Com'è organizzato il servizio di rilascio dei certificati del CNR

L'attività di rilascio di certificati X.509 per il CNR viene assicurata dal GARR che a sua volta si avvale del servizio di DigiCert erogato verso tutti le organizzazioni afferenti a TERENA.
Il rappresentante legale del CNR per l'attivazione del nuovo servizio ha espletato alcuni passaggi formali indicando un referente per tale servizio, il quale avvalendosi della funzionalità offerte dal sistema può delegare alcuni compiti e responsabilità legate alla richiesta ed alla gestione dei certificati.

Chi può richiedere un certificato

Un certificato x.509 lo può richiedere:

- un amministratore (al momento Manlio Astolfi - Daniele Vannozzi)
- un utente (referenti per istituto)

Ogni persona autorizzata ad operare su DigiCert (https://www.digicert.com) deve possedere un account e deve avere la disponibilità di un sistema di One Time Password app installata su di uno smartphone. Tutte quelle compatibili con l'algoritmo TOTP dovrebbero andar bene. Quelle verificate da Digicert sono:

- Google Authenticator: Android, iPhone, Blackberry
- Authy: Android, iPhone
- Authenticator: Windows Phone
- Duo Mobile: iPhone

La persona deve inoltre avere la disponibilità di un certificato personale con cui firmare le email con cui comunica con gli amministratori dei certificati per il CNR.

Cosa occorre fare per richiedere un certificato

Il Direttore di ogni Istituto dovrà indicare al massimo due utenti che si occuperanno della richiesta dei certificati necessari al funzionamento all'Istituto. L'attivazione dei nuovi utenti verrà fatta a cura di un "amministratore", il delegato riceverà una email da DigiCert con le indicazioni da seguire per concludere la procedura di attivazione dell'utente.
Lo "amministratore" dovrà preventivamente aver creato una entry per ogni Istituto o Area della Ricerca (la cui sigla dovrà essere riportata nella richiesta di certificato) ed avergli associato il relativo nome a dominio (es: iit.cnr.it).

Quali dati sono necessari prima richiedere un certificato?

La persona che autorizzata a richiedere un certificato dovrà preventivamente conoscere:

- il nome della macchina su cui verrà associato il certificato;
- gli eventuali altri nomi alternativi con cui sarà riconosciuta la macchina con quel certificato;
- il tipo di certificato;
- l'eventuale ulteriore validazione del certificato;
- la durata del certificato (default 3 anni).

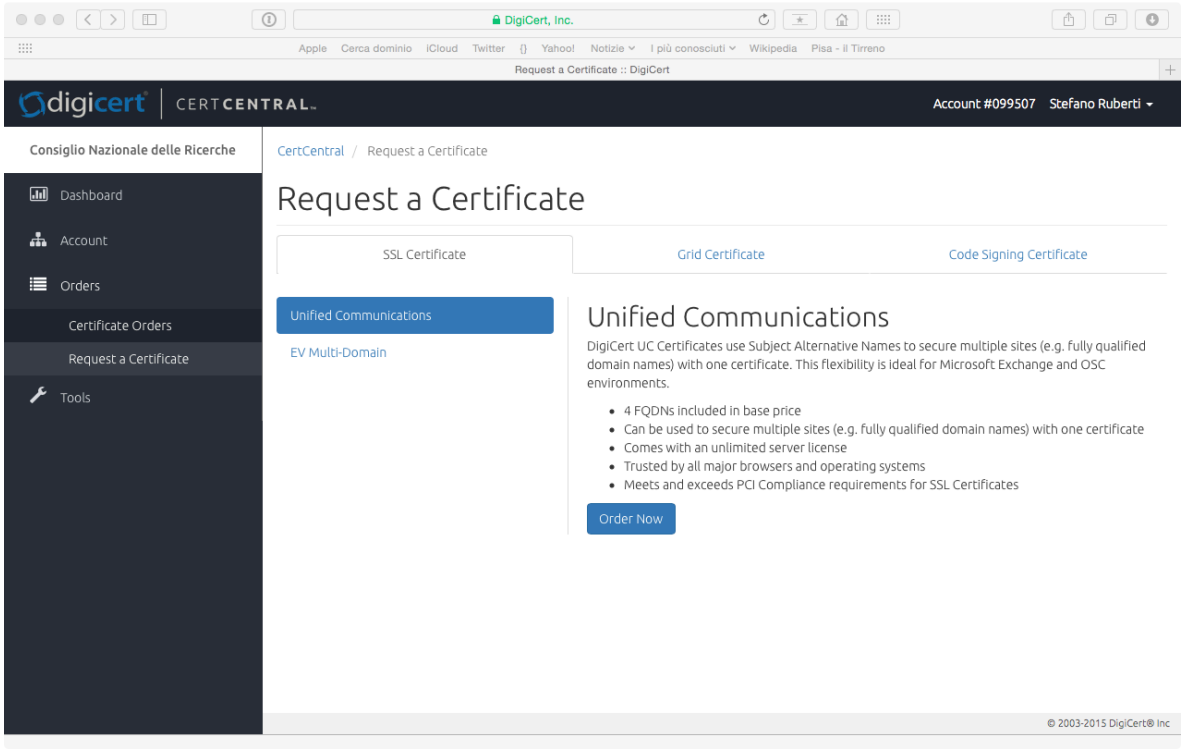
Cosa occorre fare per richiedere un certificato

La persona abilitata a richiedere un certificato dovrà attraverso una apposita Utility (es: openssl req -newkey rsa:2048 -nodes -out req-calmo.iit.cnr.it.pem -keyout key-calmo.iit.cnr.it.pem) generare un file con la "private key" del certificato facendo attenzione a rispettare i seguenti campi:

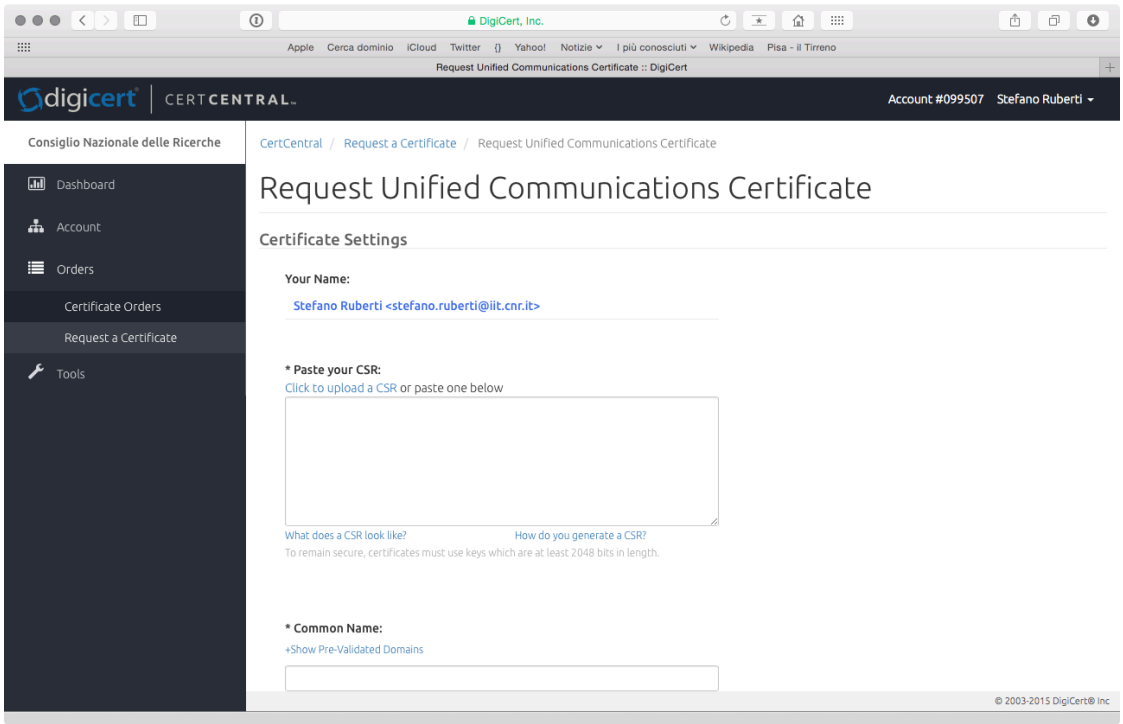
- C=IT
- ST=<regione in cui si trova il server su cui verrà utilizzato il certificato> (es: Toscana)
- L=<città in cui si trova il server su cui verrà utilizzato il certificato > (es: Pisa)
- O=Consiglio Nazionale delle Ricerche

- OU=<sigla istituto o area> (es: IIT, Area della Ricerca Roma 1)
- CN=<nome della macchina su cui verrà utilizzato il certificato> (es: calmo.iit.cnr.it)
- emailAddress= <indirizzo email della persona che sta richiedendo il certificato (es: abraham.gebrehiwot@iit.cnr.it)

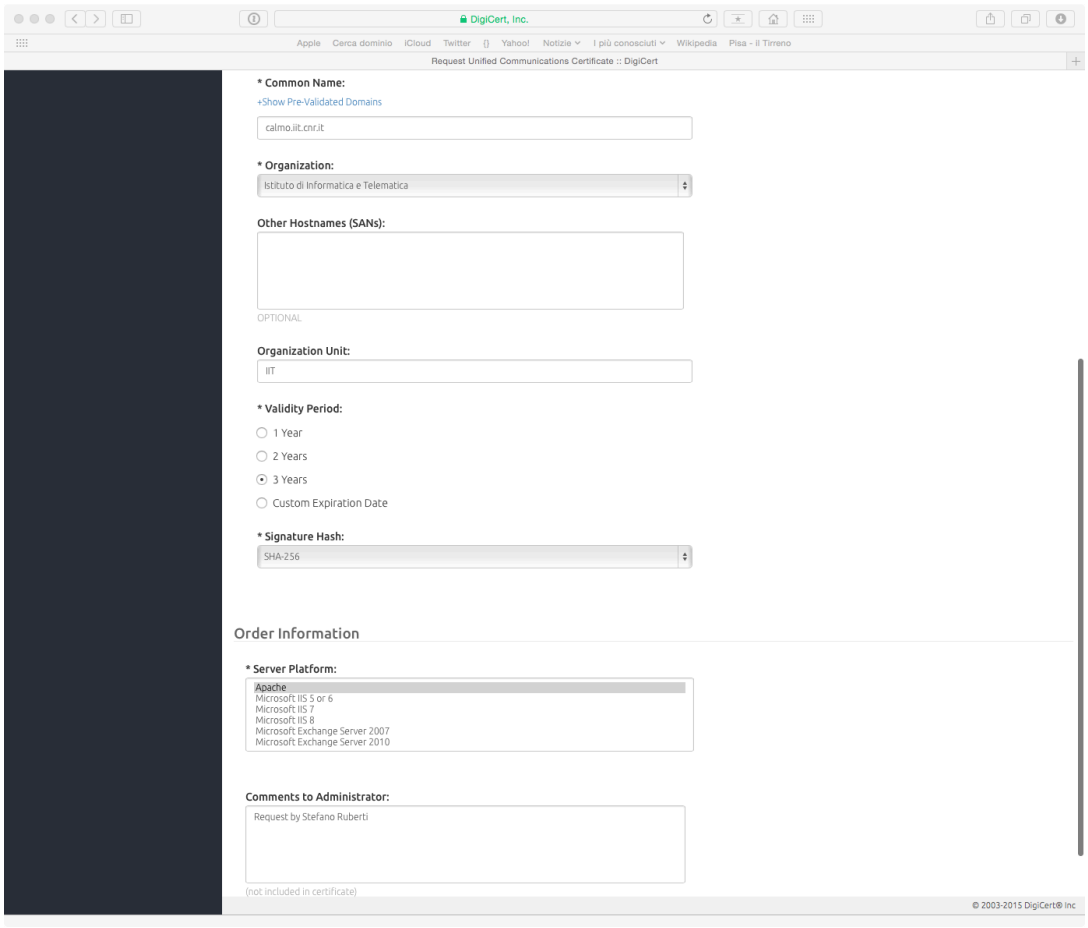
Autenticarsi su DigiCert (https://www.digicert.com) digitando le proprie credenziali (user e password) inserire la OTP, selezionare dal menù “orders” la voce “request a certificate” e cliccare su “+”



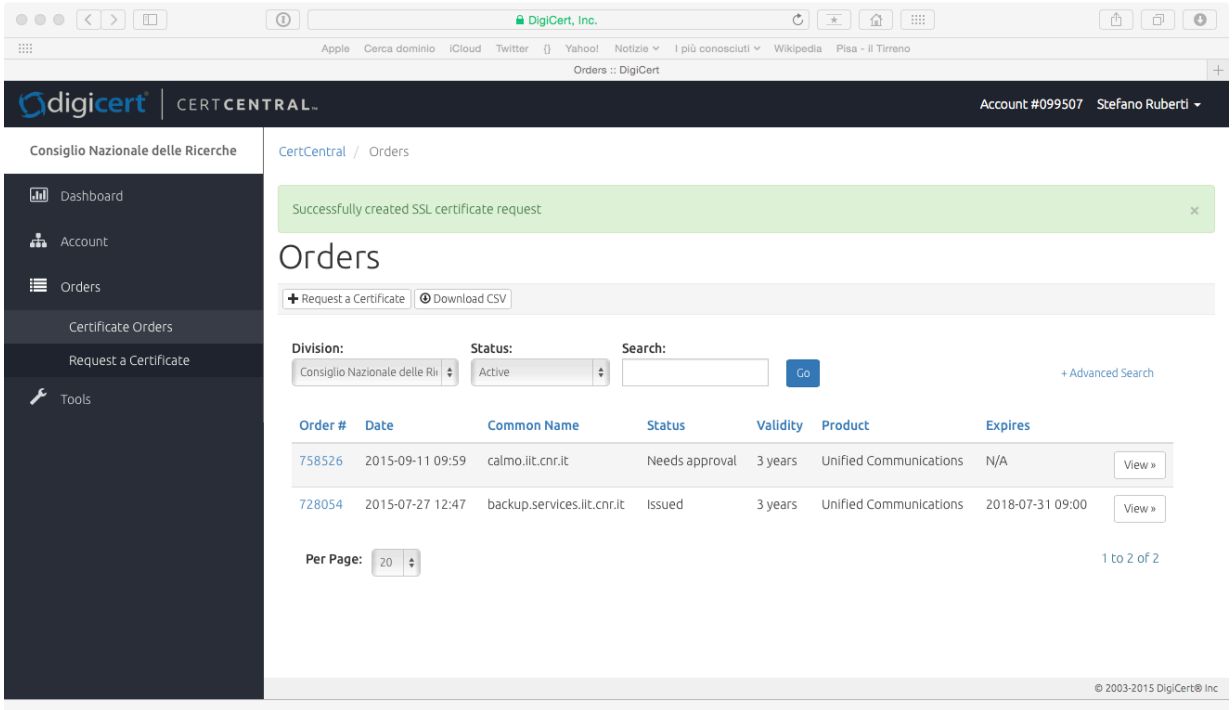
cliccare su “order now”

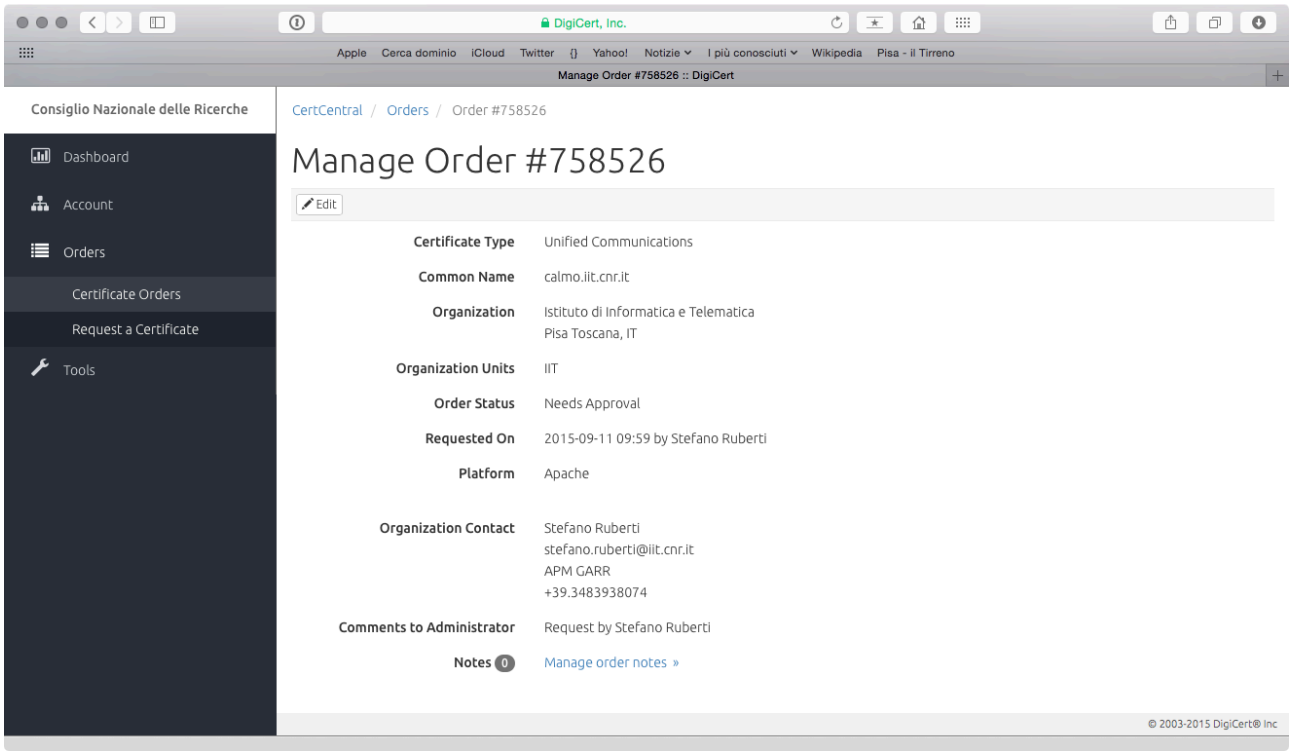


Inserire e completare i vari campi importando la richiesta di certificato precedentemente generata e cliccare su “Submit Certificate Request”.



Visualizzare il certificato richiesto cliccando sulla specifica riga per un ultimo controllo:





Il sistema DigiCert provvederà a notificare agli amministratori un avviso di una richiesta di nuovo certificato. Sarà cura degli amministratori verificare se sono stati rispettati tutti i passi sopra citati e se la richiesta e pertinente prima della sua approvazione.
Il richiedente il certificato, una volta conclusa l'approvazione da parte dell'amministratore riceverà una email da DigiCert contenente il certificato in breve tempo.