Creating a Code Signing Certificate

Source :

Creating the Code Signing Certificate Template

1. Open the "Certification Authority" console on the enterprise root certification authority
2. Click on "Certificate Templates" and check if a template called "Code Signing" exists (if it already exists, there are no further steps required for this section)
3. If the "Code Signing" template does not exist, right click on the "Certificate Templates" node and select "New" -> "Certificate Template to Issue"
4. Select "Code Signing" and click OK

Generating the Code Signing Certificate

1. Open MMC under administrative context
2. Add the "Certificates" snap-in to the MMC console (select "My user account" when prompted)
3. Expand "Personal", right click on "Certificates" and select "All Tasks" -> "Request New Certificate"
4. Select "Active Directory Enrollment Policy"
5. Tick "Code Signing" and then click on the "Details" button to the right hand side of the "Code Signing" option
6. Click on "Properties"
7. Click on the "Private Key" tab, and then expand the "Key Options" section
8. Tick "Make private key exportable" and "Strong private key protection"
9. Click OK and then click the "Enroll" button (a message may appear stating that an application is creating a protected item – click OK to acknowledge this message)

Exporting the Certificate for Publishing

1. Open MMC under administrative context
2. Add the "Certificates" snap-in to the MMC console (select "My user account" when prompted)
3. Expand "Personal", right click on the appropriate code signing certificate and select "All Tasks" -> "Export…"
4. Choose the option "Yes, export the private key" when prompted
5. Accept the default options on the "Export File Format" screen
6. Enter a password for the private key, which will need to be entered when importing the certificate
7. Save the certificate to an appropriate location

Importing the Certificate for Trusting

Local Machines

1. Open MMC under administrative context
2. Add the "Certificates" snap-in to the MMC console (select "Computer account" and select the local machine when prompted)
3. Right click "Trusted Publishers" and select "All Tasks" -> "Import…"
4. Follow the wizard to import the exported certificate, and enter in the accompanying password that was used when the certificate was exported
5. If the certificate is no longer required to be imported by other machines, it is highly recommended that the exported file is deleted

Group Policy

1. Open the appropriate group policy for editing
2. Expand "Computer Management" -> "Policies" -> "Windows Settings" -> "Security Settings" -> "Public Key Policies"
3. Right click on "Trusted Publishers" and select "Import…"
4. Follow the wizard to import the exported certificate, and enter in the accompanying password that was used when the certificate was exported
5. If the certificate is no longer required to be imported by other machines, it is highly recommended that the exported file is deleted