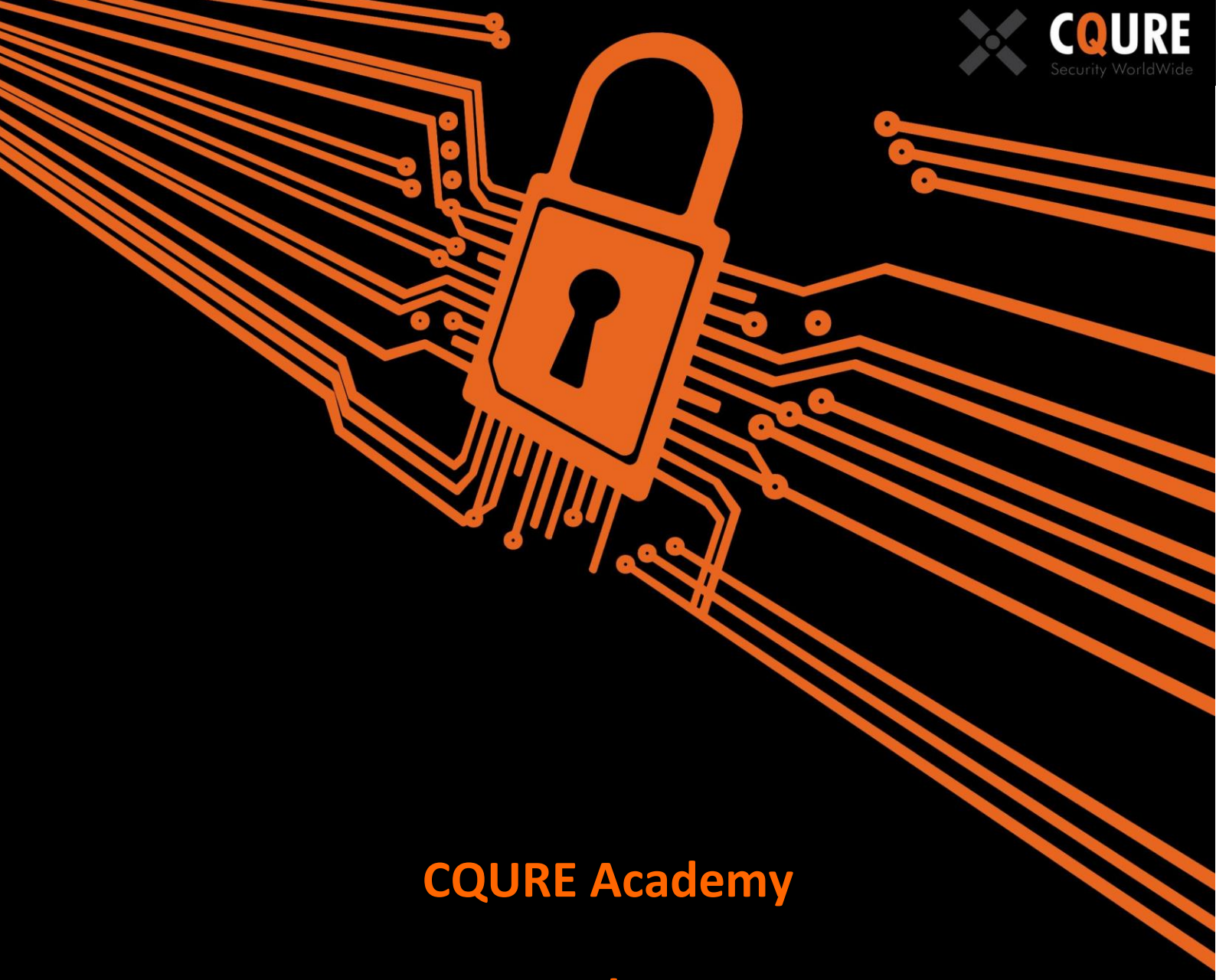

CQURE Academy

MasterClass: SCT

Code signing lab

Version 1.2

Please respect the authored content – copying prohibited.

Author: CQURE Team

Email: info@cqure.us | Twitter: @CQUREAcademy

http://cqure.us

Training Content

1 Code signing

1. Go to the lab machine.
2. Launch cmd.exe and then type “certmgr” to run the certificate management.
3. Go to Personal --> Certificates.
4. Right-click on “Certificates” and select “All tasks” --> “Request new certificate”.
5. Click “Next” twice and select the “Code Signing” template.
6. Click “Enroll” and then “Finish”.
7. Verify if you have the new certificate present.
8. Double click on the new certificate, go to the “Details” tab and scroll down to the “Thumbprint” property.Note first 4 characters.
9. Launch PowerShell ISE
10. List your certificates with “dir cert:\CurrentUser\My” Try to find the certificate with the thumbprint you have noted.
11. Assing the code signing certificate to the variable: “$cert1= dir cert:\CurrentUser\My\DEADBEEFDEADBEEF” – Remember about replacing the sample thumbprint with your one.
12. Sign the binary file: Set-AuthenticodeSignature -Certificate $cert1 -FilePath <PathToEXEfile>
13. Right click the PathToEXEfile.exe on your desktop and verify if there is any digital signature.

2 PowerShell script signing

1. Sign in to Lab machine
2. Lunch PowerShell console
3. List your certificates with “dir cert:\CurrentUser\My” Try to find the certificate with the thumbprint you have noted.
4. Assing the code signing certificate to the variable: $cert1= dir cert:\CurrentUser\My\DEADBEEFDEADBEEF – Remember about replacing the sample thumbprint with your one.
5. Create new PowerShell script on desktop script1.ps1 with code:
   Write-Host “Hello, CQURE World!”
6. Change script execution policy to AllSigned:
   Set-ExecutionPolicy -ExecutionPolicy AllSigned
7. Try to run script from desktop
8. Create signature for script
   Set-AuthenticodeSignature -Certificate $cert1 C:\Users\Administrator\Desktop\script.ps1
9. Run the script
10. Confirm to always trust the publisher
11. Open script in editor and search for signature
12. Add single space or modify file in any other way
13. Save file and try to run it again
14. Set Execution policy to remote signed
    Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
15. Try to run the script again
16. Try to run it from network share