Creazione di certificati autofirmati per protocolli https mediante OpenSSL

Ho eseguito questa procedura sul mio raspberry nella mia rete domestica, utilizzabile solo in locale.

---

1. Prima di tutto abilitiamo il modulo Apache con **a2enmod ssl**

```
root@raspberrypi:/home/pi# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL a
nd create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

2. Generiamo una chiave privata con openSSL con **openssl genrsa -out molinari.key**

```
root@raspberrypi:/home/pi#  openssl genrsa -out molinari.key
Generating RSA private key, 2048 bit long modulus
.....+++++
...................+++++
e is 65537 (0x010001)
```

3. Generiamo la richiesta per il certificato con

openssl req -new -key molinari.key -out molinari.csr

poi compiliamo i campi richiesti con le informazioni per il certificato

```
root@raspberrypi:/home/pi#  openssl req -new -key molinari.key -out m
olinari.csr
You are about to be asked to enter information that will be incorpora
ted
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.
-----
Country Name (2 letter code) [AU]:IT
State or Province Name (full name) [Some-State]:Italy
Locality Name (eg, city) []:Milan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:molinari
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:molinari.com
Email Address []:pietro@molinari.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@raspberrypi:/home/pi#
```

4. Generiamo il certificato con

openssl x509 -req -days 365 -in molinari.csr -signkey molinari.key -out molinari.crt

```
root@raspberrypi:/home/pi#  openssl x509 -req -days 365 -in molinari.
csr -signkey molinari.key -out molinari.crt
Signature ok
subject=C = IT, ST = Italy, L = Milan, O = molinari, CN = molinari.co
m, emailAddress = pietro@molinari.com
Getting Private key
root@raspberrypi:/home/pi#
```

5. Nella directory troveremo i tre nuovi file: la chiave privata, la richiesta del certificato e il certificato

```
-rw-r--r-- 1 root root    1257 mar 14 18:39 molinari.crt
-rw-r--r-- 1 root root    1029 mar 14 18:38 molinari.csr
-rw------- 1 root root    1675 mar 14 18:29 molinari.key
```

6. Spostiamo chiave e certificato in /etc/ssl/certs/

```
root@raspberrypi:/home/pi#  mv molinari.crt /etc/ssl/certs/
root@raspberrypi:/home/pi# mv molinari.key /etc/ssl/certs/
```

7. Apriamo il file di configurazione di Apache e lo modifichiamo

nano /etc/apache2/sites-enabled/000-default.conf

Inseriamo:

<VirtualHost *:443>
ServerName molinari.com
ServerAlias www.molinari.com
DocumentRoot /var/www/html
SSLEngine on
SSLCertificateFile /etc/ssl/certs/molinari.crt
SSLCertificateKeyFile /etc/ssl/certs/molinari.key
</VirtualHost>

```
  GNU nano 2.7.4     File: /etc/apache2/sites-enabled/000-default.conf


        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For examp
        # following line enables the CGI configuration for this host onl
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

 <VirtualHost *:443>
        ServerName              molinari.com
        ServerAlias             www.molinari.com
        DocumentiRoot           /var/www/html
        SSLEngine               on
        SSLCertificateFile      /etc/ssl/certs/molinari.crt
        SSLCertificateKeyFile   /etc/ssl/certs/molinari.key
</VirtualHost>
```

8. Modifichiamo il file **hosts** per poter raggiungere il nostro sito con il dominio fasullo

nano /etc/hosts

inseriamo accanto a localhost:

molinari.com www.molinari.com

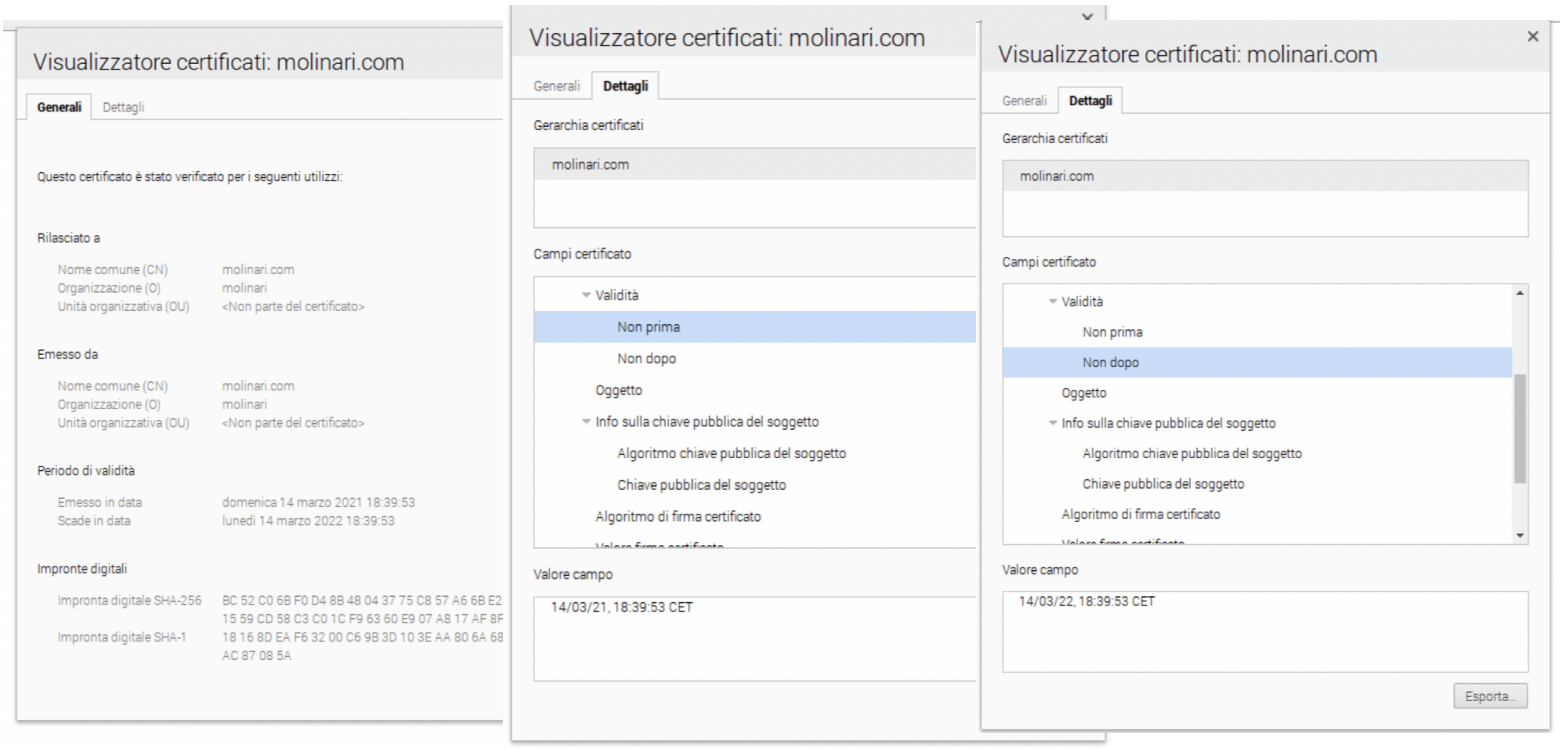
```
  GNU nano 2.7.4                                File: /etc/hosts

127.0.0.1       localhost molinari.com www.molinari.com
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

127.0.1.1       raspberrypi
```

9. Facciamo ripartire il server con **systemctl restart apache2**

10. Ora possiamo visualizzare i nostri certificati sul browser e la loro validità



NB: il browser non riconoscerà la sicurezza della connessione perché il certificato utilizzato è autofirmato e non rilasciato da una CA