Procedura per OpenSSL

Per effettuare la richiesta del certificato, bisogna generare la chiave privata e la richiesta di certificato.

L'esempio qua sotto usa *dummy* come nome del server da registrare.

- Creare un file di configurazione openssl.cnf possibilmente diverso da quello di sistema (*/etc/ssl/openssl.cnf*).

WARNING: fare degli errori nel file di configurazione openssl principale puo' corrompere il corretto funzionamento del sistema su cui si sta generando la richiesta di certificato anche e non limitatamente alla risoluzione dei nomi a DNS.

Usare pertanto i valoro sotto riportati:

Scarica il file openssl.cnf di esempio.

```
[ policy_anything ]
countryName     = supplied
commonName      = supplied

[ req ]
default_bits = 256
default_keyfile = privkey.pem
default_md = sha256
default_key = ec
distinguished_name  = req_distinguished_name
req_extensions      = v3_req

[ req_distinguished_name ]
commonName          = Server FQDN:
commonName_default      = YourServerName.units.it
countryName         = Country Name (2 letter code)
countryName_default     = IT
countryName_min         = 2
countryName_max         = 2

[ v3_req ]
subjectAltName = @alt_names

[ alt_names ]
# aggiungere gli eventuali altri nomi a dns per cui si vuole che il
certificato sia valido:
DNS.1   = dummy1.units.it
DNS.2   = dummy2.units.it
DNS.3   = dummy3.units.it
```

- Modificare il file alla sezione

```
[ alt_names ]
# aggiungere gli eventuali altri nomi a dns per cui si vuole che il
certificato sia valido:
DNS.1   = dummy2.units.it
DNS.2   = dummy2.univ.trieste.it
DNS.3   = dummy.univ.trieste.it
```

- Se si usa un solo nome FQDN per il certificato, rimuovere le sezioni `[ v3_req ]` e `[ alt_names ]`.
- Generare la chiave privata

```
# openssl ecparam -genkey -name prime256v1 -noout -out privkey.pem
```

 Con questa chiave usare sempre la CA chain a curva ellittica (ECC/ecdsa). Maggiori informazioni dopo la procedura di firma.

- Quindi generare il csr rispondendo alle domande come segue:

 l'opzione *nodes* non cifra simmetricamente la chiave privata in modo da poterla usare nei vari daemon (apache, nginx, ecc..) senza dover inserire interattivamente la passphrase per la decodifica ad ogni avvio di un nuovo processo o salvarla in chiaro nel sistema.

```
# openssl req -config openssl.cnf -new -key privkey.pem -out dummy.csr
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Server FQDN: [dummy.units.it]:
Country Name (2 letter code) [IT]:
```

Nella directory corrente viene generato un file dal nome ***privkey.pem*** che è la chiave privata a cui vanno dati i permessi minimi per essere usata dal servizio (server web, di posta elettronica, ecc.).

 Se il file esiste già, viene sovrascritto senza avviso.

Questo file ***privkey.pem*** deve rimanere **SEGRETO**.

Nella directory corrente viene anche generato un file dal nome ***dummy.csr*** che contiene la richiesta di certificato.

Rinnovo

Se si possiede già il file della chiave privata (ad es. in caso di **rinnovo**), il comando tipo da dare è

```
# openssl req -config openssl.cnf -key privkey.pem -out dummy.csr -new
```

Se si ritiene che la **chiave privata** sia stata **compromessa** o usa crittografia troppo debole, il comando tipo da dare è

```
 openssl req -config openssl.cnf -new -keyout <nome-del-file-che-conterrà-la-chiave-privata> -out <nome-del-file-che-conterrà-la-richiesta-di-certificato> -nodes
```

- Continuare con la procedura di firma.