Openssl

Checking certificates and keys

Checking Using OpenSSL

If you need to check the information within a Certificate, CSR or Private Key, use these commands. You can also check CSRs and check certificates using our online tools.

Check a Certificate Signing Request (CSR)
openssl req -text -noout -verify -in CSR.csr

Check a private key
openssl rsa -in privateKey.key -check

Check a certificate
openssl x509 -in certificate.crt -text -noout

Check a PKCS#12 file (.pfx or .p12)
openssl pkcs12 -info -in keyStore.p12

Check the fingerprint of a certificate.

Get SHA-1 fingerprint:

openssl x509 -noout -in certificate.pem -fingerprint -sha1

Get SHA-256 fingerprint:

openssl x509 -noout -in certificate.pem -fingerprint -sha256

You can check if an SSL certificate matches a Private Key by using the 2 easy commands below.

For your SSL certificate: openssl x509 -noout -modulus -in <file>.crt | openssl md5
For your RSA private key: openssl rsa -noout -modulus -in <file>.key | openssl md5

Create a .pfx file

Create a .pfx file from certificate and private key:

openssl pkcs12 -export -out domain_name.pfx -inkey privkey.pem-in fullchain.pem

Extract certificates from .pfx file

The *.pfx file is in PKCS#12 format and includes both the certificate and the private key.

export the private key: openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
export the certificate: openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
remove the passphrase from the private key: openssl rsa -in key.pem -out server.key