

Code Signing Step-by-Step Guide

Create an Enrollment Form

1. Navigate to Enrollment > Enrollment Forms > Click Add.
2. Name your Enrolment Endpoint your Organisation Name and Code Signing e.g., Jisc Services Limited Code Signing.
3. Select Type: Code Signing Certificate Enrollment Form.
4. Select Next.
5. Generate a URL Extension.
6. Press Save.

Create an Account

1. Enrollment Forms > Select the new Enrollment Form you created > Select Accounts.
2. Select Green Plus Icon.
3. Choose Name e.g., Jisc Services Limited Code Signing > Select Profile: Either Geant OV Code Signing (**Shipping Certificate on FIPS USB Token**) or Geant OV Code Signing (**Key Attestation**)*.
4. Press Save.

Creating Invitations

1. Go to Certificates > Code Signing Certificates.
2. Select Invitations > Select Green Plus Icon.
3. Enter in the email address of who requires the code signing certificate > select your Enrollment Endpoint Form > Select your Account > Select Send.

Enrol the Certificate

Note: These actions are performed by the end user.

1. Click Verify Email Address (or copy and paste the link provided). This Link will connect to the endpoint URL and the Code Signing Enrollment is partially filled in.
2. Complete the Code Signing Enrollment Form.

Field	Description
Certificate Email	Your Email Address
First Name	Your First Name
Last Name	Your Last Name
CSR	PEM format CSR. PEM header/footer lines are required.
Key Attestation	File must be Base64 encoded. PEM header/footer lines must NOT be included.
HSM Type	Luna or YubiKey

If the submitted CSR and key attestation are valid, you will receive a code signing certificate from Sectigo. Download it to your System and HSM for Code Signing Operations.

Regarding the address to which Sectigo will send your token, please note that this information is based on the address currently listed on the Sectigo portal, accessible under the Organisation tab. To ensure the accurate and timely delivery of your token, we kindly request that you provide us with the specific address where you would like the certificate to be shipped. Once you have submitted your certificate request, please forward the corresponding order number along with the precise shipping address to certificates@jisc.ac.uk. Your prompt response will enable us to get Sectigo to process your request efficiently.

***Certificate Profiles**

1. GEANT OV Code Signing (Shipping Certificate on FIPS USB Token):

Under this method, Sectigo ship out a token, allowing you to download the certificate. However, you need to be aware that due to the practicality of configuring and shipping from the United States, there might be delays associated with this option.

2. GEANT OV Code Signing (Key Attestation):

In this approach, the code signing certificate is available to download, enabling you to install it directly onto your own FIPS-compliant HSM. For this option, your hardware devices must support external key attestation. Currently, we offer support for the following hardware devices:

- Thales/Safenet Luna and nethSM devices
- Yubico FIPS Yubikeys (for ECC keys only)

If you opt for Yubico devices, you can conveniently purchase them from various platforms such as Amazon, ensuring they belong to the [FIPS series](#) for compatibility.