tuntrust
Agence Nationale de Certification Electronique

Guide de génération de certificat SSL/TLS avec le protocole ACME

Mise à jour

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

Ce guide a pour objectif de décrire les étapes à suivre pour générer des certificats SSL/TLS à travers le protocole ACME.

Note importante : Une valeur aléatoire (numéro de série) vous sera transmise par l'adresse e-mail **ssl@tuntrust.tn.** Cette valeur devra être utilisée dans le champ SerialNumber dans l'étape 02.

I. Première méthode : http-01

Vous devez, en tant que client et demandeur d'un certificat SSL avec la méthode http-01 de l'ACME, réaliser les étapes suivantes dans l'ordre décrit.

N°	Etape	Description

1.	Téléchargement et installation de acme.sh	Sur votre serveur, exécutez de la commande suivante en tant que root:
		`git clone --depth 1 https://github.com/acmesh-official/acme.sh.git`
		`cd acme.sh`
		`./acme.sh --install --accountemail "votreadressemail" --nocron`
		Prière de changer le texte en jaune avec votre adresse email. Il est à noter que les notifications automatiques de TunTrust seront envoyées à cette adresse.
		Remarques :
		1. Les utilitaires système requis pour l'installation et l'utilisation de acme.sh sont : git, socat, openssl et curl.
		2. Le serveur sur lequel acme.sh sera installé doit disposer d'un accès à Internet afin de pouvoir télécharger les fichiers nécessaires.

2.	Création de la paire de clé et du CSR	Sur votre serveur, procédez au suivant : • Création du fichier de configuration /root/csr.conf `vim /root/csr.conf` • Insertion des informations dans le fichier Exemple :

N°	Etape	Description
		[req] default_bits = 2048 distinguished_name = req_distinguished_name req_extensions = req_ext prompt = no [req_distinguished_name] countryName = TN localityName = [GOUVERNORAT] organizationName = [RaisonSociale] commonName = [***.nomdedomaine1.tn] serialNumber = [**********] [req_ext] subjectAltName = @alt_names [alt_names] DNS.1 = ***.nomdedomaine1.tn DNS.2 = ***.nomdedomaine2.tn *Prière de changer le texte en jaune avec les informations de votre entreprise. Exemple : GOUVERNORAT = ARIANA et mettre la valeur reçue par email dans le champ SerialNumber.* • Création du CSR *Prière de remplacer le texte en jaune avec le nom du fichier de votre CSR.* openssl req -new -config /root/csr.conf -newkey rsa:2048 -nodes \ -keyout /root/***.key -out /root/***.csr
3.	Ajout des noms de domaines dans le serveur DNS	Si votre nom de domaine n'est pas associé à une adresse IP publique, veuillez l'ajouter dans le serveur DNS.
4.	Envoi de la demande d'enregistrement du compte ACME	Sur votre serveur, exécutez la commande suivante : *Prière de remplacer le texte en jaune avec le nom du fichier de votre CSR.* /root/.acme.sh/acme.sh --sign-csr --csr /root/***.csr -w /var/www/html --insecure --force --debug 3 -ak 2048 --server https://acme.tuntrust.tn

N°	Etape	Description
5.	Envoi du request ID	• Envoyez le request ID obtenu dans l'étape précédente à l'adresse email « ssl @ tuntrust.tn » pour approbation de la part de Tuntrust • Une fois la demande d'enregistrement du compte ACME est approuvée par Tuntrust, un email vous sera envoyé pour le passage à l'étape 6. **Note** : Pour les certificats de type SAN, vous êtes invités à communiquer un seul request ID pour l'approbation de votre compte ACME.
6.	Lancement de la commande de génération du certificat	Sur votre serveur, exécutez la commande suivante : *Prière de remplacer le texte en jaune avec le nom du fichier de votre CSR.* `/root/.acme.sh/acme.sh --sign-csr --csr /root/***.csr -w /var/www/html --insecure --force --debug 3 -ak 2048 --server https://acme.tuntrust.tn`

Dans le cas où vous allez renouveler votre certificat (initialement obtenu avec cette méthode) suite à son expiration, vous devez exécuter les étapes 02 et 06 seulement. Toutefois, prière de prendre en considération les remarques suivantes :

1. Lors de la création du CSR, prière d'insérer dans le champ *serialNumber* la valeur aléatoire que vous a été envoyée par l'adresse email « expiration @ tuntrust.tn ».
2. Pour les certificats de type SAN, vous êtes invités à utiliser une **seule** valeur aléatoire à insérer dans le champ *serialNumber*.

II. Deuxième méthode dns-01

Vous devez, en tant que client et demandeur d'un certificat SSL avec la méthode dns-01 de l'ACME, réaliser les étapes suivantes dans l'ordre décrit.

N°	Etape	Description

1.	Téléchargement et installation de acme.sh	Sur votre serveur, exécutez la commande suivante en tant que root:
		`git clone --depth 1 https://github.com/acmesh-official/acme.sh.git`
		`cd acme.sh`
		`./acme.sh --install --accountemail "votreadressemail" --nocron`
		Prière de changer le texte en jaune avec votre adresse email. Il est à noter que les notifications automatiques de TunTrust seront envoyées à cette adresse.
		Remarques :
		1. Les utilitaires systèmes nécessaires à l'installation et l'utilisation de acme.sh sont : git, socat, openssl et curl.

<table>
<tr><th>N°</th><th>Etape</th><th>Description</th></tr>
<tr><td></td><td></td><td>2. Le serveur sur lequel acme.sh sera installé doit disposer d’un accès à Internet afin de pouvoir télécharger les fichiers nécessaires.</td></tr>
<tr><td>2.</td><td>Création de la paire de clé et du CSR</td><td>Sur votre serveur, procédez au suivant :
• Création du fichier de configuration /root/csr.conf
vim /root/csr.conf
• Insertion dans ce fichier le contenu ci-dessous
Exemple :
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no
[req_distinguished_name]
countryName = TN
localityName = [GOUVERNORAT]
organizationName = [RaisonSociale]
commonName = [***.nomdedomaine1.tn]
serialNumber =
[**********]
[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = ***.nomdedomaine1.tn
DNS.2 = ***.nomdedomaine2.tn
Prière de changer le texte en jaune avec les informations de votre entreprise. Exemple : GOUVERNORAT = ARIANA et mettre la valeur reçue par email dans le champ SerialNumber..
• Création du CSR
Prière de remplacer le texte en jaune avec le nom du fichier de votre CSR.
openssl req -new -config /root/csr.conf -newkey rsa:2048 -nodes -keyout /root/***.key -out /root/***.csr</td></tr>
</table>

<table>
<tr><th>N°</th><th>Etape</th><th>Description</th></tr>
<tr><td>3.</td><td>Ajout des noms de domaines dans le serveur DNS</td><td>Si votre nom de domaine n’est pas associé à une adresse IP publique, veuillez l’ajouter dans le serveur DNS.</td></tr>
<tr><td>4.</td><td>Envoi de la demande d’enregistrement du compte ACME</td><td>Sur votre serveur, exécutez la commande suivante :

Prière de remplacer le texte en jaune avec le nom du fichier de votre CSR.

/root/.acme.sh/acme.sh --sign-csr --csr /root/***.csr --dns --yes-I-know-dns-manual-mode-enough-go-ahead-please --insecure --force --debug 3 -ak 2048 --server https://acme.tuntrust.tn</td></tr>
<tr><td>5.</td><td>Envoi du request ID</td><td>• Envoyez le request ID obtenu dans l’étape précédente à l’adresse email « ssl @ tuntrust.tn» pour approbation de la part de Tuntrust
• Une fois la demande d'enregistrement du compte ACME approuvée par Tuntrust, un email vous sera envoyé pour le passage à l’étape 6.

Note : Pour les certificats de type SAN, vous êtes invités à communiquer un seul request ID pour l’approbation de votre compte ACME.</td></tr>
<tr><td>6.</td><td>Lancement de la commande d’obtention de(s) challenge(s)</td><td>Sur votre serveur, exécutez la commande suivante :

Prière de remplacer le texte en jaune avec le nom du fichier de votre CSR.

/root/.acme.sh/acme.sh --sign-csr --csr /root/***.csr --dns --yes-I-know-dns-manual-mode-enough-go-ahead-please --insecure --force --debug 3 -ak 2048 --server https://acme.tuntrust.tn

Vous allez obtenir une valeur aléatoire comme résultat de cette commande. Vous allez l’utiliser dans l’étape suivante.</td></tr>
<tr><td>7.</td><td>Insertion de(s) challenge(s) dans le serveur DNS</td><td>Sur le serveur DNS, procédez à l’ajout d’un enregistrement DNS de type TXT avec les spécifications suivantes :

<table><tr><td>Nom</td><td>Type</td><td>Valeur</td></tr><tr><td>_acme-challenge.***.nomdedomaine1.tn</td><td>TXT</td><td>challenge</td></tr></table>Prière de remplacer le texte en jaune avec le challenge que vous avez obtenu lors de l’étape précédente.</td></tr>
</table>

N°	Etape	Description
		Si votre CSR contient plus qu'un seul nom de domaine, prière d'ajouter un enregistrement DNS de type TXT contenant le challenge pour chaque nom de domaine.
8.	Lancement de la commande de génération du certificat	Sur votre serveur, exécutez de la commande suivante : /root/.acme.sh/acme.sh --renew --domain ***.nomdedomaine1.tn --yes-I-know-dns-manual-mode-enough-go-ahead-please --insecure --force --debug 3 -ak 2048 --server https://acme.tuntrust.tn

Dans le cas où vous allez renouveler votre certificat (initialement obtenu avec cette méthode) suite à son expiration, vous devez exécuter les étapes de 02, 06, 07 et 08 seulement. Toutefois, prière de prendre en considération les remarques suivantes :

1. Lors de la création du CSR, prière d'insérer dans le champ *serialNumber* la valeur aléatoire que vous a été envoyée par l'adresse email « expiration @ tuntrust.tn ».
2. Pour les certificats de type SAN, vous êtes invités à utiliser une **seule** valeur aléatoire à insérer dans le champ *serialNumber*.