

openssl

OpenSSL cryptographic toolkit.

- Generate a 2048bit RSA private key and save it to a file:

```
openssl genrsa -out {{filename.key}} 2048
```

- Generate a certificate signing request to be sent to a certificate authority:

```
openssl req -new -sha256 -key {{filename.key}} -out {{filename.csr}}
```

- Generate a self-signed certificate from a certificate signing request valid for some number of days:

```
openssl x509 -req -days {{days}} -in {{filename.csr}} -signkey {{filename.key}}  
-out {{filename.crt}}
```

- Display the start and expiry dates for a domain's certificate:

```
openssl s_client -connect {{host}}:{{port}} 2>/dev/null | openssl x509 -noout -  
dates
```

- Display the certificate presented by an SSL/TLS server:

```
openssl s_client -connect {{host}}:{{port}} </dev/null
```

- Display the complete certificate chain of an HTTPS server:

```
openssl s_client -connect {{host}}:443 -showcerts </dev/null
```