25.07.2024

Quick Guide

Class C SSL/TLS
Creating key pairs and CSR files

Status: Released V1.0

Creating a certificate signing request (CSR) is a two-step process.

First, a key pair is created and then the actual CSR is generated. The procedure for these steps varies slightly depending on the server and the tool used. The documentation for the server and the tool should provide the requisite information. The description below covers CSR creation using the openssl tool.

Creating the key pair

The requesters then create the CSR on their server. For this purpose, they use the key file generated in the first step:

```
openssl genrsa -out <zertifikatsname.key> 2048
```

- The created key file is used as an input in the next step.

Creating a certificate signing request (CSR)

In this first example, the keys and the CSR are created in two separate steps. Scenario: a CSR is to be created for the server sample.admin.ch. First, the keys are created. The key file is named sample-key.pem:

```
openssl req -new -key <zertifikatsname.key> -out <zertifikatsname.csr>
```

- After this command has been entered, the tool asks for various parameters. The values that have to be entered are described in detail in the example below.

Example 1: Generating a key/CSR in separate steps

In this first example, the keys and the CSR are created in two separate steps. Scenario: a CSR is to be created for the server sample.admin.ch. First, the keys are created. The key file is named sample-key.pem:

C:\OpenSSL\bin>openssl genrsa -out samplekey.pem 2048

- After the command is entered, the tool confirms the execution:

Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
....+++
....+++
unable to write 'random state' e is 65537 (0x10001)

- The error messages at the end can be ignored. The keys have now been generated and saved in the file samplekey.pem. This data is now used to create the certificate signing request. The CSR is attributed to the file name samplecsr.pem. The previously generated key file sample-key.pem is used as an input:

C:\OpenSSL\bin>openssl req -new -key samplekey.pem -out samplecsr.pem

- The tool confirms the order with a short message about the information that is subsequently queried:

Loading 'screen' into random state - done
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. -------

- The individual parameters are then queried. If a value is left blank, a full stop (".") must be entered in response to the query:

Country Name (2 letter code) [AU]:ch

- For this value, "ch" must always be entered. The next two parameters are left blank, i.e. "." is entered:

State or Province Name (full name) [Some-State]:.

Locality Name (eg, city) []:.

- For the organisation name parameter, "admin" is entered for the Federal Administration. The organisational unit name remains blank:

Organization Name (eg, company) [Internet Widgits Pty Ltd]:admin

Organizational Unit Name (eg, section) []:.

- The server's FQDN (fully qualified domain name) is now entered in the common name field. In our example, this is http://www.sample.ch/:

Common Name (e.g. server FQDN or YOUR name) []:www.sample.admin.ch

- The email address field MUST be left blank.

Email Address []:.

- Finally, the password must be set; this will be used later during certificate installation:

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

- The last query, optional company name, is left blank.

- The CSR has now been successfully generated. The file can be displayed by entering the following command:

```
C:\OpenSSL\bin>openssl req -noout -text -in samplecsr.pem
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=CH, O=admin, CN=www.sample.admin.ch
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:cf:81:66:ee:29:3c:22:cf:ab:e0:3e:8f:c4:32:
5f:5a:58:ea:7f:44:b5:41:f8:b9:66:4b:55:a5:23:
88:6c:3c:d9:35:1b:57:53:84:80:43:8a:e4:bd:9a:
8a:c3:7f:fe:26:ad:12:94:ed:6c:d5:ab:62:8a:a4:
0a:50:e1:79:d2:2c:f2:57:2c:17:fc:d3:54:27:3b:
f1:e2:4c:7b:cb:b6:de:fc:1b:1f:f7:c4:28:28:65:
14:88:60:80:f1:ce:7b:88:65:d2:c3:25:7d:11:d3:
54:44:bd:b6:9a:71:ae:41:31:71:42:89:b7:7c:df:
5b:5f:2c:b0:1b:95:7c:89:07:d4:0a:24:80:29:50:
d7:75:8c:38:fa:4e:66:bf:37:71:c8:03:87:97:2d:
75:ff:9e:cc:97:93:98:ae:60:d2:99:5d:c1:b6:b2:
c9:1d:8b:9a:d2:40:61:ac:90:43:3e:4f:70:4a:fd:
80:84:1e:44:1c:5f:f6:a5:be:18:77:bf:4c:19:48:
42:b8:4f:6f:b7:3d:81:5d:91:b0:fa:dc:69:10:9f:
7d:f6:fd:ce:98:49:42:8b:0c:11:1a:65:16:f3:ec:
c8:dd:aa:0d:67:6d:83:9d:aa:9a:60:14:b4:56:99:
7e:23:f1:5a:ed:c1:16:58:19:47:7d:64:70:ad:b8:
27:51
Exponent: 65537 (0x10001)
Attributes:
challengePassword :unable to print attribute
Signature Algorithm: sha1WithRSAEncryption
88:8f:73:c5:1e:4b:04:f5:3e:69:ac:a0:c6:bb:e5:4c:83:db:
7f:67:5b:7e:59:90:f6:0c:46:40:f8:e8:d2:c6:fe:a7:2d:db:
c0:6e:f3:f6:b1:0f:e8:33:09:01:67:2a:bd:ce:0d:46:9f:57:
cc:d9:e6:56:b7:be:ab:87:a5:6b:b8:0d:32:0e:0f:95:22:87:
44:17:88:17:b4:a2:23:5b:2e:da:35:3c:01:62:c0:6f:4b:e7:
f4:31:53:ab:f1:82:f7:b6:d6:0b:61:cf:42:c3:ff:86:55:7f:
10:2c:7b:7d:dd:5e:05:58:1d:46:28:7b:0c:d4:61:1a:91:80:
13:c0:65:17:cb:b6:4f:9e:2b:2b:5c:a5:a3:55:7f:6a:62:a3:
86:37:8b:7d:2d:6c:ff:8f:0b:ec:94:a4:7a:f0:96:55:7d:2f:
0c:7a:c1:fc:c5:9f:52:bf:f2:fe:62:78:c9:0d:d2:89:56:6d:
```

```
51:bf:39:6b:68:c1:a3:79:c8:91:fa:32:3e:2e:1b:50:61:90:
5c:ba:af:0b:5c:cb:ec:b8:38:e0:c3:3b:80:07:a7:fb:2d:02:
c1:39:3b:66:1b:b6:e1:74:f9:04:34:55:86:ba:58:4b:c6:28:
68:d4:e9:ae:98:f9:40:03:76:fe:b1:3c:f3:e3:00:82:ee:6c:
ca:03:17:cc
```

- The CSR must always be a PEM encoded PKCS#10 CSR. PKCS#10 CSRs encoded in DER cannot be processed by the web application.

- For cut-and-paste entries in the certificate request on the Swiss Government PKI web function, the CSR can easily be displayed by entering the command 'type':

```
C:\OpenSSL\bin>type samplecsr.pem
```


```
-----BEGIN CERTIFICATE REQUEST-----
MIICmTCCAYECAQAwOzELMAkGA1UEBhMCY2gxDjAMBgNVBAoMBWFkbWluMRwwGgYD
VQQDDBN3d3cuc2FtcGxlLmFkbWluLmNoMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAtvDEml9nUz/VAOXsUYoyqhFUcRa4JPHV2/DXxIn7UiAn7yZxgFuQ
gDD4jL20X8orm3Z++SkPDNLNC0oKM/OlAULbYDwAEdBucuPTMHT5q+QaBkrfV4wJ
NO7Hv7gSshPsbQIpeB7DlIxG1kKAOGOUl3vSGUJBDEfO6rHwPfW5fYgaZ06fk6Sn
fFpPZnh+SFnbzyo1EG/Y48wqntIgNKLbtFsQ27VBCGaHFfhUPvJO4XUP/+mb5gWa
KZIo2qT6wVlhs0e4NE69/ILhQ2mLD7248e24DPhONP/h/y9iGN6Ij5zcvRqFQ8mD
c6vi+qO5NnhDDhiy2gtDJ1JbSfPHu6VzjQIDAQABoBkwFwYJKoZIhvcNAQkHMQoM
CCoqKioqKioqMA0GCSqGSIb3DQEBBQUAA4IBAQCIrPnI5qCMexrCXpWeVcc/NS/Z
5CQO+9K4IKCV+8ZMLnz2AY6tIDL+C46adzWi6K7CLsW0EuPp1xF5DnjJSqenfmTy
LCbEVfiBAqF+f6jT2NSF8VU16JQFVh/zpLb8KZPY0v3jvwg4WFDSr8SP3sn1yCgj
+1ggSX09ljsdlC9UaPRUd9VwA24inEQy188zS+609YO4zS78R+Tgvp/c6y5f4nJt
i5pCvHP5I60LB/+R86m+Rs4Asfqjzy4F0CwweRyMYyf0ulyqMgRNTai47oGX+S4U
75tNfAwUBPhdarwoEvOGr9DCtS4P/orptYpKI5iNOAfaFUDL2AZbwp/CotsX
-----END CERTIFICATE REQUEST-----
```

Example 2: Creating a key/CSR in a single step

Keys and associated CSRs can also be created using a single command. It should be noted, however, that any existing key file saved under the specified name will be overwritten. If the data saved there is still needed, different names must be selected for the old and new key files.

With the command below, the files are named samplekey.pem and samplecsr.pem, as in the first example. The detailed questions and answers regarding the parameters are identical to those in example 1:

C:\OpenSSL\bin>**openssl req -nodes -new -newkey rsa:2048 -keyout samplekey.pem -out samplecsr.pem**

- After the command is entered, the dialogue is as follows:

```
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
........+++
.........................+++
writing new private key to 'samplekey.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]:ch
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:admin
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:www.sample.admin.ch
Email Address []:.
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:********
An optional company name []:.
```