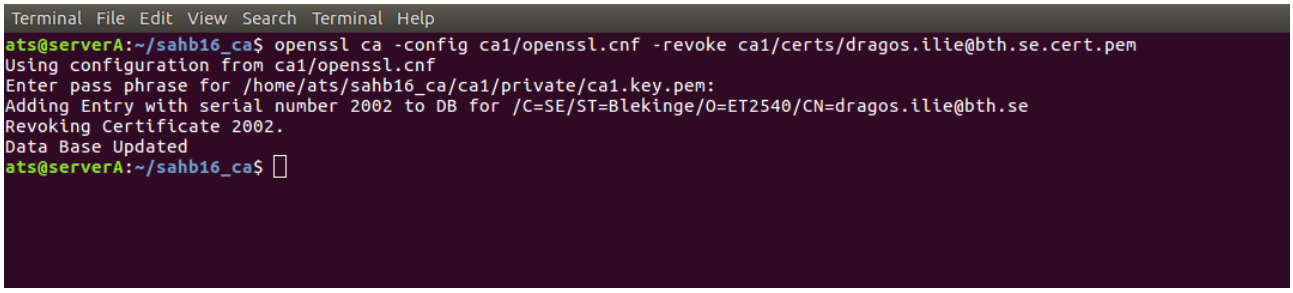
```
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [ET2540]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:dragos.ilie@bth.se
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
ats@serverA:~/sahb16_ca$ openssl req -noout -text -in ca1/csr/serverCa1.csr.pem
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=serverCa1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:28:17:84:33:56:c6:ce:34:8c:a3:ad:8d:05:
                    b7:37:fe:a2:e8:4c:10:c3:99:dc:81:bb:95:76:7e:
                    5b:91:4c:e7:cb:d8:6d:bb:79:ae:08:94:61:10:00:
                    db:0a:8e:78:62:97:d6:dc:64:f6:74:49:cb:78:db:
                    1f:6b:a2:82:a7:df:4f:9f:d3:ca:e7:56:cb:e1:0c:
                    e5:5f:5c:8c:f6:b7:c4:b7:1b:9f:d9:c8:29:24:54:
                    5f:b6:2e:d5:f5:3f:eb:76:d9:d1:29:fc:3d:58:0a:
                    12:23:21:ca:60:8c:52:3a:0c:ae:0e:f3:ed:85:fe:
                    6c:42:09:08:af:f6:69:32:6f:09:88:e4:5a:02:13:
                    f0:74:13:8d:cb:99:f4:06:89:b1:ab:f7:12:f3:1c:
                    39:49:78:fd:04:96:7c:ba:2a:d0:3c:4c:44:14:db:
                    de:1f:02:54:88:cf:b9:23:55:36:85:a8:85:0e:da:
                    f9:de:ba:d5:ea:96:03:9e:13:16:2a:a1:87:45:ee:
                    e1:4d:72:ec:14:ff:b8:a6:4a:17:8e:5e:91:7d:0b:
                    ee:1e:e5:45:a3:3a:b6:ee:5d:fd:54:ce:c9:de:10:
                    ae:ec:45:d0:a2:2d:d1:3b:40:1b:1b:43:e8:55:80:
                    9a:c0:c9:de:76:27:10:91:eb:13:e3:c1:2d:a5:da:
                    76:1f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         99:ae:24:52:af:f9:d3:d6:1a:7e:5f:25:3f:16:02:a9:e0:19:
         53:42:93:26:79:59:d5:2b:ae:62:63:aa:92:bc:6c:49:73:f4:
         25:ea:36:d2:92:6c:c2:bc:61:80:91:90:71:a6:f6:9e:82:a2:
         a2:5f:8e:9b:1e:89:5c:e8:4d:35:2a:72:76:c6:b9:42:c4:c1:
         a1:85:25:14:87:89:cb:93:bf:57:6e:e4:58:a9:73:c7:fa:3d:
         75:ec:1e:1d:83:52:4a:b5:01:0b:4e:5b:98:37:52:be:24:63:
         d1:61:38:9b:83:7a:3a:99:ad:35:6d:da:c9:97:f9:0c:e2:6b:
         26:78:b0:13:7f:21:a7:64:41:ba:27:fd:ca:02:24:6b:44:04:
         2e:33:1b:3b:2e:61:e5:a3:84:a7:93:10:c6:82:13:dc:55:82:
         00:c1:db:87:9e:89:01:26:be:f3:06:db:79:7a:3c:f5:b6:9f:
```

```
        00:8c:d5:5c:33:b1:17:bb:2a:25:61:21:46:ce:48:c7:0a:67:
        f4:ba:40:2d:23:d3:b0:f4:ea:6b:d1:62:9c:66:17:95:2c:a3:
        c3:b0:02:e2:81:bc:fa:c5:a3:74:68:03:0d:5e:d2:5d:3b:3b:
        fb:5f:13:68:a4:ac:28:e7:9a:2b:06:47:7b:10:75:cb:fc:09:
        8a:48:5f:7a
ats@serverA:~/sahb16_ca$ openssl ca -config openssl.cnf -extensions server_cert -days 3650 -
notext  -in ca1/csr/dragos.ilie@bth.se.csr.pem -out ca1/certs/dragos.ilie@bth.se.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/private/root.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8194 (0x2002)
        Validity
            Not Before: May 26 01:29:06 2018 GMT
            Not After : May 23 01:29:06 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            organizationName          = ET2540
            commonName                = dragos.ilie@bth.se
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                4B:B3:80:D7:45:0C:4C:1F:98:E3:21:E7:3C:96:6B:E0:F9:C7:09:C6
            X509v3 Authority Key Identifier:
                keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
                serial:84:DC:0E:85:21:D9:7F:54

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
Certificate is to be certified until May 23 01:29:06 2028 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
Data Base Updated
ats@serverA:~/sahb16_ca$ openssl x509 -noout -text -in ca1/certs/dragos.ilie@bth.se.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8194 (0x2002)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root
        Validity
            Not Before: May 26 01:29:06 2018 GMT
            Not After : May 23 01:29:06 2028 GMT
```

```
    Subject: C=SE, ST=Blekinge, O=ET2540, CN=dragos.ilie@bth.se
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:d5:38:0a:72:fa:5a:b7:1d:1f:29:c0:34:d5:bb:
          69:17:a1:a2:de:f6:9b:1d:67:4a:c6:d9:31:d8:35:
          b6:b3:f6:43:ea:99:9a:86:39:9f:bd:1a:01:10:21:
          32:73:ec:18:f2:69:e4:d9:92:49:6b:94:8f:90:5d:
          94:75:91:09:eb:33:c5:15:74:fc:08:5f:b6:47:ad:
          89:41:f9:3f:e2:18:1e:33:1e:b6:6f:80:81:7c:4e:
          c8:c6:3b:d7:89:1a:22:fa:c3:ba:36:c8:3c:76:e1:
          6e:13:48:29:47:6c:4b:43:eb:12:b5:41:3f:89:46:
          00:5a:ae:1d:90:d7:d9:47:4a:b6:be:bf:ce:82:0f:
          69:44:c6:64:4a:3d:56:98:cc:a1:c0:dd:3a:4f:4e:
          93:0b:8e:8c:fa:ce:00:92:85:f2:19:fe:56:28:55:
          d3:ab:73:99:9e:c7:f6:8e:86:99:85:f7:ae:84:ff:
          c6:39:bc:87:42:cc:27:d1:b1:5f:1e:f1:00:10:cb:
          cd:72:d0:ce:ed:c8:81:c4:7d:7a:b5:6e:5c:c3:d4:
          f0:1e:1b:e8:e2:5d:7d:f6:ff:a9:a7:ad:4c:76:b4:
          bf:ae:3c:96:f8:11:ea:2e:59:87:0a:a8:55:4b:ff:
          bb:66:11:6a:e3:5d:03:5d:36:f2:d3:35:8a:f0:24:
          a7:f7
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        4B:B3:80:D7:45:0C:4C:1F:98:E3:21:E7:3C:96:6B:E0:F9:C7:09:C6
      X509v3 Authority Key Identifier:
        keyid:0F:17:D6:55:00:B9:DC:43:74:D4:BB:A6:CE:9C:92:CC:82:9B:F3:4A
        DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
        serial:84:DC:0E:85:21:D9:7F:54

      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
      X509v3 Extended Key Usage:
        TLS Web Server Authentication
Signature Algorithm: sha256WithRSAEncryption
    33:5d:5e:6a:89:0d:81:28:80:97:10:ad:c8:47:0b:d9:4e:8a:
    43:f7:78:27:83:73:96:e3:b1:4e:e7:a5:e6:1b:4b:2e:51:34:
    b2:85:f7:b4:20:57:ee:e1:e1:49:72:9d:5b:7d:da:a1:d1:0a:
    2e:3c:85:de:cb:b5:81:a1:26:ac:3e:b9:7e:02:d9:cd:91:f7:
    21:88:3c:a6:90:c4:14:94:55:02:0b:29:9e:34:c0:05:67:bc:
    8a:6d:26:73:f1:9c:39:c9:30:9b:dc:ec:b5:1f:a3:e8:26:bf:
    02:2c:bf:47:0e:0b:55:ae:24:fa:58:53:39:f3:6a:d3:fa:3e:
    a9:13:f5:92:f0:16:80:be:e8:7d:eb:31:d0:8c:dc:a8:f0:ed:
    f7:34:2b:d5:60:85:ae:80:b0:f3:5f:56:04:a6:eb:b3:7e:7b:
    8b:d4:ae:21:e8:95:c5:63:e9:fc:a4:67:de:fc:ce:6f:49:75:
    e7:f6:e3:55:de:f1:4a:b3:fa:37:9f:5a:ff:7f:84:9d:a3:d8:
    ce:3a:15:55:fb:f8:ff:92:a5:1d:6b:18:57:0f:ba:c5:61:53:
    22:ac:bd:81:a2:1c:d7:75:6b:92:0c:14:25:a3:8f:3b:16:6b:
```

54:44:3e:93:60:e3:ff:33:e3:fc:e5:1e:90:de:30:7a:68:e3:
23:39:c7:0d:22:02:c9:8f:cc:86:5d:77:9a:78:62:3b:84:6d:
9f:a6:4b:19:cd:ea:fe:87:a6:98:5a:c7:c6:d1:0a:ea:39:99:
84:05:d3:48:35:23:e6:49:18:1e:c6:24:75:df:f2:e2:33:41:
2d:aa:17:20:05:9b:98:77:88:e2:0a:65:26:02:19:5a:7b:5c:
66:56:fd:50:fb:00:72:77:ea:d3:3d:42:00:56:97:e0:b1:cf:
8e:c1:31:57:18:2c:d9:ba:d5:c5:89:87:f1:7e:39:e9:8a:65:
0a:8e:49:fa:d9:af:2f:76:e5:cd:d7:67:cd:87:21:c7:b5:3f:
7e:ed:51:3b:b6:c0:ab:1b:3d:5e:68:37:13:81:34:1e:4d:f1:
66:be:a9:c3:8f:cb:cb:d6:03:02:e7:82:df:fa:da:69:aa:4c:
48:da:23:8d:56:5d:52:96:2a:4b:94:03:3e:1c:ad:6c:3c:2a:
41:a3:4d:bc:9d:8d:1f:f0:31:c5:a3:77:3d:97:ec:d5:d0:d4:
35:20:34:01:98:28:4c:f2:df:5f:9b:60:5a:c4:2e:42:7b:94:
11:e9:d6:3a:34:26:6e:45:f5:89:da:0f:fb:3c:bc:af:65:2c:
16:dd:45:a5:76:98:46:99:70:4f:67:cb:c5:7d:2e:0b:84:4c:
52:89:1e:09:f1:be:72:ed

ats@serverA:~/sahb16_ca$ openssl verify -CAfile certs/root.cert.pem
ca1/certs/dragos.ilie@bth.se.cert.pem
ca1/certs/dragos.ilie@bth.se.cert.pem: OK
ats@serverA:~/sahb16_ca$



Revoking it :

ats@serverA:~/sahb16_ca$ openssl ca -config ca1/openssl.cnf -revoke
ca1/certs/dragos.ilie@bth.se.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/ca1/private/ca1.key.pem:
Adding Entry with serial number 2002 to DB for
/C=SE/ST=Blekinge/O=ET2540/CN=dragos.ilie@bth.se
Revoking Certificate 2002.
Data Base Updated
ats@serverA:~/sahb16_ca$

Context of index.txt file

R 280523012906Z 180526013153Z 2002 unknown
/C=SE/ST=Blekinge/O=ET2540/CN=dragos.ilie@bth.se

Recreate the CRL:

```
ats@serverA:~/sahb16_ca$ openssl ca -config ca1/openssl.cnf -gencrl -out ca1/crl/ca1.crl.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/ca1/private/ca1.key.pem:
ats@serverA:~/sahb16_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=SE/ST=Blekinge/O=ET2540/CN=saddam-ca
        Last Update: May 26 01:37:38 2018 GMT
        Next Update: Jun 25 01:37:38 2018 GMT
        CRL extensions:
            X509v3 CRL Number:
                8194
Revoked Certificates:
    Serial Number: 2002
        Revocation Date: May 26 01:31:53 2018 GMT
    Signature Algorithm: sha256WithRSAEncryption
         3b:d9:c8:8a:f1:69:b0:05:b5:7c:c8:36:f9:e4:5f:72:67:bd:
         de:dd:7e:35:2b:23:ed:7b:f7:9f:aa:03:b8:4d:78:92:d5:c6:
         5d:ab:8e:80:76:b4:99:31:5a:ec:82:ec:2f:93:47:4d:84:7e:
         29:29:1f:22:c3:5f:d9:37:ef:bd:9c:a8:bc:81:da:90:4a:f8:
         73:ca:cf:4b:96:9f:91:e0:77:ce:81:41:08:69:e8:98:55:89:
         32:df:3e:ba:a5:db:41:11:8a:51:1d:47:af:62:a4:59:cc:04:
         a5:79:5c:0c:fd:8e:55:06:7e:20:2e:d8:64:e6:34:2f:e7:39:
         52:26:fb:85:0c:47:17:e4:15:e5:2f:95:9b:60:90:65:37:83:
         3a:b2:07:5b:b1:b2:41:44:f9:f7:31:2c:da:5f:ef:35:1b:41:
         b1:d6:5a:73:4e:c6:4b:f9:41:a3:7a:91:9e:39:ff:b6:72:83:
         64:aa:b1:70:11:23:6f:f5:a8:cb:41:db:67:d1:9e:05:f1:22:
         9e:6e:25:0a:04:03:30:7a:13:90:b4:ce:ad:87:ab:3a:3e:ac:
         d7:91:99:80:64:1f:a2:e0:ea:ad:95:9b:cd:37:52:6c:b6:4b:
         da:24:5b:66:15:81:a6:15:75:e1:dc:6a:be:09:12:d4:60:f0:
         47:f7:63:9b:41:7b:22:d3:c2:aa:a4:d5:19:66:60:eb:2c:f0:
         51:29:13:a9:df:ff:b8:0b:c6:89:18:94:db:ee:8e:b8:0f:b9:
         8e:d8:eb:83:90:7e:c2:bd:2f:24:72:58:2e:70:f3:3e:17:6f:
         90:d9:8f:38:fb:80:6f:c3:b4:49:1c:18:53:24:a3:4e:59:fa:
         8d:3c:b3:b9:18:a3:43:3f:34:6f:5d:9e:fd:99:b3:c6:9f:2a:
         51:9c:ed:71:76:7d:82:5b:d7:63:9d:7d:a2:f0:0b:79:43:3d:
         48:5a:37:e8:7d:8b:dc:66:94:2f:af:a3:49:66:6e:2c:2d:7a:
         d2:41:86:55:8b:61:a3:46:8a:44:95:74:13:01:96:a8:35:90:
         b2:25:70:4d:5f:ab:76:6c:aa:96:4f:83:bb:8b:c5:e5:54:d2:
```

aa:d9:84:f0:ee:8a:af:08:35:dc:fc:a0:8d:f4:4a:bf:06:e1:
e5:f6:26:c7:4d:44:e5:f9:bf:84:54:56:6f:6a:de:79:90:55:
1e:8a:48:28:c8:22:ce:4a:94:be:53:75:cf:82:63:5a:e0:51:
df:48:7b:6d:f5:1f:3f:1f:69:84:46:26:b9:11:f9:8d:8e:e4:
19:d5:23:5e:44:e2:b3:f5:ed:66:d3:3f:a0:d9:6d:a3:09:4a:
c8:1c:1f:44:0c:ff:72:69
ats@serverA:~/sahb16_ca$

```
ts@serverA:~/sahb16_ca$ openssl ca -config ca1/openssl.cnf -gencrl -out ca1/crl/ca1.crl.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/ca1/private/ca1.key.pem:
ts@serverA:~/sahb16_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=SE/ST=Blekinge/O=ET2540/CN=saddam-ca
        Last Update: May 26 01:37:38 2018 GMT
        Next Update: Jun 25 01:37:38 2018 GMT
        CRL extensions:
            X509v3 CRL Number:
                8194
Revoked Certificates:
    Serial Number: 2002
        Revocation Date: May 26 01:31:53 2018 GMT
    Signature Algorithm: sha256WithRSAEncryption
         3b:d9:c8:8a:f1:69:b0:05:b5:7c:c8:36:f9:e4:5f:72:67:bd:
         de:dd:7e:35:2b:23:ed:7b:f7:9f:aa:03:b8:4d:78:92:d5:c6:
         5d:ab:8e:80:76:b4:99:31:5a:ec:82:ec:2f:93:47:4d:84:7e:
         29:29:1f:22:c3:5f:d9:37:ef:bd:9c:a8:bc:81:da:90:4a:f8:
         73:ca:cf:4b:96:9f:91:e0:77:ce:81:41:08:69:e8:98:55:89:
         32:df:3e:ba:a5:db:41:11:8a:51:1d:47:af:62:a4:59:cc:04:
         a5:79:5c:0c:fd:8e:55:06:7e:20:2e:d8:64:e6:34:2f:e7:39:
         52:26:fb:85:0c:47:17:e4:15:e5:2f:95:9b:60:90:65:37:83:
         3a:b2:07:5b:b1:b2:41:44:f9:f7:31:2c:da:5f:ef:35:1b:41:
         b1:d6:5a:73:4e:c6:4b:f9:41:a3:7a:91:9e:39:ff:b6:72:83:
         64:aa:b1:70:11:23:6f:f5:a8:cb:41:db:67:d1:9e:05:f1:22:
         9e:6e:25:0a:04:03:30:7a:13:90:b4:ce:ad:87:ab:3a:3e:ac:
         d7:91:99:80:64:1f:a2:e0:ea:ad:95:9b:cd:37:52:6c:b6:4b:
         da:24:5b:66:15:81:a6:15:75:e1:dc:6a:be:09:12:d4:60:f0:
         47:f7:63:9b:41:7b:22:d3:c2:aa:a4:d5:19:66:60:eb:2c:f0:
         51:29:13:a9:df:ff:b8:0b:c6:89:18:94:db:ee:8e:b8:0f:b9:
         8e:d8:eb:83:90:7e:c2:bd:2f:24:72:58:2e:70:f3:3e:17:6f:
```

Task 15:

For the configuration of ServerA

Ipsec.conf file
conn serverA-to-serverB
auto=route
authby=psk
type=transport
keyexchange=ikev2
left=192.168.70.5
right=192.168.70.6

ipsec.secrets file:

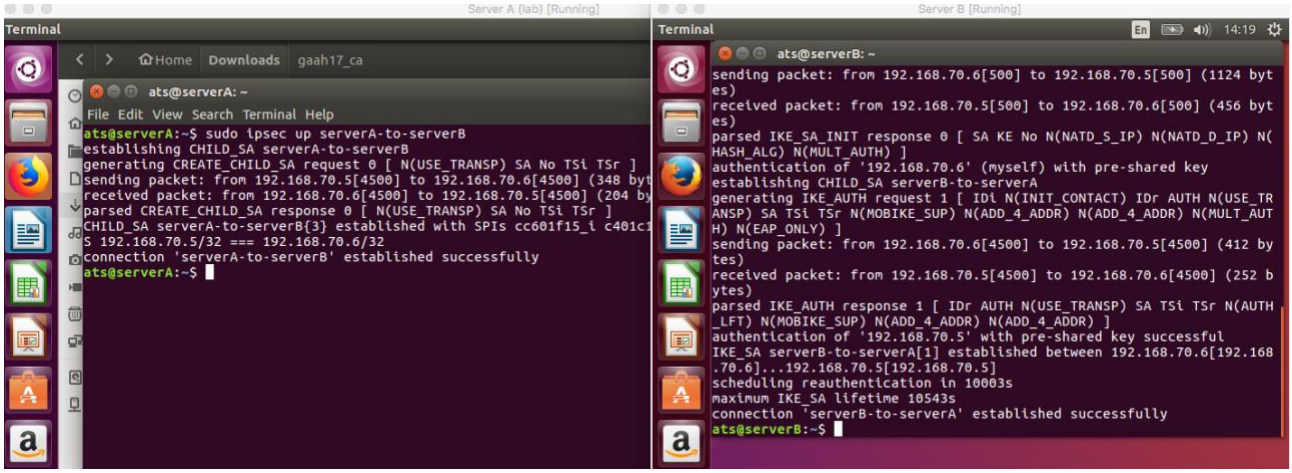
192.168.70.5 192.168.70.6 : PSK "atslabb00"

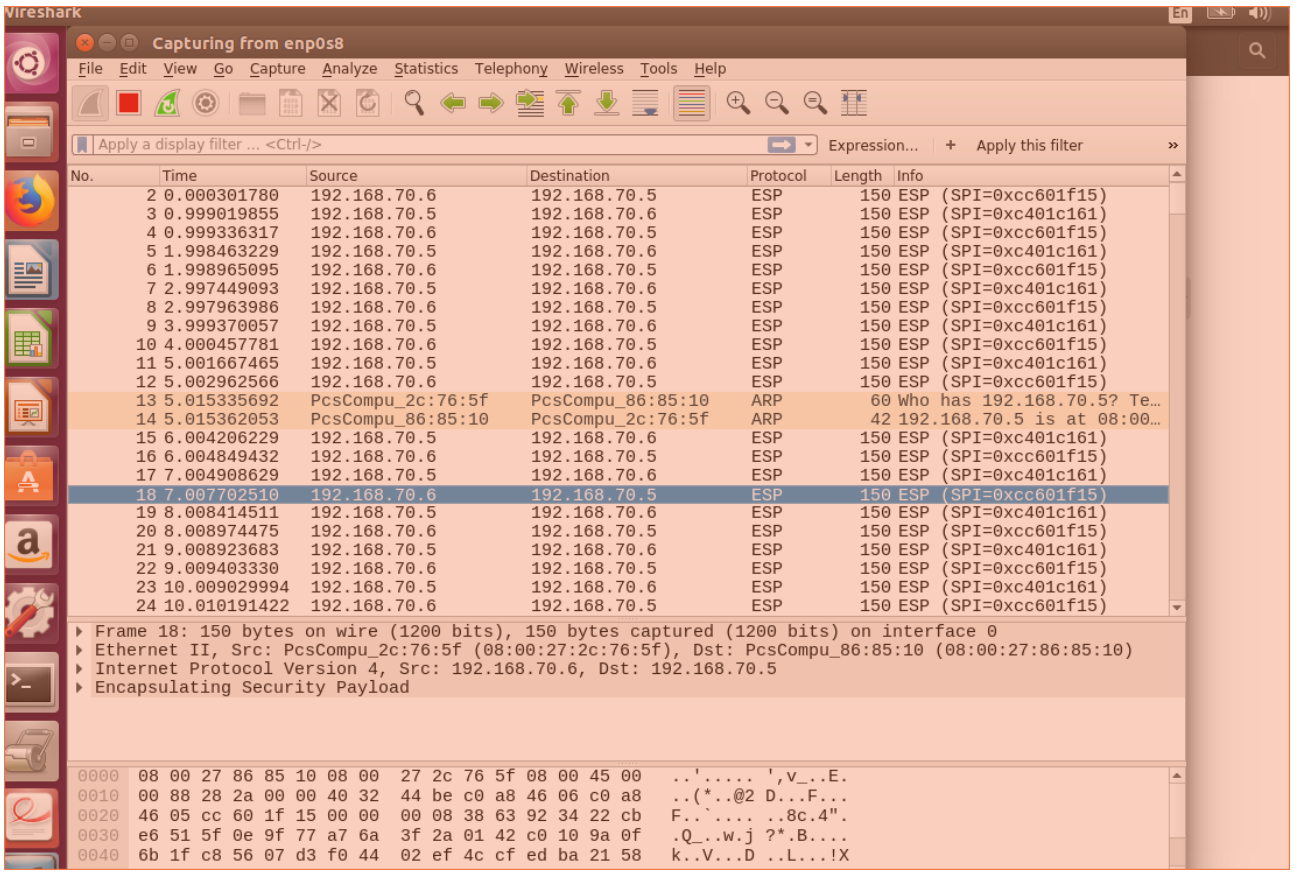
For the configuration of ServerB

Ipsec.conf file
conn serverA-to-serverB
auto=route
authby=psk
type=transport
keyexchange=ikev2
left=192.168.70.6
right=192.168.70.5

ipsec.secrets file:

192.168.70.6 192.168.70.5 : PSK "atslabb00"





Task 16

ats@serverA:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-116-generic, x86_64):
  uptime: 8 minutes, since May 26 14:46:12 2018
  malloc: sbrk 1486848, mmap 0, used 347472, free 1139376
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB: 192.168.70.5...192.168.70.6 IKEv2
serverA-to-serverB: local: [192.168.70.5] uses pre-shared key authentication
serverA-to-serverB: remote: [192.168.70.6] uses pre-shared key authentication
serverA-to-serverB: child: dynamic === dynamic TRANSPORT
Routed Connections:
serverA-to-serverB{1}: ROUTED, TRANSPORT, reqid 1
serverA-to-serverB{1}:   192.168.70.5/32 === 192.168.70.6/32
Security Associations (1 up, 0 connecting):
serverA-to-serverB[1]: ESTABLISHED 6 minutes ago, 192.168.70.5[192.168.70.5]...192.168.70.6[192.168.70.6]
serverA-to-serverB[1]: IKEv2 SPIs: 0fc3216958817afe_i* 75a48bc46319bde9_r, pre-shared key reauthentication in 2 hours

serverA-to-serverB[1]: IKE proposal:
AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
serverA-to-serverB{2}: INSTALLED, TRANSPORT, reqid 1, ESP SPIs: cc8147eb_i c97c1e8b_o
serverA-to-serverB{2}: AES_CBC_128/HMAC_SHA1_96, 3520 bytes_i (55 pkts, 62s ago), 3520 bytes_o (55 pkts, 62s ago), rekeying in 36 minutes
serverA-to-serverB{2}:   192.168.70.5/32 === 192.168.70.6/32
ats@serverA:~$

```
ts@serverA:~$ sudo ipsec statusall
tatus of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-116-generic, x86_64):
 uptime: 2 minutes, since May 26 14:46:12 2018
 malloc: sbrk 1486848, mmap 0, used 347456, free 1139392
 worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
 loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs
ey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
istening IP addresses:
 192.168.60.100
 192.168.70.5
 10.0.98.100
onnections:
erverA-to-serverB:  192.168.70.5...192.168.70.6  IKEv2
erverA-to-serverB:   local:  [192.168.70.5] uses pre-shared key authentication
erverA-to-serverB:   remote: [192.168.70.6] uses pre-shared key authentication
erverA-to-serverB:   child:  dynamic === dynamic TRANSPORT
outed Connections:
erverA-to-serverB{1}:  ROUTED, TRANSPORT, reqid 1
erverA-to-serverB{1}:   192.168.70.5/32 === 192.168.70.6/32
ecurity Associations (1 up, 0 connecting):
erverA-to-serverB[1]: ESTABLISHED 22 seconds ago, 192.168.70.5[192.168.70.5]...192.168.70.6[192.168.70.6]
erverA-to-serverB[1]: IKEv2 SPIs: 0fc3216958817afe_i* 75a48bc46319bde9_r, pre-shared key reauthentication in 2 hours
erverA-to-serverB[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
erverA-to-serverB{2}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: cc8147eb_i c97c1e8b_o
erverA-to-serverB{2}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 43 minutes
erverA-to-serverB{2}:   192.168.70.5/32 === 192.168.70.6/32
ts@serverA:~$
```

```
ts@serverA:~$ sudo ip xfrm state
[sudo] password for ats:
rc 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc97c1e8b reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x06c488ec683ae0775bf344f6f1630fbf8c5cd1ad 96
        enc cbc(aes) 0x905fc959a892d56fcbb65c2a427900e5
        anti-replay context: seq 0x0, oseq 0x37, bitmap 0x00000000
        sel src 192.168.70.5/32 dst 192.168.70.6/32
rc 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xcc8147eb reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0xaf86692b05eb546009b141864952920c4f9b38de 96
        enc cbc(aes) 0x0bf3fa73664bcd46f203723c875aa7c0
        anti-replay context: seq 0x37, oseq 0x0, bitmap 0xffffffff
        sel src 192.168.70.6/32 dst 192.168.70.5/32
ts@serverA:~$
```

Task 17: List the entries in the SPD
sudo ip xfrm policy

```
ts@serverA:~$ sudo ip xfrm policy
[sudo] password for ats:
rc 192.168.70.6/32 dst 192.168.70.5/32
        dir in priority 2819
        tmpl src 0.0.0.0 dst 0.0.0.0
                proto esp reqid 1 mode transport
rc 192.168.70.5/32 dst 192.168.70.6/32
        dir out priority 2819
        tmpl src 0.0.0.0 dst 0.0.0.0
                proto esp reqid 1 mode transport
rc 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
rc 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0
rc 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
rc 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0
rc ::/0 dst ::/0
        socket in priority 0
rc ::/0 dst ::/0
        socket out priority 0
rc ::/0 dst ::/0
        socket in priority 0
rc ::/0 dst ::/0
        socket out priority 0
ts@serverA:~$
```

in
It requires to allow traffic among hosts using VPN gateway in tunnel mode.

tmpl
The tmpl keyword defines the beginning of a template that specify how IPsec should encapsulate matching packets.

reqid
It connects an entry in the SPD with the corresponding entry in the SAD. By comparing this output to the output of the ip xfrm state command, here the same reqid value appears together with the same IP address pair.
transport
Transport is the type of tunnel mode. IPSec Transport mode is used for host-to-host communications.

The specific purpose of the other entries in the SPD is to save the policy in the database.

Task 18 :

Ipsec.conf file for server A:

```
config setup

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        mobike=no
        keyexchange=ikev2

conn serverA-to-serverB-transport
        left=192.168.70.5
        leftcert=192.168.70.5.cert.pem
        leftid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
        leftfirewall=yes
        right=192.168.70.6
        rightid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
        type=transport
        auto=route
        authby=rsa
```

Ipsec.secrets file for server A:

```
: RSA 192.168.70.5.key.pem
```

Ipsec.conf file for server B:

```
config setup

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        mobike=no
        keyexchange=ikev2

conn serverA-to-serverB-transport
        left=192.168.70.6
        leftcert=192.168.70.6.cert.pem
        leftid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
        leftfirewall=yes
        right=192.168.70.5
        rightid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
        type=transport
        auto=route
        authby=rsa
```

Ipsec.secrets file for server A:

```
: RSA 192.168.70.6.key.pem
```

```
ats@serverA:~/sahb16_ca$ openssl genrsa -out ca1/private/192.168.70.5.key.pem 2048
Generating RSA private key, 2048 bit long modulus
.............+++
.......+++
e is 65537 (0x10001)
```

Creating Server A certificate

```
ats@serverA:~/sahb16_ca$ openssl genrsa -out ca1/private/192.168.70.5.key.pem 2048
Generating RSA private key, 2048 bit long modulus
.................+++
.........................................+++
e is 65537 (0x10001)
```

```
ats@serverA:~/sahb16_ca$ clear
ats@serverA:~/sahb16_ca$ openssl req -config ca1/openssl.cnf -new -key
ca1/private/192.168.70.5.key.pem -out ca1/csr/192.168.70.5.csr.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) [SE]:
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [ET2540]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.70.5
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
ats@serverA:~/sahb16_ca$ openssl req -noout -text -in ca1/csr/192.168.70.5.csr.pem
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:d0:55:10:0c:b9:c1:53:c4:21:da:19:b3:14:
                    bf:98:f0:e0:2f:e9:1f:6e:db:2c:e8:67:d1:1f:4c:
                    a3:bf:bf:57:8e:cb:f6:17:8f:58:bb:94:01:96:d4:
                    94:06:6a:77:a3:47:f5:8d:e6:0a:fb:e6:b4:27:4e:
                    5b:b4:62:1d:83:97:d2:30:6d:30:88:a1:6f:0c:4d:
                    a7:09:f7:94:eb:19:74:87:13:3b:36:55:59:77:ed:
                    b2:e5:c0:48:3a:6e:e9:28:09:b3:62:77:9c:8f:e7:
                    23:3a:27:1a:ba:f1:4b:ed:48:e8:bd:fa:23:a7:6d:
                    ad:1b:4d:d1:54:83:b2:b0:8a:2b:95:48:bc:04:b2:
                    16:9e:a9:04:5d:a2:48:97:97:e3:9b:22:15:d0:08:
                    5d:26:20:b5:dd:f8:e8:43:1e:b7:a3:4c:bb:5c:67:
                    83:27:94:6c:20:c0:e6:7c:fa:1e:41:f8:7d:38:34:
                    63:ab:1f:1c:b1:c5:fd:c4:62:cd:a7:8f:87:e5:b5:
                    14:77:b3:55:8c:52:d6:5f:02:17:70:7a:33:42:d7:
                    eb:a3:1e:90:30:54:bf:de:2e:ff:80:25:f7:79:12:
                    79:c6:6f:c5:38:bf:a4:1c:e3:43:0d:44:fe:91:dc:
                    fb:5d:e8:3b:a0:a7:73:8d:bb:42:e9:7f:37:e5:cd:
                    4a:25
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         75:2c:00:50:73:8b:32:10:9f:4a:0f:38:07:e5:86:03:35:99:
         96:b4:1f:9c:7e:40:6a:cc:92:bf:38:cc:bd:5a:7d:d5:99:b1:
         45:72:78:6f:4c:c6:3d:7c:42:46:f4:8c:02:fe:18:32:2e:27:
```

```
        7b:81:a3:eb:25:50:01:ea:2c:23:ca:40:92:cd:4a:66:e9:2a:
        de:04:49:66:b1:9c:35:59:28:ab:4f:a2:6e:e3:4c:21:4f:a4:
        4e:95:a4:46:89:6c:58:62:a0:78:90:1c:81:6b:db:82:20:47:
        2b:89:36:4c:1e:78:2f:3c:e0:7d:d0:72:b4:39:91:01:50:fd:
        42:ff:e7:0f:f7:01:86:82:c0:95:f3:94:e4:7a:c8:13:9e:0d:
        1e:19:81:f9:bb:8e:2f:f4:16:c9:3f:66:af:c4:e2:5b:a3:67:
        87:31:9d:6d:c4:c4:8a:60:f8:ad:36:b9:d4:89:e7:ec:6b:e3:
        a0:ae:8f:8c:7e:16:ae:0e:45:fe:1e:f8:a0:98:b3:e1:f1:ce:
        c2:86:ef:c8:6a:c9:86:14:1f:12:3b:c6:6f:5e:14:c4:b8:4c:
        10:f9:00:72:74:33:42:2a:b9:68:fd:8b:1a:a7:34:82:a0:b4:
        7c:4b:4e:6a:84:5c:d2:d1:76:1f:f3:a9:a1:1b:94:61:c8:d8:
        b4:d9:02:2c
ats@serverA:~/sahb16_ca$

ats@serverA:~/sahb16_ca$ openssl ca -config ca1/openssl.cnf -extensions server_cert -days 3650 -
notext -in ca1/csr/192.168.70.5.csr.pem -out ca1/certs/192.168.70.5.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/ca1/private/ca1.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8192 (0x2000)
        Validity
            Not Before: May 26 14:17:51 2018 GMT
            Not After : May 23 14:17:51 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            localityName              = Karlskrona
            organizationName          = ET2540
            commonName                = 192.168.70.5
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                38:F2:17:AA:8E:6A:CC:D1:B8:21:3D:93:88:A0:08:5E:37:BC:A5:E1
            X509v3 Authority Key Identifier:
                keyid:C7:C8:67:63:C1:21:73:CC:9E:F7:1D:8C:71:F4:B9:4F:BE:2F:73:5F
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
                serial:20:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:https://localhost/ca1.crl.pem

Certificate is to be certified until May 23 14:17:51 2028 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
Data Base Updated
ats@serverA:~/sahb16_ca$ openssl x509 -noout -text -in ca1/certs/192.168.70.5.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8192 (0x2000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca
        Validity
            Not Before: May 26 14:17:51 2018 GMT
            Not After : May 23 14:17:51 2028 GMT
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:d0:55:10:0c:b9:c1:53:c4:21:da:19:b3:14:
                    bf:98:f0:e0:2f:e9:1f:6e:db:2c:e8:67:d1:1f:4c:
                    a3:bf:bf:57:8e:cb:f6:17:8f:58:bb:94:01:96:d4:
                    94:06:6a:77:a3:47:f5:8d:e6:0a:fb:e6:b4:27:4e:
                    5b:b4:62:1d:83:97:d2:30:6d:30:88:a1:6f:0c:4d:
                    a7:09:f7:94:eb:19:74:87:13:3b:36:55:59:77:ed:
                    b2:e5:c0:48:3a:6e:e9:28:09:b3:62:77:9c:8f:e7:
                    23:3a:27:1a:ba:f1:4b:ed:48:e8:bd:fa:23:a7:6d:
                    ad:1b:4d:d1:54:83:b2:b0:8a:2b:95:48:bc:04:b2:
                    16:9e:a9:04:5d:a2:48:97:97:e3:9b:22:15:d0:08:
                    5d:26:20:b5:dd:f8:e8:43:1e:b7:a3:4c:bb:5c:67:
                    83:27:94:6c:20:c0:e6:7c:fa:1e:41:f8:7d:38:34:
                    63:ab:1f:1c:b1:c5:fd:c4:62:cd:a7:8f:87:e5:b5:
                    14:77:b3:55:8c:52:d6:5f:02:17:70:7a:33:42:d7:
                    eb:a3:1e:90:30:54:bf:de:2e:ff:80:25:f7:79:12:
                    79:c6:6f:c5:38:bf:a4:1c:e3:43:0d:44:fe:91:dc:
                    fb:5d:e8:3b:a0:a7:73:8d:bb:42:e9:7f:37:e5:cd:
                    4a:25
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                38:F2:17:AA:8E:6A:CC:D1:B8:21:3D:93:88:A0:08:5E:37:BC:A5:E1
            X509v3 Authority Key Identifier:
                keyid:C7:C8:67:63:C1:21:73:CC:9E:F7:1D:8C:71:F4:B9:4F:BE:2F:73:5F
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
                serial:20:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
```

```
            TLS Web Server Authentication
        X509v3 CRL Distribution Points:

            Full Name:
              URI:https://localhost/ca1.crl.pem

    Signature Algorithm: sha256WithRSAEncryption
         42:b4:29:eb:b5:81:09:0f:0e:2c:a3:0b:2c:e9:aa:c9:6d:be:
         49:4d:f3:4f:99:5f:d2:2f:4b:f6:58:4b:65:e1:6d:50:da:02:
         8f:b6:72:48:03:6d:23:72:b9:e8:af:2a:83:29:b4:ba:d3:60:
         54:33:f0:d7:65:d7:b3:e5:7c:63:d7:4a:c8:8f:b3:51:5e:60:
         f7:74:01:5b:0b:78:49:a2:49:7e:3f:0b:e7:93:cd:de:1f:c8:
         43:79:43:8e:cc:76:1b:ad:fe:b0:f9:d8:6a:1a:9d:6a:f1:8e:
         16:89:b0:51:b0:5e:a1:ac:30:a4:74:96:08:e4:ac:a1:74:f8:
         67:79:95:65:09:83:5d:7d:6d:b7:d2:bc:dd:40:0c:cd:57:8f:
         65:47:f1:07:cc:9b:d4:3e:d4:f8:3c:2e:d6:06:39:89:a4:83:
         c8:eb:b4:66:5e:1b:d0:2e:08:bb:d8:a2:51:57:00:79:e0:de:
         9c:57:c1:2c:0a:e0:07:1d:2a:24:ee:4f:b3:06:87:33:97:3d:
         fc:24:46:d1:2f:be:ec:68:ec:0d:6e:58:16:26:f0:3d:58:1f:
         7c:30:50:3c:80:46:1a:aa:88:83:1e:cf:71:41:67:b0:b3:3f:
         f1:a2:53:b9:d7:9a:b8:08:d5:e2:b4:17:0e:f6:38:2c:f2:0b:
         cd:f8:a8:76:f9:42:1f:86:63:5f:97:98:fc:62:17:b6:19:5c:
         51:f3:12:a1:2a:f6:8e:fc:a6:bf:26:49:27:98:b2:a0:f4:a5:
         e1:d2:d6:6c:2a:5e:8a:12:8c:1e:8e:fb:b8:30:a8:a5:8f:51:
         85:59:c9:c8:92:94:0c:b7:ef:3f:3b:d8:bc:11:34:dc:98:97:
         c8:39:96:50:73:a8:70:7a:f3:29:b1:db:d1:26:e8:80:96:a6:
         ab:01:c7:cb:c2:96:d8:89:be:fb:0e:c2:78:b9:ba:a7:52:81:
         77:1d:be:5d:44:63:dc:28:82:a4:d1:63:2c:d2:ab:d3:67:d7:
         53:cb:d1:57:0f:65:41:0c:55:ea:15:a3:40:5b:0c:af:a7:bb:
         64:11:e5:f7:4b:76:6f:75:37:bd:8e:50:d7:4e:ea:07:85:32:
         95:26:cf:63:9b:dc:55:f6:e8:91:2e:7f:60:36:73:c4:2e:ce:
         aa:12:81:20:fe:64:74:78:2d:f2:83:de:1f:15:c9:33:cd:9b:
         98:5c:81:2c:93:98:c3:7e:49:ca:ec:7f:af:0d:d7:30:56:e0:
         48:eb:66:64:eb:d8:a1:91:de:86:f0:31:c7:44:4f:ab:3c:dd:
         40:0f:e2:22:86:26:90:25:20:06:66:30:8f:90:bb:eb:01:4e:
         92:4c:b1:15:df:5f:0f:2d
ats@serverA:~/sahb16_ca$ openssl verify -CA
-CAfile  -CApath
ats@serverA:~/sahb16_ca$ openssl verify -CAfile ca1/certs/ca1.cert-chain.pem
^C
ats@serverA:~/sahb16_ca$ openssl verify -CAfile ca1/certs/ca1.cert-chain.pem
ca1/certs/192.168.70.5.cert.pem
```

Server B certificate

```
ats@serverA:~/sahb16_ca$  openssl genrsa -out ca1/private/192.168.70.6.key.pem 2048
Generating RSA private key, 2048 bit long modulus
```

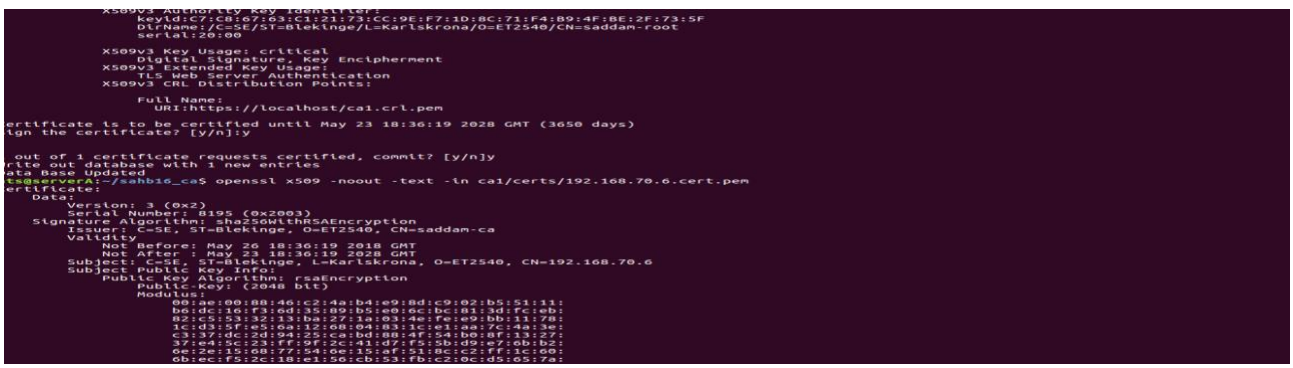
```
.....................................................+++
.....................+++
e is 65537 (0x10001)
ats@serverA:~/sahb16_ca$  openssl req -config ca1/openssl.cnf -new -key
ca1/private/192.168.70.6.key.pem -out ca1/csr/192.168.70.6.csr.pem
You are about to be asked to enter information that will 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) [SE]:
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [ET2540]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.70.6
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

ats@serverA:~/sahb16_ca$ openssl req -noout -text -in ca1/csr/192.168.70.6.csr.pem
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:86:8f:08:16:4d:d5:0c:cd:b6:aa:16:f9:94:
                    04:c4:6f:0a:da:2f:33:d3:55:03:0a:b3:10:a8:9e:
                    77:a3:1c:d4:19:fc:e4:47:a8:8b:6d:45:d7:ab:93:
                    ac:85:11:84:91:fd:62:25:f8:c9:a2:45:25:f0:93:
                    6f:57:c0:a3:ea:d3:c0:e1:3e:e3:3f:81:ed:1d:ad:
                    fd:38:04:6b:e6:1f:98:72:66:29:11:f8:2b:0c:57:
                    8e:93:ee:a7:6b:7d:3a:fd:04:4c:8d:6e:e0:31:39:
                    3c:de:94:84:b0:bc:bc:da:4f:f4:89:2b:7f:63:1d:
                    26:08:8e:b6:e0:46:84:cb:f8:b2:1d:37:d7:dd:24:
                    b1:0e:91:75:90:63:59:68:0b:dd:5b:a9:10:16:5e:
                    5c:44:bc:5e:ca:2b:61:7d:08:b8:71:49:97:47:9f:
                    54:da:79:af:7d:a2:91:01:cf:bc:cb:9d:9e:de:b5:
                    91:69:6f:ac:0f:45:5c:a1:32:7d:56:5c:c1:43:48:
                    e6:56:85:49:7d:0e:67:54:92:af:40:ac:e4:67:6d:
                    3a:60:b1:d6:42:bb:11:94:1a:a2:58:7e:23:33:f5:
                    24:bc:1e:ba:41:3a:43:5d:ea:5c:7b:53:74:c0:af:
                    b2:eb:96:dd:dd:cf:9a:8d:05:94:43:97:8e:80:3f:
                    1d:bd
```

```
            Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         39:d5:64:93:1c:b7:ef:5a:0b:00:0e:e7:0a:83:3b:a0:ab:d9:
         cc:a4:8e:58:ae:18:bf:34:2b:9c:05:ec:1d:3e:0c:4c:3a:37:
         5b:b3:3f:17:91:01:f7:06:af:57:50:cc:fc:ae:56:83:7a:e8:
         27:9f:e2:1c:10:ef:63:a9:9b:98:f0:f5:a8:9b:44:d2:15:77:
         a7:81:8a:7e:d6:83:58:39:77:26:30:4e:7c:f0:5c:9d:ac:c3:
         42:2a:64:20:8f:c7:36:60:08:3f:71:7b:0a:e5:49:ea:e1:7a:
         cf:81:c6:24:fd:41:5a:a5:8c:fa:42:c3:83:e7:29:ba:b4:90:
         4b:6f:b0:69:bf:97:4a:f3:7f:74:ae:44:e5:72:f5:f7:90:09:
         70:97:23:44:83:25:63:2d:bb:e0:01:da:2d:e8:e9:d4:bb:be:
         83:6d:b5:87:a1:e4:92:b4:c3:a8:5c:15:54:de:a6:48:e2:a2:
         be:7b:1f:91:bb:fd:84:d8:73:28:c1:52:7a:18:88:84:0f:f1:
         14:29:52:2c:98:59:8f:96:8f:c8:44:cc:d2:94:9a:fa:ef:21:
         00:0e:08:9e:80:0b:ac:f7:2c:bf:ca:3c:7d:0d:46:a3:54:61:
         95:60:0d:19:0f:f4:83:41:99:5c:7d:7f:ce:53:b0:41:22:43:
         ec:e7:ff:92
ats@serverA:~/sahb16_ca$ openssl ca -config ca1/openssl.cnf -extensions server_cert -days 3650 -
notext -in ca1/csr/192.168.70.6.csr.pem -out ca1/certs/192.168.70.6.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/ats/sahb16_ca/ca1/private/ca1.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8193 (0x2001)
        Validity
            Not Before: May 26 14:53:38 2018 GMT
            Not After : May 23 14:53:38 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            localityName              = Karlskrona
            organizationName          = ET2540
            commonName                = 192.168.70.6
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                3E:75:57:14:AB:10:27:34:8B:38:A9:01:37:3E:F4:ED:39:8F:02:C7
            X509v3 Authority Key Identifier:
                keyid:C7:C8:67:63:C1:21:73:CC:9E:F7:1D:8C:71:F4:B9:4F:BE:2F:73:5F
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
                serial:20:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 CRL Distribution Points:
```

```
            Full Name:
              URI:https://localhost/ca1.crl.pem

Certificate is to be certified until May 23 14:53:38 2028 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
Data Base Updated
ats@serverA:~/sahb16_ca$  openssl x509 -noout -text -in ca1/certs/192.168.70.6.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8193 (0x2001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca
        Validity
            Not Before: May 26 14:53:38 2018 GMT
            Not After : May 23 14:53:38 2028 GMT
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:86:8f:08:16:4d:d5:0c:cd:b6:aa:16:f9:94:
                    04:c4:6f:0a:da:2f:33:d3:55:03:0a:b3:10:a8:9e:
                    77:a3:1c:d4:19:fc:e4:47:a8:8b:6d:45:d7:ab:93:
                    ac:85:11:84:91:fd:62:25:f8:c9:a2:45:25:f0:93:
                    6f:57:c0:a3:ea:d3:c0:e1:3e:e3:3f:81:ed:1d:ad:
                    fd:38:04:6b:e6:1f:98:72:66:29:11:f8:2b:0c:57:
                    8e:93:ee:a7:6b:7d:3a:fd:04:4c:8d:6e:e0:31:39:
                    3c:de:94:84:b0:bc:bc:da:4f:f4:89:2b:7f:63:1d:
                    26:08:8e:b6:e0:46:84:cb:f8:b2:1d:37:d7:dd:24:
                    b1:0e:91:75:90:63:59:68:0b:dd:5b:a9:10:16:5e:
                    5c:44:bc:5e:ca:2b:61:7d:08:b8:71:49:97:47:9f:
                    54:da:79:af:7d:a2:91:01:cf:bc:cb:9d:9e:de:b5:
                    91:69:6f:ac:0f:45:5c:a1:32:7d:56:5c:c1:43:48:
                    e6:56:85:49:7d:0e:67:54:92:af:40:ac:e4:67:6d:
                    3a:60:b1:d6:42:bb:11:94:1a:a2:58:7e:23:33:f5:
                    24:bc:1e:ba:41:3a:43:5d:ea:5c:7b:53:74:c0:af:
                    b2:eb:96:dd:dd:cf:9a:8d:05:94:43:97:8e:80:3f:
                    1d:bd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                3E:75:57:14:AB:10:27:34:8B:38:A9:01:37:3E:F4:ED:39:8F:02:C7
            X509v3 Authority Key Identifier:
                keyid:C7:C8:67:63:C1:21:73:CC:9E:F7:1D:8C:71:F4:B9:4F:BE:2F:73:5F
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=saddam-root
                serial:20:00
            X509v3 Key Usage: critical
```

Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 CRL Distribution Points:
Full Name:
URI:https://localhost/ca1.crl.pem

Signature Algorithm: sha256WithRSAEncryption
28:c2:15:92:29:0a:18:fa:4f:d9:23:d3:8e:40:f1:04:6b:86:
e5:6e:f9:1a:89:44:4d:b6:fc:28:13:0e:eb:7c:98:18:0c:98:
1b:fd:59:f1:aa:08:c9:ee:c2:9c:95:c3:f5:d3:f1:d6:ab:87:
8d:bc:d7:a1:8f:8d:78:65:e1:6d:44:07:d6:67:97:29:62:63:
4c:15:75:11:df:92:eb:ab:1c:c7:a9:f1:00:45:7c:82:11:49:
21:88:c0:c4:43:13:f7:ad:ed:2e:39:18:02:6b:c7:57:83:91:
5a:ee:70:2c:ae:7c:c4:d3:e2:91:3e:13:17:67:f7:ac:b3:1e:
31:34:cd:91:ae:7f:59:f1:f0:7b:5e:3e:04:96:0c:fb:cd:58:
b3:ae:ec:8c:86:ad:81:38:f6:97:25:43:29:5b:d5:15:8e:9d:
08:dd:00:4e:8d:36:32:15:08:24:8a:14:21:dd:23:e6:c5:50:
b2:56:93:d4:37:00:c1:00:23:8a:f7:66:ea:6e:82:f7:62:10:
60:2f:b9:dd:d6:32:56:9e:3d:05:33:09:8d:f7:e2:3d:ef:bd:
4b:13:c0:a9:e8:6a:66:17:77:31:90:e0:40:6e:b6:a5:5c:0e:
6a:2b:71:82:f0:d4:a9:ee:d7:9d:c6:b3:6a:c0:ad:cd:1a:44:
64:c2:d8:94:4a:8f:d2:f1:9e:af:88:64:48:34:12:2c:78:75:
0c:67:7d:ef:f5:63:b3:a5:9d:16:74:a0:9c:02:ea:34:b1:bc:
52:2a:10:ee:4d:a4:e4:bc:d0:1e:9f:39:4f:d8:60:04:f9:28:
45:95:84:2f:4a:a1:fa:8f:83:df:64:53:5d:cd:f1:21:48:33:
81:e8:e0:6c:45:8d:0d:eb:15:1c:7c:02:f7:13:c2:c7:72:1f:
95:d1:4b:bf:7c:28:7e:25:57:de:f1:e4:40:5a:fe:6f:69:7c:
22:b1:57:08:d2:08:3a:81:a3:26:8d:44:e7:c1:2d:b7:07:35:
46:ca:7f:26:db:51:71:8a:35:82:34:e4:f3:e5:5c:de:42:d3:
0e:b6:a8:cb:df:fb:36:12:4c:f5:9b:ea:f5:42:49:7c:fc:ec:
08:f7:bf:06:e8:32:53:c4:cf:50:7a:87:14:67:a9:1b:90:eb:
50:8d:50:a4:96:0d:ca:23:ef:14:b6:d4:d9:2f:2e:b4:79:6a:
ab:7d:27:5e:82:57:64:52:bb:e0:11:dd:d6:ba:8a:c1:12:e1:
34:cd:52:b2:f9:ee:11:d5:d8:7a:f7:a8:92:86:5d:90:3b:28:
90:c7:53:ab:31:d7:bb:e5:f0:97:b2:22:a7:17:c2:e3:dc:7c:
f5:54:40:d7:8d:fe:68:7f
ats@serverA:~/sahb16_ca$ openssl verify -CAfile ca1/certs/ca1.cert-chain.pem
ca1/certs/192.168.70.6.cert.pem
ca1/certs/192.168.70.6.cert.pem: OK
ats@serverA:~/sahb16_ca$

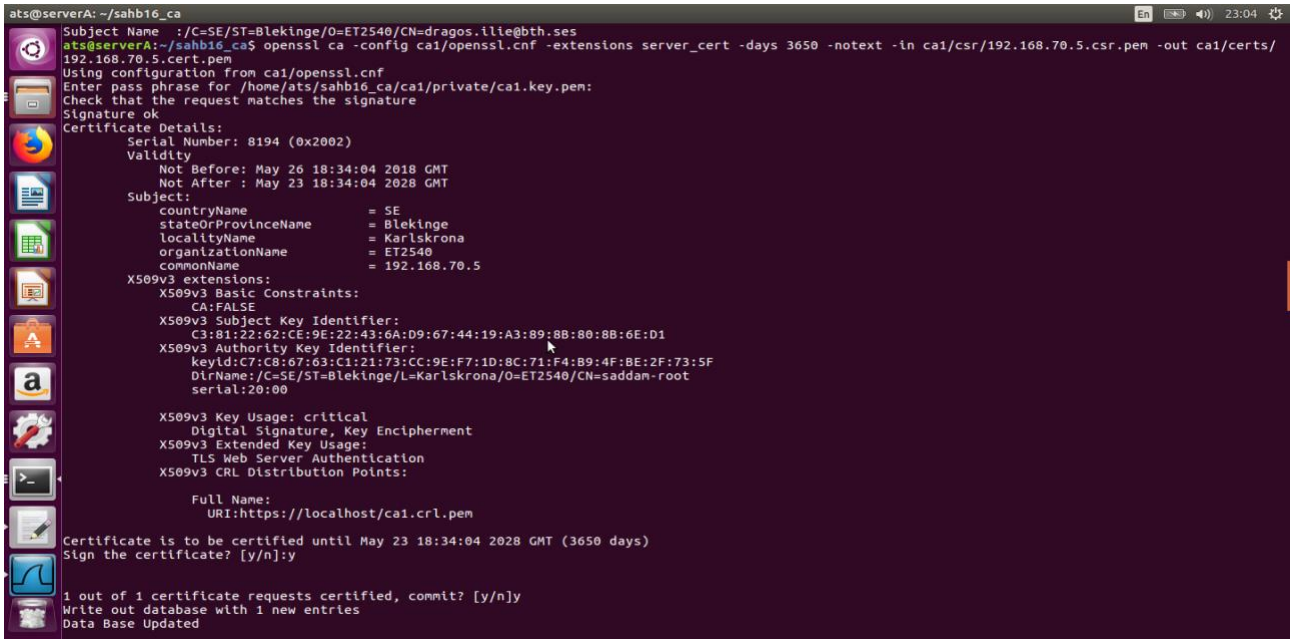


ipsec tunnel up:

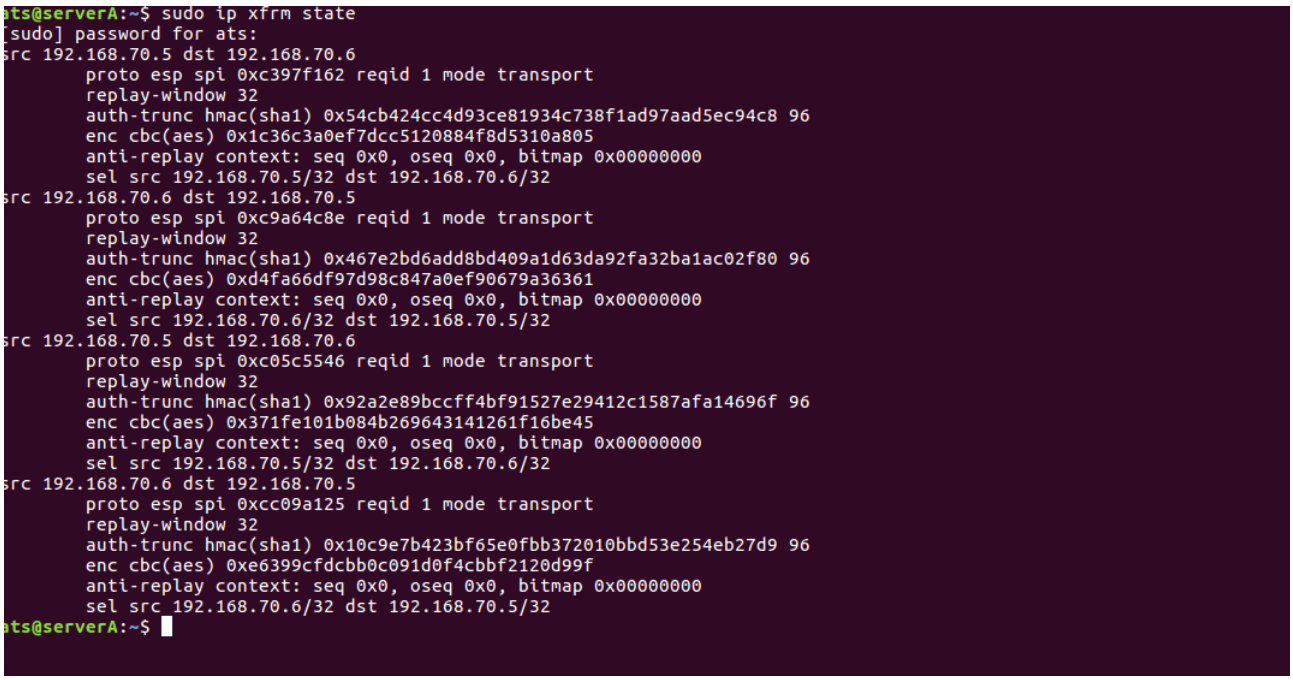
```
ats@serverA:~$ sudo ipsec up serverA-to-serverB-transport
initiating IKE_SA serverA-to-serverB-transport[1] to 192.168.70.6
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(HASH_ALG) ]
sending packet: from 192.168.70.5[500] to 192.168.70.6[500] (1124 bytes)
received packet: from 192.168.70.6[500] to 192.168.70.5[500] (501 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(HASH_ALG) N(MULT_AUTH) ]
received cert request for "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
received cert request for "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
sending cert request for "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
sending cert request for "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
authentication of 'C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5' (myself) with RSA_EMSA_PKCS1_SHA256 successful
sending end entity cert "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
establishing CHILD_SA serverA-to-serverB-transport
generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH N(USE_TRANSP) SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) ]
sending packet: from 192.168.70.5[500] to 192.168.70.6[500] (2188 bytes)
received packet: from 192.168.70.6[500] to 192.168.70.5[500] (1900 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH N(USE_TRANSP) SA TSi TSr N(AUTH_LFT) ]
received end entity cert "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
  using certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
  using trusted intermediate ca certificate "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
checking certificate status of "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
  fetching crl from 'https://localhost/ca1.crl.pem' ...
unable to fetch from https://localhost/ca1.crl.pem, no capable fetcher found
crl fetching failed
certificate status is not available
  using trusted ca certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
checking certificate status of "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
certificate status is not available
  reached self-signed root ca with a path length of 1
authentication of 'C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6' with RSA_EMSA_PKCS1_SHA256 successful
IKE_SA serverA-to-serverB-transport[1] established between 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=SE
, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
scheduling reauthentication in 3371s
maximum IKE_SA lifetime 3551s
connection 'serverA-to-serverB-transport' established successfully
ats@serverA:~$
```

ipsec statusall

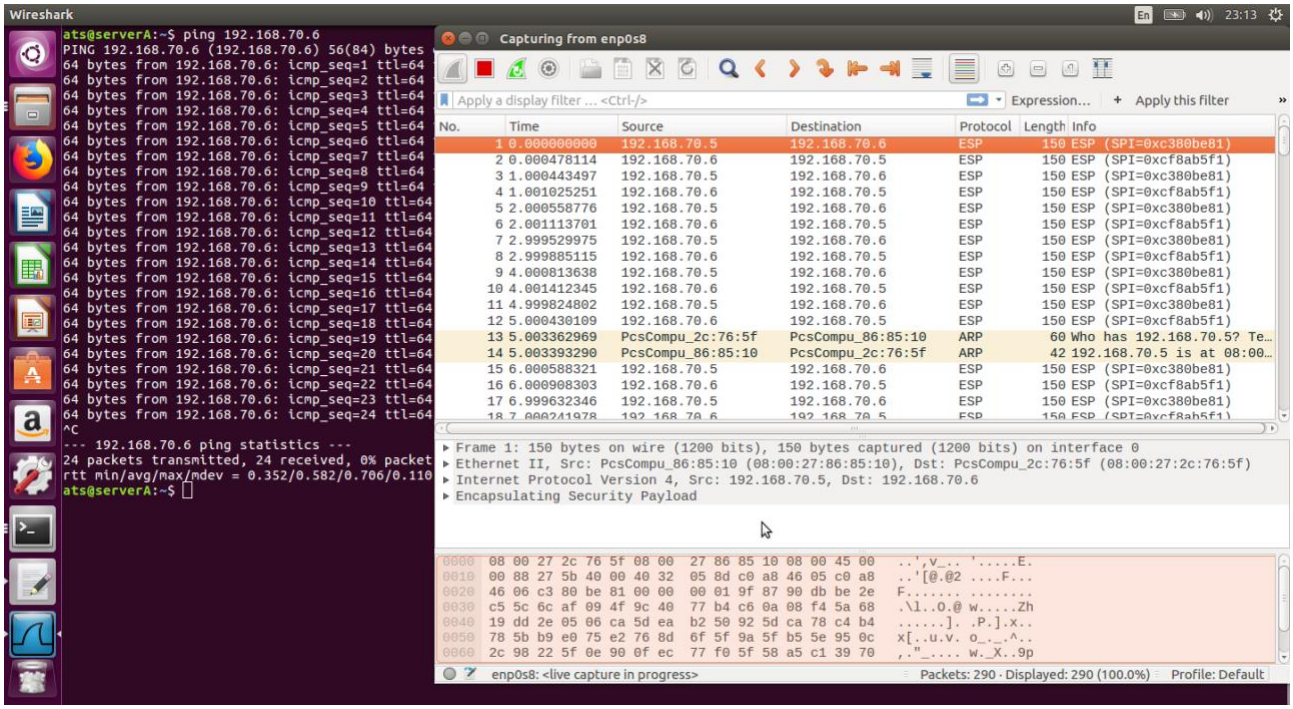
```
ats@serverA:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-116-generic, x86_64):
  uptime: 23 minutes, since May 26 21:02:22 2018
  malloc: sbrk 1466368, mmap 0, used 382128, free 1084240
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey ssh
key pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB-transport:  192.168.70.5...192.168.70.6  IKEv2
serverA-to-serverB-transport:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverA-to-serverB-transport:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
serverA-to-serverB-transport:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverA-to-serverB-transport:   child:  dynamic === dynamic TRANSPORT
Routed Connections:
serverA-to-serverB-transport{1}:  ROUTED, TRANSPORT, reqid 1
serverA-to-serverB-transport{1}:   192.168.70.5/32 === 192.168.70.6/32
Security Associations (1 up, 0 connecting):
serverA-to-serverB-transport[1]: ESTABLISHED 22 minutes ago, 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=
SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
serverA-to-serverB-transport[1]: IKEv2 SPIs: 8d5e813dae587c36_i* a62c887370ed6b4a_r, public key reauthentication in 29 minutes
serverA-to-serverB-transport[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
serverA-to-serverB-transport{4}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: cc09a125_i c05c5546_o
serverA-to-serverB-transport{4}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 6 minutes
serverA-to-serverB-transport{4}:   192.168.70.5/32 === 192.168.70.6/32
serverA-to-serverB-transport{5}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c9a64c8e_i c397f162_o
serverA-to-serverB-transport{5}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 8 minutes
serverA-to-serverB-transport{5}:   192.168.70.5/32 === 192.168.70.6/32
ats@serverA:~$
```



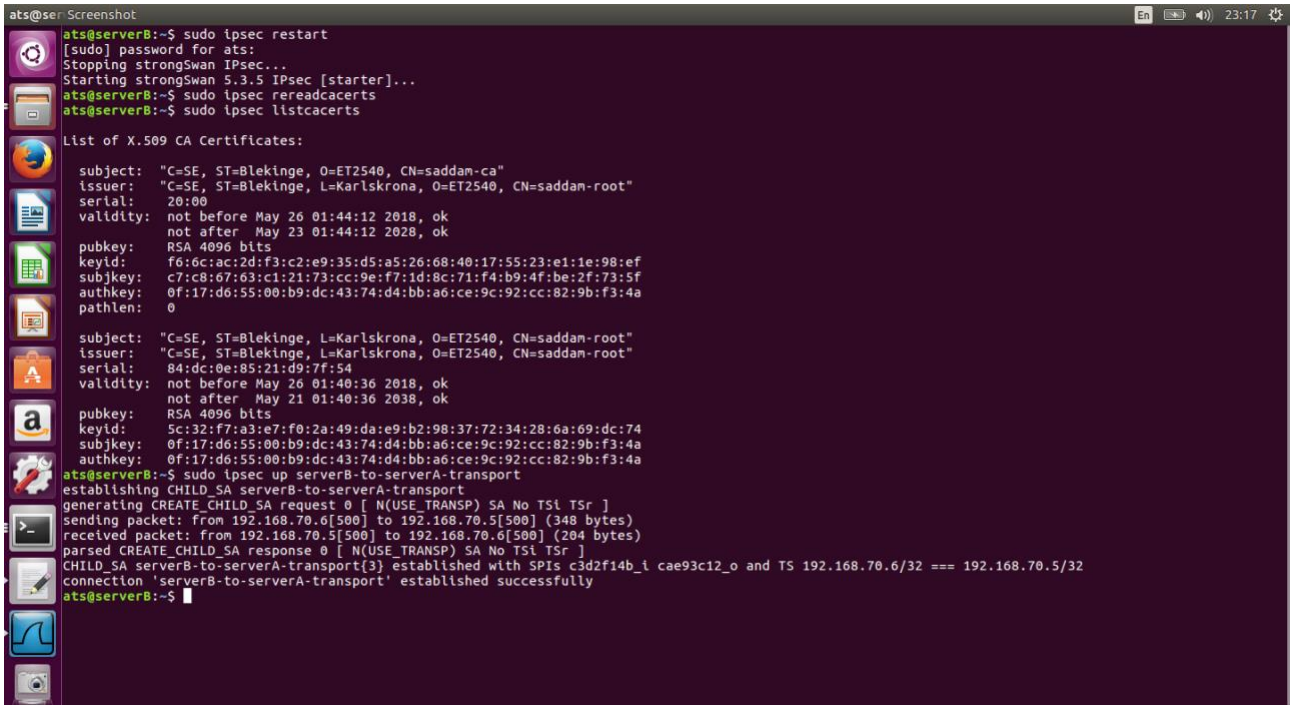
ip xfrm state



Wireshark output

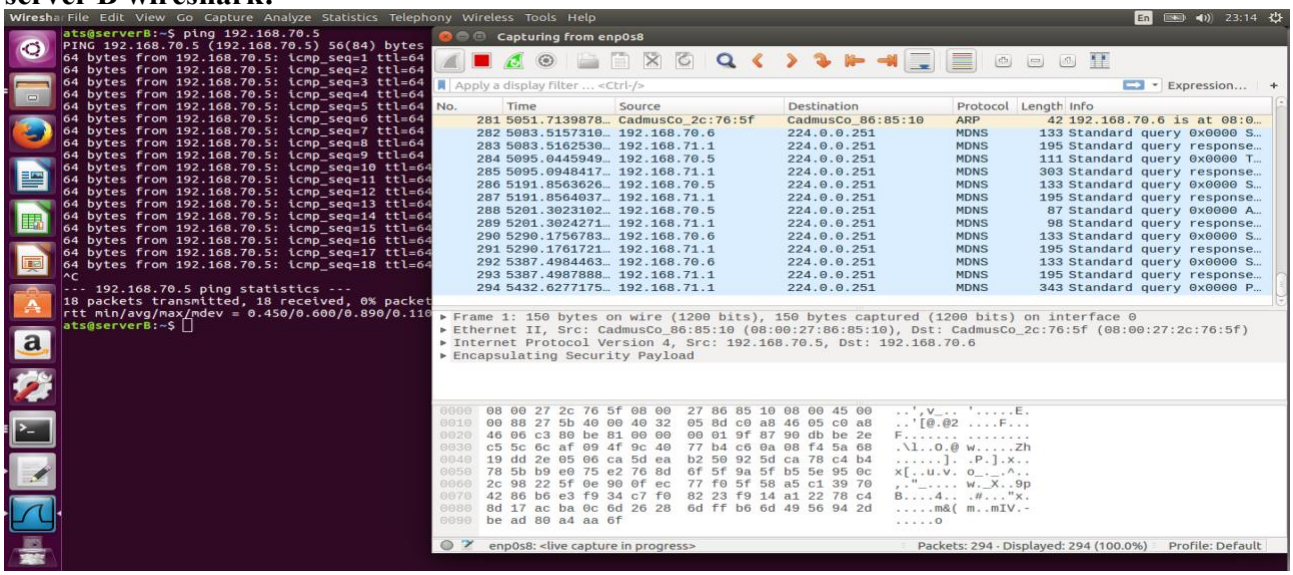


SERVER B screenshots:



```
ts@serverB:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-47-generic, x86_64):
  uptime: 25 minutes, since May 26 21:01:36 2018
  malloc: sbrk 1466368, mmap 0, used 382032, free 1084336
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey ssh
key pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6
  10.0.99.100
Connections:
serverB-to-serverA-transport:  192.168.70.6...192.168.70.5  IKEv2
serverB-to-serverA-transport:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverB-to-serverA-transport:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
serverB-to-serverA-transport:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverB-to-serverA-transport:   child:  dynamic === dynamic TRANSPORT
Routed Connections:
serverB-to-serverA-transport{1}:  ROUTED, TRANSPORT, reqid 1
serverB-to-serverA-transport{1}:   192.168.70.6/32 === 192.168.70.5/32
Security Associations (1 up, 0 connecting):
serverB-to-serverA-transport[1]: ESTABLISHED 24 minutes ago, 192.168.70.6[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]...192.168.70.5[C=
SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]
serverB-to-serverA-transport[1]: IKEv2 SPIs: 8d5e813dae587c36_i a62c887370ed6b4a_r*, public key reauthentication in 30 minutes
serverB-to-serverA-transport[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
serverB-to-serverA-transport{4}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c05c5546_i cc09a125_o
serverB-to-serverA-transport{4}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 4 minutes
serverB-to-serverA-transport{4}:   192.168.70.6/32 === 192.168.70.5/32
serverB-to-serverA-transport{5}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c397f162_i c9a64c8e_o
serverB-to-serverA-transport{5}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 5 minutes
serverB-to-serverA-transport{5}:   192.168.70.6/32 === 192.168.70.5/32
ts@serverB:~$
```

server B wireshark:



server B xfrm state:

```
ts@serverB:~$ sudo ip xfrm state
[sudo] password for ats:
src 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xc9a64c8e reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x467e2bd6add8bd409a1d63da92fa32ba1ac02f80 96
        enc cbc(aes) 0xd4fa66df97d98c847a0ef90679a36361
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.6/32 dst 192.168.70.5/32
src 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc397f162 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x54cb424cc4d93ce81934c738f1ad97aad5ec94c8 96
        enc cbc(aes) 0x1c36c3a0ef7dcc5120884f8d5310a805
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.5/32 dst 192.168.70.6/32
src 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xcc09a125 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x10c9e7b423bf65e0fbb372010bbd53e254eb27d9 96
        enc cbc(aes) 0xe6399cfdcbb0c091d0f4cbbf2120d99f
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.6/32 dst 192.168.70.5/32
src 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc05c5546 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x92a2e89bccff4bf91527e29412c1587afa14696f 96
        enc cbc(aes) 0x371fe101b084b269643141261f16be45
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.5/32 dst 192.168.70.6/32
ts@serverB:~$
```

```
ats@serverB:~$ sudo su
[sudo] password for ats:
root@serverB:/home/ats# cp /home/ats/Desktop/cert_key/certs/192.168.70.6.cert.pem
/etc/ipsec.d/certs
root@serverB:/home/ats# cp /home/ats/Desktop/cert_key/private/192.168.70.6.key.pem
/etc/ipsec.d/private
root@serverB:/home/ats# cd /etc/ipsec.d
root@serverB:/etc/ipsec.d# cd private
root@serverB:/etc/ipsec.d/private# ls
192.168.70.6.key.pem
root@serverB:/etc/ipsec.d/private# cd ..
root@serverB:/etc/ipsec.d# cd certs
root@serverB:/etc/ipsec.d/certs# ls
192.168.70.6.cert.pem
root@serverB:/etc/ipsec.d/certs# cd ..
root@serverB:/etc/ipsec.d# cd cacerts
root@serverB:/etc/ipsec.d/cacerts# ls
ca1.cert.pem  root.cert.pem
root@serverB:/etc/ipsec.d/cacerts#
```

```
ats@serverB:~$ sudo ipsec restart
[sudo] password for ats:
Stopping strongSwan IPsec...
Starting strongSwan 5.3.5 IPsec [starter]...
ats@serverB:~$ sudo ipsec rereadcacerts
ats@serverB:~$ sudo ipsec listcacerts

List of X.509 CA Certificates:

  subject:  "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
  issuer:   "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
  serial:    20:00
  validity:  not before May 26 01:44:12 2018, ok
             not after  May 23 01:44:12 2028, ok
  pubkey:    RSA 4096 bits
  keyid:     f6:6c:ac:2d:f3:c2:e9:35:d5:a5:26:68:40:17:55:23:e1:1e:98:ef
  subjkey:   c7:c8:67:63:c1:21:73:cc:9e:f7:1d:8c:71:f4:b9:4f:be:2f:73:5f
  authkey:   0f:17:d6:55:00:b9:dc:43:74:d4:bb:a6:ce:9c:92:cc:82:9b:f3:4a
  pathlen:   0

  subject:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
  issuer:   "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
  serial:    84:dc:0e:85:21:d9:7f:54
  validity:  not before May 26 01:40:36 2018, ok
             not after  May 21 01:40:36 2038, ok
  pubkey:    RSA 4096 bits
  keyid:     5c:32:f7:a3:e7:f0:2a:49:da:e9:b2:98:37:72:34:28:6a:69:dc:74
  subjkey:   0f:17:d6:55:00:b9:dc:43:74:d4:bb:a6:ce:9c:92:cc:82:9b:f3:4a
```

```
  authkey:   0f:17:d6:55:00:b9:dc:43:74:d4:bb:a6:ce:9c:92:cc:82:9b:f3:4a
ats@serverB:~$
```

```
ats@serverB:~$ sudo ipsec up serverB-to-serverA-transport
establishing CHILD_SA serverB-to-serverA-transport
generating CREATE_CHILD_SA request 0 [ N(USE_TRANSP) SA No TSi TSr ]
sending packet: from 192.168.70.6[500] to 192.168.70.5[500] (348 bytes)
received packet: from 192.168.70.5[500] to 192.168.70.6[500] (204 bytes)
parsed CREATE_CHILD_SA response 0 [ N(USE_TRANSP) SA No TSi TSr ]
CHILD_SA serverB-to-serverA-transport{3} established with SPIs c3d2f14b_i cae93c12_o and TS
192.168.70.6/32 === 192.168.70.5/32
connection 'serverB-to-serverA-transport' established successfully
ats@serverB:~$
```

```
ats@serverB:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-47-generic, x86_64):
  uptime: 25 minutes, since May 26 21:01:36 2018
  malloc: sbrk 1466368, mmap 0, used 382032, free 1084336
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation
constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent
xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6
  10.0.99.100
Connections:
serverB-to-serverA-transport:  192.168.70.6...192.168.70.5  IKEv2
serverB-to-serverA-transport:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.6] uses public key authentication
serverB-to-serverA-transport:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.6"
serverB-to-serverA-transport:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.5] uses public key authentication
serverB-to-serverA-transport:   child:  dynamic === dynamic TRANSPORT
Routed Connections:
serverB-to-serverA-transport{1}:  ROUTED, TRANSPORT, reqid 1
serverB-to-serverA-transport{1}:   192.168.70.6/32 === 192.168.70.5/32
Security Associations (1 up, 0 connecting):
serverB-to-serverA-transport[1]: ESTABLISHED 24 minutes ago, 192.168.70.6[C=SE,
ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]...192.168.70.5[C=SE, ST=Blekinge,
L=Karlskrona, O=ET2540, CN=192.168.70.5]
serverB-to-serverA-transport[1]: IKEv2 SPIs: 8d5e813dae587c36_i a62c887370ed6b4a_r*, public
key reauthentication in 30 minutes
serverB-to-serverA-transport[1]: IKE proposal:
AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
```

```
serverB-to-serverA-transport{4}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c05c5546_i
cc09a125_o
serverB-to-serverA-transport{4}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o,
rekeying in 4 minutes
serverB-to-serverA-transport{4}:   192.168.70.6/32 === 192.168.70.5/32
serverB-to-serverA-transport{5}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c397f162_i
c9a64c8e_o
serverB-to-serverA-transport{5}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o,
rekeying in 5 minutes
serverB-to-serverA-transport{5}:   192.168.70.6/32 === 192.168.70.5/32
ats@serverB:~$
```

```
ats@serverB:~$ sudo ip xfrm state
[sudo] password for ats:
src 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xc9a64c8e reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x467e2bd6add8bd409a1d63da92fa32ba1ac02f80 96
        enc cbc(aes) 0xd4fa66df97d98c847a0ef90679a36361
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.6/32 dst 192.168.70.5/32
src 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc397f162 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x54cb424cc4d93ce81934c738f1ad97aad5ec94c8 96
        enc cbc(aes) 0x1c36c3a0ef7dcc5120884f8d5310a805
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.5/32 dst 192.168.70.6/32
src 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xcc09a125 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x10c9e7b423bf65e0fbb372010bbd53e254eb27d9 96
        enc cbc(aes) 0xe6399cfdcbb0c091d0f4cbbf2120d99f
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.6/32 dst 192.168.70.5/32
src 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc05c5546 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x92a2e89bccff4bf91527e29412c1587afa14696f 96
        enc cbc(aes) 0x371fe101b084b269643141261f16be45
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.70.5/32 dst 192.168.70.6/32
ats@serverB:~$
```

Task 19:

Ipsec.conf file at Server A:

```
config setup

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        mobike=no
        keyexchange=ikev2

conn serverA-to-serverB-tunnel
        left=192.168.70.5
        leftcert=192.168.70.5.cert.pem
        leftid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
        leftfirewall=yes
        right=192.168.70.6
        rightid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
        type=tunnel
        auto=route
        authby=rsa
```

Ipsec.conf file at Server B:

```
config setup

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        mobike=no
        keyexchange=ikev2

conn serverA-to-serverB-tunnel
        left=192.168.70.5
        leftcert=192.168.70.5.cert.pem
        leftid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
        leftfirewall=yes
        right=192.168.70.6
        rightid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
        type=tunnel
        auto=route
        authby=rsa
```

Ipsec tunnel in tunnel mood:

```
ats@serverA:~$ sudo ipsec up serverA-to-serverB-transport
initiating IKE_SA serverA-to-serverB-transport[1] to 192.168.70.6
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(HASH_ALG) ]
sending packet: from 192.168.70.5[500] to 192.168.70.6[500] (1124 bytes)
received packet: from 192.168.70.6[500] to 192.168.70.5[500] (501 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(HASH_ALG) N(MULT_AUTH) ]
received cert request for "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
received cert request for "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
sending cert request for "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
sending cert request for "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
authentication of 'C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5' (myself) with RSA_EMSA_PKCS1_SHA256 successful
sending end entity cert "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
establishing CHILD_SA serverA-to-serverB-transport
generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) ]
sending packet: from 192.168.70.5[500] to 192.168.70.6[500] (2188 bytes)
received packet: from 192.168.70.6[500] to 192.168.70.5[500] (1884 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH SA TSi TSr N(AUTH_LFT) ]
received end entity cert "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
  using certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
  using trusted intermediate ca certificate "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
checking certificate status of "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
  fetching crl from 'https://localhost/ca1.crl.pem' ...
unable to fetch from https://localhost/ca1.crl.pem, no capable fetcher found
crl fetching failed
certificate status is not available
  using trusted ca certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=saddam-root"
checking certificate status of "C=SE, ST=Blekinge, O=ET2540, CN=saddam-ca"
certificate status is not available
  reached self-signed root ca with a path length of 1
authentication of 'C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6' with RSA_EMSA_PKCS1_SHA256 successful
IKE_SA serverA-to-serverB-transport[1] established between 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=SE
, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
scheduling reauthentication in 3275s
maximum IKE_SA lifetime 3455s
connection 'serverA-to-serverB-transport' established successfully
ats@serverA:~$
```

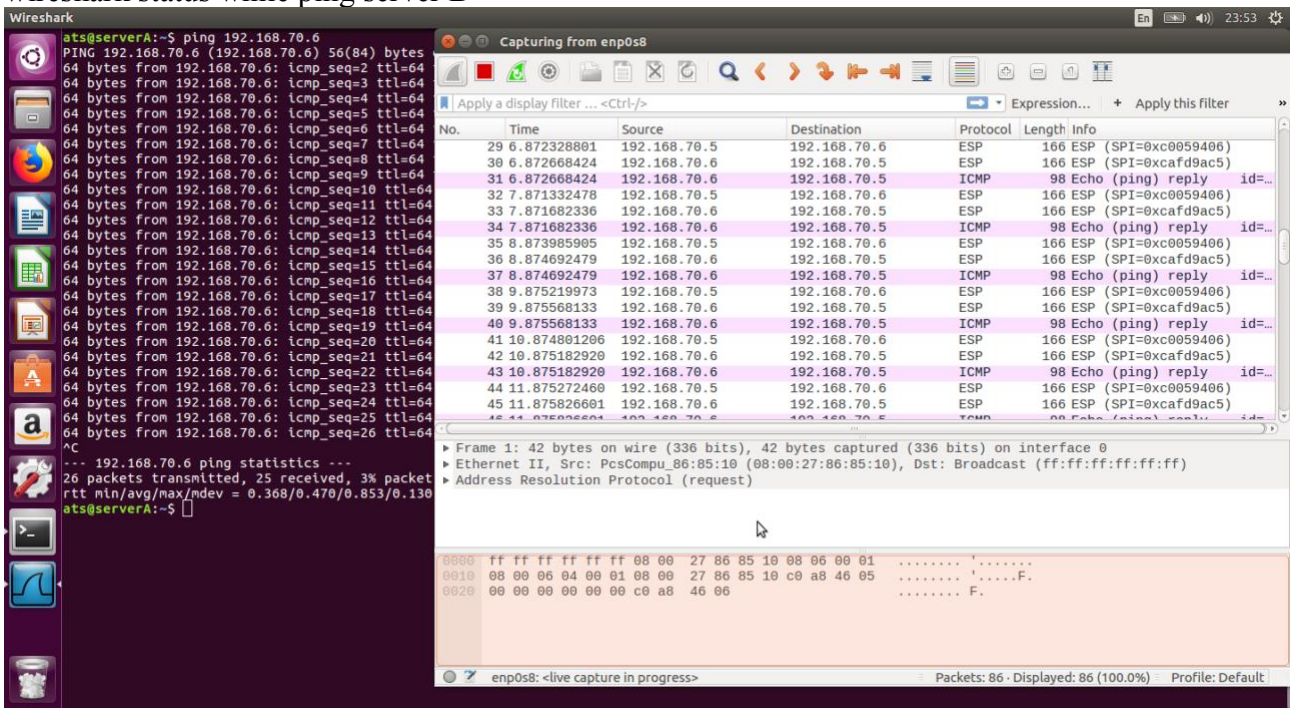
Ipsec status all

```
ats@serverA:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-116-generic, x86_64):
  uptime: 3 minutes, since May 26 23:29:21 2018
  malloc: sbrk 1466368, mmap 0, used 386112, free 1080256
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey ssh
key pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB-transport:  192.168.70.5...192.168.70.6  IKEv2
serverA-to-serverB-transport:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverA-to-serverB-transport:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
serverA-to-serverB-transport:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverA-to-serverB-transport:   child:  dynamic === dynamic TUNNEL
Routed Connections:
serverA-to-serverB-transport{1}:  ROUTED, TUNNEL, reqid 1
serverA-to-serverB-transport{1}:   192.168.70.5/32 === 192.168.70.6/32
Security Associations (1 up, 0 connecting):
serverA-to-serverB-transport[1]: ESTABLISHED 3 minutes ago, 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=S
E, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
serverA-to-serverB-transport[1]: IKEv2 SPIs: 67cb0a52a6ca83f6_i* d0a5a4b4b2111bfd_r, public key reauthentication in 50 minutes
serverA-to-serverB-transport[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
serverA-to-serverB-transport{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c33e8b0f_i c409d9b4_o
serverA-to-serverB-transport{2}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 10 minutes
serverA-to-serverB-transport{2}:   192.168.70.5/32 === 192.168.70.6/32
serverA-to-serverB-transport{3}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cba5045b_i c90aa412_o
serverA-to-serverB-transport{3}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 11 minutes
serverA-to-serverB-transport{3}:   192.168.70.5/32 === 192.168.70.6/32
ats@serverA:~$
```

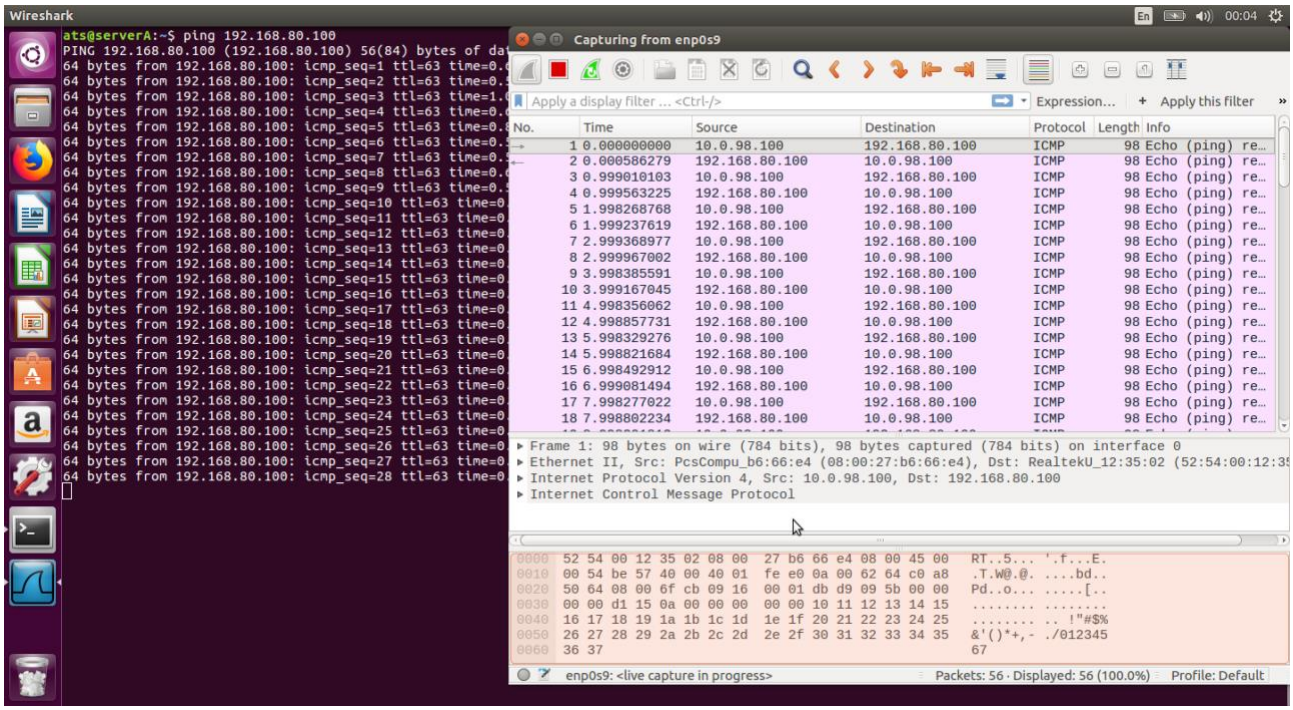
xfrm state:

```
ts@serverA:~$ sudo ip xfrm state
rc 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc90aa412 reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0xdd63459b5dac44ab27942e6d5608b9ec946a2af8 96
        enc cbc(aes) 0x1a816070304e09753ee5ff22bd4f1325
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
rc 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xcba5045b reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0x2d2cefd0e8ee5051e85d6f255ebcd9b16535855f 96
        enc cbc(aes) 0x379bf78479c1e2d76e4f20f792961d74
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
rc 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc409d9b4 reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0x8413cfd9ecc1f43ccf6728308b04d1a5eb10b1cf 96
        enc cbc(aes) 0xd6e46678e1d7c2cedebf805ef2c603f4
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
rc 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xc33e8b0f reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0xf9348fc706ab3364b189a028dbacdbbb6c0562ac 96
        enc cbc(aes) 0x1989d7251d2e048bb092d01ce95b4f98
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
ts@serverA:~$
```

wireshark status while ping server B



wireshark status while ping 192.168.80.100



Server B statusall

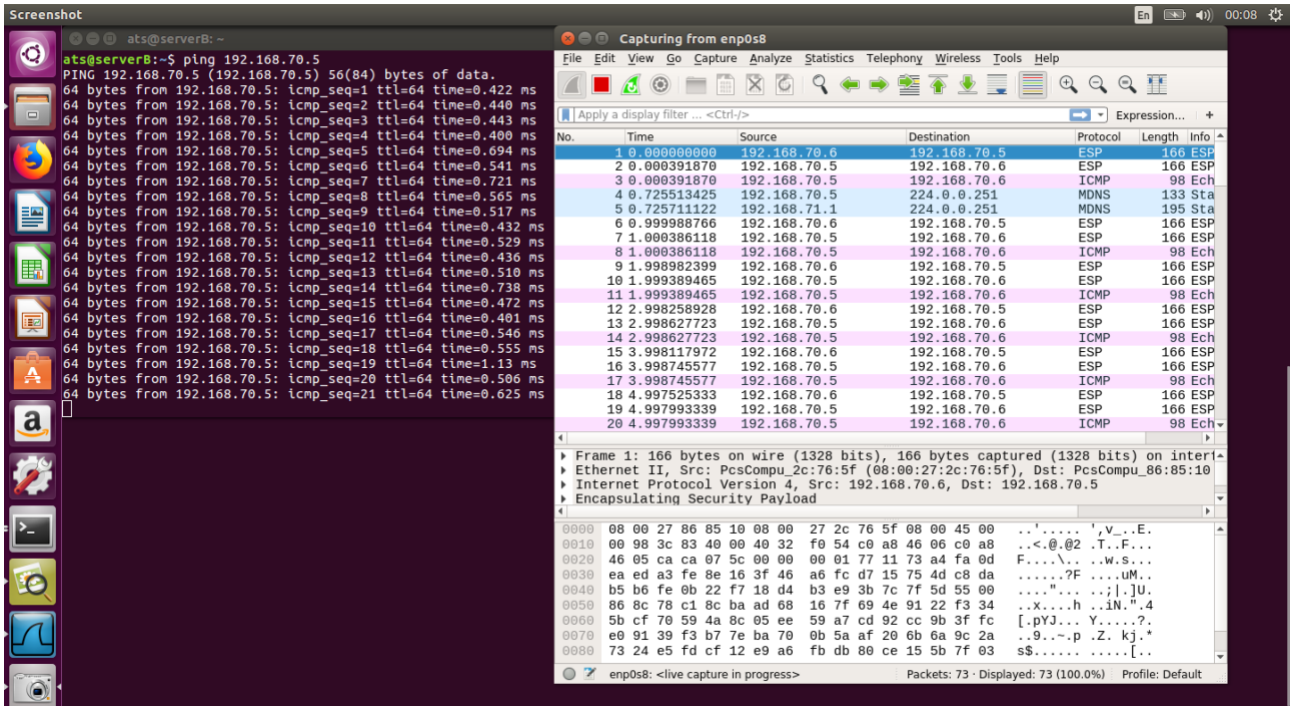
```
ats@serverB:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-47-generic, x86_64):
  uptime: 7 minutes, since May 26 23:47:54 2018
  malloc: sbrk 1466368, mmap 0, used 388112, free 1078256
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey ssh
key pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6
  10.0.99.100
Connections:
serverB-to-serverA-transport:  192.168.70.6...192.168.70.5  IKEv2
serverB-to-serverA-transport:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverB-to-serverA-transport:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
serverB-to-serverA-transport:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverB-to-serverA-transport:   child:  dynamic === dynamic TUNNEL
Routed Connections:
serverB-to-serverA-transport{1}:  ROUTED, TUNNEL, reqid 1
serverB-to-serverA-transport{1}:   192.168.70.6/32 === 192.168.70.5/32
Security Associations (1 up, 0 connecting):
serverB-to-serverA-transport[1]: ESTABLISHED 2 minutes ago, 192.168.70.6[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]...192.168.70.5[C=S
E, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]
serverB-to-serverA-transport[1]: IKEv2 SPIs: 44f7e4fa7d630760_i 899bfa0f659c2a22_r*, public key reauthentication in 53 minutes
serverB-to-serverA-transport[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
serverB-to-serverA-transport{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c0059406_i cafd9ac5_o
serverB-to-serverA-transport{2}:  AES_CBC_128/HMAC_SHA1_96, 5292 bytes_i (63 pkts, 24s ago), 5292 bytes_o (63 pkts, 24s ago), rekeying in 12 minutes
serverB-to-serverA-transport{2}:   192.168.70.6/32 === 192.168.70.5/32
ats@serverB:~$
```

```
ats@serverB:~$ sudo ipsec up serverB-to-serverA-transport
establishing CHILD_SA serverB-to-serverA-transport
generating CREATE_CHILD_SA request 0 [ SA No TSi TSr ]
sending packet: from 192.168.70.6[500] to 192.168.70.5[500] (332 bytes)
received packet: from 192.168.70.5[500] to 192.168.70.6[500] (204 bytes)
parsed CREATE_CHILD_SA response 0 [ SA No TSi TSr ]
connection 'serverB-to-serverA-transport' established successfully
ats@serverB:~$
```

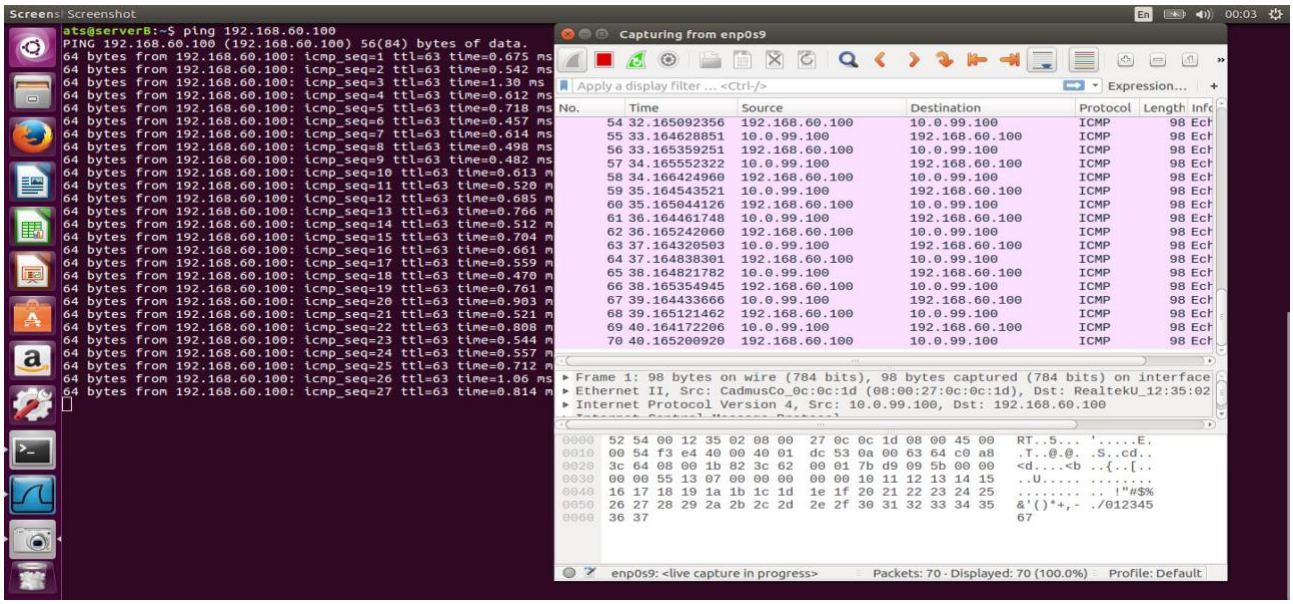
Xfrm state for server B

```
ats@serverB:~$ sudo ip xfrm state
src 192.168.70.6 dst 192.168.70.5
        proto esp spi 0xcafd9ac5 reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0x352fd630db4d6cc086b0574a3ba8fdabb61b3d63 96
        enc cbc(aes) 0xa412f8e8636d8c2379bd2fc351e49779
        anti-replay context: seq 0x0, oseq 0x3f, bitmap 0x00000000
src 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc0059406 reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0x53b22b67e649d3d64f5cd8a5ae2a3fd880b7bdaf 96
        enc cbc(aes) 0x7f5916276a4f429cbd8e4a797de8ed1f
        anti-replay context: seq 0x3f, oseq 0x0, bitmap 0xffffffff
ats@serverB:~$
```

wireshark status for server B while ping to server A

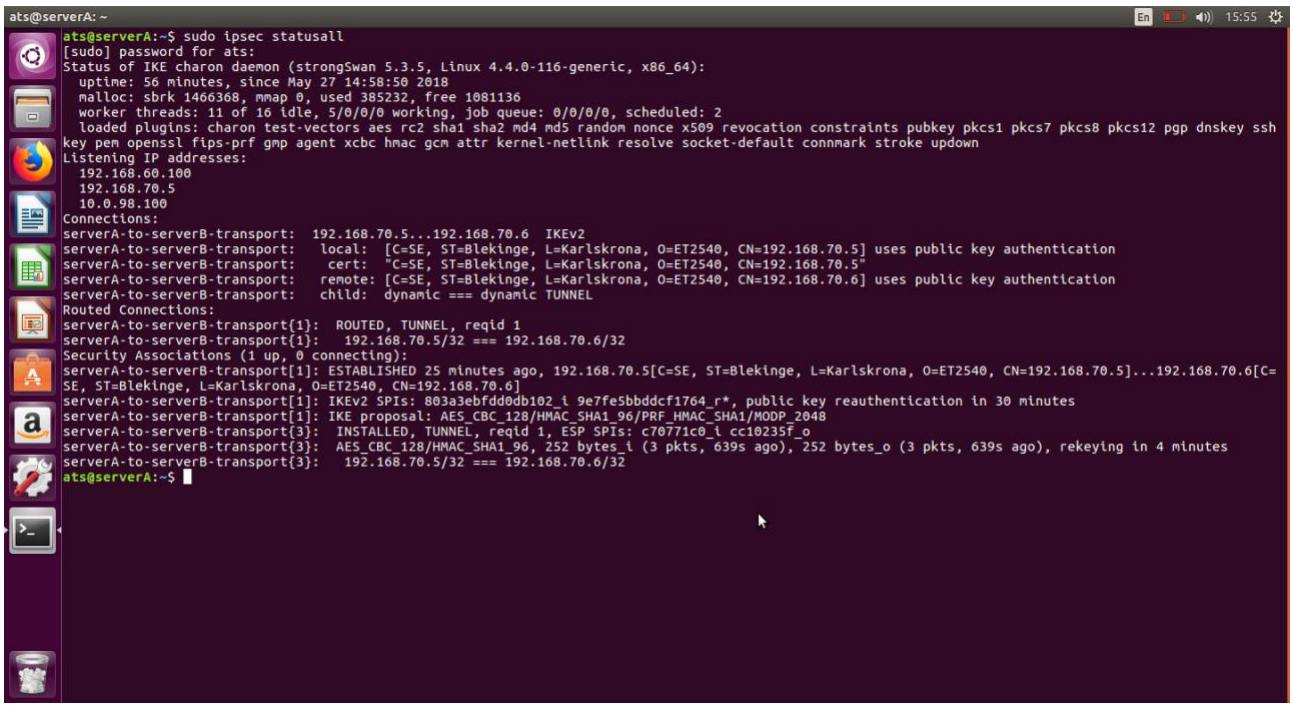


While ping to 192.168.60.100



Task 20:

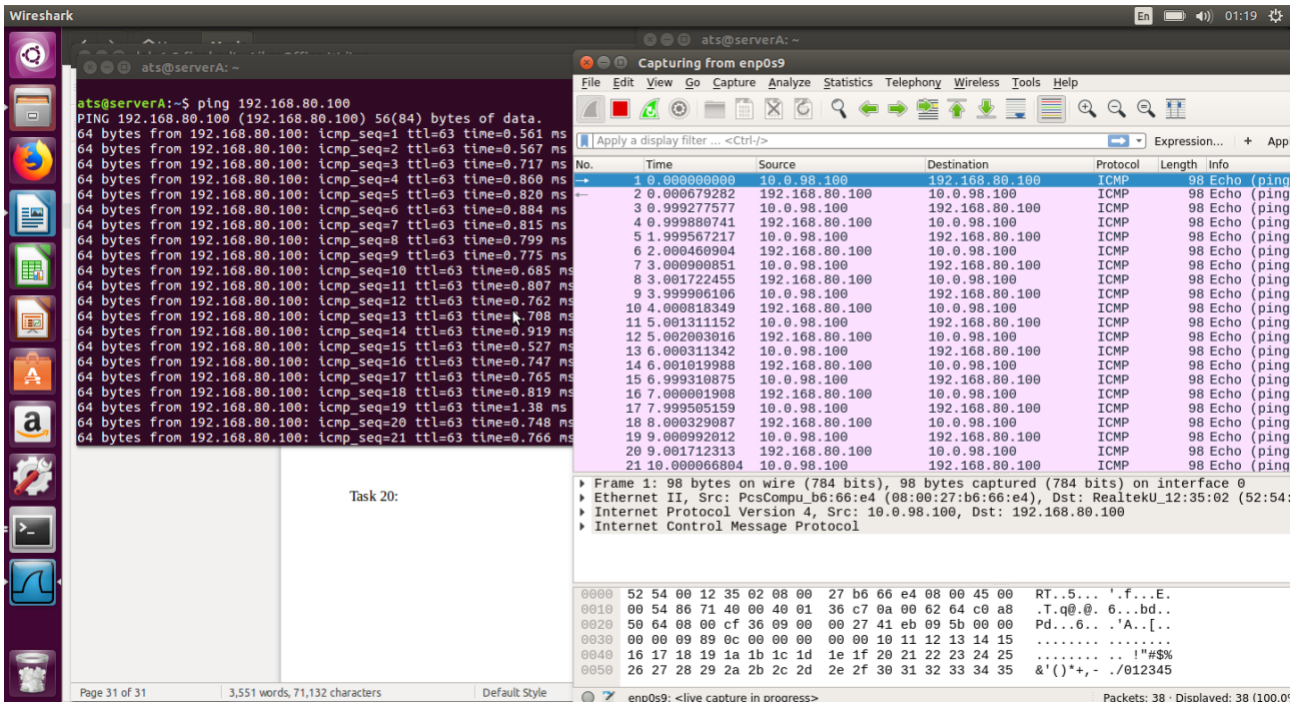
```
ats@serverA:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-116-generic, x86_64):
  uptime: 56 minutes, since May 27 14:58:50 2018
  malloc: sbrk 1466368, mmap 0, used 385232, free 1081136
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation
constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent
xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB-transport:  192.168.70.5...192.168.70.6  IKEv2
serverA-to-serverB-transport:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.5] uses public key authentication
serverA-to-serverB-transport:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.5"
serverA-to-serverB-transport:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.6] uses public key authentication
serverA-to-serverB-transport:   child:  dynamic === dynamic TUNNEL
Routed Connections:
serverA-to-serverB-transport{1}:  ROUTED, TUNNEL, reqid 1
serverA-to-serverB-transport{1}:   192.168.70.5/32 === 192.168.70.6/32
Security Associations (1 up, 0 connecting):
serverA-to-serverB-transport[1]: ESTABLISHED 25 minutes ago, 192.168.70.5[C=SE,
ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=SE, ST=Blekinge,
L=Karlskrona, O=ET2540, CN=192.168.70.6]
serverA-to-serverB-transport[1]: IKEv2 SPIs: 803a3ebfdd0db102_i 9e7fe5bbddcf1764_r*, public
key reauthentication in 30 minutes
serverA-to-serverB-transport[1]: IKE proposal:
AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
serverA-to-serverB-transport{3}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c70771c0_i
cc10235f_o
serverA-to-serverB-transport{3}:  AES_CBC_128/HMAC_SHA1_96, 252 bytes_i (3 pkts, 639s
ago), 252 bytes_o (3 pkts, 639s ago), rekeying in 4 minutes
serverA-to-serverB-transport{3}:   192.168.70.5/32 === 192.168.70.6/32
ats@serverA:~$
```



x

ats@serverB:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-127-generic, x86_64):
  uptime: 48 minutes, since May 27 15:08:08 2018
  malloc: sbrk 1466368, mmap 0, used 384560, free 1081808
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6
  10.0.99.100
Connections:
serverB-to-serverA-transport: 192.168.70.6...192.168.70.5 IKEv2
serverB-to-serverA-transport: local: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverB-to-serverA-transport: cert: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
serverB-to-serverA-transport: remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverB-to-serverA-transport: child: dynamic === dynamic TUNNEL
Routed Connections:
serverB-to-serverA-transport{1}: ROUTED, TUNNEL, reqid 1
serverB-to-serverA-transport{1}:   192.168.70.6/32 === 192.168.70.5/32
Security Associations (1 up, 0 connecting):
serverB-to-serverA-transport[1]: ESTABLISHED 26 minutes ago, 192.168.70.6[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]...192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]
serverB-to-serverA-transport[1]: IKEv2 SPIs: 803a3ebfdd0db102_i* 9e7fe5bbddcf1764_r, public key reauthentication in 26 minutes

serverB-to-serverA-transport[1]: IKE proposal:
AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
serverB-to-serverA-transport{3}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: cc10235f_i
c70771c0_o
serverB-to-serverA-transport{3}: AES_CBC_128/HMAC_SHA1_96, 252 bytes_i (3 pkts, 722s
ago), 252 bytes_o (3 pkts, 722s ago), rekeying in 3 minutes
serverB-to-serverA-transport{3}: 192.168.70.6/32 === 192.168.70.5/32
ats@serverB:~$

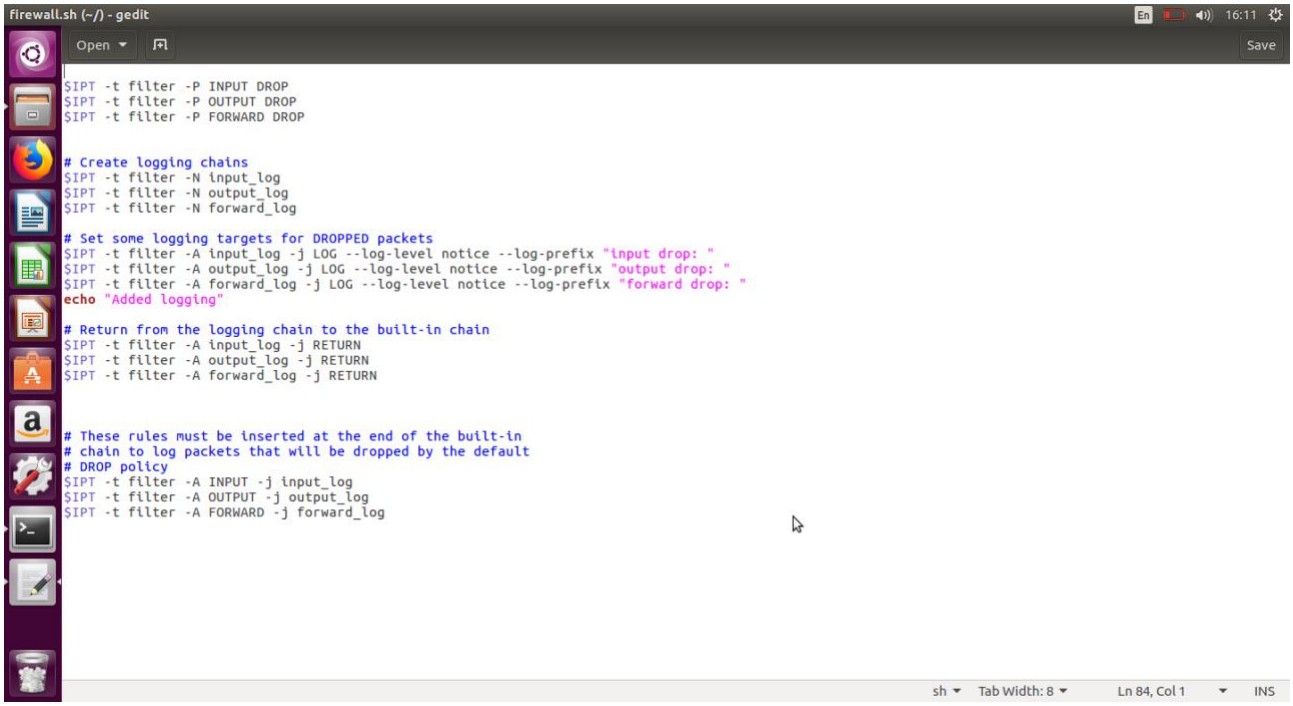


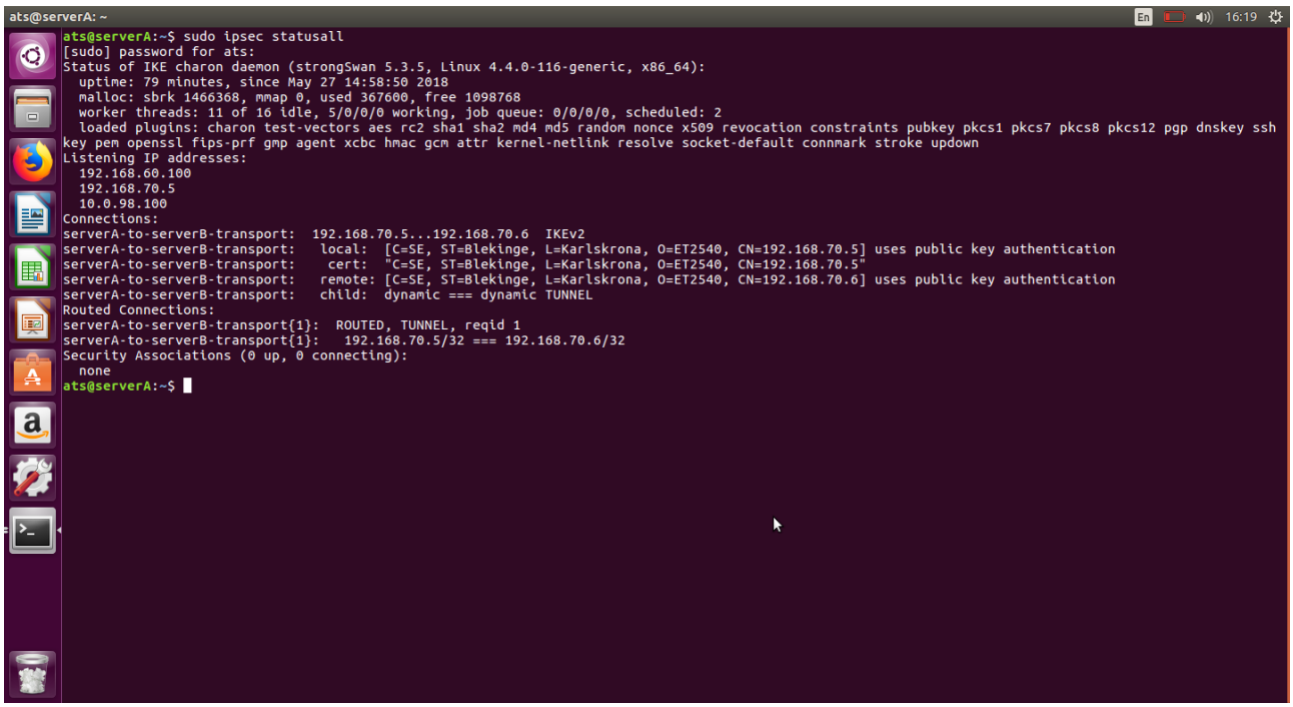
x

Task 21

ats@serverB:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-127-generic, x86_64):
  uptime: 71 minutes, since May 27 15:08:08 2018
  malloc: sbrk 1466368, mmap 0, used 368048, free 1098320
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation
constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent
xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6

10.0.99.100
Connections:
serverB-to-serverA-transport: 192.168.70.6...192.168.70.5 IKEv2
serverB-to-serverA-transport: local: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverB-to-serverA-transport: cert: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
serverB-to-serverA-transport: remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverB-to-serverA-transport: child: dynamic === dynamic TUNNEL
Routed Connections:
serverB-to-serverA-transport{1}: ROUTED, TUNNEL, reqid 1
serverB-to-serverA-transport{1}:   192.168.70.6/32 === 192.168.70.5/32
Security Associations (0 up, 0 connecting):
  none
ats@serverB:~$





ats@serverA:~$ sudo ipsec statusall
[sudo] password for ats:
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-116-generic, x86_64):
  uptime: 79 minutes, since May 27 14:58:50 2018
  malloc: sbrk 1466368, mmap 0, used 367600, free 1098768
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB-transport: 192.168.70.5...192.168.70.6 IKEv2
serverA-to-serverB-transport: local: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverA-to-serverB-transport: cert: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
serverA-to-serverB-transport: remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverA-to-serverB-transport: child: dynamic === dynamic TUNNEL
Routed Connections:
serverA-to-serverB-transport{1}: ROUTED, TUNNEL, reqid 1
serverA-to-serverB-transport{1}:   192.168.70.5/32 === 192.168.70.6/32

```
Security Associations (0 up, 0 connecting):
  none
ats@serverA:~$
```