Creating a CSR and a Key Attestation Using YubiKey Token

Step-by-Step Guide For Generating CSR and Key Attestation with YubiKey Token

To ensure compliance with the new regulations for Code Signing Certificates, it is essential to securely generate and store private keys on external hardware devices that meet the FIPS validation criteria. We understand the importance of these changes and offer Code Signing Certificates that come pre-installed on USB tokens validated against the FIPS 140-2 security standard.

In addition to using our pre-installed USB tokens, users can generate a key pair on their existing YubiKey. Using a YubiKey, users can obtain an attestation certificate proving that the private key was generated on the device itself. This attestation certificate can manually order and install code signing certificates on YubiKey.

If you own a YubiKey but are uncertain about generating a Certificate Signing Request (CSR) and Key Attestation, there’s no cause for concern. This comprehensive article is designed to easily guide you through the process, presenting clear and concise instructions at every step.

Generating a CSR

Note: If you have downloaded and installed YubiKey Manager, directly move to Step 3.

1: Download YubiKey Manager

Open any browser of your choice, say Firefox.

In the URL bar, type https://www.yubico.com/support/download/yubikey-manager, and press Enter.

Click on Download and select the OS (Operating System).

The configuration file will start to download.

2: Install YubiKey Manager

Open the configuration file.

In the YubiKey Manager Setup window, on the Welcome to YubiKey Manager Setup page, click Next.

Select the Destination Folder from the Choose Install Location page and click Next.

In the Choose Start Menu Folder page, select a folder where you want to create the program's shortcut, and click Install.

Click Finish.

3: Insert Your Existing Token

Once the YubiKey Manager window opens, plug your existing FIPS-compliant token into the machine.

You will be able to see the details of the token in the same window.

4: Generate CSR

In the YubiKey Manager window, click Applications.

From the list, select PIV.

Click Configure Certificates.

In the Authentication tab, click Generate.

Check the radio button in front of the Certificate Signing Request (CSR) option and click Next.

From the Algorithm list, select ECCP384, and click Next.

Enter the Subject name (your organization name or the individual name you want the certificate under).

Verify the details and click Generate.

In the Save CSR to file dialog box, in the File name box, add the file name of your choice, and click Save.

From the "Please enter the Pin" dialog box, enter the PIN of your choice, & click OK.

Congratulations, you have successfully created the CSR.

Create Attestation File

1: Open PowerShell as Administrator

Click on the Search option situated on the Taskbar.

Type Powershell and select Run as Administrator.

From the User Account Control dialog box, click on Yes.

2: Save Attestation and Intermediate Files Under the YubiKey Manager Folder

Type the cd “C:\Program Files\Yubico\YubiKey Manager” command in Powershell and press Enter. (After cd, input the path where your YubiKey Manager is located.)

Type the “.\ykman.exe piv keys attest 9a ATTESTATION-TEST.crt” command and press Enter. (Replace the term “TEST” with any name of your choice to rename the Attestation File name.)

Type the “.\ykman.exe piv certificates export f9 INTERMEDIATE-TEST.crt” command and press Enter.(Replace the term “TEST” with any name of your choice to rename the Intermediate File name)

3: Save all Three Files Together

Open File Manager and navigate to the YubiKey Manager window.

Select Attestation and Intermediate files.

Paste both files into the folder which contains the CSR.

Now you have all three files needed to enroll for your order.

4: Combine Attestation and Intermediate Files

Right-click on the Attestation file, select Open with, and click Notepad.

Right-click on the Intermediate file, select Open with, and click Notepad.

Open a new Notepad window.

Copy all the content from the Attestation certificate and paste that into the new Notepad window.

Now, copy all the content from the Intermediate certificate and paste that into the new Notepad window.

Save the new Notepad window and close all other Notepad windows.

Note: It is essential to combine the intermediate and the attestation file in the sequence where Attestation comes first and then the Intermediate certificate.

5: Enroll your Certificate.

Right-click on the CSR file, select Open with, and click Notepad.

Copy all the content.

Open the Portal and paste the copied CSR content in the Enter Your CSR box.

In the Organization Detail section, enter the details.

In the Organization Contact Information section, enter the details.

In the Select HSM Type section, from the HSM Type list, select YubiKey 5 FIPS Series.

In the Input Attestation box, paste the combination of Attestation and the intermediate in content. (Step 4 – Last Point)

Scroll down, check the checkbox before the I agree to the Certificate Services Agreement option, and click Submit.

Congratulations, you have successfully generated the Attestation File.