Role LB - Certificates for load balancers

The certificates are located in:

```
/etc/haproxy/haproxy.pem
```

The correct permissions are 400. (read only for root) and can be set as follows:

```
chmod 400 haproxy.pem
```

The file contains Sections:

Note

certificate chain:

- end_entity_cetificate.crt
- intermediate_certificate.crt
- root_certificate.crt

Private Key

- private_key.key

The end entity certificate and the matching private key are mandatory

haproxy.pem

- **end_entity_cetificate.crt**
- intermediate_certificate.crt
- root_certificate.crt
- **private_key.key**

Command to generate the haproxy.pem file

Generate the haproxy.pem file

```
$ cat end-entity.crt intermediate_certificate.crt root_certificate.crt private-key.key > haproxy.pem
```

- Make sure the private key is not corrupted

  ```
  $ openssl rsa -check -noout -in private_key.key
  ```

  If the output “RSA key ok“ then the private key is correct.

- Make sure the end entity certificate and the private key match together

Calculate the modulus of the of the private key

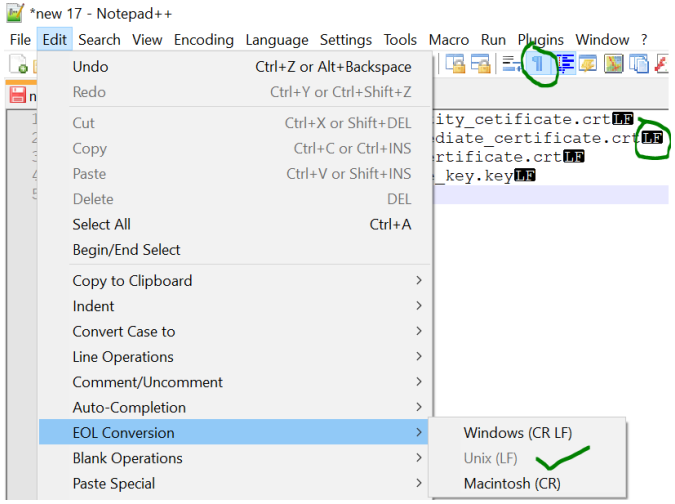
```
$ openssl rsa -modulus -noout -in private_key.key | openssl md5
```

Calculate the modulus of the server certificate

```
$ openssl x509 -modulus -noout -in end_entity_certificate.crt| openssl md5
```

If both outputs are identical then the private key matches to the end entity certificate.

- The end entity certificate muss be in the first position and the matching private key muss be in the last position
- The intermediate(s) and the root certificate are optional. In case they are included, the intermediate(s) certificates muss before the root certificate
- Make sure the end of line (EOL) in the file are Linux EOL (LF). Windows EOL (CR LF) or Macintosh EOL (CR) will fail, because the Load Balancer is a Linux distribution.



- You can check the content (Check the Validity) after with this command:

```
$ openssl x509 -text -in haproxy.pem
```

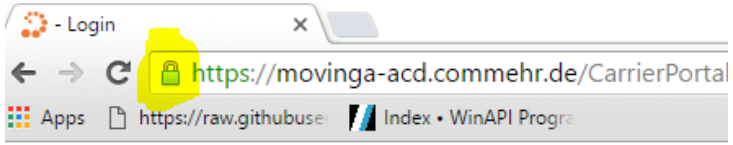
```
-----BEGIN CERTIFICATE-----
MIIEzjCCA7agAwIBAgISESGiWLxseXetsJGbfZKEfehiMA0GCSqGSIb3DQEBCwUA
MEwxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYD
...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAsDGatsqSubHWmDG2IOVbocgwJfX9dB3EtXFw6HN87zDvAvvE
9KUsDqMQiU2+aORZapzhl0oL1cfznPpQYyo4WGprQiNyL82TTxeWhCNRnBv4tnJw
...

-----END RSA PRIVATE KEY-----
```


The minimum is that the certificate for the load balancer and private key are included. The file is referenced in haproxy.cfg:

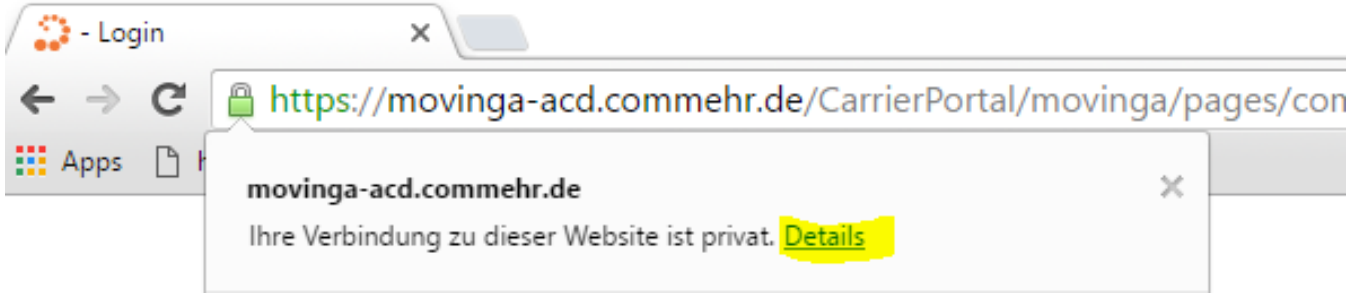
```
frontend acdportal_https
 mode http
 bind :443 ssl crt /etc/haproxy/haproxy.pem #verify optional
```

If an intermediate certificate must be inserted (example sales force if the certification chain is not known in SalesForce), this can be done as follows

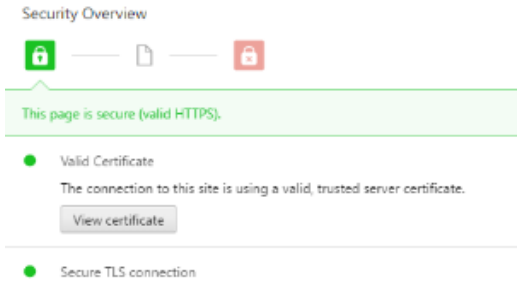
- Right mouse click on the certification in the browser:



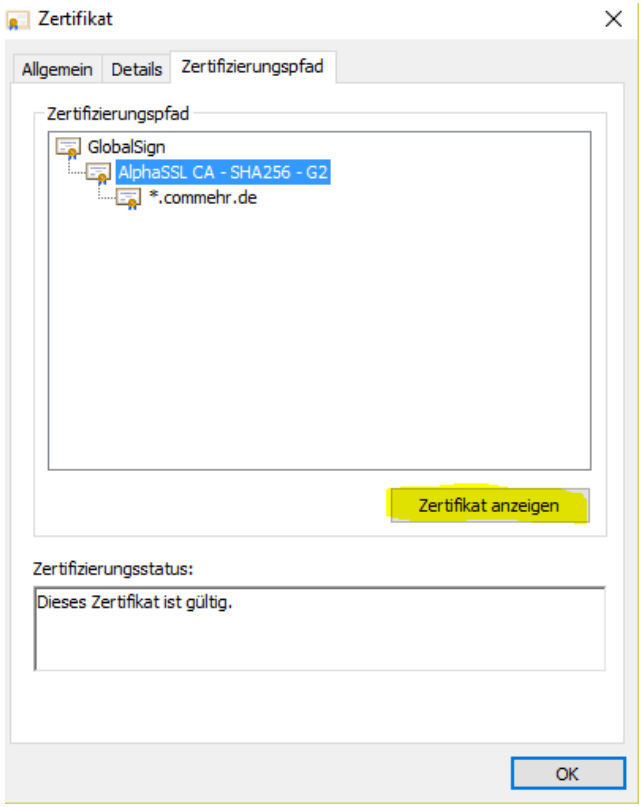
- Display details of the certificate:



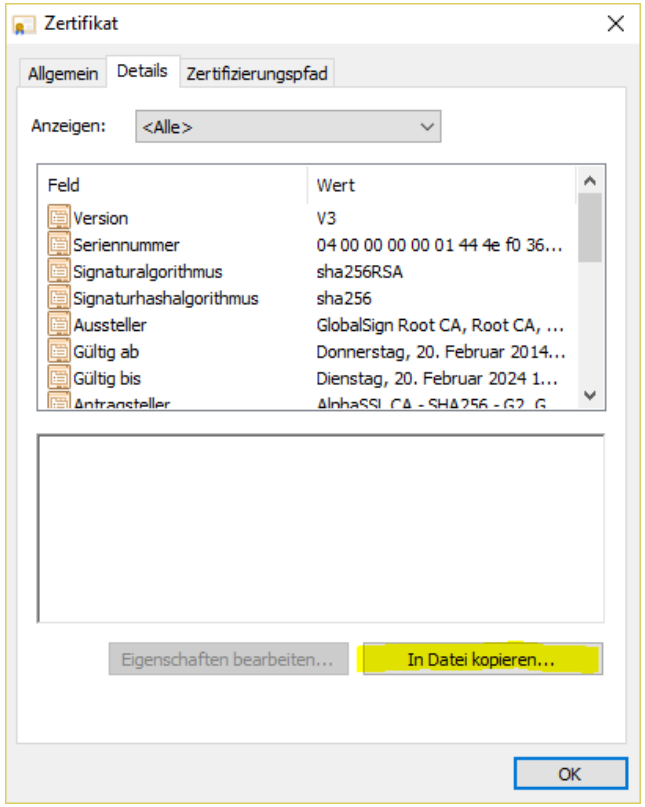
- view certificate



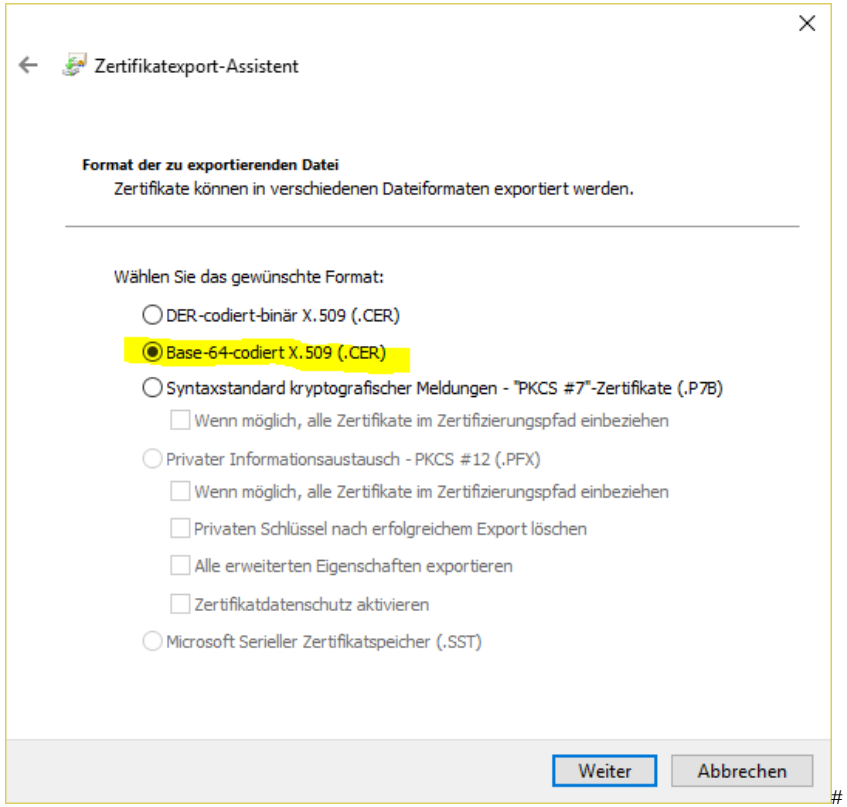
- Display intermediate certificate:


Zertifikat
Allgemein
Details
Zertifizierungspfad
Zertifizierungspfad
GlobalSign
AlphaSSL CA - SHA256 - G2
*.commehr.de
Zertifikat anzeigen
Zertifizierungsstatus:
Dieses Zertifikat ist gültig.
OK

- Save as file:

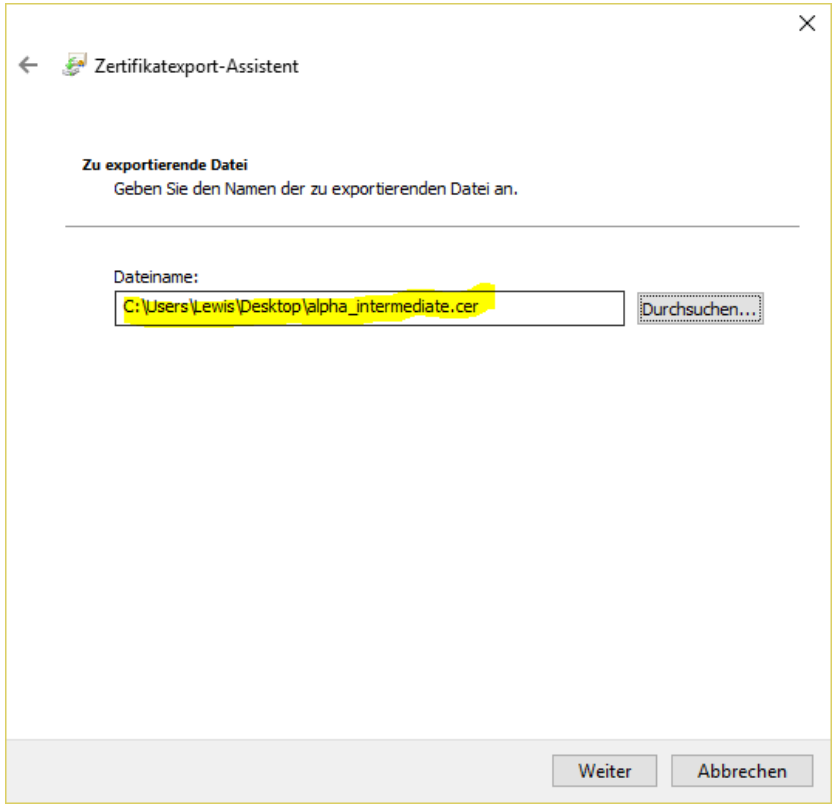


- In base 64 format:



#

- Save to the local computer:



Then edit the file with a text editor, then copy the content of the intermediate certificate into the haproxy.pem file at the very bottom.

Then:

```
service haproxy reload
```

Converting pfx Certificates to .pem Format

The following command can be used to convert a .pfx certificate file to .pem Format (the password for the certificate will be required):

```
openssl pkcs12 -in acd.cg.internal.pfx -out /root/haproxy.pem -nodes
```