

Emisión de certificados de firma de código (CS) mediante SCM

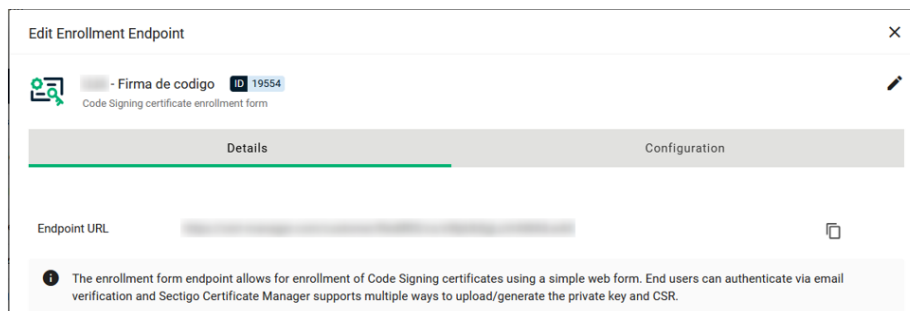
(actualizado a noviembre 2024)

En este procedimiento se indican los pasos necesarios para solicitar desde el portal **SCM** (*Sectigo Certificate Manager*) certificados de tipo CS (*Code Signing*) para firma de código. El procedimiento a seguir cambia respecto al que estaba establecido originalmente, debido al hecho de que ahora se han reforzado los niveles de seguridad y es obligatorio el uso de un token físico.

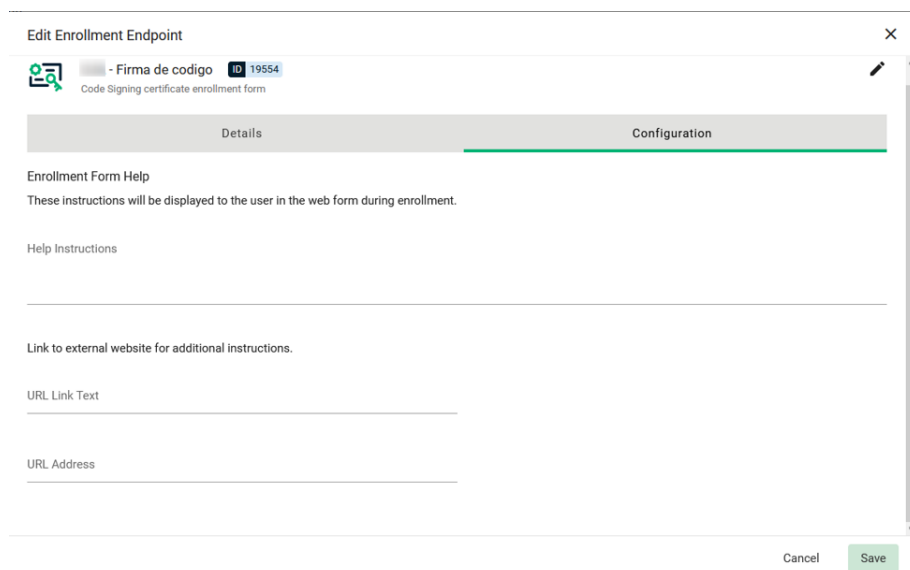
1.1. Pasos previos

- **Enrollment Endpoint.** Tenemos que tener definido un formulario web de solicitud (**Enrollment > Enrollment Forms**), para que nuestros usuarios autorizados (aquellos con cuenta en SCM) puedan solicitarnos certificados CS. Aunque ahí podemos ver el de todas las universidades que han definido uno, cada organismo debería tener el suyo propio, con una URL asociada al Enrollment Form que es la que tenemos que facilitar a nuestros solicitantes.

NOTA: a esta URL solo pueden acceder los usuarios autorizados, y en la pestaña **Configuration** podemos indicar instrucciones para dichos solicitantes:

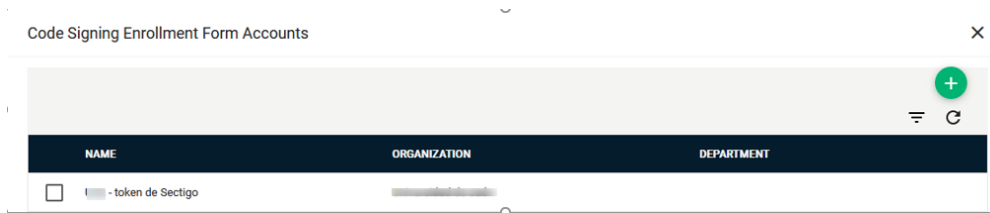


The screenshot shows the 'Edit Enrollment Endpoint' dialog box with the 'Details' tab selected. The title bar reads 'Edit Enrollment Endpoint'. Below the title bar, there is a header area with a gear icon, the text '- Firma de código' and 'ID 19554', and a sub-header 'Code Signing certificate enrollment form'. A horizontal bar below the header has two tabs: 'Details' (selected) and 'Configuration'. Under the 'Details' tab, there is a field for 'Endpoint URL' with a copy icon to its right. Below this field is a note: 'The enrollment form endpoint allows for enrollment of Code Signing certificates using a simple web form. End users can authenticate via email verification and Sectigo Certificate Manager supports multiple ways to upload/generate the private key and CSR.'



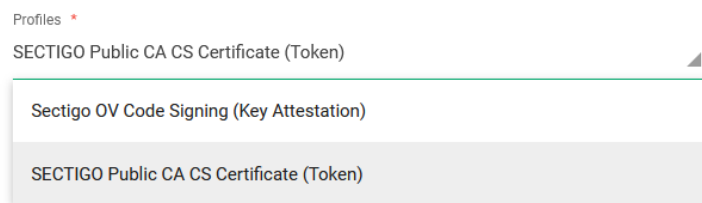
The screenshot shows the 'Edit Enrollment Endpoint' dialog box with the 'Configuration' tab selected. The title bar reads 'Edit Enrollment Endpoint'. Below the title bar, there is a header area with a gear icon, the text '- Firma de código' and 'ID 19554', and a sub-header 'Code Signing certificate enrollment form'. A horizontal bar below the header has two tabs: 'Details' and 'Configuration' (selected). Under the 'Configuration' tab, there is a section titled 'Enrollment Form Help' with the text 'These instructions will be displayed to the user in the web form during enrollment.' Below this is a section titled 'Help Instructions' with a text input field. Further down is a section titled 'Link to external website for additional instructions.' with two text input fields labeled 'URL Link Text' and 'URL Address'. At the bottom right of the dialog box are 'Cancel' and 'Save' buttons.

- **Cuentas asociadas.** Un Enrollment Endpoint tiene una serie de cuentas asociadas (se pueden ver seleccionando el form y pulsando el botón **Accounts**. Ejemplo:



IMPORTANTE: seleccionar las opciones correctas para la cuenta:

- Los campos **Name**, **Organization** y **Department** se explican por sí mismos.
- En **Profiles**, seleccionamos **SECTIGO Public CA CS Certificate (Token)**. Este es el perfil necesario para que SECTIGO nos cifre y nos envíe su propio token físico.



- En **CSR generation method**, seleccionamos el único que está disponible para el perfil seleccionado en el paso anterior:

CSR generation method

Sectigo Shipped FIPS Certified USB Token/Key

ALTERNATIVA

La opción más fácil y recomendable es que el token físico nos lo envíe directamente SECTIGO con las opciones descritas anteriormente.

Como alternativa, podríamos usar nuestro propio token físico, de entre los soportados por SECTIGO. Pero con esta opción, además de requerir una marca y modelo soportados que tenemos que comprar nosotros, el cifrado lo debemos hacer nosotros y se necesitan más opciones, que pueden ser complejas. Si usamos este método alternativo, las opciones que se deben seleccionar son:

Profiles *

Sectigo OV Code Signing (Key Attestation)

CSR generation method

Provided by user

1.2. Procedimiento para la solicitud

Una vez configurados los elementos anteriores (esto solo se hace la primera vez), de forma resumida, el proceso a seguir es el siguiente:

- 1) Un **RAO/DRAO invita** a un usuario (que puede ser el mismo RAO/DRAO) para que pueda solicitar un certificado CS. Esto se hace desde **Certificates > Code Signing Certificates > botón Invitations**.
- 2) Pulsamos el botón + y rellenamos los datos de la invitación:

Send Invitation

Email *

Details

Enrollment Endpoint *

- Firma de codigo

Account *

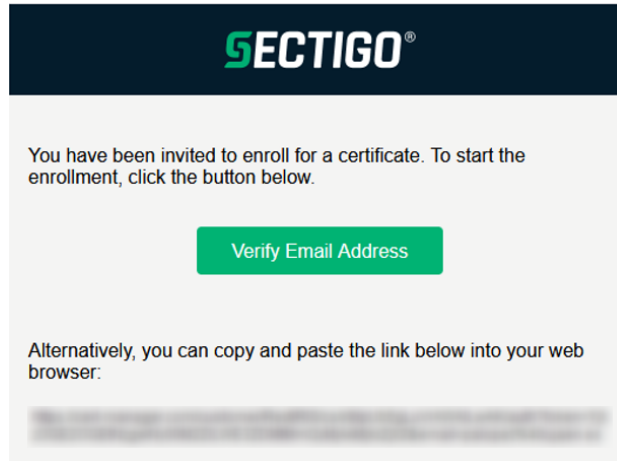
- token de Sectigo

Profile SECTIGO Public CA CS Certificate (Token)

Cancel Send

Básicamente hay que indicar la dirección de e-mail a la que enviar la invitación, y seleccionar el Enrollment Endpoint y la cuenta asociada.

- 3) El **usuario** recibe un email para que verifique la dirección de correo e inicie el proceso de solicitud del certificado:



- 4) Una vez confirmada, el usuario es conducido a una web para confirmar su dirección de e-mail:

Welcome to Code Signing Certificate Management

Before enrolling or managing existing certificates you must authenticate.

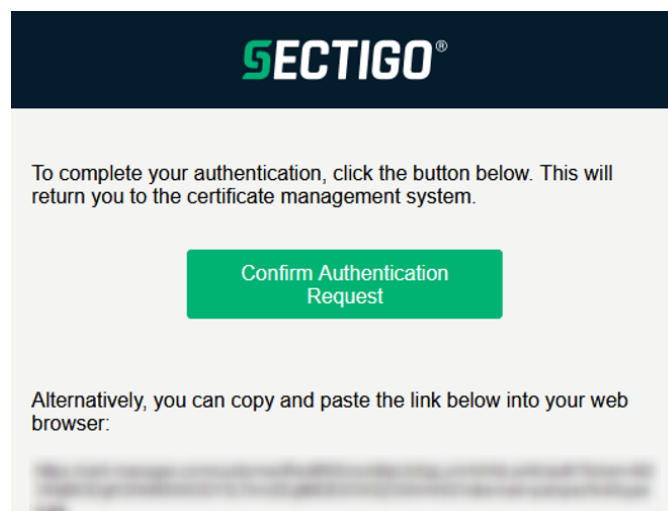
Email Confirmation

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

Email *

Submit

- 5) El solicitante recibe un segundo correo para confirmar la autenticación de la petición:



Y es entonces cuando es redirigido al formulario de solicitud

Code Signing Certificate Enrollment

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.

Organization

Department **None**

Email

Certificate Term *
3 years ▼

Certificate Email (SAN)

First name *

Last name *

Shipping Type * ▼
Shipping Type can not be empty

Provide additional shipping details

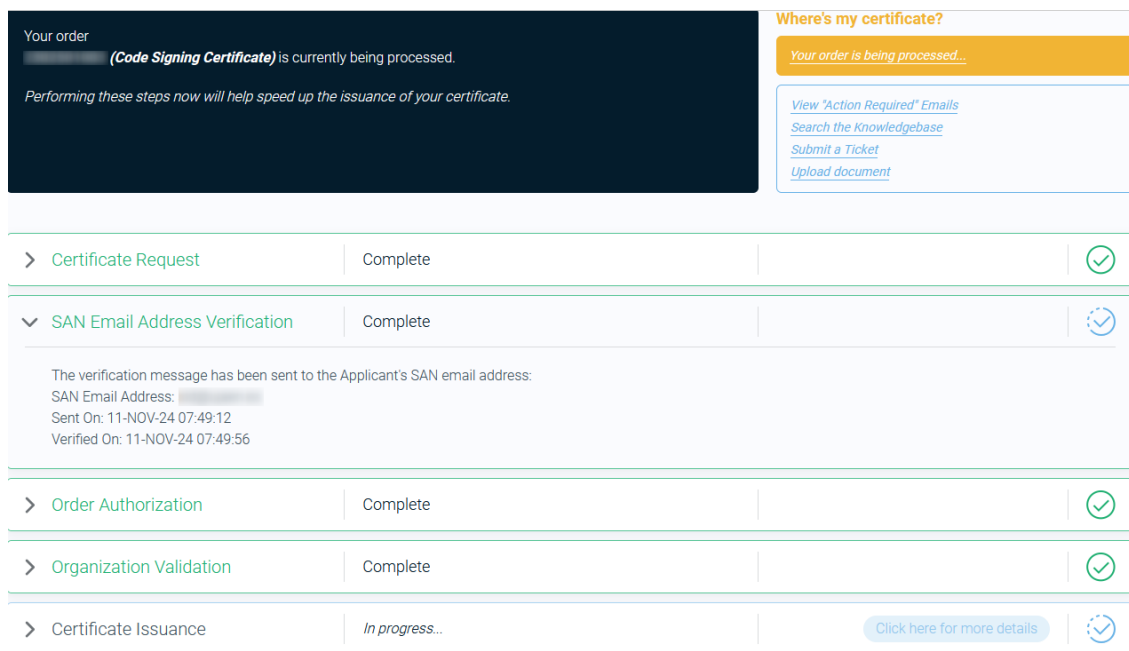
I have read and agree to the terms of the Sectigo Code Signing Certificate EULA

6) Aquí, el solicitante debe rellenar los campos solicitados. Muy importante el campo **Shipping Type** y marcar la casilla **Provide additional shipping details**, donde le pedirá con todo detalle la información necesaria para el envío por parte de SECTIGO.

7) Llegados a este punto, el certificado aparecerá en el portal SCM como **APPLIED** y habrá que ir esperando la información que SECTIGO vaya enviando por correo electrónico a la dirección indicada:

Code Signing Certificates		Search by ID or Subject Alt Name					
	STATUS	ORDER NUMBER	CERTIFICATE P...	TERM	REQUESTED VIA	ORGANIZATION	DEPARTMENT
<input type="checkbox"/>	APPLIED		SECTIGO Publi...	1095	Enrollment Form		

- 8) El solicitante, recibirá un código de verificación que tiene que confirmar y a partir de ahí, queda esperar que la emisión siga su curso. Se puede consultar el estado en todo momento, mediante un link recibido que lleva a un panel de estado similar a este:



Where's my certificate?

Your order is being processed...

View "Action Required" Emails
Search the Knowledgebase
Submit a Ticket
Upload document

> Certificate Request	Complete	✓
∨ SAN Email Address Verification	Complete	⌚
The verification message has been sent to the Applicant's SAN email address: SAN Email Address: [redacted] Sent On: 11-NOV-24 07:49:12 Verified On: 11-NOV-24 07:49:56		
> Order Authorization	Complete	✓
> Organization Validation	Complete	✓
> Certificate Issuance	In progress...	⌚

Click here for more details

- 9) Finalmente, el **usuario** recibirá el token físico con el certificado emitido y ya estará en disposición de usarlo.

1.3. Uso del token

Una vez recibido el token físico, las instrucciones para hacer uso de él son las siguientes:

- El primer paso es instalar Safenet Authentication Client (SAC):
<https://www.sectigo.com/knowledge-base/detail/SafeNet-Authentication-Client-Download-for-Sectigo-Certificates-on-eToken/kA03I000000o6kl>
- En el zip que se descarga hay que buscar el .msi y ejecutarlo con las opciones por defecto. Instala la versión 10.9 R1.
- Una vez instalado abrimos Safenet Authentication client y entonces es cuando conectamos el token USB. Si no se hace en ese orden el programa no lo reconoce.
- Pulsamos en la rueda dentada para entrar en la vista avanzada. En el árbol de la izquierda pinchamos con el botón derecho en **nuestra organización > Iniciar sesión en el dispositivo**. Es importante usar esta opción y no la otra que dice "Iniciar sesión como administrador".
- Nos pedirá contraseña del dispositivo. Este viene en un correo de tokenorders@sectigo.com que habremos recibido. Insisten mucho en que esto no es la password del administrador sino la del token del cual tenemos 3 intentos para entrar. A la cuarta vez se bloquea y hay que contactar con SECTIGO para que lo restablezcan.

- El password del administrador no es accesible para nosotros. Se bloquea al quinto intento y en ese caso el bloqueo del token es permanente y hay que comprar otro. Tampoco se debe inicializar ni borrar el token ni el certificado. Tampoco se debe cambiar el certificado de código una vez que se aprovisiona en el token.