



SignMyCode

COMPLETE CODE SIGNING PLATFORM

User Guide for Order and Enrollment Process at SignMyCode



SignMyCode, your trusted re-seller and platinum partner of CA Sectigo, brings you a wide range of code signing certificates from trusted certificate authorities at affordable prices. We understand the importance of securing and ensuring your code's authenticity, so we offer excellent 24/7 customer support.

Table of Contents

| | |
|---|-----------|
| Introduction | 3 |
| How to Get and Install Code Signing Certificate? | 4 |
| Different Delivery Mode Options for Private Key | 5 |
| How to Place Order at SignMyCode? [Order Process] | 6 |
| How to Install or Enroll Code Signing Certificate? | 9 |
| [Enrollment Process] | |
| - Option 1: CSR and Key Attestation using Luna HSM | 10 |
| - Option 2: Key Generation and Attestation with YubiKey | 11 |
| Wrapping Up | 21 |

User Guide for Order and Enrollment Process at SignMyCode

Introduction

SignMyCode, your trusted re-seller and platinum partner of CA Sectigo, brings you a wide range of code signing certificates from trusted certificate authorities at affordable prices. We understand the importance of securing and ensuring your code's authenticity, so we offer excellent 24/7 customer support.

Choose from our two types of code signing certificates: Standard and EV.

Our Standard code signing certificates provide a reliable solution for individual developers and organizations to signing software and applications, giving your users the confidence that your code has not been tampered with. For an enhanced level of trust, our EV (Extended Validation) code signing certificates offer the highest level of assurance, displaying your company's name prominently to build credibility and increase user trust.

Following the new [CA/B Forum guidelines](#), we strive to stay current with the latest industry standards. These guidelines ensure the security and integrity of code signing certificates, promoting a safer digital environment. The new CA/B guidelines reinforce the importance of rigorous validation processes and stringent security measures for storing digitally signing certificates. Adhering to these guidelines ensures our customers' highest trust and reliability.

Trust SignMyCode for code signing certificates and solutions that meet the latest industry standards and provide peace of mind for your software applications.

How to Get and Install Code Signing Certificate?

Code signing is a digital process that adds a cryptographic signature to software or applications. This signature verifies the authenticity and integrity of the code, assuring users that it has not been tampered with. In recent developments, CA/B Forum BRs for Code Signing Certificates v2.8 now require the verification of hardware-backed keypairs as part of the Code Signing Certificate issuance and management process.

CA/B Requirements and Key Attestation:

To meet the CA/B Forum requirements for Code Signing Certificates, Sectigo Certificate Services utilizes a hosted key attestation service. This service verifies that the keypairs used to generate the Certificate Signing Request (CSR) were created within secure hardware.

The HSM attestation is a standalone service that non-interactively verifies key attestation packages from hardware security modules (HSMs). The Sectigo key attestation service supports the validation of cryptographic data and can authorize the issuance of OV (Organization Validation) and EV code signing certificates.

Supported Hardware Security Modules (HSM):

Currently, Sectigo supports the verification of the following hardware security modules

Luna HSMs: The Sectigo key attestation service can successfully verify Luna HSMs' public key confirmation packages.

YubiKey: The attestation certificates of YubiKey can also be verified by the Sectigo key attestation service.

Whereas DigiCert Supports: SafeNet 5110 CC, SafeNet 5110 FIPS, or SafeNet 5110+ FIPS Tokens and YubiKey and Azure KeyVault HSMs, etc

Different Delivery Mode Options for Private Key

You can choose from the following delivery modes when ordering your certificate:

1. **Token + Shipping:** The Certificate Authority (CA) will send you a token to the specified address.
2. **Install on Existing HSM (Advanced Users):** This option is suitable for advanced users with a hardware security module (HSM). You can install the certificate on your existing HSM device.
3. **Install on Existing Token (DigiCert Only):** This option is specific to customers with an existing token. The certificate will be installed on the designated token such as SafeNet CC, SafeNet FIPS.



How to Place Order at SignMyCode? [Order Process]

1. Begin by selecting the desired product and indicating the certificate's preferred delivery mode and number of years.

The screenshot displays the SignMyCode ordering interface. On the left, three subscription options are listed: 1 Year @ \$321.99 per year (34% savings), 2 Year @ \$273.99 per year (36% savings), and 3 Year @ \$225.99 per year (44% savings, marked as the 'Best Deal'). A dashed blue arrow points from the 'Best Deal' badge to the '3 Year' option. In the center, the 'Quantity' is set to 01. Below it, the 'Delivery Mode*' dropdown is open, showing 'Select Delivery Mode'. A dashed blue arrow points from the 'Delivery Mode*' label to the dropdown. Below the dropdown, an 'Upgrade to Extended Validation' option is available for \$70.00/yr. A dashed blue arrow points from the 'Upgrade to Extended Validation' checkbox to the 'ADD TO CART' button. To the right of the main form, a vertical list of benefits is shown: Time Stamp, Increase Software Downloads, Increase Trust, Decrease Window Warnings, and Sales & Live Support. At the bottom of the main form, the 'Total' is \$677.97, and there are 'ADD TO CART' and 'RENEW NOW' buttons.

☐ 1 Year @ \$321.99 per year
~~\$489.00~~ You Save \$167.01 (34%)

☐ 2 Year @ \$273.99 per year
~~\$858.00~~ You Save \$310.02 (36%)

☒ 3 Year @ \$225.99 per year
~~\$1,207.00~~ You Save \$529.03 (44%) **Best Deal**

Quantity: 01

Delivery Mode* [More Info](#)

Select Delivery Mode

☐ Upgrade to Extended Validation
Gain instant trusted status on Microsoft Defender SmartScreen Reputation filter ([example](#)), reducing warning messages and increasing brand reputation and end-user trust. **Adds \$70.00/yr**

Total: **\$677.97**

ADD TO CART **RENEW NOW**

Time Stamp

Increase Software Downloads

Increase Trust

Decrease Window Warnings

Sales & Live Support

The summary section contains three items: 'Delivery Mode: Existing HSM or External Physical Device', 'Secure Key Storage: FIPS-compliant Hardware Device', and 'Issuance Time: 1-5 Days'.

Delivery Mode:
Existing HSM or External Physical Device

Secure Key Storage:
FIPS-compliant Hardware Device

Issuance Time:
1-5 Days

SignMyCode Order and Enrollment Process User Guide

2. Proceed with the shipping and payment process, providing the necessary information as prompted.

Secure Checkout

Please note below details provided are just for **billing purpose** only. Details for Certificate will be asked separately. Billing and Certificate details may be different.

1 Billing Address
Setup Your Address

2 Purchase
Review and Submit

Email *

Company Name *

Phone No*

First name*

Last name*

Password*

Confirm Password*

Address*

VAT/GST (Optional)

City*

State*

Zip/Postal Code*

Country*

VISA

MasterCard

AMERICAN EXPRESS

PayPal

We do not store any part of the credit card or any other sensitive details on our servers.

Card Holder Name*

Card Number*

Expiry*

CVV*

0000-0000-0000-000

MM/YY

NEXT STEP →

SignMyCode
COMPLETE CODE SIGNING PLATFORM

www.signmycode.com

7

3. Once the shipping and payment process is complete, finalize the order to initiate the certificate issuance.



Transaction ID: [SMC10001275](#)

Thank you for ordering
Comodo Code Signing

Next Step : Follow the below link to generate certificate [Enroll Now](#)

How to Install or Enroll Code Signing Certificate? [Enrollment Process]

Code Signing Certificate enrollment process will be different based on certificate you select along with delivery mode and CA.

For Token + Shipping Certificate

Delivery Mode:

If you have selected the Token + Shipping option, the CA will send the pre-installed token to the address you specified during the order process, you just need to activate based on the instruction provided.



For Existing Token and Install on Existing HSM Device Certificate Delivery Mode:

1. Ensure that you have suitable hardware available for installing and generating keys in a non-exportable form.
2. Generate the keys within the hardware, ensuring they remain non-exportable. Create a certificate signing request (CSR) and key attestation, which confirms that the private key was generated within the suitable hardware.
3. Add generated CSR and key attestation in your certificate enrollment form and submit the form.
4. CA will verify the details and send you digital token and link via email for installation.

Supported Hardware and Browsers

CA like Sectigo and DigiCert supports the following hardware devices:

1. **Luna Network Attached is HSM, Version 7.x**
2. **YubiKey 5 FIPS Series**
3. **Azure Vault HSM (DigiCert)**

To create the necessary cryptographic materials using these supported devices and submit the cryptographic data (CSR and attestation) to the key attestation service, refer to the specific sections provided by Sectigo. The supported browsers for this process include Chrome, Firefox, and Edge.

These instructions help you complete enrollment and obtain your code signing certificate based on your preferred delivery mode and supported hardware.

Option 1: CSR and Key Attestation using Luna HSM

The Luna Network Attached HSM 7.x provides a reliable method for generating a key attestation using a public key confirmation package (PKC). This PKC is created to verify that the keypair was indeed generated and stored within the Luna HSM.

Attestation Package Format:

The Luna HSM public key confirmation (PKC) files are DER-encoded PKCS7 files that contain the key attestation and key pair.

For RSA Keypairs:

When generating a PKC for an RSA keypair, there are two possible formats available:

1. **TC-Trust Center Format:** The PKC contains three certificates in this format, and the chain does not end with a root certificate.
2. **Chrysalis-ITS Format:** The PKC contains five certificates in this format, and the chain ends with a root certificate.

For more detailed information, please refer to the Luna HSM documentation provided by Thales.

Generating CSR and PKC in Chrysalis-ITS Format

To generate an RSA keypair, CSR, and attestation in the Chrysalis-ITS format, follow these steps:

1. Log in to the Luna HSM using the Luna remote client. Use the LunaCM2 utility with the following command to generate an RSA keypair on a Luna Partition1 (replace LABEL with your desired keypair identification):

Windows (any shell):

```
cd C:\Program Files\SafeNet\LunaClient  
lunacm
```

Linux:

```
cd /usr/safenet/lunaclient/bin  
./lunacm
```


Linux:

```
cd /usr/safenet/lunaclient/bin  
./lunacm
```

Command:

```
cmu gen -modulusBits=3072 -publicExp=65537 -sign=T -verify=T -  
label=LABEL -extractable=false
```

Quick Note:

Before executing these commands, ensure the Luna client is registered with one or more partitions to manage the cryptographic objects created and stored within the partition. The LunaCM utility (lunacm) is the client-side administrative command interface for Luna HSMs. Open a command prompt or console window, navigate to the LunaClient software directory, and start the lunacm utility.



!!Warning!! The parameters **-extractable=false** and **-sign=T** are mandatory to prevent CSR generation failure. Luna will only use this key for signing the CSR with these parameters.

2. Determine the handle numbers of your public and private keys by executing the following commands and noting the output:

```
cmu list -class public -label=LABEL  
cmu list -class private -label=LABEL
```

3. Generate a CSR using the following command (replace AAA and BBB with your public and private key handles, respectively):

```
cmu requestcert -publichandle=AAA -privatehandle=BBB -C=CA -L=Ottawa  
-O=Sectigo -CN="PKC Test Cert" -outputFile=rsacsr.pem
```

4. Generate a PKC by running the following command (replace AAA with your public key handle and attestation.p7b with your desired file name):

```
cmu getpkc -handle=AAA -outputfile=attestation.p7b -pkctype=2 -verify
```

5. The key attestation service requires the attestation blob to be base64 encoded. Use the following commands to encode the p7b file to base64 (note that the `certutil encode` command adds PEM header/footer, which should be excluded by using `findstr`):

Windows (any shell):

```
certutil -encode attestation.p7b attestation.b64  
findstr /v CERTIFICATE attestation.b64 > attestation.b64
```

Linux:

```
base64 attestation.p7b > attestation.b64
```

6. Submit the CSR and base64 encoded attestation to the order enrollment form.
(Go to SignMyCode >> My Order >> Enrollment Form)

These steps lead you to generate a CSR and key attestation using the Luna HSM in the Chrysalis-ITS format. Ensure to provide the necessary files during the order enrollment process.

Option 2: Key Generation and Attestation with YubiKey

Supported YubiKey Versions:

The YubiKey 5 FIPS Series USB tokens offer key generation and attestation capabilities. The attestation certificate, which has the same key as the CSR (Certificate Signing Request), is signed by the intermediate attestation certificate. The intermediate attestation certificate can be downloaded from the device and is signed by the YubiKey private root certificate.

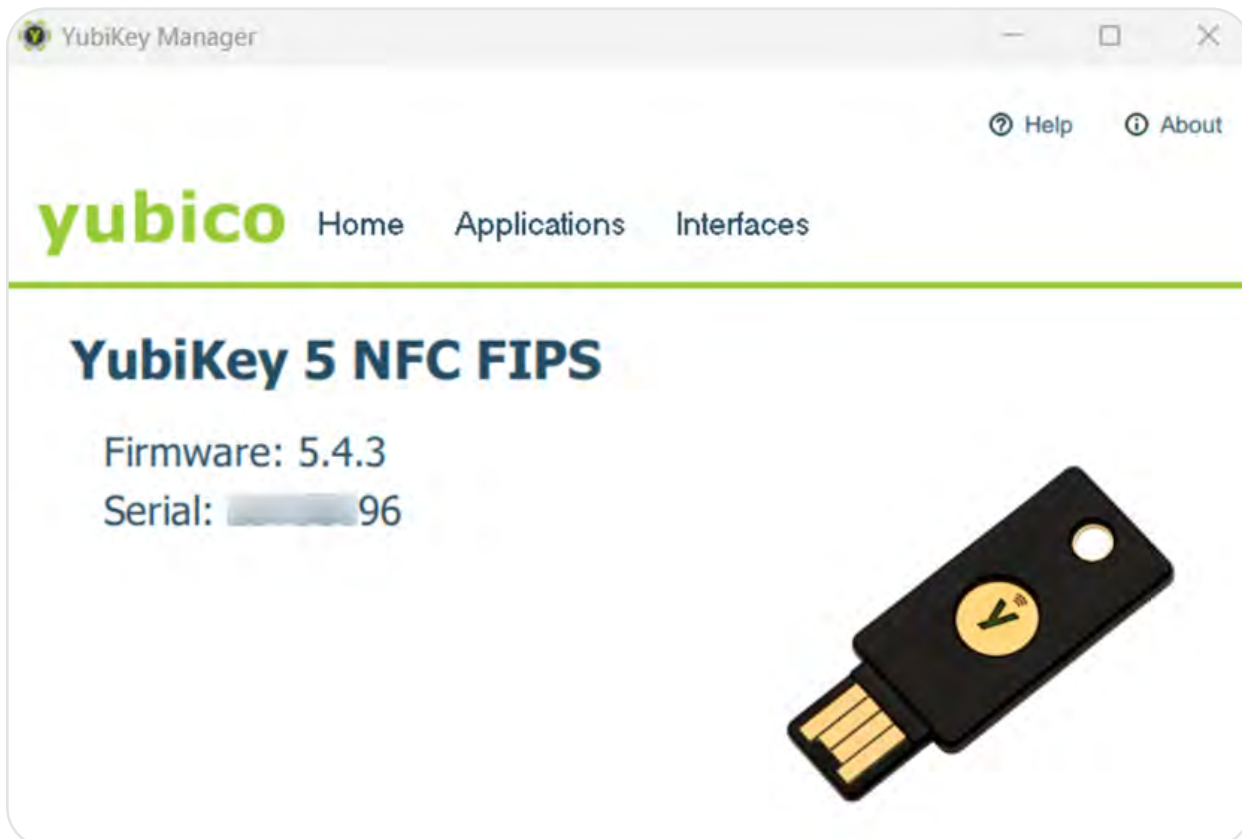
Attestation Package Format:

YubiKey attestations are standard x.509 certificates that contain the key attestation. More than the attestation certificate is required for attestation validation. The device's intermediate attestation certificate is also required. The key attestation service expects a base64 blob that concatenates PEM-encoded certificates.

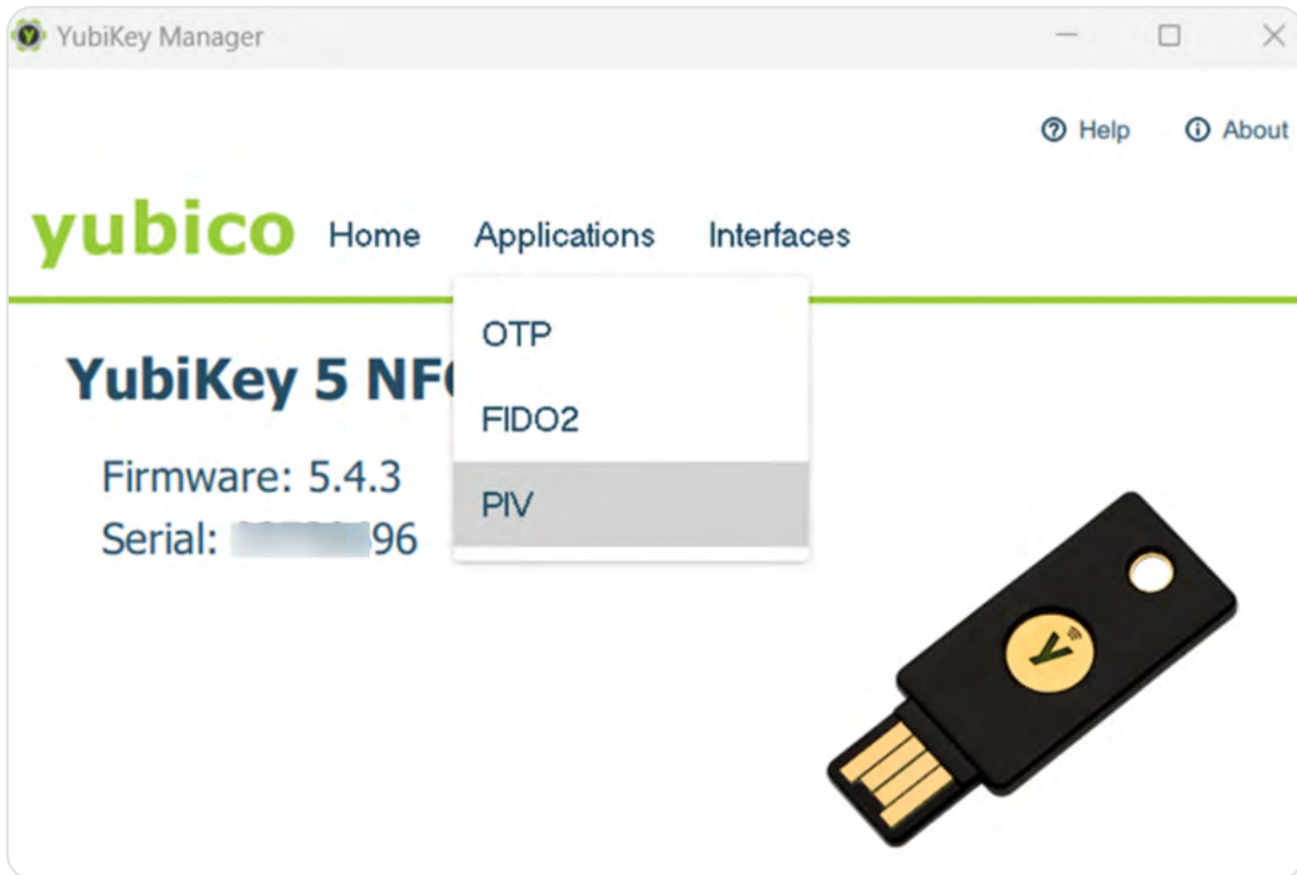
Generate CSR and Attestation Certificate:

To generate an ECC keypair, CSR, attestation certificate, and obtain the device's intermediate attestation certificate, follow these steps (Windows instructions provided; refer to YubiCo for instructions on different operating systems):

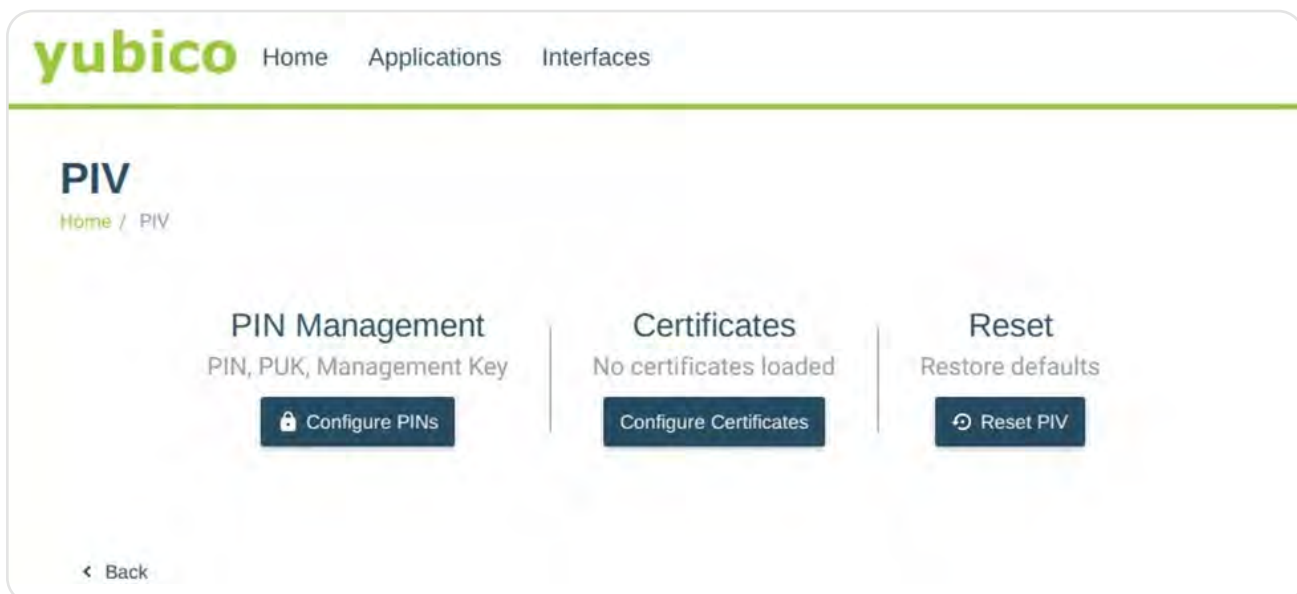
1. Launch YubiKey Manager.



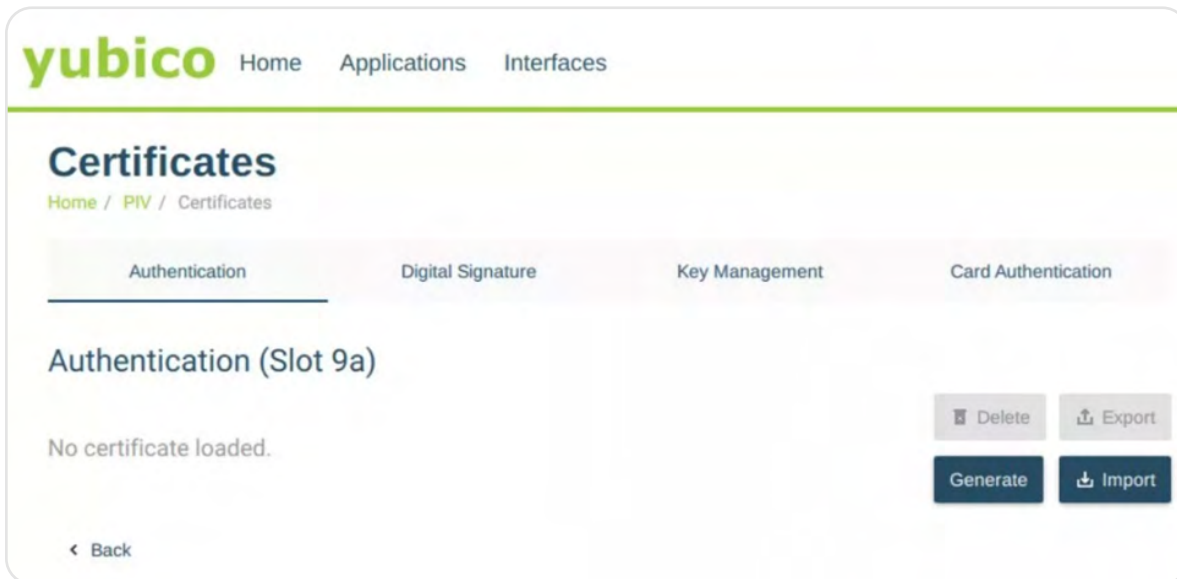
2. Go to Applications, and select PIV



3. Then, click on Configure Certificates.

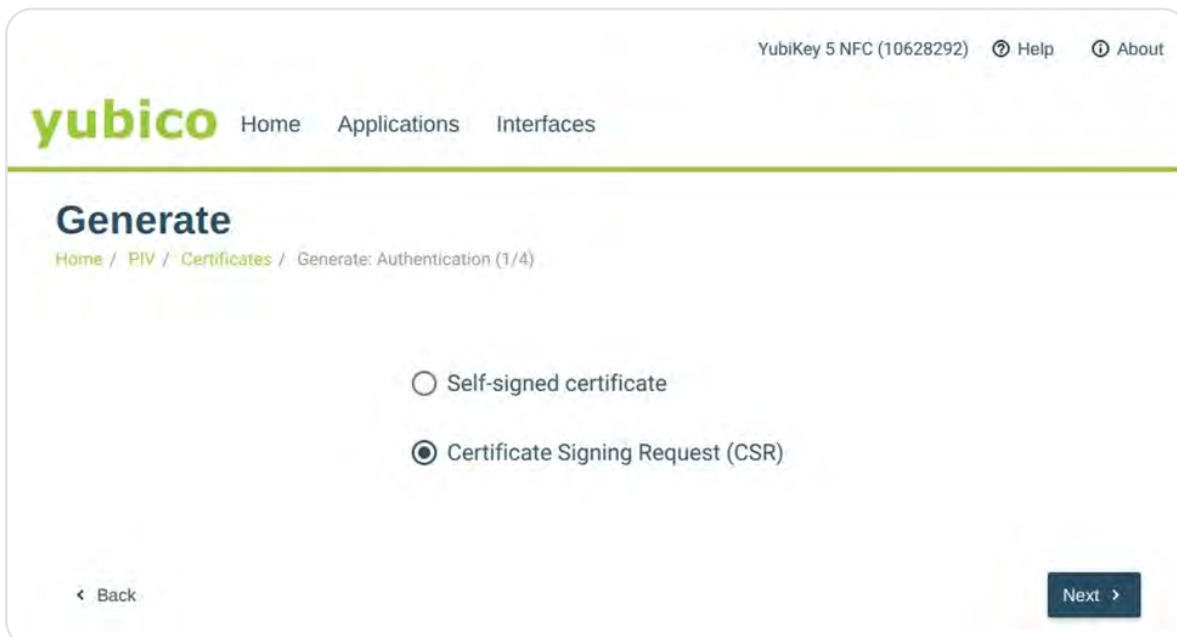


4. Select Authentication (Slot 9a) for EV code signing certificates and click Generate.



The screenshot shows the Yubico web interface. At the top, there's a navigation bar with the Yubico logo and links for Home, Applications, and Interfaces. Below this, the main heading is "Certificates", with a breadcrumb trail: Home / PIV / Certificates. There are four tabs: Authentication (selected), Digital Signature, Key Management, and Card Authentication. Under the Authentication tab, the text "Authentication (Slot 9a)" is displayed. Below that, it says "No certificate loaded." On the right side, there are four buttons: "Delete" (disabled), "Export" (disabled), "Generate" (active), and "Import" (disabled). At the bottom left, there is a "< Back" link.

5. Choose Certificate Signing Request (CSR) and click Next.



The screenshot shows the Yubico web interface. At the top right, it says "YubiKey 5 NFC (10628292)" with links for Help and About. The navigation bar at the top left has the Yubico logo and links for Home, Applications, and Interfaces. The main heading is "Generate", with a breadcrumb trail: Home / PIV / Certificates / Generate: Authentication (1/4). There are two radio button options: "Self-signed certificate" and "Certificate Signing Request (CSR)". The "Certificate Signing Request (CSR)" option is selected. At the bottom left, there is a "< Back" link. At the bottom right, there is a "Next >" button.

6. Select an algorithm from the drop-down menu and click Next.

Generate

Home / PIV / Certificates / Generate: Digital Signature (2/4)

Algorithm: RSA2048
ECCP256
ECCP384

< Back

2 Next >

Quick Note:

Select ECCP256 or ECCP384 for EV Code Signing Certificates as YubiKey only supports ECC algorithms for EV Code Signing.

7. Enter a Subject Name for the certificate and click Next.

Generate

Home / PIV / Certificates / Generate: Digital Signature (2/4)

Algorithm: RSA2048
ECCP256
ECCP384

< Back

2 Next >

8. Click on Generate.

Generate

Home / PIV / Certificates / Generate: Authentication (4/4)

Slot: Authentication (9a)

Output format: Certificate Signing Request (CSR)

Algorithm: RSA2048

Subject name: Janki Mehta

[< Back](#)[✓ Generate](#)

9. Provide the required information, including the location to store the CSR, management key, and PIN.

yubico

Generate

Home / PIV / Certific

YubiKey 5 NFC (10628292) ? Help ? About

Look in:

| Name | Size | Type | Date Modified |
|------|------|-------|-------------------|
| / | | Drive | 11/23/18 12:37 PM |

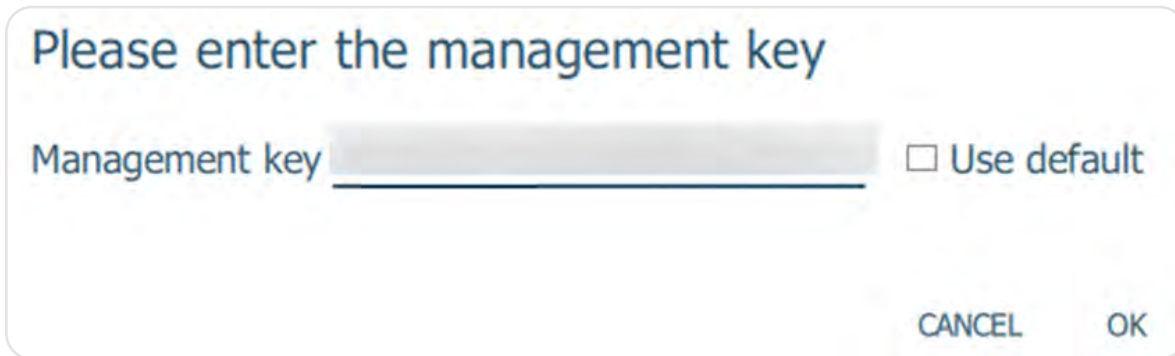
File name: jankimehta.csr

Files of type: CSR files (*.csr *.pem)

[Save](#)[Cancel](#)

[< Back](#)[✓ Generate](#)

10. enter your YubiKey's management key and click OK.



Generate Attestation Certificate

Open **power shell as Administrator** and **navigate** to the YubiKey directory:

```
cd 'C:\Program Files\Yubico\YubiKey Manager\'
```

1. Execute the following command to create the attestation certificate (adjust the path to save the attestation certificate as needed):

```
.\ykman.exe piv keys attest -F PEM 9a attestation.crt
```

2. Execute the following command to obtain the intermediate certificate:

```
cd 'C:\Program Files\Yubico\YubiKey Manager\'
```

3. The HSM-attestation service expects the attestation blob to be base64 encoded. Use the following commands to encode the attestation certificates as a single base64 encoded file (the `certutil encode` command adds PEM header/footer, which should be excluded using `findstr`):

Windows (any shell):

```
type attestation.crt intermediateCA.crt > attestation.pem  
certutil -encode attestation.pem attestation.b64  
findstr /v CERTIFICATE attestation.b64 > attestation.b64
```

4. Submit the CSR and base64 encoded attestation through the dashboard enrollment form ([Go to SignMyCode >> My Order >> Enrollment Form](#))

Once the submission is successful, the CA will contact you for verification. After successful verification, you will receive a token based on the selected delivery mode: a physical address with a token or an e-token with installation instructions via email.

Wrapping Up

If you are using Azure Key Vault, [Follow the steps to generate CSR and Import Certificate](#) (For DigiCert Code Signing).

If you need more knowledge-based content related to YubiKey, Luna HS or Azure Vault, feel free to explore our more helpful content!

- [Token Based Code Signing](#)
- [Code Signing Installation Guide and Tutorials](#)



THANK YOU