EasyRSA

- Code Signing

Code Signing

Creating the certificate

Below are the steps to create a code signing certificate using OpenSSL and an established EasyRSA CA.

```
# Step 1: Generate either an RSA or an EC private key... pick one...
openssl genrsa -out SuperCodeSigning.key 2048
openssl ecparam -name secp384r1 -genkey -noout -out SuperCodeSigning.key
openssl ecparam -name secp521r1 -genkey -noout -out SuperCodeSigning.key

# Step 2: Make certificate request.
openssl req -new -key SuperCodeSigning.key -out SuperCodeSigning.req

# Step 3: Import certificate request to easyrsa.
./easyrsa import-req SuperCodeSigning.req SuperCodeSigning

# Step 4: Sign certificate request, and make SPC certificate.
./easyrsa sign-req code-signing SuperCodeSigning

# Step 5: Make PFX.
openssl pkcs12 -export -out SuperCodeSigning.pfx -inkey SuperCodeSigning.key -in
SuperCodeSigning.crt -certfile SigningCA.crt
```

Signing PowerShell Scripts

```
$ScriptToSign = "C:\Path\To\Your\Script.ps1"

#$HashAlgo = "SHA256"
$HashAlgo = "SHA512"

#$TimeStampingAuthority = "http://timestamp.comodoca.com/authenticode"
$TimeStampingAuthority = "http://timestamp.digicert.com"
```

```
#$TimeStampingAuthority = "http://timestamp.sectigo.com"

$SigningCertificate = Get-ChildItem -Path Cert:\CurrentUser\My -CodeSigningCert | Select-Object -First 1

Set-AuthenticodeSignature -Certificate $SigningCertificate -TimestampServer $TimeStampingAuthority -HashAlgorithm $HashAlgo -FilePath $ScriptToSign
Get-AuthenticodeSignature -FilePath $ScriptToSign
```

Sign all scripts in current directory

Load a key:

```
try {
  Write-Host "[INFO] Attempting to load a code signing certificate." -ForegroundColor Yellow
  $SigningCertificate = Get-ChildItem -Path Cert:\CurrentUser\My -CodeSigningCert | Select-Object -First 1
  Write-Host "[INFO] Displaying loaded code signing certificate for verification:" -ForegroundColor Green
  $SigningCertificate | Format-List
} catch {
  Write-Host "[ERROR] The following error has occurred attempting to load an available code signing certificate: $($_.Exception.Message)" -ForegroundColor Red
}
```

Sign all of the unsigned scripts in the current directory:

```
# sign all unsighted ps1 files in the current directory
dir *.ps1 | foreach {Get-AuthenticodeSignature $_.Name} | Where-Object {$_.Status -eq "NotSigned"} | foreach {Set-AuthenticodeSignature -Certificate $SigningCertificate -TimestampServer "http://timestamp.digicert.com" -HashAlgorithm SHA512 -FilePath $_.Path}
```

Signing DLL Files

```
signtool sign /f "C:\cert\SuperCodeSigning.pfx" /p "your_certificate_password" /t "http://timestamp.digicert.com" /td sha256 "your_dll_file.dll"
```

#end