Guide de génération du fichier « .csr » avec l'outil open SSL

Mise à jour

Version	Date	Nature de la révision	Page
01	21/07/2025	Première Rédaction	Toutes les pages

Ceci est un guide qui vous permet de générer un fichier CSR (Certificate Signing Request). Ce fichier est souvent requis lors de la demande d'un certificat SSL auprès d'une autorité de certification (CA).

Prérequis :

- Avoir **OpenSSL** installé sur votre machine.
- Disposer d'un **nom de domaine** pour lequel vous souhaitez générer le certificat SSL.
- Accès en ligne de commande.

Etape1 : Générer une clé privée (Private Key)

Cette clé est nécessaire pour la génération du CSR. Elle doit être conservée en toute sécurité.

- Générez la clé privée en utilisant la commande suivante :

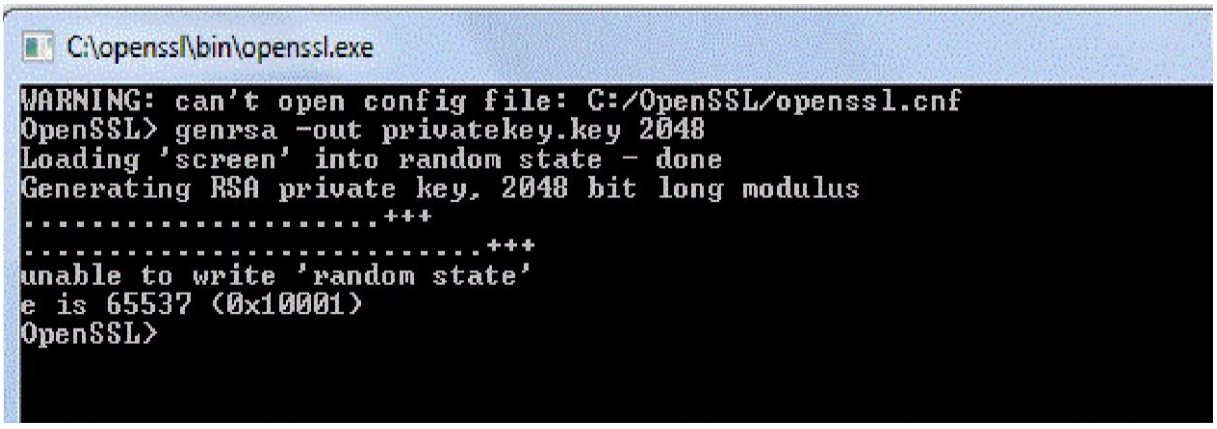
```
genrsa -out privatekey.key 2048
```

Note :

1- *2048 :* taille de la clé
2- *privatekey.key* **:** le fichier de clé privée généré

⇨ Un fichier *privatekey*.key est créé

Exemple :



Etape 2 : Générer le CSR à partir de la clé privée

Cette étape est de créer le CSR, qui est un fichier contenant les informations nécessaires à l'autorité de certification (CA) pour générer un certificat SSL.

- Générez le fichier « .csr » en utilisant la commande suivante **:**

```
req -new -key privatekey.key -out server.csr -sha256 -config openssl.cnf
```

Lorsque vous exécutez cette commande, un formulaire vous sera présenté pour saisir les informations suivantes :

Champ	Description
Country Name (2 letter code)	Code pays (ex : TN pour Tunisie)
State or Province Name	Gouvernorat (ex : TUNIS, Ariana)
Locality Name	Gouvernorat (ex : TUNIS, Ariana)
Organization Name	Raison Sociale de votre organisation
Organizational Unit Name	Département (ex : IT, Sécurité, etc.)
Common Name	FQDN / Nom de domaine complet (ex : www.exemple.tn)
Email	A laisser vide.

Note :

- *Le champ* Common Name (CN) *doit correspondre exactement au nom de domaine pour lequel vous demandez le certificat.*
- *Prière de ne pas utiliser l'algorithme Sha1 et exécuter les commandes telles que décrites dans ce guide.*
- *Le champ adresse email doit rester vide*
- *Les caractères suivants ne sont pas acceptés : é è ^ à < > ~ ! @ # $ % ^ * / \ ( ) ?.,&. En cas de doute, veuillez nous contacter par email sur l'adresse « assistance @ tuntrust.tn »*
- Si vous avez besoin de certificat **SAN (Subject Alternative Name)**, veuillez les ajouter dans un fichier de configuration)

Etape 3 : vérification de requête

Pour vérifier que le CSR a été généré correctement, vous pouvez afficher son contenu avec la commande suivante :

```
req -text -in nom de votre requête CSR
```

Cela vous montrera les détails du CSR, y compris l'algorithme utilisé (qui devrait être SHA-256).