Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication
Swiss Government PKI

25.07.2024

Guide rapide

Classe C SSL/TLS
Création de la paire de clés et du fichier CSR

Statut : Publié V1.0

La génération d'une demande de signature de certificat (CSR) s'effectue en **deux étapes**.

La première étape consiste à créer une paire de clés. La CSR est ensuite générée. Le déroulement de ces deux étapes est susceptible de varier selon le serveur et l'outil utilisés. Il convient donc de se référer à la documentation relative à ces derniers. La marche à suivre pour générer une CSR au moyen de l'outil OpenSSL est décrite ci-après.

Création d'une paire de clés

Pour commencer, le demandeur crée une paire de clés (clé publique et clé privée) sur son serveur (par ex. serveur web) avec la spécification «2048 bit RSA key encrypted by Tripple-DES»:

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

- Le fichier clé ainsi généré devra être utilisé comme entrée (<input>) lors de l'étape suivante.

Génération d'une Certificate Signing Request (CSR)

Le demandeur génère ensuite la CSR sur son serveur. Pour ce faire, il utilise le fichier clé créé lors de la première étape:

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

- Une fois cette commande saisie, l'outil demande de régler divers paramètres. Une description détaillée des éléments à saisir se trouve dans l'exemple qui suit.

Exemple 1: génération des clés et de la CSR en deux étapes

Dans ce premier exemple, les clés et la CSR sont générées lors de deux étapes distinctes. On suppose ici que la CSR doit être générée pour le serveur sample.admin.ch. On commence par créer les clés et on nomme le fichier clé samplekey.pem:

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

- Une fois la commande saisie, l'outil en confirme l'exécution:*:*

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

- Les messages d'erreur qui s'affichent à la fin peuvent être ignorés. Les clés sont ainsi générées et déposées dans le fichier samplekey.pem. Ces données serviront à générer la CSR. On attribue à la CSR le nom de fichier samplecsr.pem et utilise en entrée le fichier clé samplekey.pem généré précédemment:

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

- L'outil confirme la commande en indiquant les éléments qui seront ensuite requis:

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. -------

- L'outil demande ensuite d'entrer différents paramètres. Si un champ doit rester vide, il convient de saisir un point («.»):

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

- Il faut toujours entrer «ch» dans ce champ. Les deux paramètres suivants doivent rester vides, il faut donc saisir «.»:

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

- Pour le paramètre «Organization Name», il faut entrer «admin» pour l'administration fédérale. Le paramètre «Organisational Unit Name» reste vide:

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

- Dans le champ «Common Name», il convient d'indiquer le nom de domaine complet (Fully Qualified Domain Name, ou FQDN) du serveur. Dans notre exemple, il s'agit de http://www.sample.ch/:

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

- Le champ «Email Address» doit impérativement rester vide.

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 []:.

- Le dernier champ «Optional Company Name» reste vide.
- La CSR est maintenant générée. La commande suivante permet d'afficher le fichier:

```
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
```

- La CSR (PKCS#10) doit toujours être encodée au format PEM. Les CSR PKCS#10 encodées au format DER ne peuvent pas être traitées par l'application web.

- Pour saisir la CSR dans la fonction web de Swiss Governemnt PKI, il suffit de l'afficher en entrant la commande «type» puis de la copier-coller:

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-----

Exemple 2: génération des clés et de la CSR en une seule étape

Il est également possible de générer les clés et la CSR correspondante au moyen d'une seule commande. Il convient de noter que cette opération écrasera tout fichier clé qui existe déjà sous le nom indiqué. Si l'on a encore besoin des données qui y sont stockées, on veillera à choisir un autre nom pour le nouveau fichier clé.

Dans la commande qui suit, les fichiers sont nommés samplekey.pem et samplecsr.pem comme dans le premier exemple. Les différents paramètres demandés et les réponses à saisir sont les mêmes que dans l'exemple 1:

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

- Une fois la commande saisie, le processus se déroule comme suit:

```
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 []:.
```