UNIVERSITÀ di VERONA

GENERAZIONE DI CERTIFICATI SSL

Procedura per la generazione di certificati SSL server Sectigo per l'Università degli Studi di Verona

La procedura complessiva si articola nei seguenti punti:

A. Creazione della richiesta **CSR**;
B. Trasmissione della **CSR** alla Certification Authority **CA**;
C. Approvazione della richiesta da parte del personale dell'Area Networking;
D. Creazione, da parte della **CA**, del certificato **CERT** firmato dalla **CA** stessa.

A cura del Richiedente:
Ci sarà poi l'installazione del certificato e della **CHAIN** sul server, su cui è già presente la chiave privata **KEY** ed Eventuale riconfigurazione del servizio per la trasmissione cifrata dei dati (es. https).

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.

Validità: 1 anno

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).

UNIVERSITÀ di VERONA

A.
Creazione richiesta CSR
su macchine Unix-like (Mac, Linux)

Le macchine Unix-like generalmente offrono nella dotazione di base il comando openssl, che permette la creazione e manipolazione di certificati e chiavi SSL di tutti i tipi.

Il comando da eseguire, è il seguente:

openssl req -newkey rsa:4096 -nodes -subj "/CN=nomeserver.univr.it" -out nomeserver.univr.it-csr.pem -keyout nomeserver.univr.it-key.pem

nomeserver.univr.it va ovviamente sostituito, **in tutte e tre le occorrenze**, dal nome principale (o unico) del server per il quale si intende richiedere il certificato.
rsa:4096 potrebbe non risultare compatibile con tutti gli ambienti, in caso di problemi sostituirlo con **rsa:2048**

Si suggerisce di fare attenzione a dove eseguire il comando in modo che vi ritroviate, per praticità negli step successivi.

Questo comando genera due file:

nomeserver.**univr.it-csr.pem**, la richiesta di firma, **CSR**

nomeserver.**univr.it-key.pem**, la chiave privata, **KEY**

ATTENZIONE: Porre particolare attenzione alla gestione della chiave privata: da questo punto in poi, la perdita o sovrascrittura della chiave privata comporta il dover ripetere la procedura dall'inizio.

UNIVERSITÀ
di VERONA

A.
Creazione richiesta CSR
su macchine Windows

Per la generazione di una CSR su un sistema Windows Server, fare riferimento a queste istruzioni:

https://sectigo.com/resource-library/generate-csr-microsoft-iis-8-x

Valorizzare i campi della richiesta come segue:

Common name:
nome del server

Organization:
Universita di Verona

Organizational Unit:
Nome del dipartimento o Centro

City/Locality:
Verona

State/Province:
Verona

Country/Region:
IT

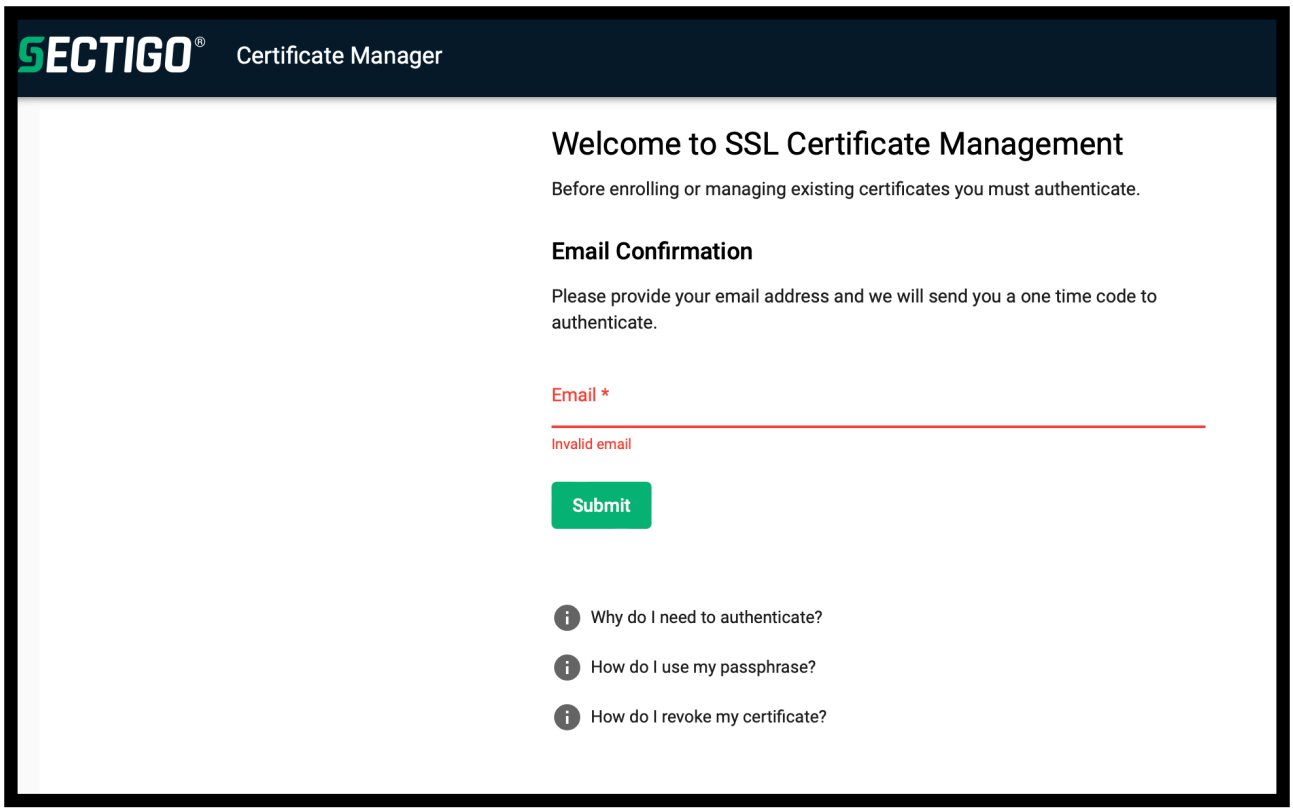
UNIVERSITÀ di VERONA

B.
Trasmissione della **CSR** alla Certification Authority **CA**
Accesso a Sectigo Certificate Manager

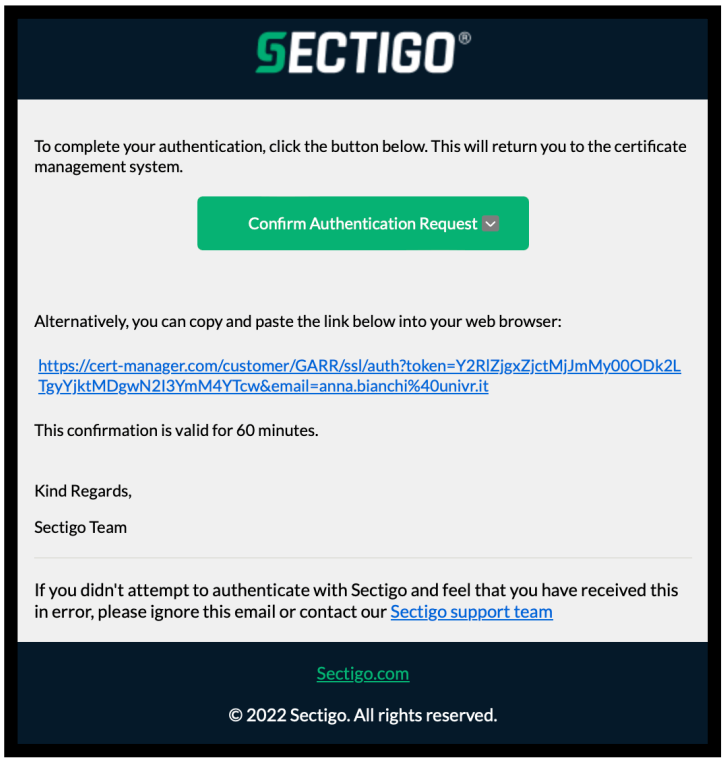
Accedere al portale Sectigo di richiesta certificati via browser tramite il seguente indirizzo:

https://cert-manager.com/customer/GARR/ssl/login

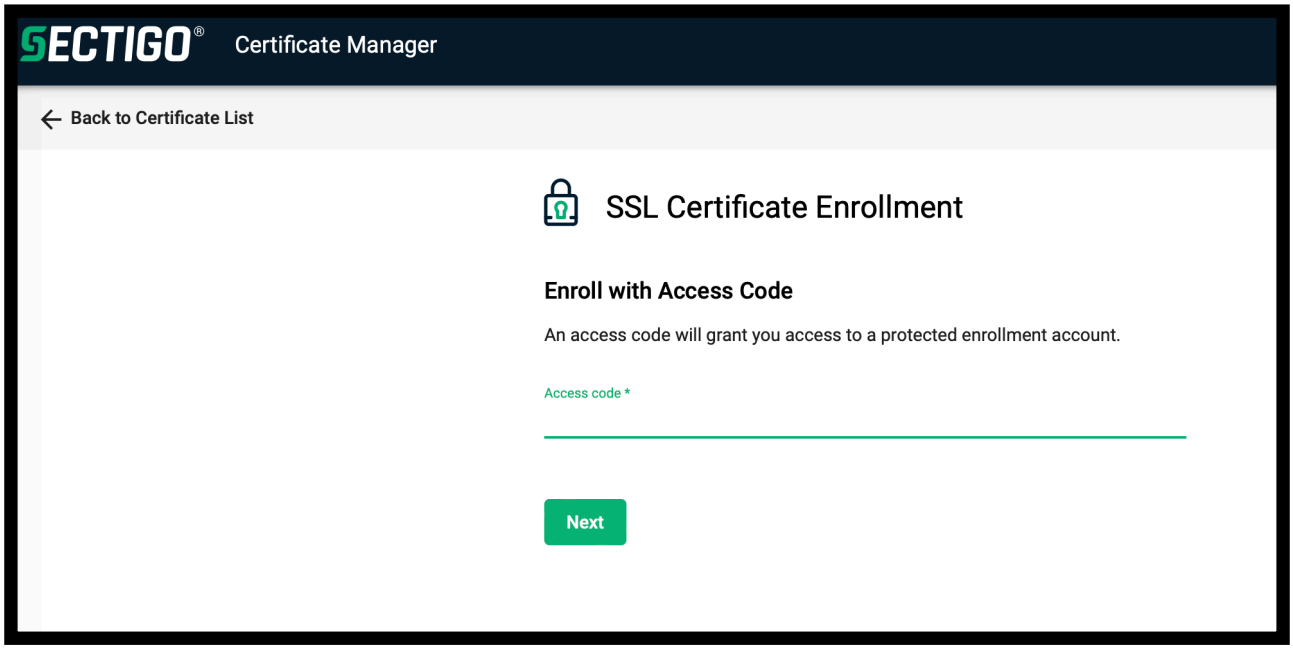
La pagina sarà la seguente:
Compilare il campo con la propria mail istituzionale individuale (**non verranno approvate richieste provenienti da mail non individuali**).



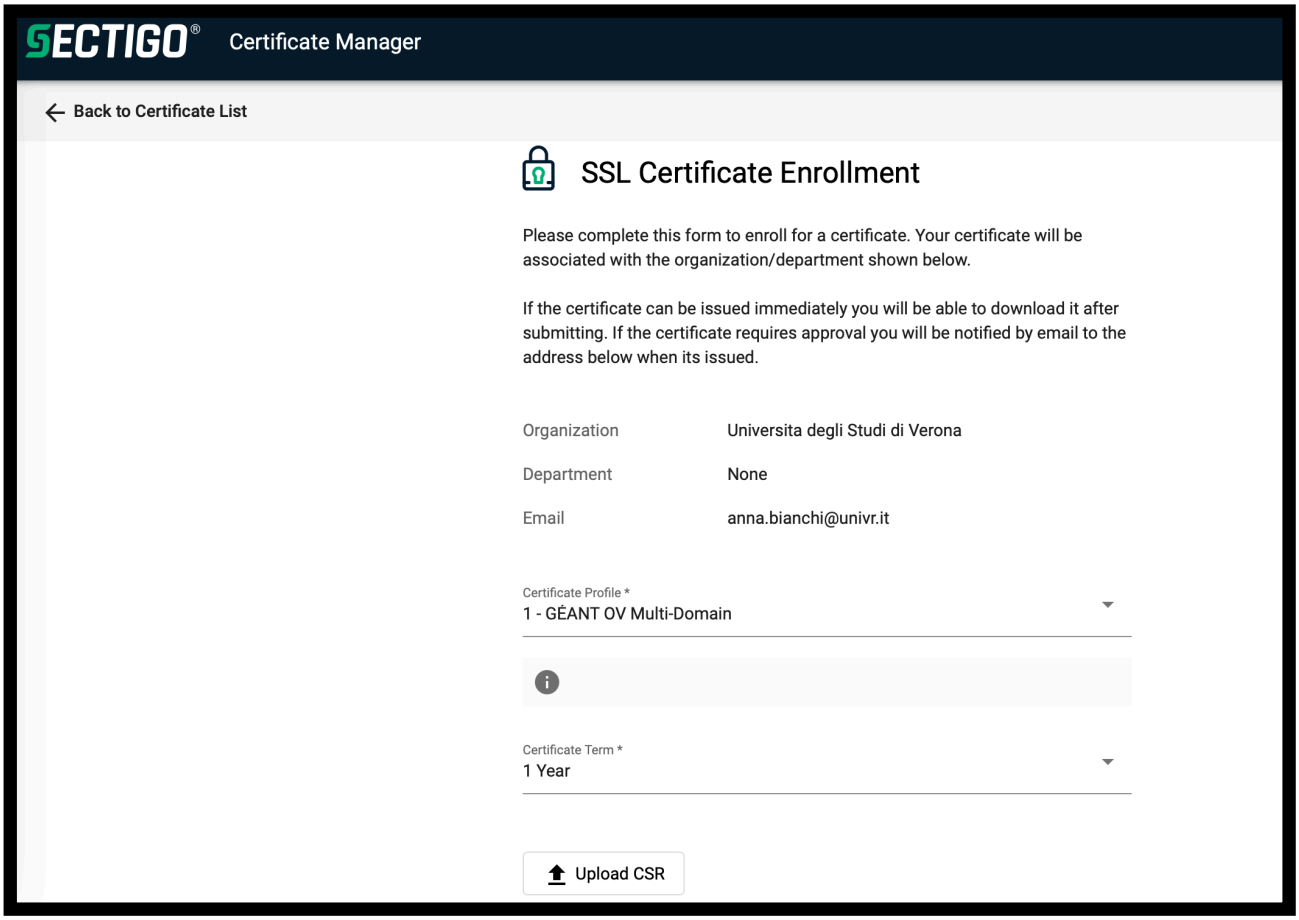
Verrà poi inviata alla vostra mail la seguente richiesta di autorizzazione da confermare:



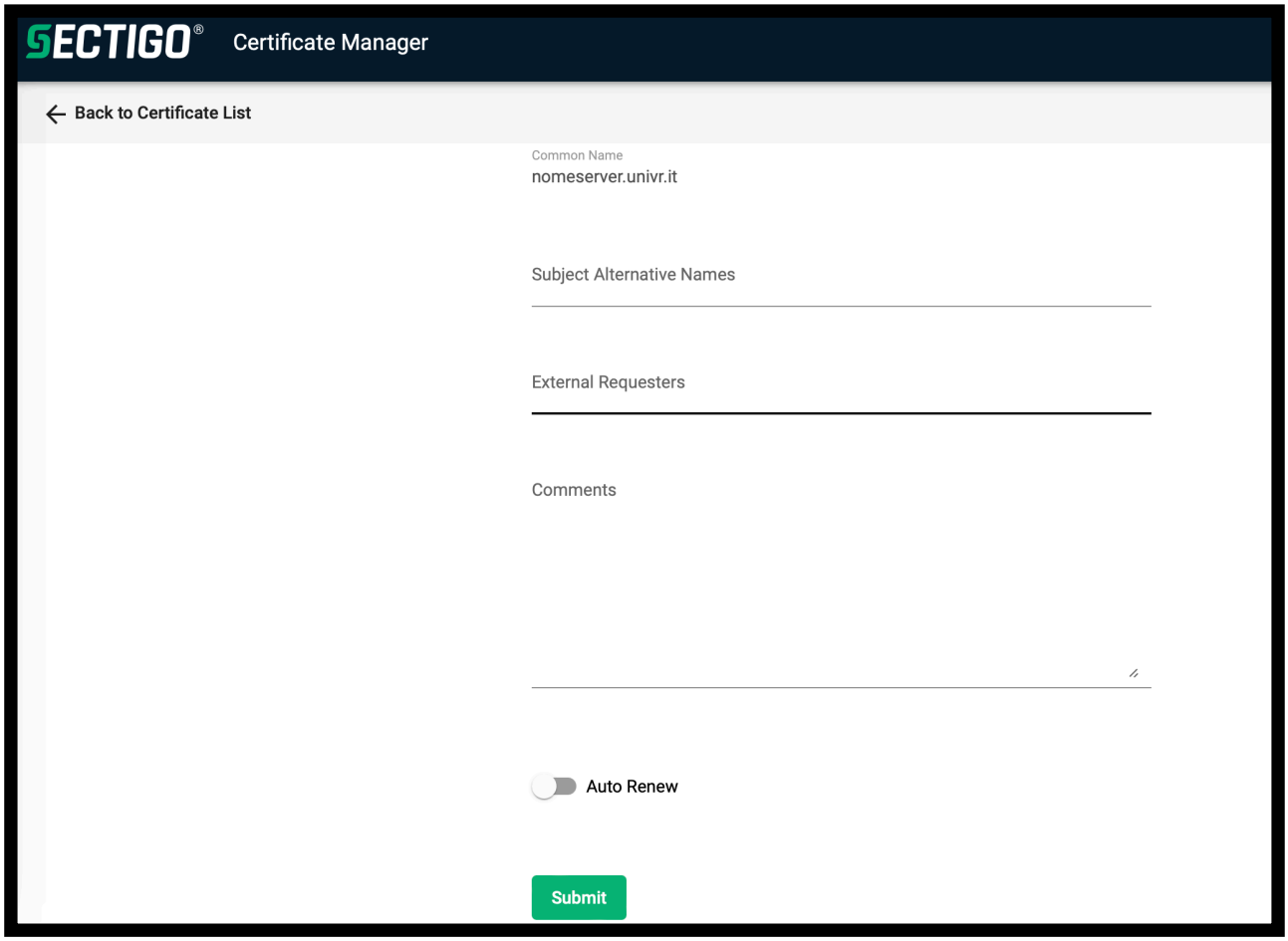
Compilare il campo Access Code con: **CCT223pm** e cliccare **Next**



La pagina successiva sarà la seguente:



In questa pagina si andrà ad inserire il CSR precedentemente creato dal comando di pagina 2



Common Name: viene ricavato dalla CSR;

Subject Alternative Names: sono eventuali nomi aggiuntivi richiesti per il server;

External Requester: eventuali indirizzi aggiuntivi ai quali devono essere inviate eventuali notifiche relative al certificato (es. colleghi, indirizzo di Area o Gruppo, ecc.), separati da virgola

OPZIONALE: **Auto Renew** per autorizzare il rinnovo automatico

Al termine cliccare il bottone **Submit**

UNIVERSITÀ
di VERONA

C.
Approvazione della richiesta
da parte del personale dell'Area Networking

Una volta completata la procedura di richiesta, viene mandata una mail

Certificate Services Manager <support@cert-manager.com>
SSL certificate for (nomeserver.univr.it) AWAITING APPROVAL

Al richiedente e al personale dell'Area Networking, che poi procederà alla verifica e di seguito all'approvazione.

ATTENZIONE ricordiamo che:
Non verranno approvati 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;

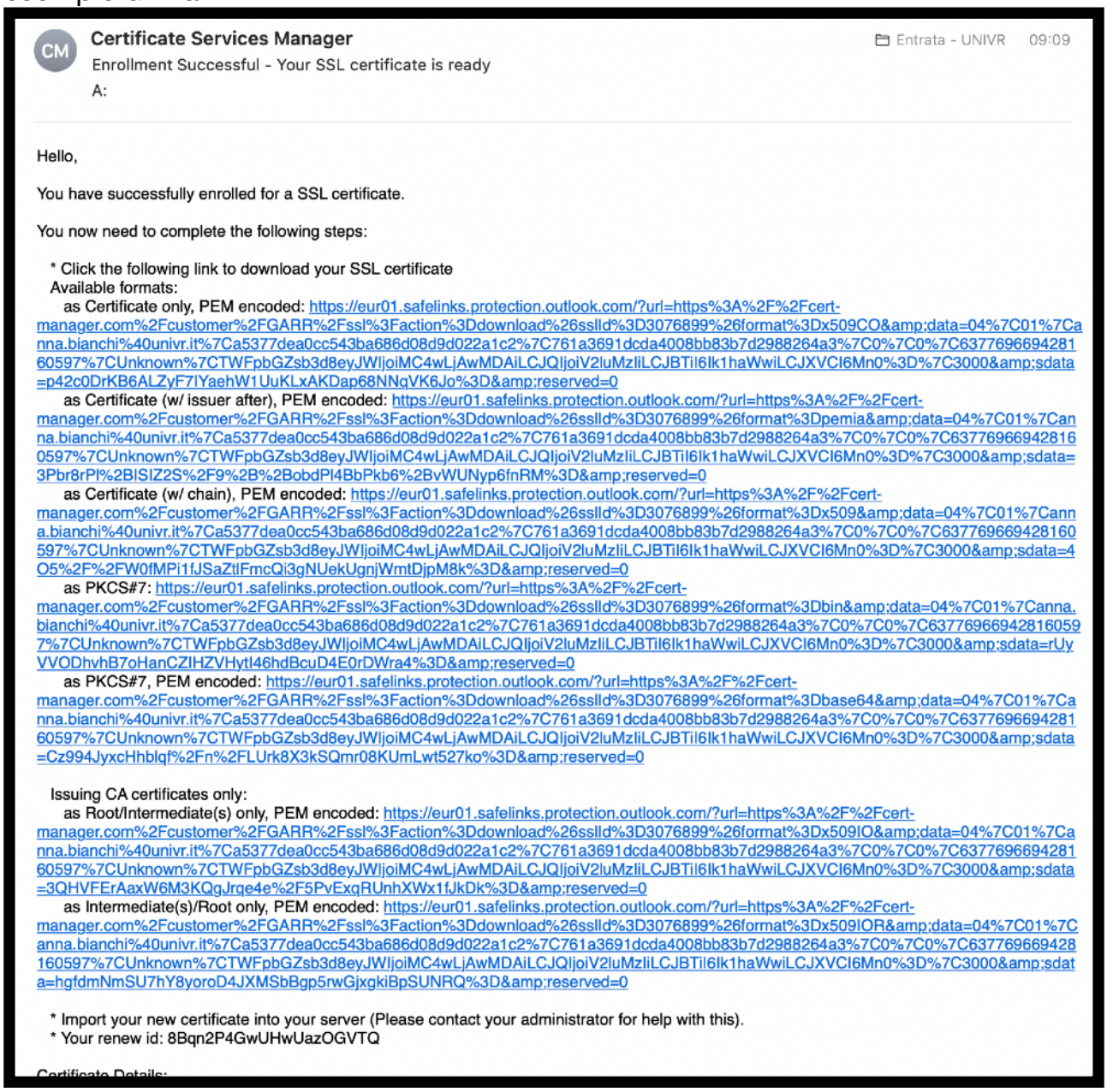
Con Common Name o Subject Alternative Names in conflitto con altri certificati emessi in precedenza, salvo eccezioni concordate individualmente.

A seguito dell'approvazione, sia il richiedente sia gli External Requesters riceveranno notifica via mail della disponibilità del certificato.

UNIVERSITÀ di VERONA

D.
Creazione (da parte della CA) del certificato CERT firmato dalla CA stessa

Una volta approvata la richiesta da parte del personale dell'Area Networking arriverà una mail con i link per tutte le componenti dei certificati richiesti. Ecco un esempio di mail:



CM **Certificate Services Manager** Entrata - UNIVR 09:09

Enrollment Successful - Your SSL certificate is ready

A:

Hello,

You have successfully enrolled for a SSL certificate.

You now need to complete the following steps:

* Click the following link to download your SSL certificate
Available formats:
as Certificate only, PEM encoded: https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcert-manager.com%2Fcustomer%2FGARR%2Fssl%3Faction%3Ddownload%26sslId%3D3076899%26format%3Dx509CO&data=04%7C01%7Canna.bianchi%40univr.it%7Ca5377dea0cc543ba686d08d9d022a1c2%7C761a3691dcda4008bb83b7d2988264a3%7C0%7C0%7C637769669428160597%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=p42c0DrKB6ALZyF7IYaehW1UuKLxAKDap68NNqVK6Jo%3D&reserved=0
as Certificate (w/ issuer after), PEM encoded: https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcert-manager.com%2Fcustomer%2FGARR%2Fssl%3Faction%3Ddownload%26sslId%3D3076899%26format%3Dpemia&data=04%7C01%7Canna.bianchi%40univr.it%7Ca5377dea0cc543ba686d08d9d022a1c2%7C761a3691dcda4008bb83b7d2988264a3%7C0%7C0%7C637769669428160597%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=3Pbr8rPl%2BISIZ2S%2F9%2B%2BobdPl4BbPkb6%2BvWUNyp6fnRM%3D&reserved=0
as Certificate (w/ chain), PEM encoded: https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcert-manager.com%2Fcustomer%2FGARR%2Fssl%3Faction%3Ddownload%26sslId%3D3076899%26format%3Dx509&data=04%7C01%7Canna.bianchi%40univr.it%7Ca5377dea0cc543ba686d08d9d022a1c2%7C761a3691dcda4008bb83b7d2988264a3%7C0%7C0%7C637769669428160597%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=4O5%2F%2FW0fMPi1fJSaZtlFmcQi3gNUekUgnjWmtDjpM8k%3D&reserved=0
as PKCS#7: https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcert-manager.com%2Fcustomer%2FGARR%2Fssl%3Faction%3Ddownload%26sslId%3D3076899%26format%3Dbin&data=04%7C01%7Canna.bianchi%40univr.it%7Ca5377dea0cc543ba686d08d9d022a1c2%7C761a3691dcda4008bb83b7d2988264a3%7C0%7C0%7C6377696694281605597%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=rUyVVODhvhB7oHanCZIHZVHytI46hdBcuD4E0rDWra4%3D&reserved=0
as PKCS#7, PEM encoded: https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcert-manager.com%2Fcustomer%2FGARR%2Fssl%3Faction%3Ddownload%26sslId%3D3076899%26format%3Dbase64&data=04%7C01%7Canna.bianchi%40univr.it%7Ca5377dea0cc543ba686d08d9d022a1c2%7C761a3691dcda4008bb83b7d2988264a3%7C0%7C0%7C637769669428160597%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=Cz994JyxcHhblqf%2Fn%2FLUrk8X3kSQmr08KUmLwt527ko%3D&reserved=0

Issuing CA certificates only:
as Root/Intermediate(s) only, PEM encoded: https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcert-manager.com%2Fcustomer%2FGARR%2Fssl%3Faction%3Ddownload%26sslId%3D3076899%26format%3Dx509IO&data=04%7C01%7Canna.bianchi%40univr.it%7Ca5377dea0cc543ba686d08d9d022a1c2%7C761a3691dcda4008bb83b7d2988264a3%7C0%7C0%7C637769669428160597%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=3QHVFErAaxW6M3KQgJrqe4e%2F5PvExqRUnhXWx1fJkDk%3D&reserved=0
as Intermediate(s)/Root only, PEM encoded: https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcert-manager.com%2Fcustomer%2FGARR%2Fssl%3Faction%3Ddownload%26sslId%3D3076899%26format%3Dx509IOR&data=04%7C01%7Canna.bianchi%40univr.it%7Ca5377dea0cc543ba686d08d9d022a1c2%7C761a3691dcda4008bb83b7d2988264a3%7C0%7C0%7C637769669428160597%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=hgfdmNmSU7hY8yoroD4JXMSbBgp5rwGjxgkiBpSUNRQ%3D&reserved=0

* Import your new certificate into your server (Please contact your administrator for help with this).
* Your renew id: 8Bqn2P4GwUHwUazOGVTQ

Certificate Details:

Suggeriamo di salvare le parti di un certificato in una cartella protetta e facilmente recuperabile