Security - Create a Code Signing Template

Here’s a step-by-step guide to create a new **code signing certificate template** in Active Directory Certificate Services (**AD CS**) based on the built-in "Code Signing" template. This new template can be used by domain users (from your current domain or trusted domains in the same forest) to enroll for code signing certificates.

The phrase "for a different domain name" likely means you want certificates where the **subject name** (or Subject Alternative Name / UPN) reflects a different domain/organization/branding (e.g., "Code Signing Authority - othercompany.com" instead of the user's actual AD name like "Steve@contoso.com"). The standard "Code Signing" template builds the subject from Active Directory (user's CN + UPN), which ties it to the enrolling user's domain identity.

To allow a custom / different subject name (common for organizational code signing certs), set the template to **Supply in the request**. This lets the user provide their own subject during enrollment (via certreq.exe, MMC Certificates snap-in, or PowerShell).

Important security note: Setting "Supply in the request" without tight controls is risky (ESC vulnerabilities like ESC1/ESC2). Limit enrollment to a small, trusted group (e.g., developers or a code-signing admins group). Avoid enabling this broadly for all Domain Users unless necessary.

Step 1: Open the Certificate Templates Console

- Log in to a domain-joined machine with Enterprise Admin rights (or delegated rights to manage templates).
- Run certtmpl.msc (Certificate Templates MMC snap-in).

Step 2: Duplicate the Built-in Code Signing Template

- In the list, find the template named **Code Signing**.
- Right-click it → **Duplicate Template**.
- In the **Compatibility** tab (if shown):
  - Certification Authority: Windows Server 2016 / 2019 / 2022 (or highest supported).
  - Certificate recipient: Same or highest.
- Click **OK** to open the new template properties.

Step 3: Configure General Tab

- **Template display name**: Something descriptive, e.g., Custom Code Signing - OtherDomain or Code Signing - branding.otherdomain.com.
- **Template name**: Auto-filled (spaces removed from display name).
- **Validity period**: 1–3 years (common for code signing; match your policy).
- **Renewal period**: e.g., 6 weeks.
- Check **Publish certificate in Active Directory** if you want the cert discoverable (usually **not** needed for code signing).

Step 4: Request Handling Tab

- **Purpose**: Signature and encryption (default is fine; code signing mainly needs signature).
- Check **Allow private key to be exported** (very common for code signing — developers often need to export to other machines or build servers).
- **Minimum key size**: 2048 (or 4096 for stronger security).
- Uncheck **Strong private key protection** unless required.

Step 5: Subject Name Tab (Key Change for "Different Domain Name")

- Select **Supply in the request** (this is the main change — it allows custom subject during enrollment instead of pulling from AD).
  - This enables users to specify a different/common organizational name (e.g., CN = "Code Signing", E = "sales@otherdomain.com").
- **Do NOT** select "Build from this Active Directory information" unless you want the cert tied to the user's actual AD name/UPN.

Step 6: Extensions Tab

- **Application Policies** → Ensure **Code Signing** is present (it should be inherited).
  - You can add others if needed (e.g., **Time Stamping** via additional policies).
- **Key Usage**: Digital signature (required), non-repudiation (recommended).
- Optional: Add **Certificate Template Information** extension if you want to include metadata.

Step 7: Security Tab (Critical — Restrict Enrollment)

- Remove **Domain Users** / **Authenticated Users** if present (or set their permissions to **Read** only).
- Add your intended group(s), e.g.:
  - A security group like "Code Signing Users" or "Developers - OtherDomain".
  - Grant them **Read** + **Enroll** (and **Autoenroll** if you want GPO auto-enrollment, though rare for custom-subject code signing).
- **Do not** give Domain Users Enroll unless this is intentional (very broad).

Step 8: Issue the New Template on Your CA

- Open **certsrv.msc** (Certification Authority snap-in) on your CA server.
- Right-click **Certificate Templates → New → Certificate Template to Issue**.
- Select your new template (e.g., Custom Code Signing - OtherDomain) → **OK**.

Revision #1
Created 23 February 2026 02:07:37 by Steve Ling
Updated 23 February 2026 02:10:48 by Steve Ling