Alcuni suggerimenti per il troubleshooting con openssl

Verificare che la chiave pubblica, la certificate sign request e quella privata corrispondano

Bisogna verificare in effetti che le chiavi abbiano lo stesso modulo. Per praticità di comparazione, ne calcoleremo il valore MD5:

```
$ openssl x509 -noout -modulus -in server.pem | openssl md5
$ openssl rsa -noout -modulus -in server.key | openssl md5
$ openssl req -noout -modulus -in server.csr | openssl md5
```

Verificare la correttezza della CA-Chain

```
$ openssl verify -CAfile cachain.pem servercaert.pem
```

Se la catena non è completa viene visualizzato un errore del tipo: “error 20 at 0 depth lookup:unable to get local issuer certificate”

How to view and download and verify server SSL/TLS certificate and connection

```
$ openssl s_client -connect host:port
```

Famous “over SSL” protocols table

```
Protocol    Port
https    443/tcp
nntps    563/tcp
ldaps    636/tcp
ftps-data    989/tcp
telnets  992/tcp
imaps    993/tcp
ircs     994/tcp
pop3s    995/tcp
ssmtp    465/tcp
```

To verify connection parameters you need at least to specify a CA certificate, at most a client secret key and public certificate.

```
$ openssl s_client -CAfile /etc/ssl/certs/AddTrust_External_Root.pem -
```

```
connect host:443
```

```
$ openssl s_client -CAfile /etc/ssl/certs/AddTrust_External_Root.pem -cert
/my/cert.pub -key /my/key.priv -connect host:443
```

Successful connection ends with:

```
Verify return code: 0 (ok)
```

Verificare date di validita' e altri parametri di un certificato usato da un server non web

Alcuni esempi possono essere server ldap, imap, pop, ecc....

```
openssl s_client -connect <server fqdn>:<port> | openssl x509 -in - -text
```

dove <port> può essere anche espresso in notazione well known: ldaps, pops, imaps, ecc...