Création certificat SSL

sécurité, SSL

Création clé privée

Pour créer une clé privée RSA (ici 4096 bits) :

```
openssl genrsa -out example.rsa.key 4096
```

Pour créer une clé privée

```
openssl ecparam -genkey -name secp384r1 | openssl ec -out example.ec.key
```

Création CSR

```
sudo openssl req -new -key /etc/ssl/private/example.ec.key -out example.csr
-sha256
```

Let's Encrypt

```
sudo certbot-auto certonly --server
https://acme-v02.api.letsencrypt.org/directory --manual --csr
/etc/letsencrypt/grohub.pro/grohub.pro.csr --cert-path
/etc/letsencrypt/grohub.pro/grohub.pro.crt --register-unsafely-without-email
```

Diffie-Hellman key exchanges

```
openssl dhparam -out /etc/ssl/dhparam.pem 4096
```

TLS Ticket

```
openssl rand 48 > /etc/ssl/ticket.key
```

Déchiffrer la clé

```
openssl rsa -in server.key -out decrypted.key
```

Générer un certificat auto-signé

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/domain-selfsigned.key -out /etc/ssl/certs/domain-
selfsigned.crt
```

Liens

- deploying tls the hard way
- howto SSL
- configurer https sur Nginx
- Openssl command sheatsheet
- Cryptcheck

From:
https://wiki.grohub.org/ - **Grohub wiki**

Permanent link:
https://wiki.grohub.org/infrastructure/securite/ssl/certificat-creation

Last update: **27/04/2023 07:47**