OpenSSL - Commandes Utiles

Demande de certificat

Générer une demande de certificat avec la création d'une clé privée RSA de 2048 bits

```
openssl req -new -newkey rsa:2048 -nodes -sha256 -keyout mykey.key -out mycsr.csr -subj "/C=US/ST=Ohio/L=Columbus/O=Widgets Inc/OU=Some Unit/CN=myserver.com"
```

Générer une demande de certificat avec la création d'une clé privée ECDSA de 256 bits.

```
openssl req -newkey ec:<(openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256) -nodes -sha256 -keyout mykey.key -out mycsr.csr -subj "/C=US/ST=Ohio/L=Columbus/O=Widgets Inc/OU=Some Unit/CN=myserver.com"
```

Générer un certificat auto-signé

```
openssl req -newkey rsa:2048 -nodes -sha256 -keyout mykey.key -x509 -days 365 -out mycrt.crt -subj "/C=US/ST=Ohio/L=Columbus/O=Widgets Inc/OU=Some Unit/CN=myserver.com"
```

Générer une demande de certificat à partir d'une clé et d'un certificat existants

```
openssl x509 -x509toreq -in mycrt.crt -signkey mykey.key -out mycsr.csr
```

Gestion des clés

Générer une nouvelle clé RSA

```
openssl genrsa 2048 > mykey.key
```

Générer une nouvelle clé ECC

```
openssl ecparam -name prime256v1 -genkey > mykey.key
```

Enlever la passphrase d'une clé privée

```
openssl rsa -in mykey-with-passphrase.key -out mykey.key
```

Vérification des clés, des demandes et des certificats

Vérifier une clé

```
openssl rsa -noout -text -check -in mykey.key
```

Vérifier une demande

```
openssl req -noout -text -verify -in mycsr.csr
```

Vérifier un certificat

```
openssl x509 -noout -text -in mycrt.crt
```

Vérifier que la demande et le certificat sont bien associés à une clé :

- Le résultat des commandes doit retourner la même valeur

```
openssl x509 -noout -modulus -in mycrt.crt
openssl req -noout -modulus -in mycsr.csr
openssl rsa -noout -modulus -in mykey.key
```

Afficher le contenu d'un certificat en format PKCS#7:

```
openssl pkcs7 -print_certs -in www.server.com.p7b
```

Afficher le contenu d'un certificat et d'une clé en format PKCS#12:

```
openssl pkcs12 -info -in www.server.com.pfx
```

Contrôler une connection SSL et afficher tous les certificats intermédiaires:

```
openssl s_client -connect www.server.com:443
```

Conversion des certificats

Conversion d'un fichier PKCS#12 vers le format PEM (clé privée + certificat + chaine de certification)

```
openssl pkcs12 -nodes -in www.server.com.pfx -out www.server.com.crt
```

Conversion du format PEM vers le format PKCS#12:

```
openssl pkcs12 -export -in www.server.com.crt -inkey www.server.com.key -out www.server.com.pfx
```

Conversion du format PKCS#7 (.p7b .p7c) vers le format PEM:

```
openssl pkcs7 -print_certs -in www.server.com.p7b -out www.server.com.crt
```

Conversion du format PEM vers le format PKCS#7:

```
openssl crl2pkcs7 -nocrl -certfile www.server.com.crt -out www.server.com.p7b
```

Conversion du format DER vers le format PEM:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Références

- **https://www.kinamo.fr/base-de-connaissanse/openssl-commandes-utiles**

Revision #24
Created 30 January 2024 20:21:19 by NoNo
Updated 23 February 2024 08:09:51 by NoNo