

# Certificati per server windows (IIS) con Sectigo

Procedura testata e funzionante con un server Windows 2016 e IIS 10

- 1) da un qualsiasi computer unix con openssl (provata con client macOSX 10.13.6) creare la CSR e la rispettiva chiave privata con openssl:

```
openssl req -newkey rsa:3072 -nodes -subj "/CN=handyman.unito.it" -out req-  
handyman.unito.it.csr -keyout key-handyman.unito.it.pem
```

- 2) richiesta di certificato tramite portale web Sectigo aggiungendo eventuali alternative names e la mail dell'external requester tutto il resto lasciato il default

- 3) scaricare il seguente formato tra quelli disponibili nella email di Sectigo con oggetto "Enrollment Successful - Your SSL certificate is ready":

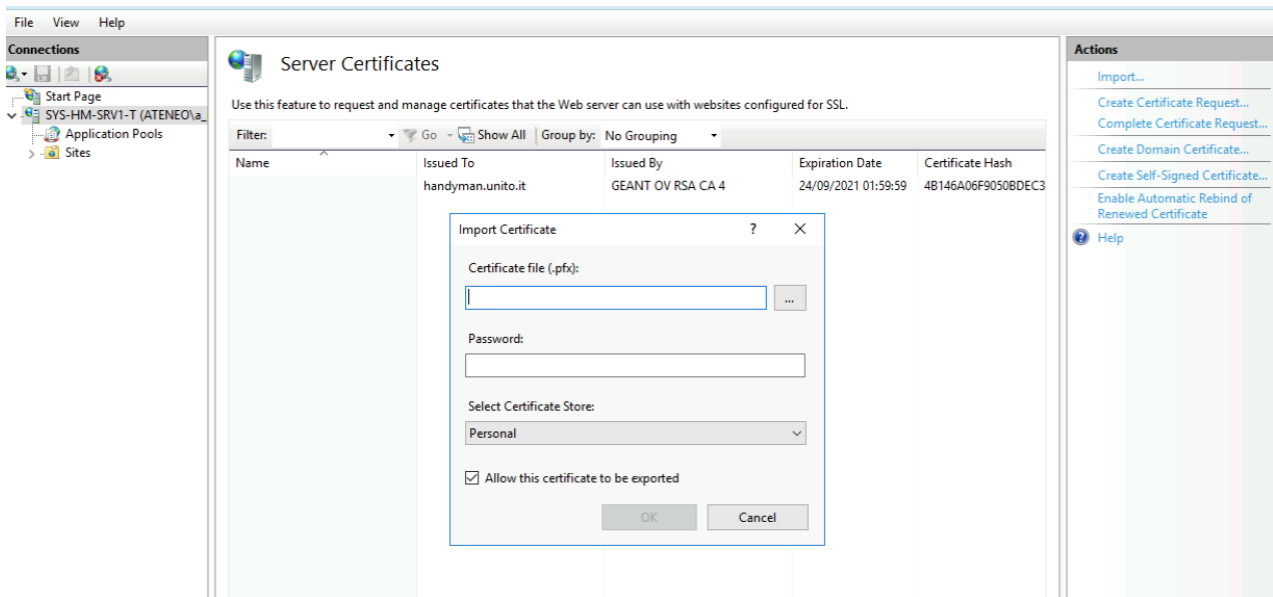
as Certificate only, PEM encoded: <https://cert-manager.com/customer/GARR/ssl?action=download&sslId=2009747&format=x509CO>

- 4) unire chiave privata e certificato in un unico file PFX con openssl:

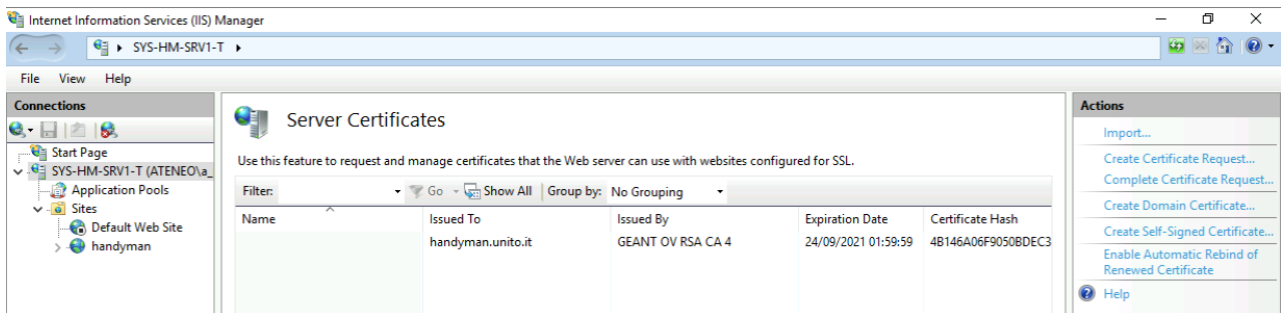
```
openssl pkcs12 -export -out cert-handyman.unito.it.pfx -inkey key-  
handyman.unito.it.pem -in handyman_unito_it_cert.cer
```

(nota: richiede la creazione di una passphrase)

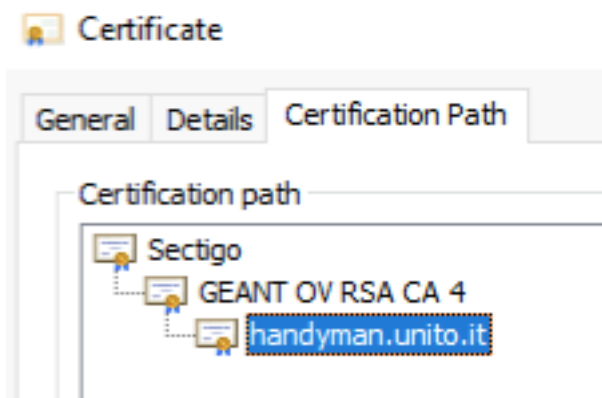
- 5) dal server IIS importare il certificato PFX (vedi immagini allegate)



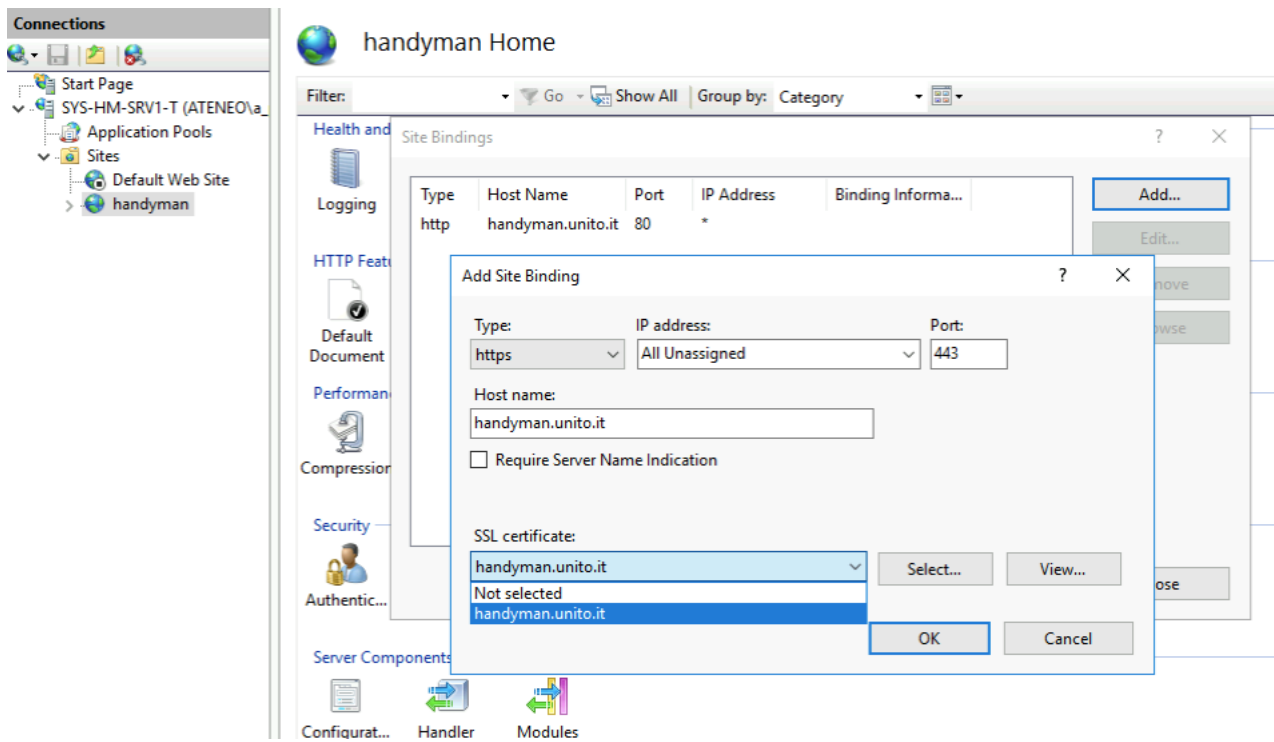
6) il certificato è installato sul server



e la chain è corretta



7) abilitare https sul sito e selezionare il nuovo certificato



8) FINE



USERTrust RSA Certification Authority

↳ GEANT OV RSA CA 4

↳ handyman.unito.it



### handyman.unito.it

Emesso da: GEANT OV RSA CA 4

Scade: venerdì 24 settembre 2021 01:59:59 Ora legale dell'Europa centrale

✔ Il certificato è valido

#### ▼ Dettagli

**Nome soggetto** \_\_\_\_\_

**Paese** IT

**Codice postale** 10124

**Località** Torino

**Indirizzo** Via Giuseppe Verdi 8

**Società** Università degli Studi di Torino

**Nome comune** handyman.unito.it

**Nome emittente** \_\_\_\_\_

**Paese** NL

**Società** GEANT Vereniging

**Nome comune** GEANT OV RSA CA 4

OK