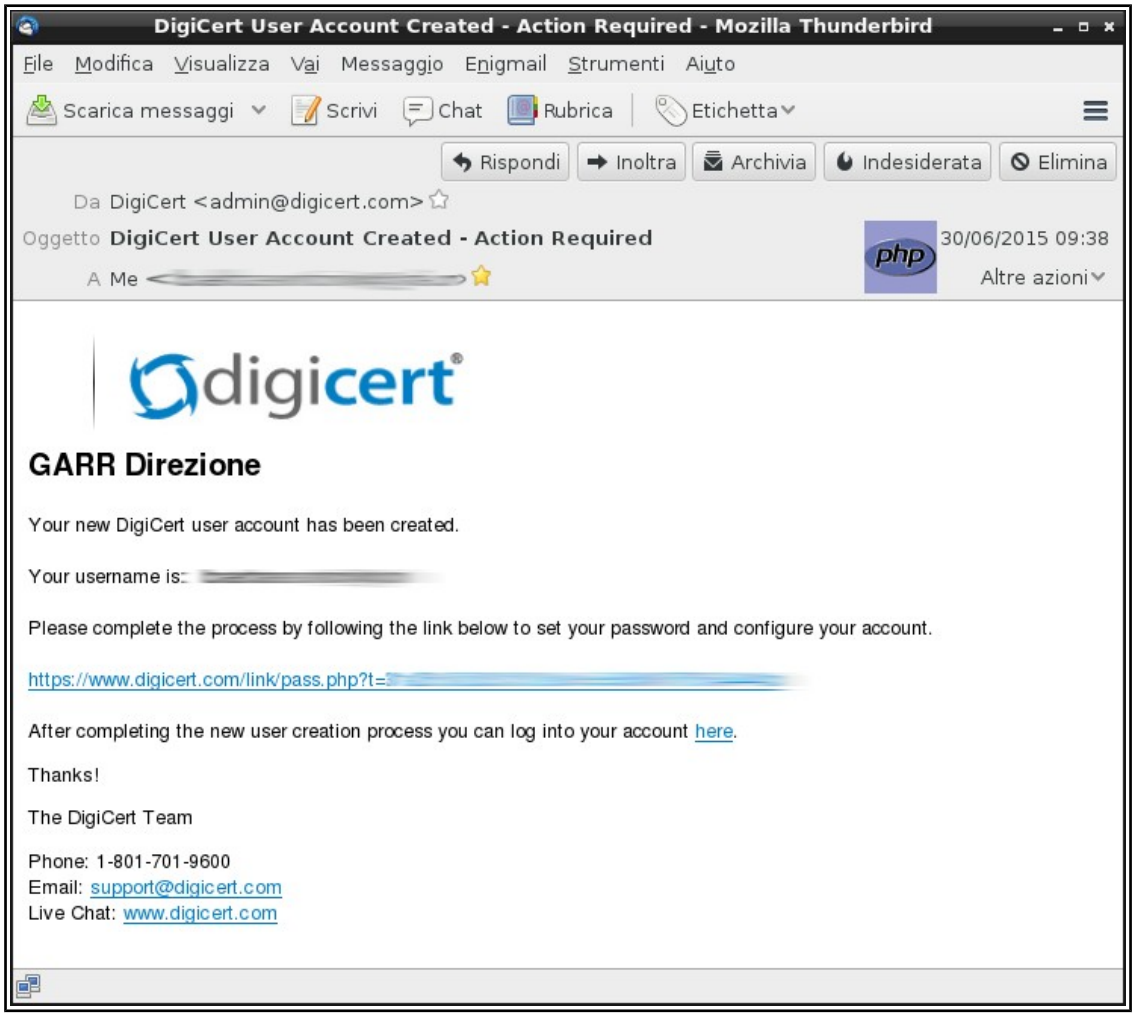
Guida per Amministratori TCS

Indice generale

Attivare l'account di Primo Amministratore

Il Primo Amministratore, nominato dal Rappresentante Legale della propria Istituzione, riceve l'invito a creare l'account di amministratore per la propria **Divisione** sul portale Digicert:

Seguire le istruzioni nella mail e dopo aver creato l'account effettuare il login



Per motivi di sicurezza il login richiede una One Time Password app installata su di uno smartphone. Tutte quelle compatibili con il protocollo TOTP dovrebbero andar bene. Quelle verificate da Digicert sono:

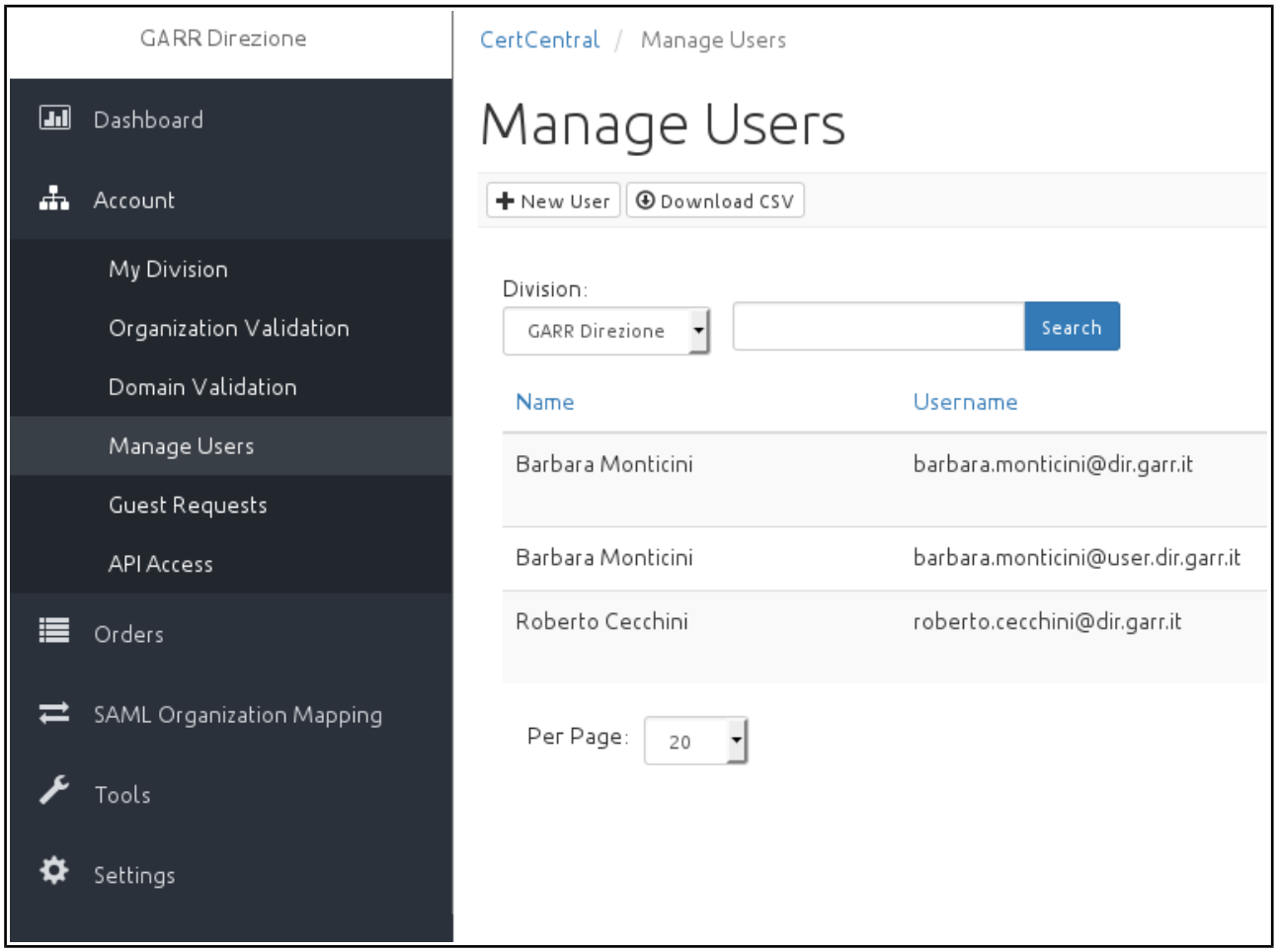
- **Google Authenticator**: Android, iPhone, Blackberry
- **Authy**: Android, iPhone
- **Authenticator**: Windows Phone
- **Duo Mobile**: iPhone

In alternativa si possono utilizzare estensioni per Chrome, ad es. Authy, Authenticator o Gauth.

Funzioni e poteri degli Amministratori

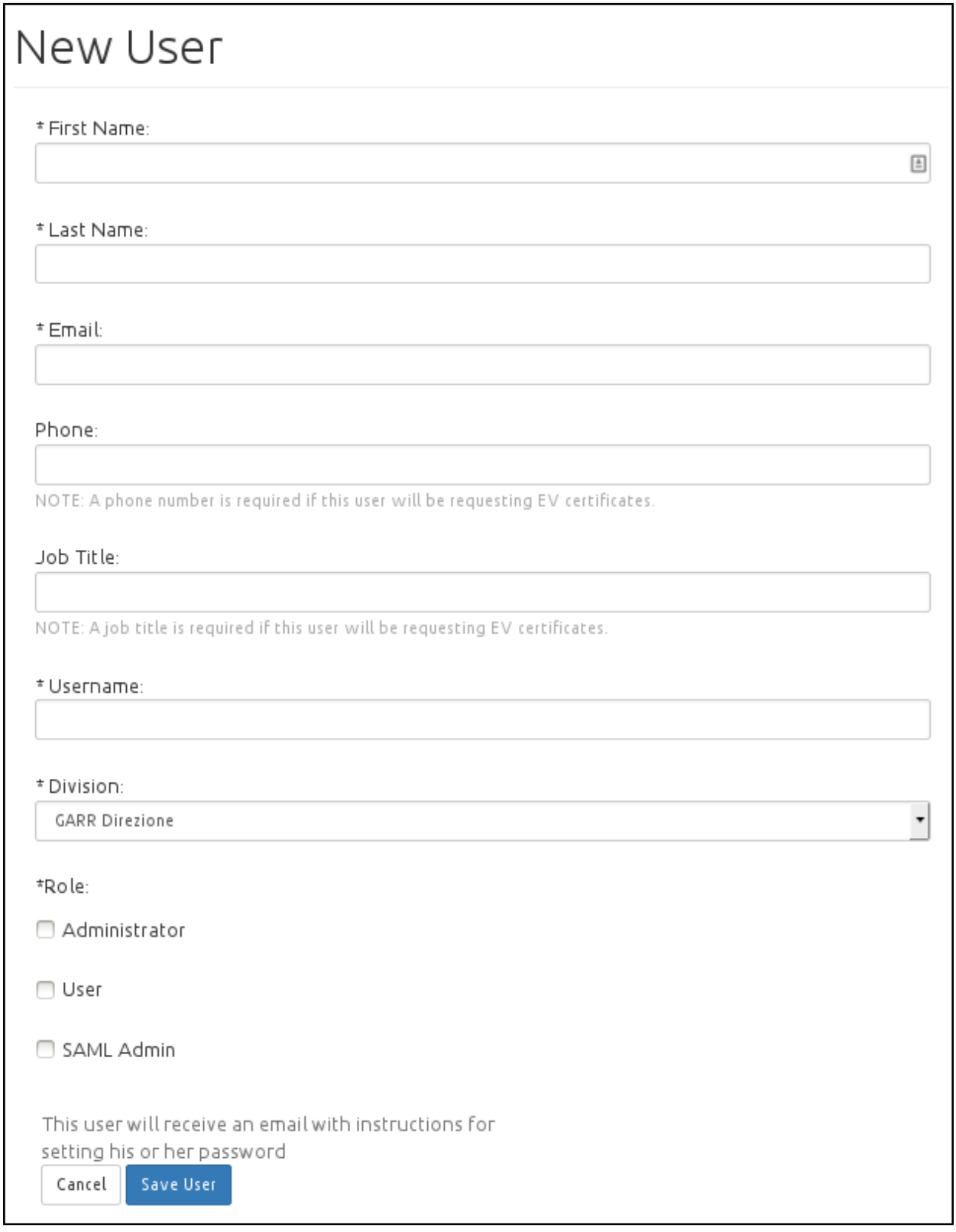
Creare e invitare i successivi Amministratori

Nella sezione **Account**, in **Manage Users** creare il nuovo utente con il bottone **+New User**



Dopo la creazione il nuovo utente apparirà nella lista degli utenti e potrà essere modificato successivamente (con i bottoni **View** e **Edit User**)

Affinché il nuovo utente sia abilitato ad essere amministratore della Divisione dovra' essere impostata la checkbox **Role: Administrator** (non è necessario selezionare User)


New User
* First Name:
* Last Name:
* Email:
Phone:
NOTE: A phone number is required if this user will be requesting EV certificates.
Job Title:
NOTE: A job title is required if this user will be requesting EV certificates.
* Username:
* Division:
GARR Direzione
*Role:
Administrator
User
SAML Admin
This user will receive an email with instructions for setting his or her password
Cancel
Save User

Creare e invitare utenti non Amministrativi

Per creare un utente semplice, non amministrativo, impostare durante la creazione solo la checkbox **User**.

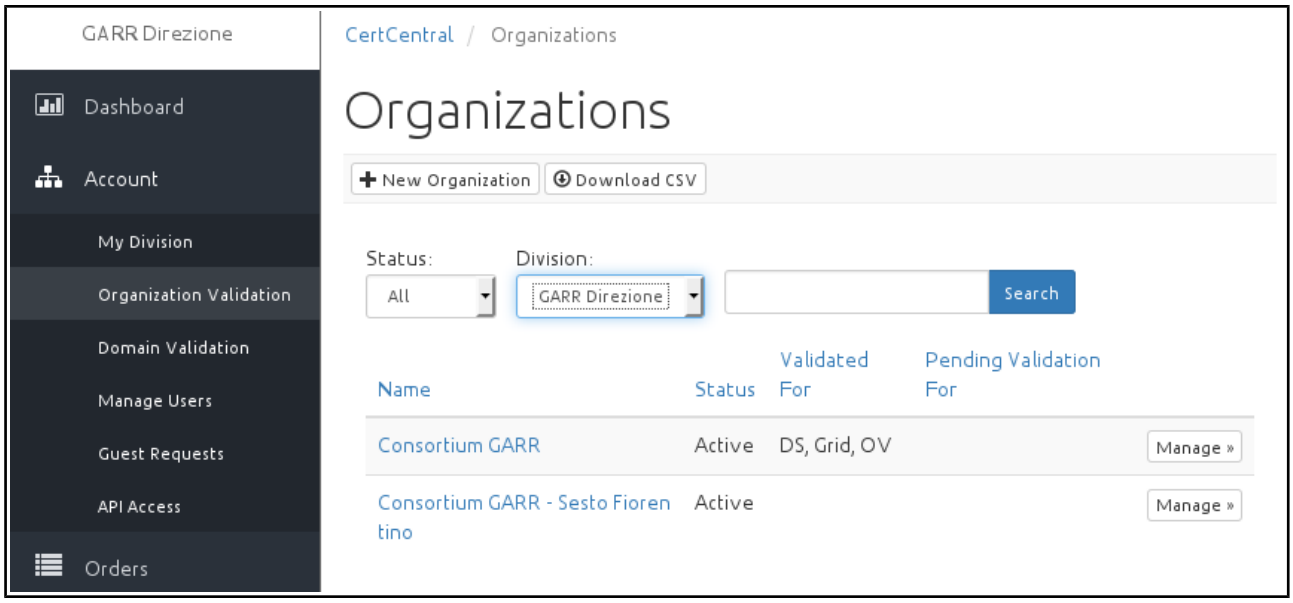
Questo tipo di utente può solamente richiedere certificati. L'approvazione delle richieste sottomesse è sempre compito dell'amministratore della Divisione.

Creare il campo O per i certificati

Consigliamo di creare inizialmente una sola **Organizzazione** per Divisione (per Istituzione). Il valore di **Organizzazione** coincide con il **campo O** dei certificati emessi dalla Divisione.

L'esempio che segue è il ritratto di quando fatto all'interno della nostra Divisione come sperimentazione.

Attenzione: le Organizzazioni non possono essere cancellate, ma solo modificate.

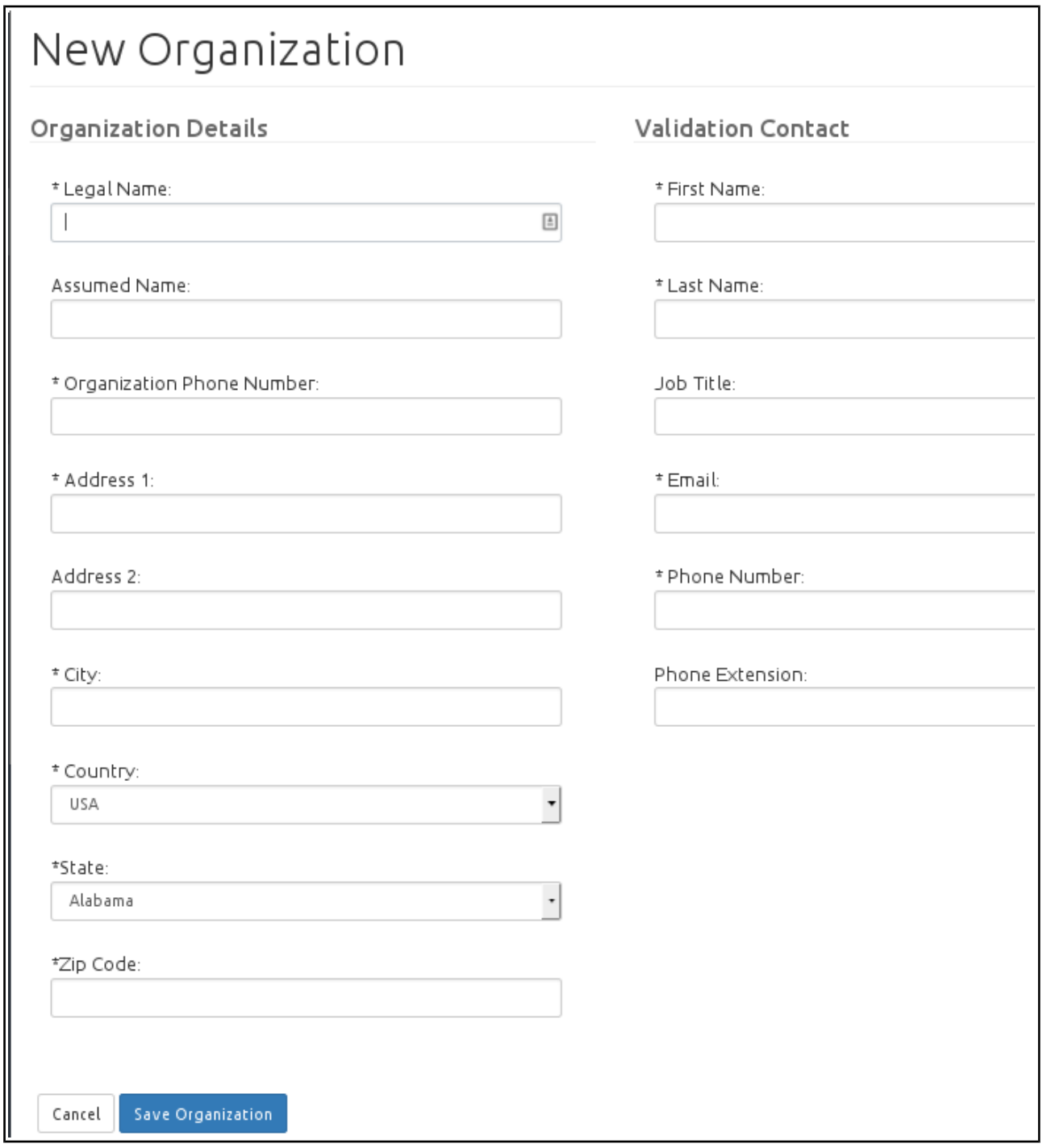


Per creare una nuova O premere **+New Organization**

Durante la definizione dell'Organizzazione oltre al nome ufficiale dell'Ente, che ricordiamo apparirà nel campo O dei certificati emessi, è necessario indicare anche il nome e i riferimenti di una persona denominata **Validation Contact**. Non abbiamo consigli particolari su quale nominativo indicare come Validation Contact: potrebbero essere dei validi candidati il Rappresentante Legale, l'APA o il Direttore Generale.

Tutti i campi indicati con * **sono obbligatori**.

Consigliamo di indicare sia **Country** che **State** come Italia.



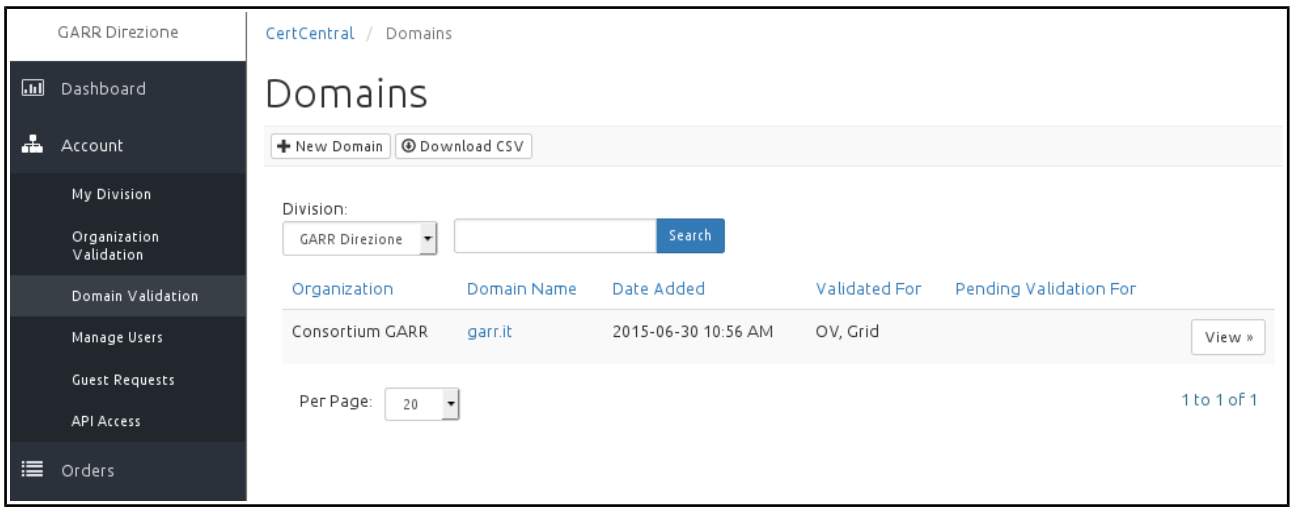
Validare i domini intestati all'ente

La validazione dei domini è **necessaria** per poter emettere certificati e la si richiede alla voce **Account** -> **Domain Validation**

L'elenco dei domini già validati o per i quali si è richiesta la validazione appare nella lista assieme

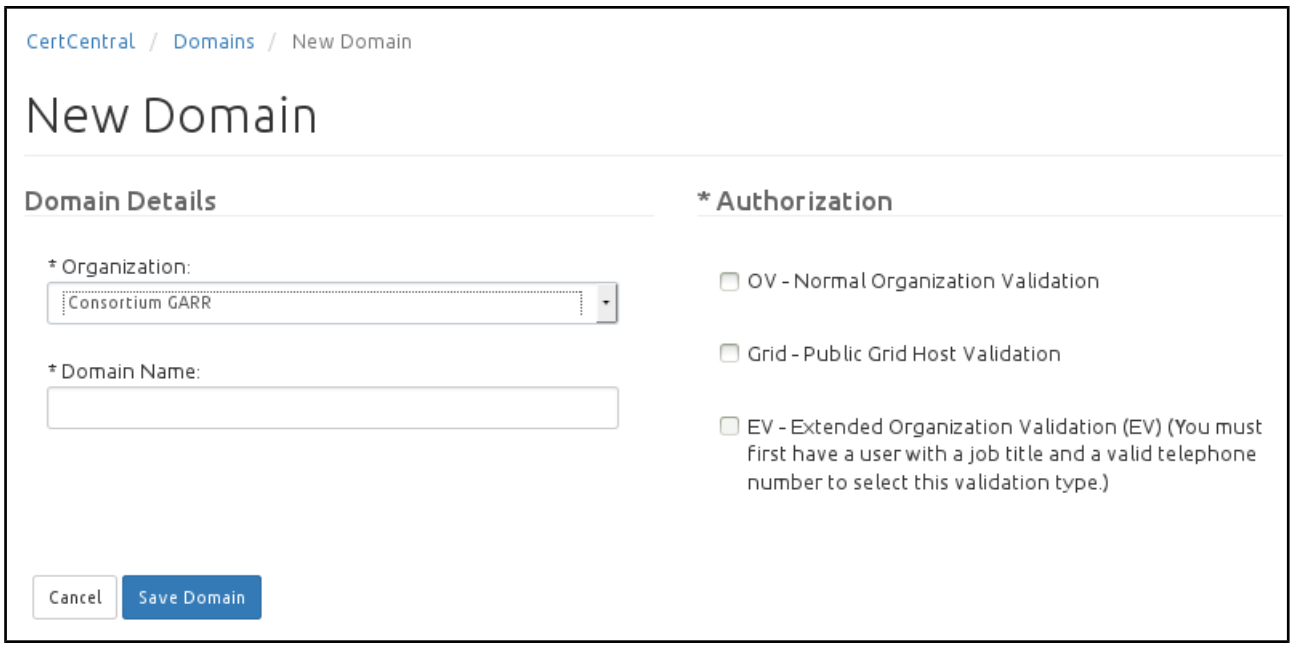
allo stato della richiesta che può essere **Validated** o **Pending Validation**

Per richiedere la validazione di un nuovo dominio è presente il bottone **+ New Domain**



Quando si crea un nuovo dominio è necessario specificare il campo **O** (cioè l'Organizzazione alla quale il dominio è associato), il dominio e il tipo di certificato per il quale si richiede la validazione (e successivamente l'emissione).

Consigliamo di richiedere inizialmente OV e Grid. Per EV è necessario aver preventivamente definito un'utenza con i campi **job title** e **telephone number** validi.



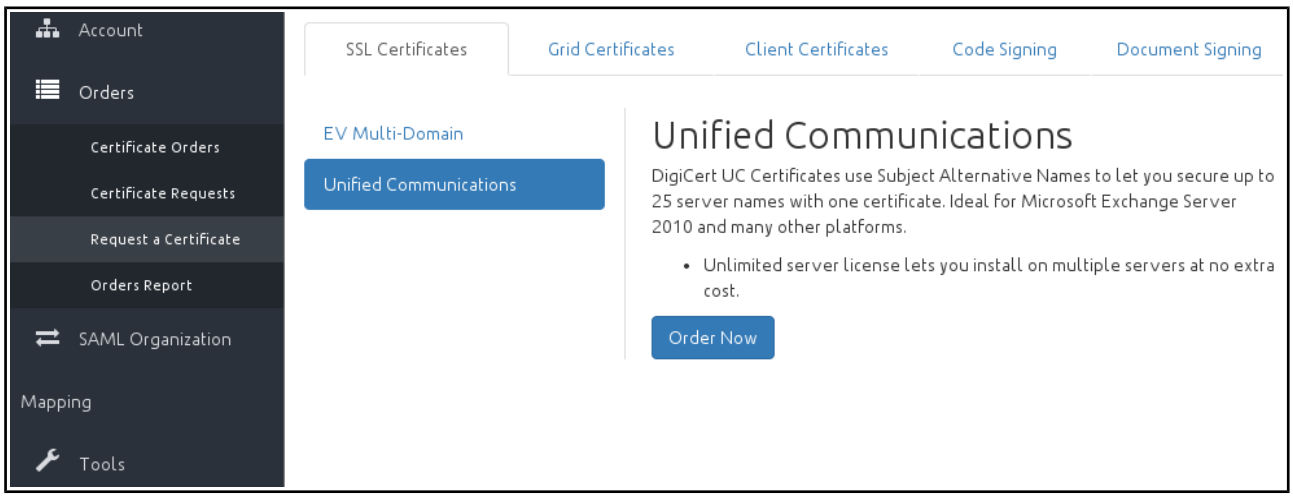
Richiedere un certificato

Per poter richiedere certificati è necessario **aver creato almeno una Organization** e **aver validato all'interno della O stessa i domini presenti nella CSR**

La richiesta di nuovo certificato si sottomette nella sezione **Orders** -> **Request a Certificate**

Comando standard per generare una CSR

```
openssl req -newkey rsa:2048 -nodes -subj "/CN=nome-server.dominio.it" -out req-nome-server.pem -keyout key-nome-server.pem
```

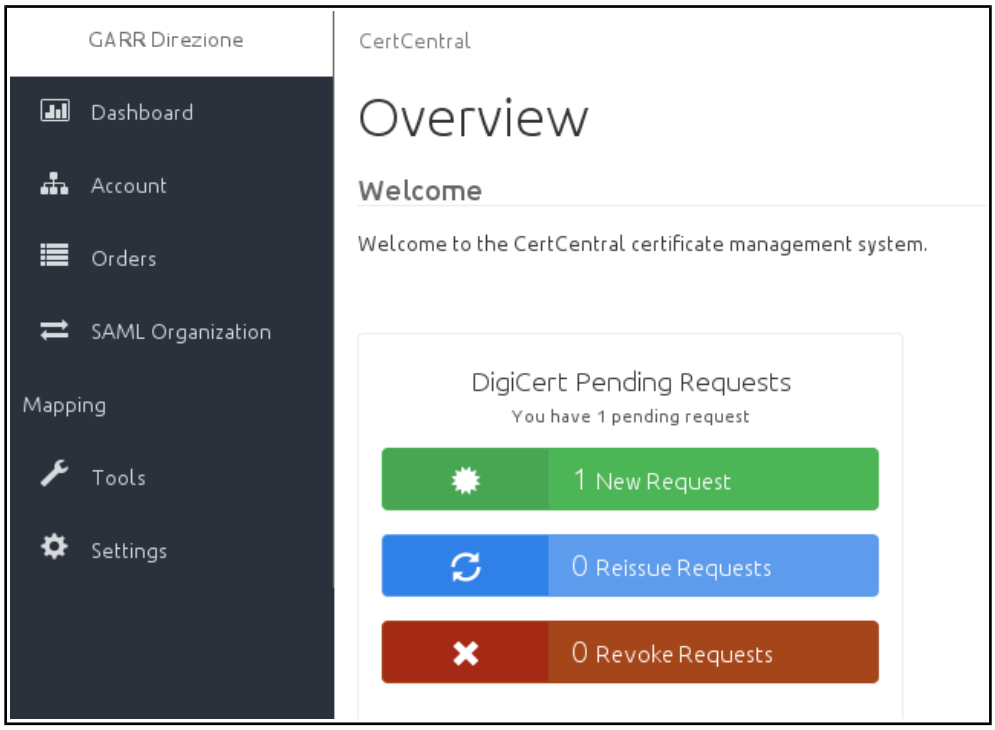


Il tipo di certificati standard è UC che consiste in un certificato multi-nome (testati fino a 150 nomi alternativi).

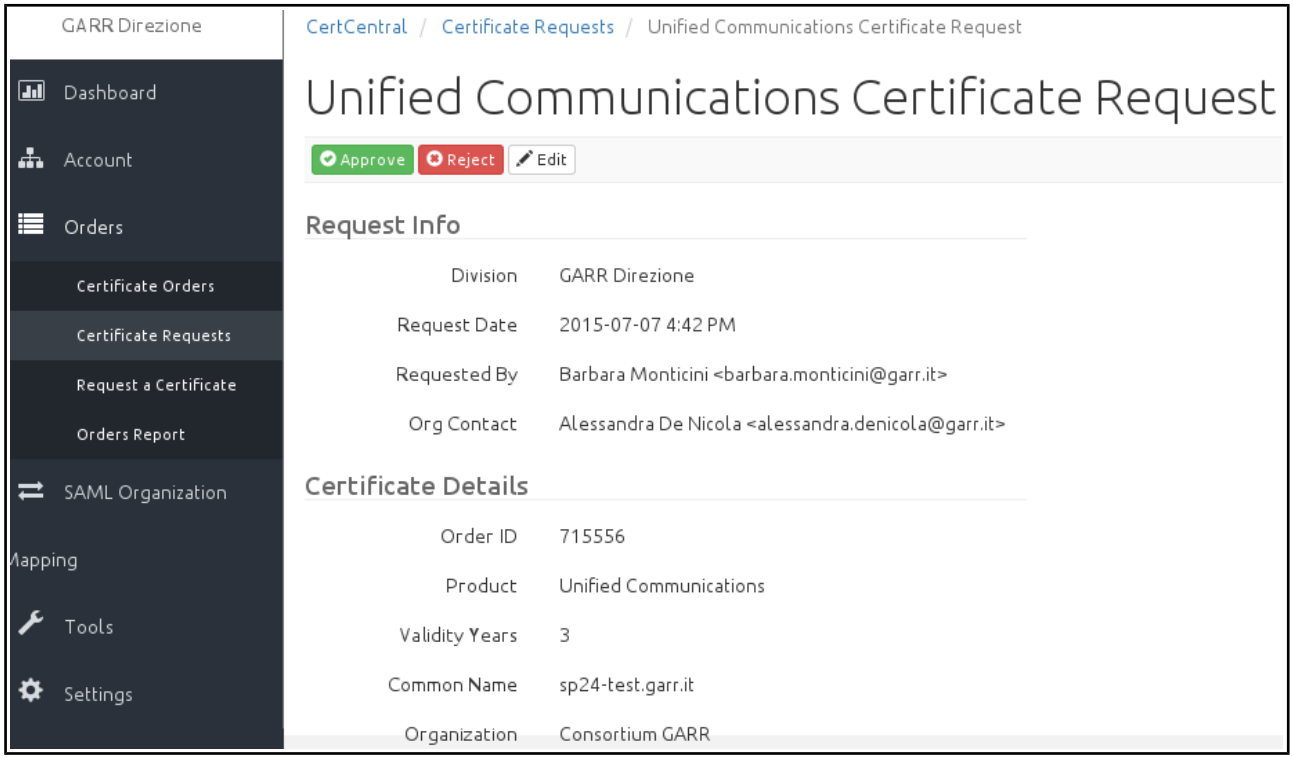
Per i certificati wildcard è necessario contattare il servizio TCS (garr-ca@garr.it) motivando la richiesta.

Approvare richieste di certificato pendenti

La presenza di azioni pendenti è visibile nella sezione **Dashboard**



Per approvare le richieste pendenti basta cliccare sull'elemento presente in **dashboard** o andare nella sezione **Orders**. Selezionata la richiesta premere il bottone **Approve** (o **Reject** per rifiutare).

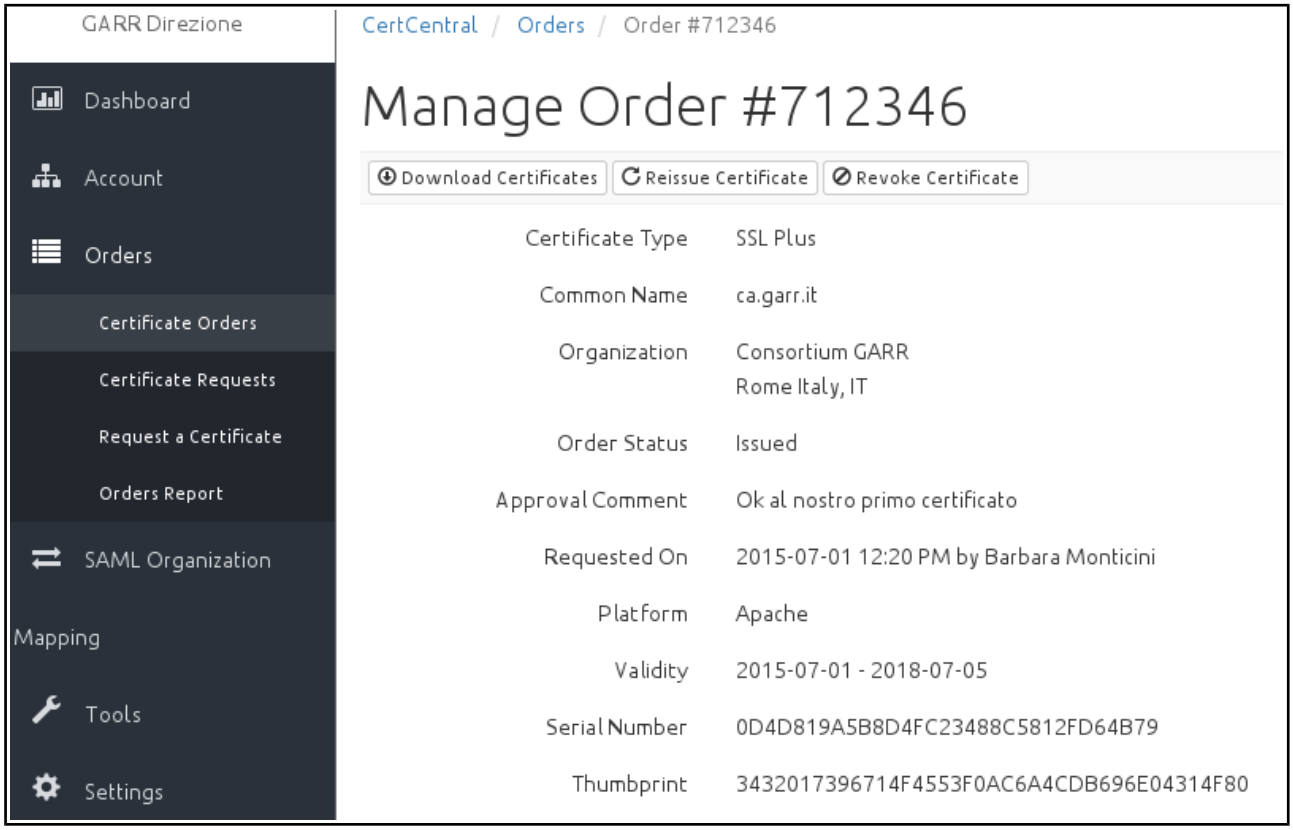

GARR Direzione
Dashboard
Account
Orders
Certificate Orders
Certificate Requests
Request a Certificate
Orders Report
SAML Organization
Mapping
Tools
Settings
CertCentral / Certificate Requests / Unified Communications Certificate Request
Unified Communications Certificate Request
Approve
Reject
Edit
Request Info
Division GARR Direzione
Request Date 2015-07-07 4:42 PM
Requested By Barbara Monticini <barbara.monticini@garr.it>
Org Contact Alessandra De Nicola <alessandra.denicola@garr.it>
Certificate Details
Order ID 715556
Product Unified Communications
Validity Years 3
Common Name sp24-test.garr.it
Organization Consortium GARR

Revocare un certificato

Un amministratore ha i permessi per richiedere la revoca dei certificati emessi.

Da **Certificate Orders** selezionare il certificato da revocare ed entrare nei dettagli.

Tra le opzioni possibili c'è **Revoke Certificate**. Procedere con la revoca indicando anche il motivo per il quale si richiede la revoca.



Certificati Personali

Attivare il SSO con l'idp istituzionale per abilitare la richiesta di certificati personali

E' necessario che un amministratore abbia il ruolo di SAML Admin e che l'ente abbia attivato un Identity Provider all'interno della Federazione IDEM (http://www.idem.garr.it)

Maggiori informazioni su come abilitare il SSO nella sezione “Funzioni e poteri di SAML Admin”

Funzioni e poteri di SAML Admin

Un utente con ruolo SAML Admin ha i permessi per modificare le impostazioni relative al mapping tra campo O (Organization) e l'Identity Provider eventualmente già attivo per l'Ente e iscritto alla Federazione IDEM.

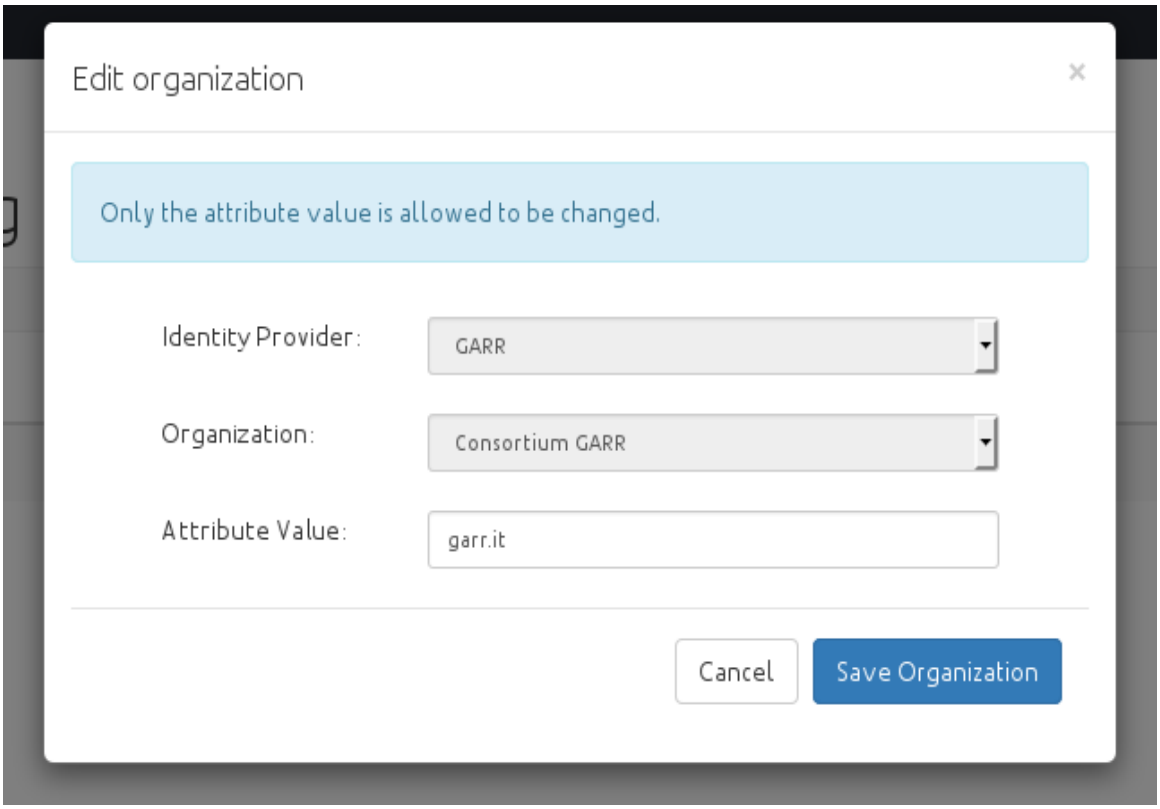
Il mapping è necessario per attivare il servizio di rilascio certificati personali con autenticazione federata via IDEM. Per portare a termine con successo l'operazione l'ente dovrà aver attivato un Identity Provider in IDEM.

Tutti gli Identity Provider già iscritti a IDEM appariranno nel menù a tendina **Identity Provider**

Nel campo **Organisation** potrà essere selezionata solo una Organisation già validata.

Attribute Value richiede l'immissione di una stringa pari al valore dell'attributo *SchacHomeOrganisation*

L'attributo *SchacHomeOrganisation* dovrà essere configurato all'interno dell'IdP. Per maggiori informazioni su questo aspetto e su quali altri attributi dovranno essere rilasciati dall'IdP contattare il supporto IDEM all'indirizzo **idem-help@garr.it**



Consigli e suggerimenti generali

- Ulteriori informazioni sono disponibili sul wiki GEANT TCS: https://wiki.geant.org/display/TCSNT/Trusted+Certificate+Service+%28new+TCS%29+Home
- Non limitare troppo il numero degli Amministratori, in modo da ridurre la possibilità che non ce ne siano disponibili per approvare le richieste di certificati
- Valutare l'opportunità di creare utenti non privilegiati per la sottomissione di richieste di certificato, in modo da ridurre il carico di lavoro degli Amministratori.
- Imporre regole sul contenuto del campo OU.