Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

25.07.2024

Quick Guide

Klasse C SSL/TLS
Erstellung Schlüsselpaar und CSR-Files

Status: Freigegeben V1.0

Die Erstellung eines Certificate Signing Requests (CSR) wird in **zwei Schritten** ausgeführt.

Zuerst wird ein Schlüsselpaar erstellt und danach der eigentliche CSR generiert. Die Verfahren für diese Schritte sind je nach Server und verwendetem Tool etwas unterschiedlich. Die Dokumentation der Server und der Tools sollte darüber Auskunft geben. Nachstehend ist die CSR-Erstellung mithilfe des Tools openssl beschrieben.

Erstellung des Schlüsselpaares

Zuerst erstellt der Antragsteller auf seinem Server (z.B. Webserver) ein Schlüsselpaar (öffentlicher und privater Schlüssel) mit der Spezifikation '2048 bit RSA key encrypted by Tripple-DES':

openssl genrsa -out <zertifikatsname.key> 2048

- Das erzeugte Keyfile wird im folgenden Schritt als Input verwendet.

Erzeugen eines Certificate Signing Request (CSR)

Anschliessend erzeugt der Antragsteller auf seinem Server den CSR (Certificate Signing Request) zum Signieren eines Zertifikates. Dabei verwendet er das im ersten Schritt generierte Keyfile:

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

- Nach Eingabe dieses Befehls fragt das Tool verschiedenen Parameter ab. Die Werte, die dabei eingegeben müssen, sind im nachstehenden Beispiel detailliert beschrieben.

Beispiel 1: Generierung Key/CSR in separaten Schritten

In diesem ersten Beispiel werden die Schlüssel und der CSR in zwei separaten Schritten erstellt. Die Annahme ist, dass für den Server sample.admin.ch ein CSR erstellt werden soll.Zuerst werden die Schlüssel erzeugt. Das Keyfile wird samplekey.pem genannt:

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

- *Nach der Eingabe des Befehls quittiert das Tool die Ausführung:*

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

- *Die Fehlermeldungen am Schluss können ignoriert werden. Damit wurden die Schlüssel generiert und in der Datei samplekey.pem abgelegt. Nun wird mit diesen Daten der Certificate Signing Request erstellt. Dem CSR wird der Filename samplecsr.pem zugeordnet. Als Input dient das vorher generierte Keyfile samplekey.pem:*

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

- *Das Tool quittiert den Befehl mit einer Kurzinfo über die Informationen, die in der Folge abgefragt werden:*

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. -------

- Anschliessend werden die einzelnen Parameter abgefragt. Soll ein Wert leer gelassen werden, so muss bei der Abfrage ein Punk ('.') eingegeben werden:

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

- *Dieser Wert ist immer mit 'ch' auszufüllen. Die nächsten beiden Parameter werden leer gelassen, also mit '.' gefüllt:*

State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.

- *Der Parameter Organization Name wird für die Bundesverwaltung mit admin gefüllt. Organisational Unit Name bleibt leer:*

Organization Name (eg, company) [Internet Widgits Pty Ltd]:admin
Organizational Unit Name (eg, section) []:.

- *Im Feld Common Name wwird nun der FQDN (Fully Qualified Domain Name) des Servers angegeben. In unserem Beispiel ist dies http://www.sample.ch/:*

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

- *Das Feld Email Address muss unbedingt leer sein.*

Email Address []:.

- *Zum Schluss muss das Passwort spezifiziert werden, das später bei der Installation des Zertifikats verwendet wird:*

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

- *Die letzte Abfrage Optional Company Name wird leer gelassen.*

- *Damit wurde der CSR erfolgreich generiert. Die Datei lässt sich mit folgendem Befehl anzeigen:*

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

- *Der CSR muss immer als PEM encoded PKCS#10 CSR vorliegen. In DER encodierte PKCS#10 CSR, können von der Webapplikation nicht verarbeitet werden.*
- *Für die Eingabe in den Zertifikatsantrag auf der Web-Funktion der Swiss Government PKI via Cut&Paste kann der CSR einfach mit dem 'type' Befehl angezeigt werden:*

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-----

Beispiel 2: Erstellung Schlüssel/CSR in einem Schritt

Schlüssel und zugehöriger CSR können auch in einem einzigen Befehl erzeugt werden. Dabei ist zu beachten, dass ein bereits unter dem spezifizierten Namen vorhandenes Keyfile überschrieben wird. Sollte man die dort abgespeicherten Daten noch benötigen, muss sichergestellt werden, dass die Namen des alten und des neuen Keyfiles unterschiedlich gewählt werden.

Beim nachfolgenden Befehl werden die Dateien wie im ersten Beispiel mit samplekey.pem und samplecsr.pem benannt. Die detaillierten Fragen und die einzugebenden Antworten zu den Parametern sind identisch mit denjenigen in Beispiel 1:

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

- *Nach der Eingabe des Befehls läuft der Dialog wie folgt ab:*

```
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 []:.
```