Sectigo - HowTo: Personal/Client Certificate

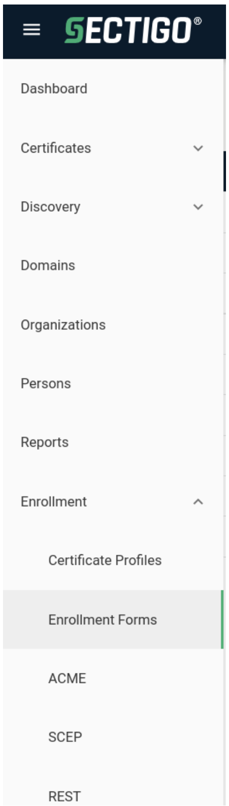
Table of Contents

1. Step-by-step guide

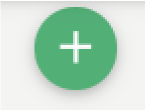
1.1. Create an Enrollment Form

First things first you'll need to **create** on SCM **an Enrollment Endpoint** for your Organization.

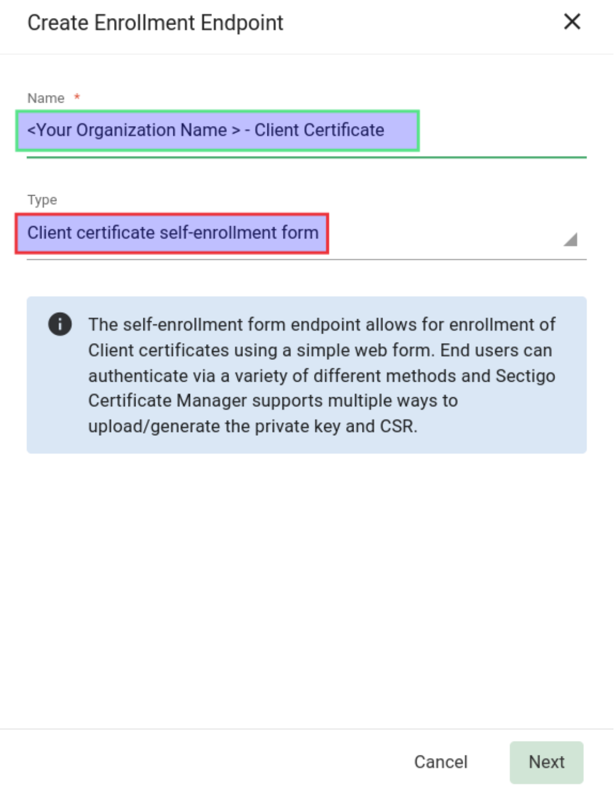
- Log on on Sectigo Certificate Manager
- Dashboard (Left Pane) Enrollment   Enrollment Forms



- Click on the + sign at the top right



- Within the *Create Enrollment Endpoint* window:
  - Name: Set here the name of the Enrollment Form for your Organization. We recommend to specify also the type of the Form: (e.g.) **<Your Organization Name > - Client Certificate**
  - Type: select **Client certificate self-enrollment form**



Create Enrollment Endpoint

Name *

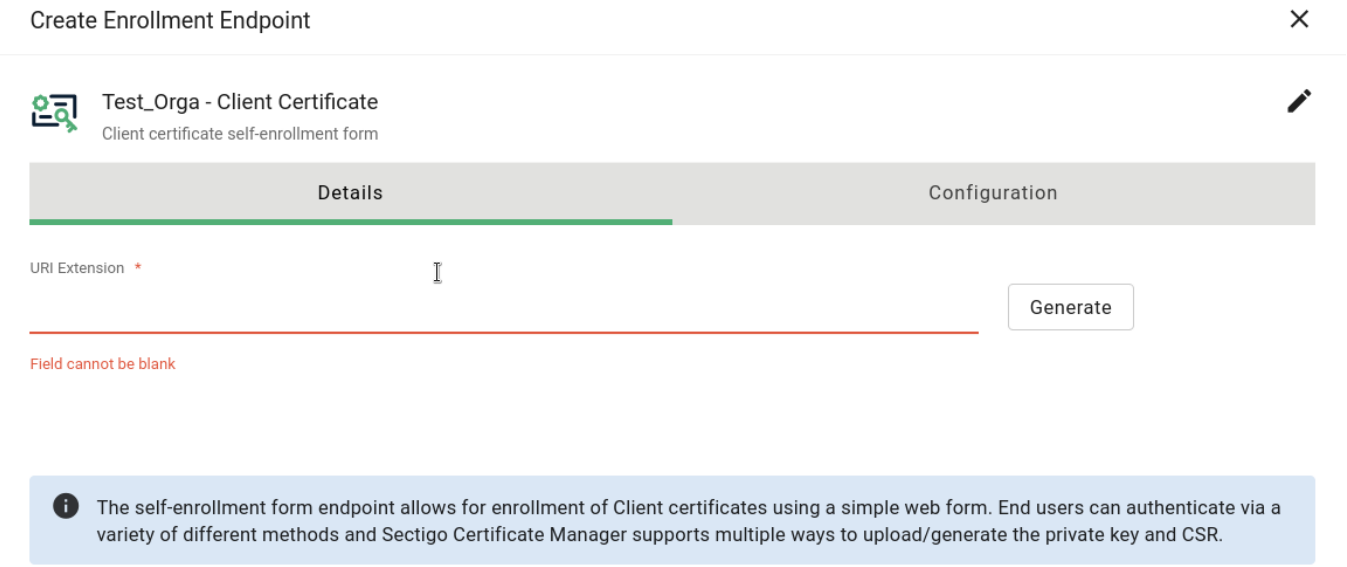
<Your Organization Name > - Client Certificate

Type

Client certificate self-enrollment form

The self-enrollment form endpoint allows for enrollment of Client certificates using a simple web form. End users can authenticate via a variety of different methods and Sectigo Certificate Manager supports multiple ways to upload/generate the private key and CSR.

  - Click **Next**
- On the ***Details*** tab, click on Generate to get your Enrollment Endpoint Form URL



Create Enrollment Endpoint

Test_Orga - Client Certificate

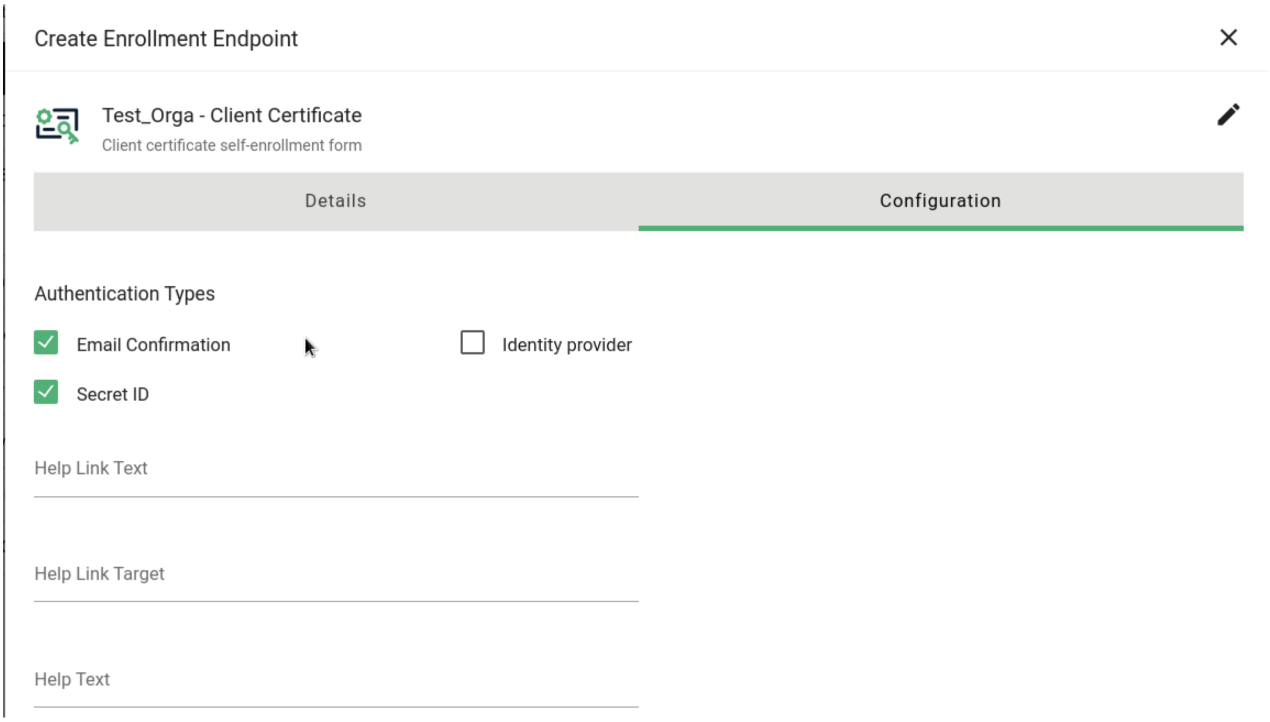
Client certificate self-enrollment form

URI Extension *

Field cannot be blank

The self-enrollment form endpoint allows for enrollment of Client certificates using a simple web form. End users can authenticate via a variety of different methods and Sectigo Certificate Manager supports multiple ways to upload/generate the private key and CSR.

- In the ***Configuration*** tab, select both *Authentication Types*:
  - **Email Confirmation**
  - **Secret ID**



Create Enrollment Endpoint

Test_Orga - Client Certificate

Client certificate self-enrollment form

Details | Configuration

Authentication Types

☑ Email Confirmation ☐ Identity provider

☑ Secret ID

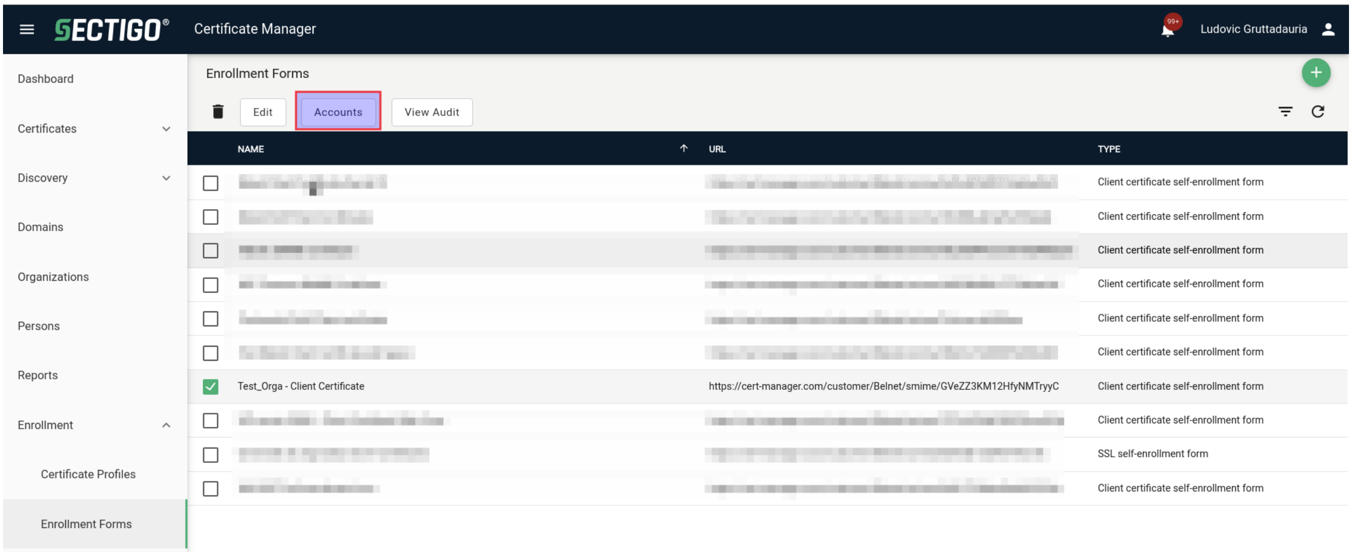
Help Link Text

Help Link Target

Help Text

1.2. Create an account for the Enrollment Form Endpoint

- SCM Dashboard (Left Pane) Enrollment   Enrollment Forms: **Select** your newly created Enrollment Form Endpoint
- Click on **Accounts**



Enrollment Forms

	NAME	URL	TYPE
☐	[redacted]	[redacted]	Client certificate self-enrollment form
☐	[redacted]	[redacted]	Client certificate self-enrollment form
☐	[redacted]	[redacted]	Client certificate self-enrollment form
☐	[redacted]	[redacted]	Client certificate self-enrollment form
☐	[redacted]	[redacted]	Client certificate self-enrollment form
☐	[redacted]	[redacted]	Client certificate self-enrollment form
☑	Test_Orga - Client Certificate	https://cert-manager.com/customer/Belnet/smime/GVeZZ3KM12HfyNMTryyC	Client certificate self-enrollment form
☐	[redacted]	[redacted]	Client certificate self-enrollment form
☐	[redacted]	[redacted]	SSL self-enrollment form
☐	[redacted]	[redacted]	Client certificate self-enrollment form

- A new window is prompted to you. Now click on the **+** sign at the top right to add an Account.

1.2.1. Authorization Type: Access Code

Access Code is one of the two Authorization Method.
The Access Code method will allow you to communicate an access code to all users of your Organisation who wish to obtain a Client Certificate via your Enrollment Form URL.

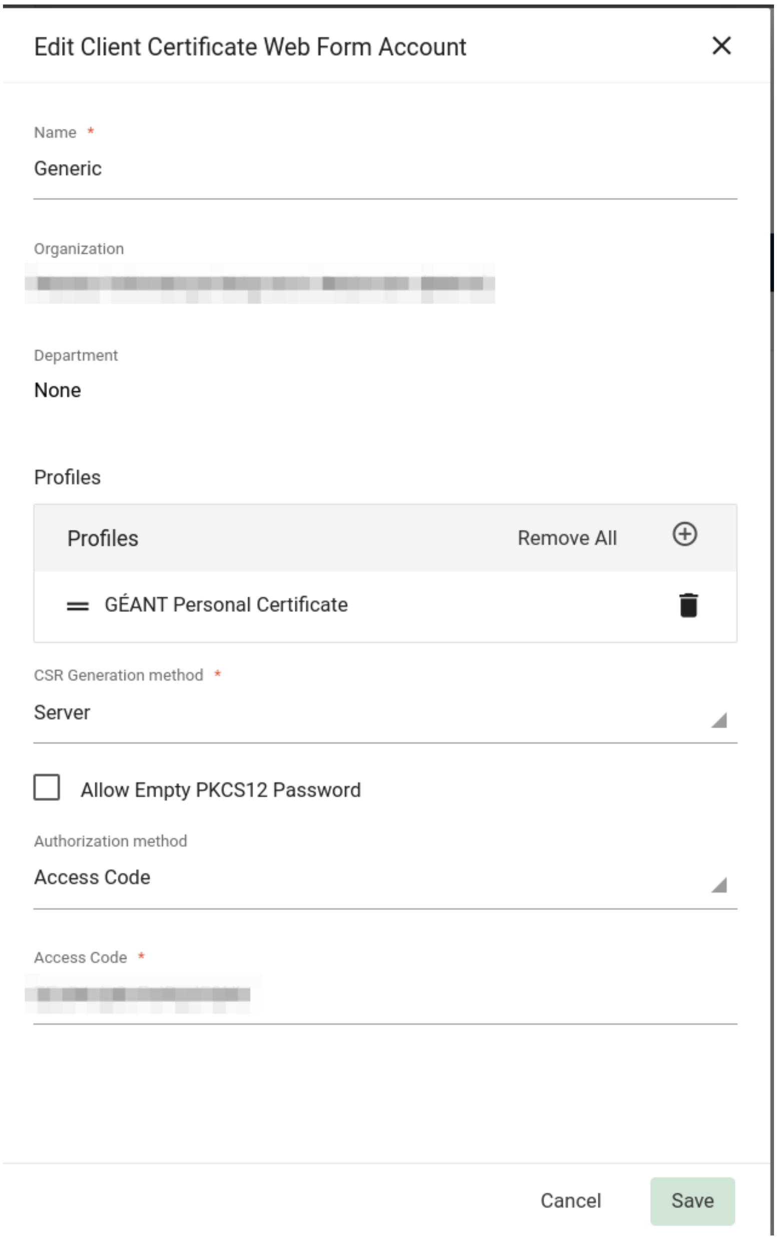
> It is important to note that this code must NEVER leave your institution.
>
> It should be noted that Sectigo does however check the domain of the email address before generating the certificate(s).

- Edit the Client Certificate Web Form Account
  - Give an account name: (e.g.) **<Org.Name> - Access Code**
  - Organization: **Select your Organization** in the drop down list

- Department: **None**

  "!!ATTENTION!! If you do specify a Department of your Organization here, all Client Certificate will have the specified department assigned to people requesting the Client Certificate using this Enrollment Account."

- Profiles: add **Géant Personal Certificate**
- CSR Generation method: **Server**
- Authorization Method: **Access Code**
- Access Code: **<enter_here_your_desired_access_code>** (mix of numbers, letters, capital letters and special characters)



Edit Client Certificate Web Form Account ✕

Name *

Generic

Organization

[redacted]

Department

None

Profiles

Profiles	Remove All ⊕
GÉANT Personal Certificate	

CSR Generation method *

Server

□ Allow Empty PKCS12 Password

Authorization method

Access Code

Access Code *

[redacted]

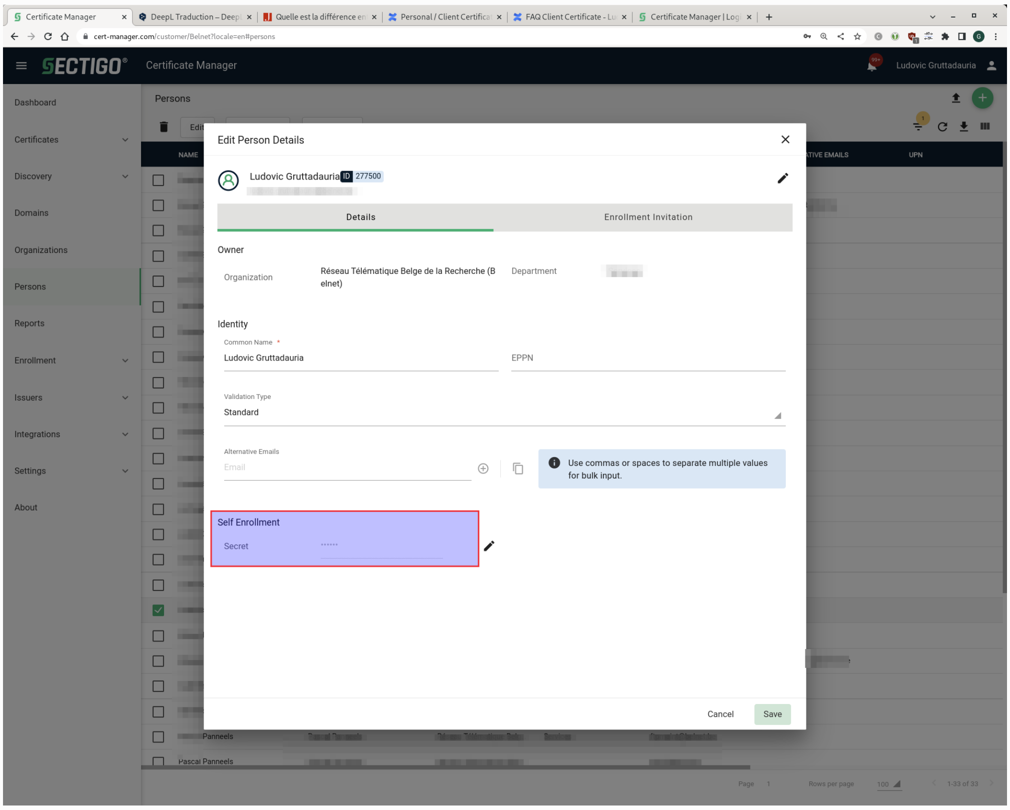
Cancel Save

1.2.2. Authorization Type: Secret ID

1.2.2.1. Create the person prior to let him/her requesting a Personal/client Certificate via Secret ID

Unlike the method via Access Code, the method via SecretID requires that a (D)RAO of your Organisation **FIRST** creates the user in SCM by specifying a SecretID for this person.

SCM Dashboard (Left Pane) **Persons**



Edit Person Details

Ludovic Gruttadauria ID 277500

Owner

Organization: Réseau Télématique Belge de la Recherche (Belnet)

Department:

Identity

Common Name *: Ludovic Gruttadauria

EPPN:

Validation Type: Standard

Alternative Emails: Email

Use commas or spaces to separate multiple values for bulk input.

Self Enrollment

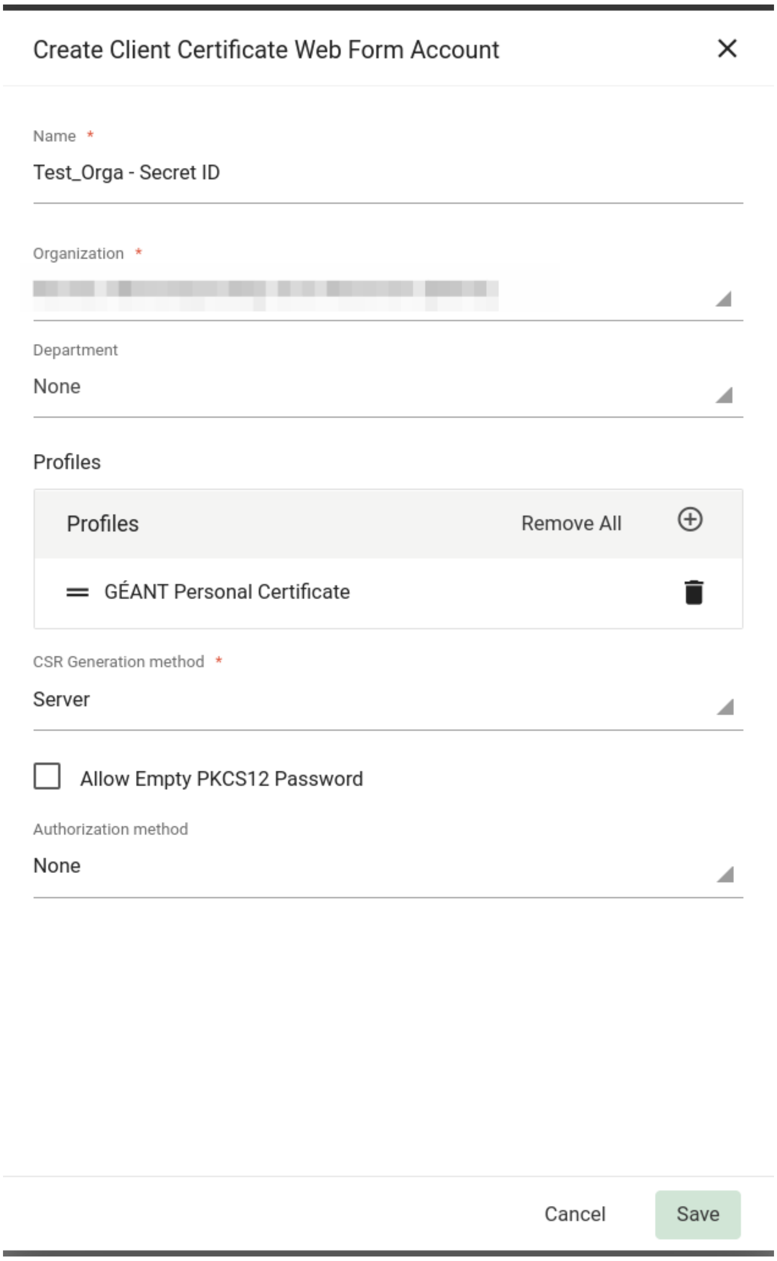
Secret: ••••••

1.2.2.2. Create the account to be used for SecreID method within your Enrollment Form

- Edit the Client Certificate Web Form Account
  - Give an account name: (e.g.) **<Org.Name> - SecretID**
  - Organization: **Select your Organization** in the drop down list
  - Department: **None**

    "!!ATTENTION!! If you do specify a Department of your Organization here, the person must be first assigned to the specified department to make use this account to request a Client Certificate using this Enrollment Account via SecretID."

  - Profiles: add **Géant Personal Certificate**
  - CSR Generation method: **Server**
  - Authorization Method: **None**



Create Client Certificate Web Form Account

Name *
Test_Orga - Secret ID

Organization *
[redacted]

Department
None

Profiles

Profiles	Remove All
GÉANT Personal Certificate	

CSR Generation method *
Server

□ Allow Empty PKCS12 Password

Authorization method
None

2. How to request Personnal / Client Certificate

Via Sectigo you can request a personal client certificate, this can be used for

- s/mime email signing and encryption
- authentication to websites

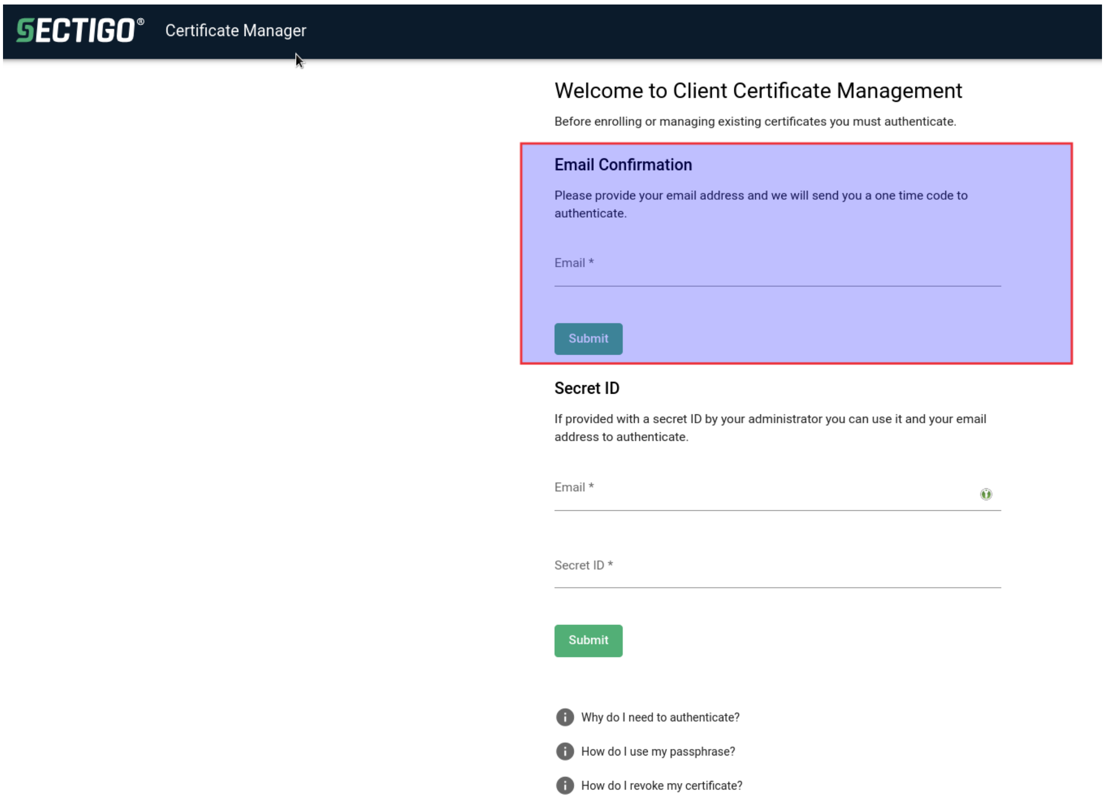
2.1. Request via Access Code

Employees of your organisation can request customer certificates via Access Code in the following way:

- Ask them to log in to the Enrollment Form URL you created for your Organization.

  You can review the URL on SCM dashboard (Left Pane) Enrollment   Enrollment Forms

- Use the first option with **"Email Confirmation**" (not valid for Secret ID method)


SECTIGO® Certificate Manager

Welcome to Client Certificate Management

Before enrolling or managing existing certificates you must authenticate.

Email Confirmation

Please provide your email address and we will send you a one time code to authenticate.

Email *

Secret ID

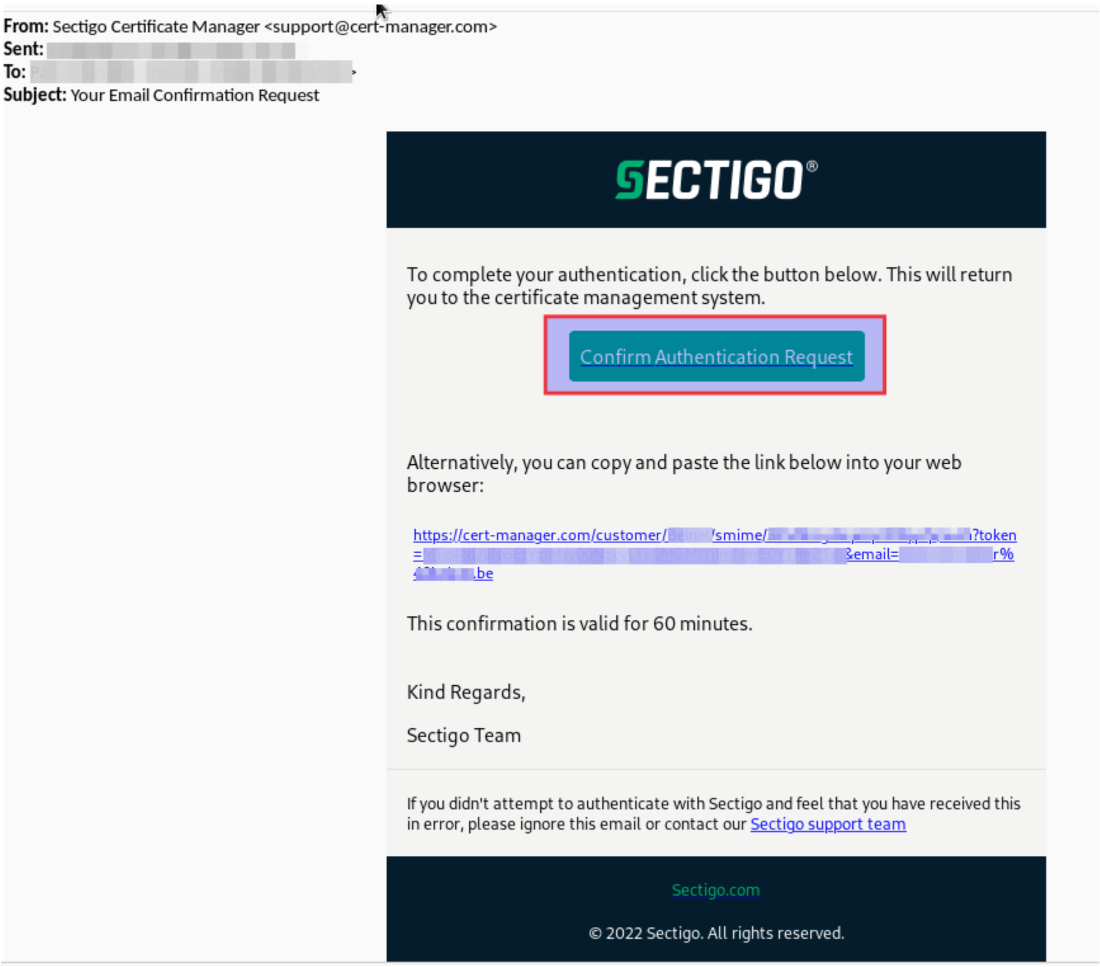
If provided with a secret ID by your administrator you can use it and your email address to authenticate.

Email *

Secret ID *

Why do I need to authenticate?
How do I use my passphrase?
How do I revoke my certificate?

- Enter your Organization email (firstname.lastname@your_org.tld)
- The person must now check your his/her email and **confirm the link received**.



From: Sectigo Certificate Manager <support@cert-manager.com>
Sent: [redacted]
To: [redacted]
Subject: Your Email Confirmation Request

To complete your authentication, click the button below. This will return you to the certificate management system.

Alternatively, you can copy and paste the link below into your web browser:

https://cert-manager.com/customer/[redacted]/smime/[redacted]?token=[redacted]&email=[redacted]r%[redacted].be

This confirmation is valid for 60 minutes.

Kind Regards,

Sectigo Team

If you didn't attempt to authenticate with Sectigo and feel that you have received this in error, please ignore this email or contact our Sectigo support team

Sectigo.com

© 2022 Sectigo. All rights reserved.

- The link will redirect the person to a page where they will have to specify your organization's Access Code: **<enter_the_access_code>**

Your Organization access code can be communicated to the person directly or published on your intranet for example (with this procedure).

(⚠ please don't distribute it outside your Organization)

- **Complete the form**:
  - You can change 'certificate term' to 3 years
  - PKCS#12 password is used to protect your certificate (you need it later when you import the certificate)
- Click '**Submit**'
- Now you can download your certificate (.p12 file). You can them import this .p12 file in your browser and/or mail client (you need your PKCS#12 password for this).

2.2. Request Via Secret ID

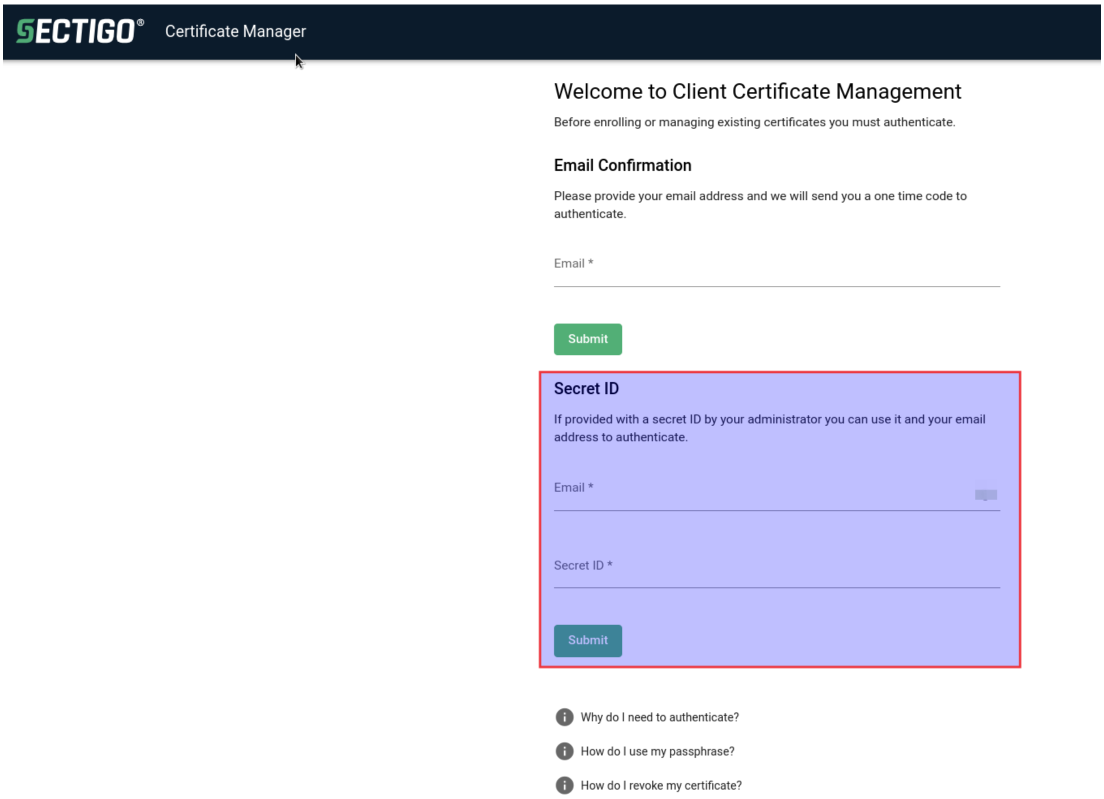
The method via SecretID requires that a (D)RAO of your Organisation **FIRST** creates the user in SCM by specifying a SecretID for this person.

Employees of your organisation can request customer certificates via Secret ID in the following way:

- Ask them to log in to the Enrollment Form URL you created for your Organization.

  You can review the URL on SCM dashboard (Left Pane) Enrollment   Enrollment Forms

- Use the first option with "**Secret ID**
- Enter your Organization email (firstname.lastname@your_org.tld)
- Enter the **SecretID code** for the person requesting the certificate (See **SCM Dashboard Persons)**



Welcome to Client Certificate Management

Before enrolling or managing existing certificates you must authenticate.

Email Confirmation

Please provide your email address and we will send you a one time code to authenticate.

Email *

Submit

Secret ID

If provided with a secret ID by your administrator you can use it and your email address to authenticate.

Email *

Secret ID *

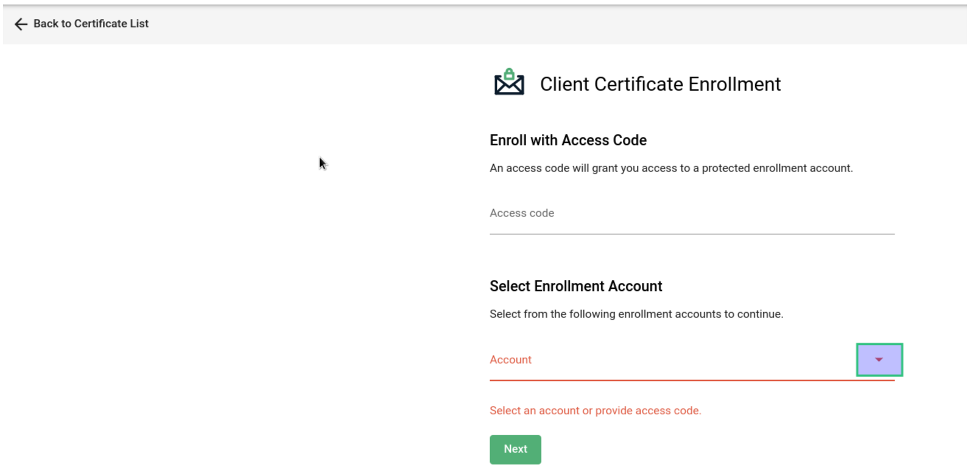
Submit

Why do I need to authenticate?

How do I use my passphrase?

How do I revoke my certificate?

- **Select** your Organization **account set for Secret ID** using the drop-down list, then click on **Next**



Client Certificate Enrollment

Enroll with Access Code

An access code will grant you access to a protected enrollment account.

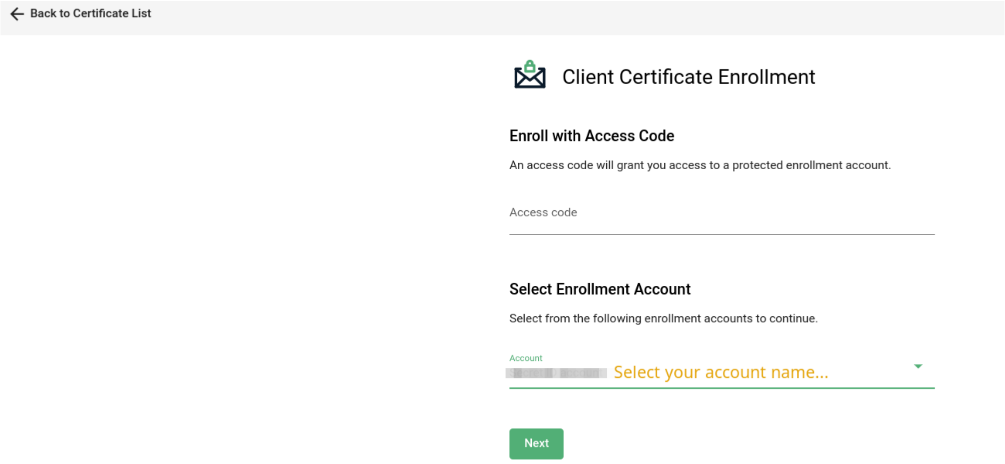
Access code

Select Enrollment Account

Select from the following enrollment accounts to continue.

Account

Select an account or provide access code.



Client Certificate Enrollment

Enroll with Access Code

An access code will grant you access to a protected enrollment account.

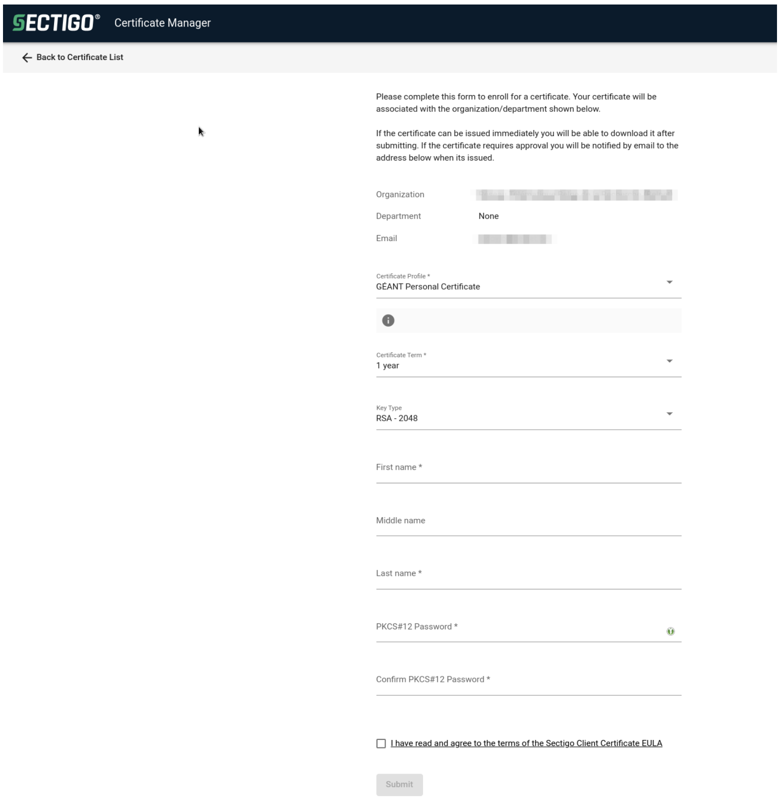
Access code

Select Enrollment Account

Select from the following enrollment accounts to continue.

Account: [redacted] Select your account name...

- The person is now invited to complete the form to enroll for a certificate. The certificate will be associated with the organization/department shown in the form. E.G.:
  - **Complete the form:**
    - You can change 'certificate term' to 3 years
    - PKCS#12 password is used to protect your certificate (you need it later when you import the certificate)
  - **accept EULA** conditions
  - Click '**Submit**'
  - Now you can download your certificate (.p12 file). You can them import this .p12 file in your browser and/or mail client (you need your PKCS#12 password for this).



Please complete this form to enroll for a certificate. Your certificate will be associated with the organization/department shown below.

If the certificate can be issued immediately you will be able to download it after submitting. If the certificate requires approval you will be notified by email to the address below when its issued.

Organization	[redacted]
Department	None
Email	[redacted]

Certificate Profile *
GÉANT Personal Certificate

Certificate Term *
1 year

Key Type
RSA - 2048

First name *

Middle name

Last name *

PKCS#12 Password *

Confirm PKCS#12 Password *

□ I have read and agree to the terms of the Sectigo Client Certificate EULA

3. Related articles

The Sectigo KB is a good source of documentation: https://sectigo.com/knowledge-base/detail/Sectigo-Certificate-Manager-SCM-Administrator-s-Guide/kA01N000000bvJA
The document "Sectigo® Certificate Manager Administrator Guide.pdf" explains the different methods.

If the number of client certificates is massive, a large number of people within an Organisation, the method "end-user self-enrollment by Access Code" is preferable.

If the number of client certificates is limited to a few people, we recommend the "end-user self-enrollment by secret identifier" method explained in chapter 3.3.3.2 on page 111.

> However, the Secret ID method requires that an RAO in your organization creates the person (who wants a client certificate) in SCM BEFORE that person logs into the Enrollment Form to request the client certificate.