



## REQUISITI PER LA RICHIESTA CERTIFICATI SSL

Requisiti per la richiesta dei  
certificati SSL per i server di Sectigo



### TEORIA

## Come funziona il processo di emissione di certificati SSL server

I certificati SSL si basano su due elementi: una catena di certificazione pubblica che parte da un'entità nota e verificata a priori (Certification Authority, CA) e arrivano all'entità da certificare (il server, in questo caso) ed un elemento (chiave privata) noto esclusivamente al server stesso, con il quale vengono codificati i dati in transito che possono essere autenticati e decifrati da parte di chiunque sia in possesso della corrispondente catena pubblica.

Avremo quindi tre elementi da prendere in considerazione:

Catena di certificazione (**CHAIN**)

Certificato server (**CERT**)

Chiave privata (**KEY**)



## VALIDITA'

### 1 anno

Per limitare la possibilità che un'intrusione sui server comporti la perdita di riservatezza della chiave privata, i certificati SSL hanno un termine massimo di validità. Tale termine è stato più volte accorciato, ed è attualmente (novembre 2021) raccomandato sia massimo di un anno. Certificati di validità superiore ad un anno non vengono ritenuti sicuri da parte dei produttori di browser (Google, Mozilla), né emessi dalla CA con cui è attiva la nostra convenzione.

Non è pertanto ascrivibile a scelte effettuate dall'Università degli Studi di Verona la mancata possibilità di emettere certificati di durata superiore ad 1 anno.

Una volta emesso il certificato è necessario annotarsi e provvedere per tempo al suo rinnovo, per evitare disservizi al momento della scadenza.

## LIMITAZIONI

### Non si accettano richieste di certificati

- Non riconducibili ad una persona specifica in qualità di richiedente;
- Con un numero di **Subject Alternative Names** superiore a 3 (salvo eccezioni concordate individualmente);
- Con **Common Name** o **Subject Alternative Names** in conflitto con altri certificati emessi in precedenza (salvo eccezioni concordate individualmente).

## REQUISITI

Utenza istituzionale Univr;

Strumento per la generazione di richieste CSR;

Elenco dei nomi DNS (\*.univr.it) per i quali si intende registrare il dominio.