Alcuni suggerimenti per il troubleshooting con OpenSSL e certutil

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

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

Procedura per chiavi a crittografia ellittica:

```
$ openssl x509 -noout -in server.pem -pubkey | openssl md5
$ openssl pkey        -in server.key -pubout | openssl md5
$ openssl req  -noout -in server.csr -pubkey | openssl md5
```

Procedura per chiavi RSA:

```
$ 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 -show_chain -CAfile RootCACert.pem -CAfile
IntermediateCACert.pem ServerCert.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”

Su Windows command line o PowerShell, allo stesso scopo, è possibile usare il comando

```
certutil -verify servercert.pem cachain.pem
```

oppure se avete installato OpenSSL

```
openssl verify -CAstore org.openssl.winstore:// -show_chain -CAfile
RootCACert.pem -CAfile IntermediateCACert.pem ServerCert.pem,
```

che mostra invece i vari step dal leaf certificate fino alla root.

Come visualizzare, scaricare e verificare il certificato server

SSL/TLS e la connessione

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

Tabella di protocolli well-known che usano SSL:

```
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
```

Per verificare i parametri di connessione è necessario specificare almeno un certificato CA, al massimo una chiave segreta client e un certificato pubblico.

```
$ openssl s_client -CAfile /etc/ssl/certs/root_ca.pem -connect host:443
```

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

Una connessione riuscita restituisce alla fine:

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

Verificare date di validità 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...

Credits: Daniele Albrizio, Alberto Bianco per alcune info su Windows