1. Le protocole ACME pour la délivrance et la révocation des certificats SSL/TLS

1.1. Ressources

- https://www.ssl.com/fr/guide/ssl-tls-d%C3%A9livrance-et-r%C3%A9vocation-de-certificat-avec-acme/

1.2. Préentation

ACME (Automated Certificate Management Environment) est un protocole standard pour la validation de domaine automatisée et l'installation de certificats X.509, documenté dans IETF RFC8555.

ACME et une norme bien documentée avec de nombreux logiciels open source implémentations client et permet * simplement de fournir à des des sites Web ou Appareils IoT (modems, routeurs) des certificats numériques de confiance publique ou privée et maintenez ces certificats à jour au fil du temps.

1.3. Installation de ACME

Lien : https://wiki.maxcorp.org/acme-sh/

```
wget -O - https://get.acme.sh | sh
```

L'installateur effectuera 3 actions:

- Créer le dossier .acme.sh dans le répertoire personnel ($HOME): ~/.acme.sh/. Tous les certificats seront placés dans ce dossier. Ce dossier contient le fichier acme.sh
- Créer un alias pour: acme.sh=~/.acme.sh/acme.sh.
- Créez un job cron quotidien pour vérifier et renouveler les certificats si nécessaire.

Exemple d'entrée Cron:

```
crontab -e
```

```
0 0 *  *  *  " /home/user/.acme.sh " /acme.sh --cron --home " /home/utilisateur/.acme.sh "  > / dev / null
```

Après l'installation, fermer le terminal actuel et le rouvrir pour que l'alias soit actif.

acme.sh is using ZeroSSL as default CA now. [Thu Nov 16 08:48:34 UTC 2023] Please update your account with an email address first. [Thu Nov 16 08:48:34 UTC 2023] acme.sh –register-account -m my@example.com [Thu Nov 16 08:48:34 UTC 2023] See: https://github.com/acmesh-official/acme.sh/wiki/ZeroSSL.com-CA

1.4. Enregistrement de son compte auprès de ZeroSSL.com CA

- Lien : https://github.com/acmesh-official/acme.sh/wiki/ZeroSSL.com-CA

ACME utilise maintenant ZeroSSL. Il est possible d'émettre un nombre illimité de certificat valable TLS/SSL valables 90 jours. Il faut au préalable soit enregistrer son adresse de courriel soit se créer un compte. * Enregistrer son adresse de courriel

1.5. Générer un certificat SSL

```
acme.sh --issue -d exemple.fr -w /var/www/html/
```

- -d exemple.fr ⇒ domaine principal pour lequel vous souhaitez émettre le certificat : au moins un domaine doit être défini
- w /var/www/html ⇒ site Web de publication
- Les certs seront placés dans ~/.acme.sh/example.com/
- Les certificats seront renouvelés automatiquement tous les 60 jours.

1.6. Installer le certificat

Utilisation de la commande suivante pour installer / copier le certificat sur le serveur Web Apache dans les dossiers cibles.

```
acme.sh --install-cert -d example.com \
--cert-file /path/to/certfile/in/apache/cert.pem \
--key-file /path/to/keyfile/in/apache/key.pem \
--fullchain-file /path/to/fullchain/certfile/apache/fullchain.pem \
--reloadcmd      " service apache2 force-recharge "
```

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/certificat/acme/accueil

Last update: **2023/11/16 08:57**