Security - Code Signing Enroll User For Different Domain

This is how to enroll into a cert from the users computer.

How Users Enroll for Certificates with Custom ("Different") Domain Name

Users with Enroll permission can now request a certificate:

Option A – Using MMC (easiest for testing)

1. Run certmgr.msc (Current User).
2. Right-click **Personal** → **All Tasks** → **Request New Certificate**.
3. Select your enrollment policy (Active Directory Enrollment Policy).
4. Choose your new template.
5. When prompted, click **Details** → **Properties**.
6. On **Subject** tab: Enter custom values (e.g., Common name = "OtherDomain Code Signing Authority").
7. On **Subject** tab: Enter custom values (e.g., Organtization = "The Home Stack").
8. On **Subject** tab: Enter custom values (e.g., Locality = "Loveland").
9. On **Subject** tab: Enter custom values (e.g., State = "Ohio").
10. On **Subject** tab: Enter custom values (e.g., Country = "US").
11. On **Extensions** tab: Add SAN if needed (e.g., email=signing@otherdomain.com).
12. Enroll.

Using certreq.exe (scriptable / automated) Create an .inf file:

codesign-request.inf

```
[Version]
Signature="$Windows NT$"


[NewRequest]
```

```
Subject = "CN=Code Signing, O=The Home Stack, L=Loveland, S=Ohio, C=US"
; You can make Subject empty if you prefer only SAN / no CN, but most code signing tools expect a CN
KeySpec = 1
KeyLength = 4096                ; 3072 or 4096 is strongly recommended in 2025+
Exportable = TRUE               ; Usually yes for code signing
MachineKeySet = FALSE             ; User context (most common for code signing)
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"
ProviderType = 24
RequestType = PKCS10
KeyUsage = 0x80                 ; digitalSignature = required for code signing

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.3           ; Code Signing EKU

; Optional: if you really want to add DNS SANs (rare for pure code signing)
[Extensions]
2.5.29.17 = "{text}"
_continue_ = "dns=www.sflservicesllc.com&"
_continue_ = "email=sales@sflservicesllc.com"
```

Then:

Create a powershell script **createCert.ps1**, Run the script

Note: Change the template name to the name you chose when creating HERE it with no spaces.

```
certreq -new codesign-request.inf codesign.csr
certutil -dump codesign.csr
certreq -submit -attrib "CertificateTemplate:YourTemplateName" codesign.csr codesign.cer
certreq -accept codesign.cer
certutil -store my
```

Revision #0
Created 23 February 2026 02:10:55 by Admin
Updated 24 October 2026 14:13:11 by Admin