1. Create a new digital certificate by using command

New-SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My `

-Subject "CN=anyName" `

-KeyAlgorithm RSA `

-KeyLength 1024 `

-Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" `

-KeyExportPolicy Exportable `

-KeyUsage DigitalSignature `

-Type CodeSigningCert

Export the certificate

* 1. To see the certificate use keyboard combination “windows + r”
  2. Now type “certmgr.msc”
  3. Double click on “Personal”, double click on “certificate”

A screenshot of a computer

Description automatically generated

* 1. Now you can see your certificate name
  2. Now right click on certificate and go to “All task” then click on “Export”
  3. A wizard will be opened and click on next
  4. Click on “yes, export the private key”
  5. Click on next
  6. Click on password and give the password
  7. Now click on browse to save the file and give the name.
  8. Click on next and then finish.

1. Import/install certificate
   1. Double click on exported Certificate clicks on next
   2. Give the password and click on next
   3. Now click on “Place all certificate on following store”
      1. Click on Browse
      2. Click on “Trusted Root Certification Authorities”
      3. Click on next
   4. Click on finish
2. Create a script
   1. Open Windows PowerShell ISE
   2. Create a new script with command “get-date” and save using name “script”
3. Bind certificate and script together
   1. Use the following commands
4. $a = (Get-ChildItem Cert:\CurrentUser\My | Where-Object {$\_.Subject -eq "CN=<certificate canonical name>"}).Thumbprint

b. note down the alphanumeric string

c. use command

d. now the status should be “valid” & you are good to go

$cent = Get-ChildItem Cert:\CurrentUser\My\132CFE0499A933FC335457C95501D43B8200876F

Set-AuthenticodeSignature -Certificate $cent -FilePath .\script.ps1

