

CNT 4603: System Administration Spring 2014

Project Six – PowerShell Scripting And Digitally Signing Scripts

Instructor : Dr. Mark Llewellyn
 markl@cs.ucf.edu
 HEC 236, 4078-823-2790
 <http://www.cs.ucf.edu/courses/cnt4603/spr2014>

Department of Electrical Engineering and Computer Science
Computer Science Division
University of Central Florida



Project Six

- **Title:** “Project Six: PowerShell Scripting And Digitally Signing Scripts”
- **Points:** 40 points
- **Due Date:** April 16, 2014 by 11:59 pm WebCourses time.

- **Objectives:** To create a PowerShell script using best standards and practices for script creation and to digitally sign the script.
- **Deliverables:**
 1. Screen shots as shown on pages 6, 7, 8, 9, 10, and 11.
 2. The digitally signed source code for your script.



Project Six – Background

- We'll take a diversion from dealing with our `savn.local` network and focus on PowerShell scripting for this assignment. While we haven't dealt with all of the various aspects of PowerShell scripting, we have covered enough in the lecture notes for you to be able to create a useful system administrator script.
- In keeping with the discussions in PowerShell – Parts 4 and 5 lecture notes, that dealt with best practices and standards for scripting, you will need to follow these principles for this project. Namely, in the overall layout of the script, naming conventions, and appending digital signatures to your scripts.
- Use either your `Mark-Server1` or `Mark-Server2` for this project, whichever server you installed PowerShell onto. You can also use any Windows 7 or 8 client system.



Project Six – Background

- The script you will create will list all of the currently stopped services that begin with a certain, user supplied (an input parameter to the script), prefix (e.g., A*, *c*, m*, A*, or some variation).
- Your script should be named according to the verb-noun conventions we discussed (see page 42 – part 4 notes).
- Your script should follow a professional format (see pages 12-on in part 4 notes).
- Your script must be digitally signed (see part 5 notes).

The pages that follow explain the details of the project, stepping you through the actions. In the various callouts, the items that appear in **bold green** text require you to do screen captures and/or answer questions. These screen captures and answers will constitute your submission for this project.



Project Six – Output of the Script

```
PS C:\users\Administrator\MyScripts> .\Project.ps1 *m*

The following *m* services are currently stopped on: TESTBEDSERVER

Name                                     DisplayName
-----
AppMgmt                                 Application Management
clr_optimization_v2.0.50727_32          Microsoft .NET Framework NGEN v2.0.50727_X86
clr_optimization_v4.0.30319_32          Microsoft .NET Framework NGEN v4.0.30319_X86
hkmsvc                                   Health Key and Certificate Management
IPBusEnum                               PnP-X IP Bus Enumerator
MMCSS                                    Multimedia Class Scheduler
MSiSCSI                                  Microsoft iSCSI Initiator Service
msiserver                               Windows Installer
OracleMTSRecoveryService                OracleMTSRecoveryService
OracleOraDb11g_home1TNSListener         OracleOraDb11g_home1TNSListener
RasMan                                   Remote Access Connection Manager
RemoteAccess                            Routing and Remote Access
SNMPTRAP                                SNMP Trap
SysMain                                  Superfetch
Themes                                   Themes
Tomcat7                                  Apache Tomcat 7.0 Tomcat7
UmRdpService                            Terminal Services UserMode Port Redirector
vmss                                     VMware Snapshot Provider
wmiApSrv                                 WMI Performance Adapter
MPDBusEnum                              Portable Device Enumerator Service

List of Stopped Services Complete
Script terminating...

PS C:\users\Administrator\MyScripts>
```

The list of services named *m* that are currently stopped are listed (your set of services might vary).

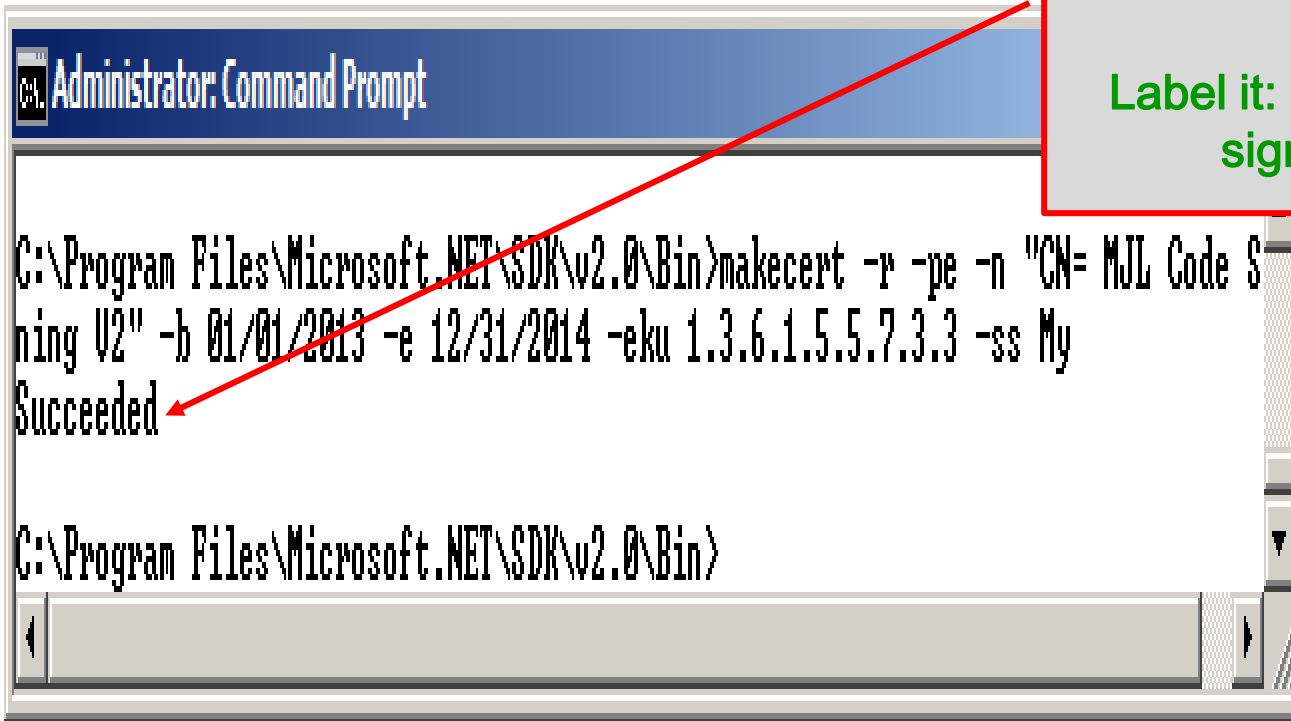
Your output (except for the actual stopped services) should look exactly like this.



Project Six – Creating The Digital Signature

Do a screen capture of this page illustrating the creation of your digital signature

Label it: "1: Successful digital signature creation"



```
Administrator: Command Prompt

C:\Program Files\Microsoft.NET\SDK\v2.0\Bin>makecert -r -pe -n "CN= MJL Code Signing V2" -b 01/01/2013 -e 12/31/2014 -eku 1.3.6.1.5.5.7.3.3 -ss My
Succeeded

C:\Program Files\Microsoft.NET\SDK\v2.0\Bin>
```



Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

```
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts> get-childitem cert:\CurrentUser\My -codesign
```

Directory: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

<u>Thumbprint</u>	<u>Subject</u>
DCA4819298B909E764A20ED8FD2030DABC8E38A5	CN=MJL Code Signing U2
D5F99C4AC4CA7734BC1186AF751E45F384F6E040	CN=MJL Code Signing

```
PS C:\users\Administrator\MyScripts> _
```

Do a screen capture of this page illustrating that PowerShell has recognized your digital certificate. (note I have two, you'll only have one)

Label it: "2: Successful PowerShell recognition of digital certificate"



```
Administrator: Windows PowerShell

PS C:\users\Administrator\MyScripts> set-authenticodesignature -filePath PS-Part5-p15-signed.ps1 -ce
ditem cert:\CurrentUser\My -codeSigningCert>[0] -includeChain "All"

Directory: C:\users\Administrator\MyScripts

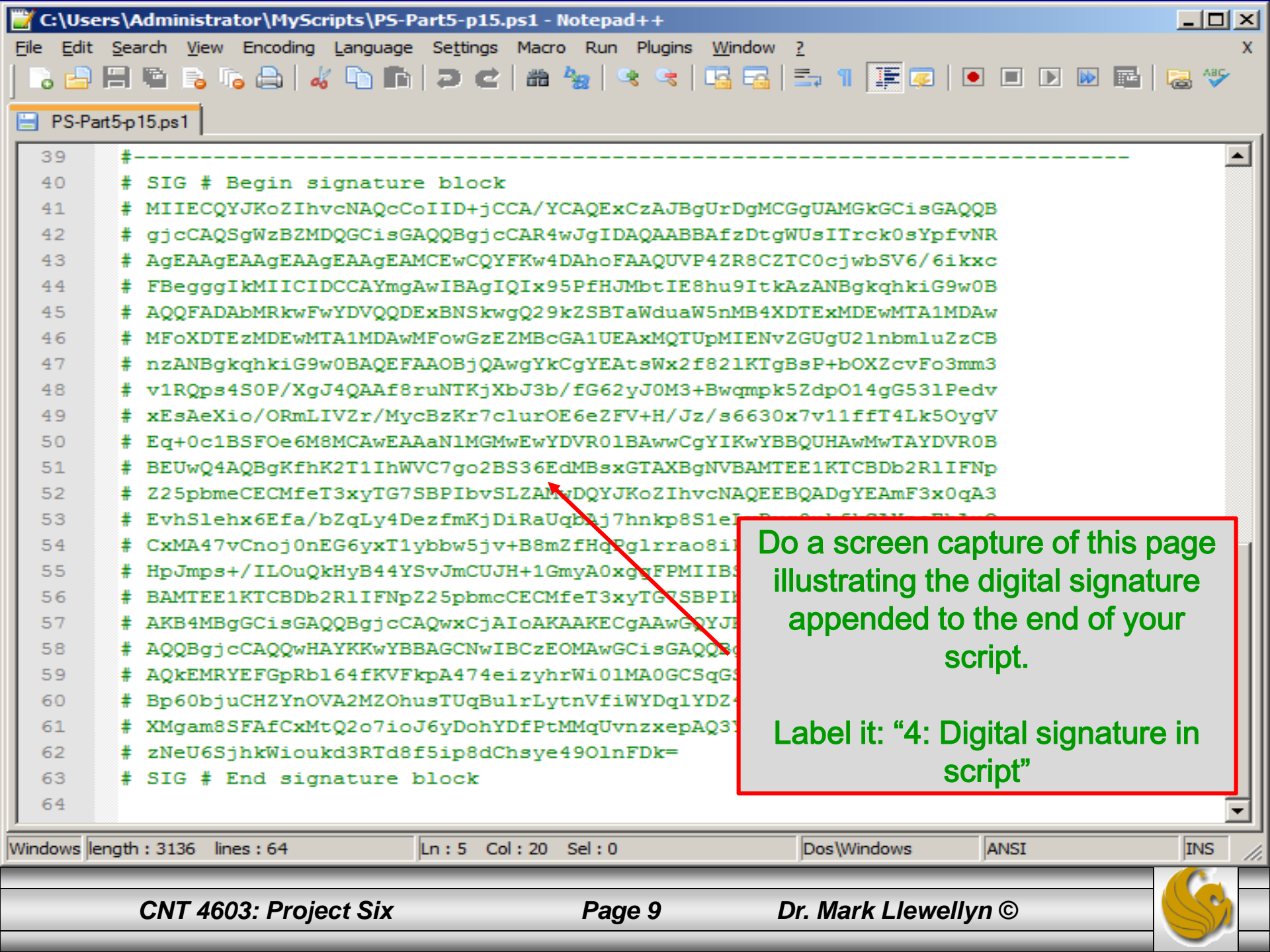
SignerCertificate          Status          Path
-----
D5F99C4AC4CA7734BC1186AF751E45F384F6E040  Valid          PS-Part5-p15-signed

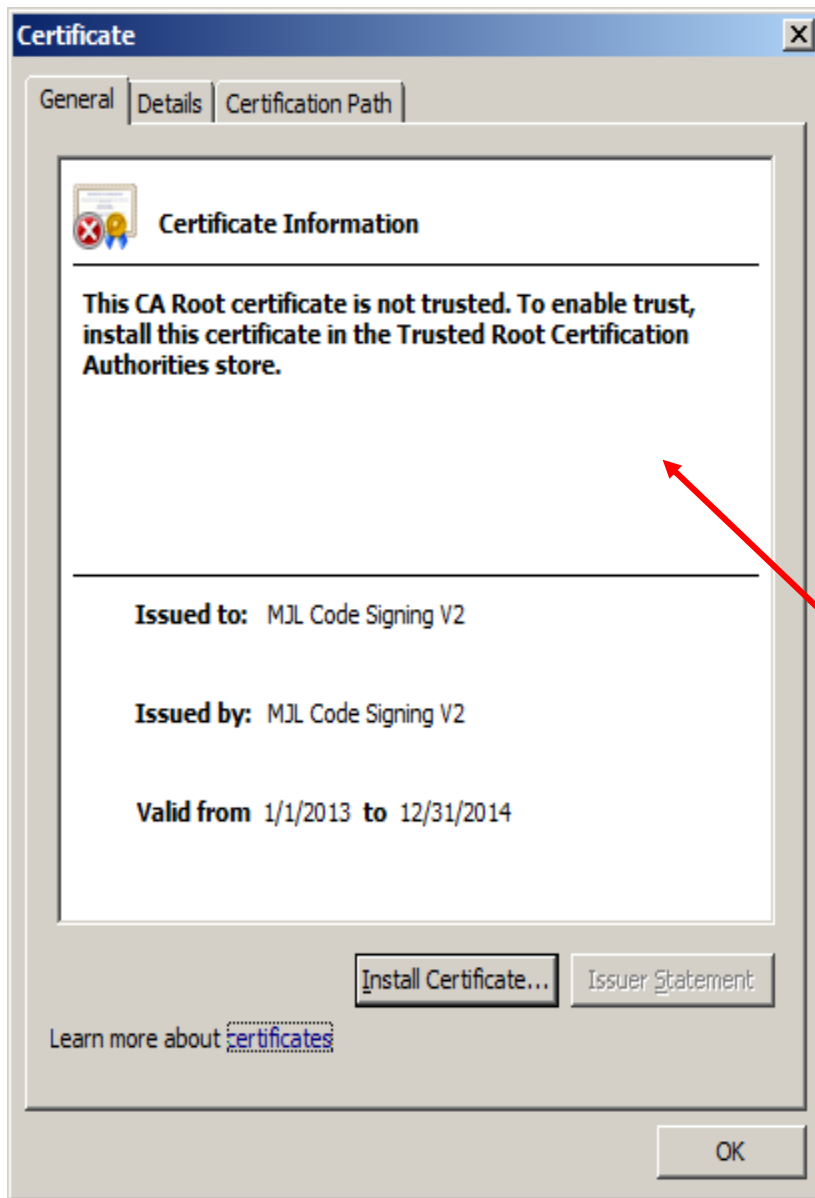
PS C:\users\Administrator\MyScripts>
```

Do a screen capture of this page illustrating that PowerShell has successfully attached the digital signature to your script.

Label it: "3: PowerShell valid status of digital certificate"







Do a screen capture of this dialog that appears during the process of registering your CA.

Label it: "5: Preparing to install certificate."



Project Six – Output of the Script

Mark - TestBed Server - VMware Player (Non-commercial use only)

Player ▾ | [Icons]

Not proper naming convention!

Parameter to the script (user supplied)

Select Administrator: Windows PowerShell

```
PS C:\users\Administrator\MyScripts> .\Project.ps1 a*
```

Name of server

```
The following a* services are currently stopped on: TESTBEDSERVER
```

The stopped services

<u>Name</u>	<u>DisplayName</u>
ALG	Application Layer Gateway Service
Appinfo	Application Information
AppMgmt	Application Management
AudioEndpointBuilder	Windows Audio Endpoint Builder
Audiosrv	Windows Audio

Feedback to the user

```
List of Stopped Services Complete  
Script terminating...
```

```
PS C:\users\Administrator\MyScripts>
```

Do a screen capture from PowerShell that shows the execution of your script. Be sure that the command to execute the script shows in the screen capture.

Label it: "6: Script execution."

