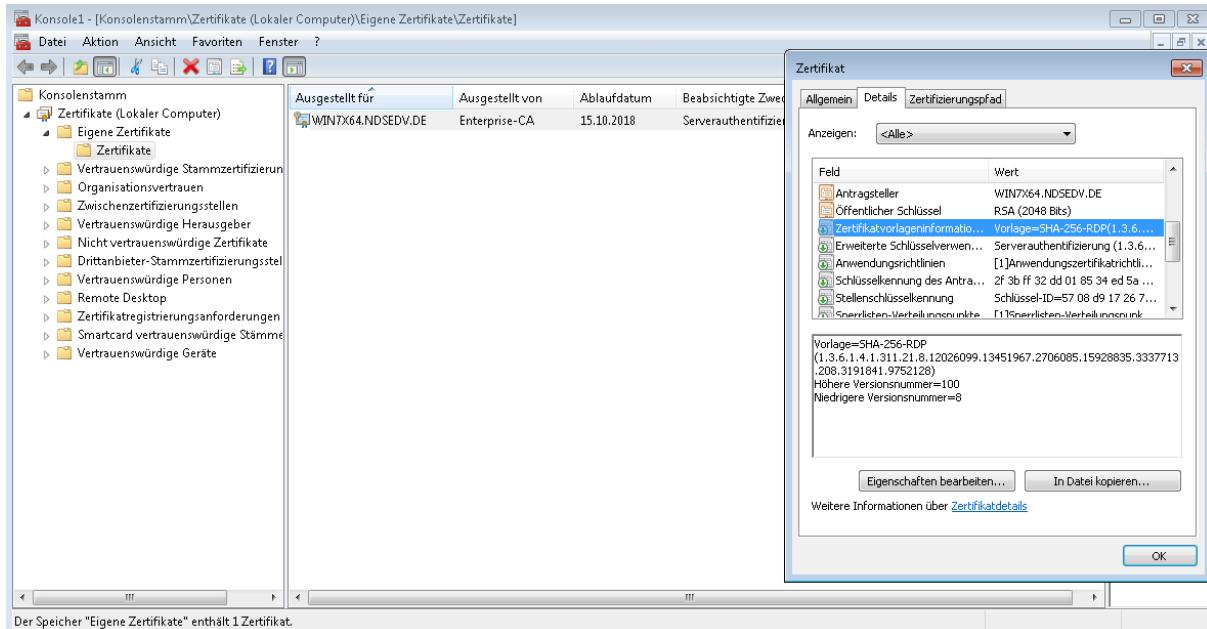
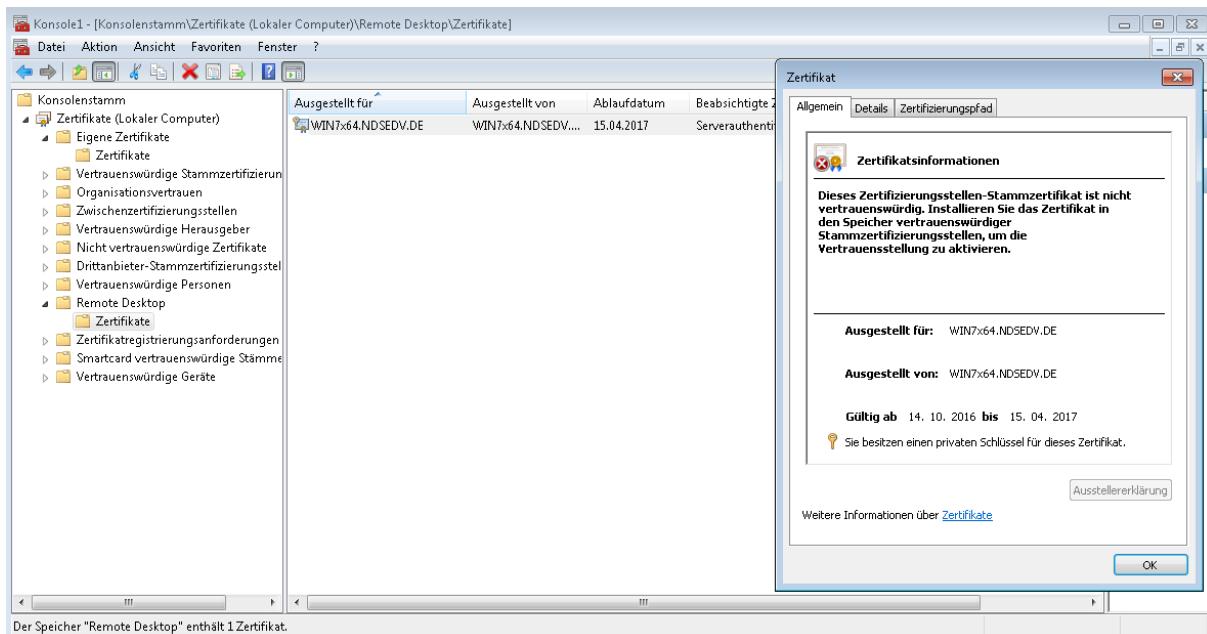
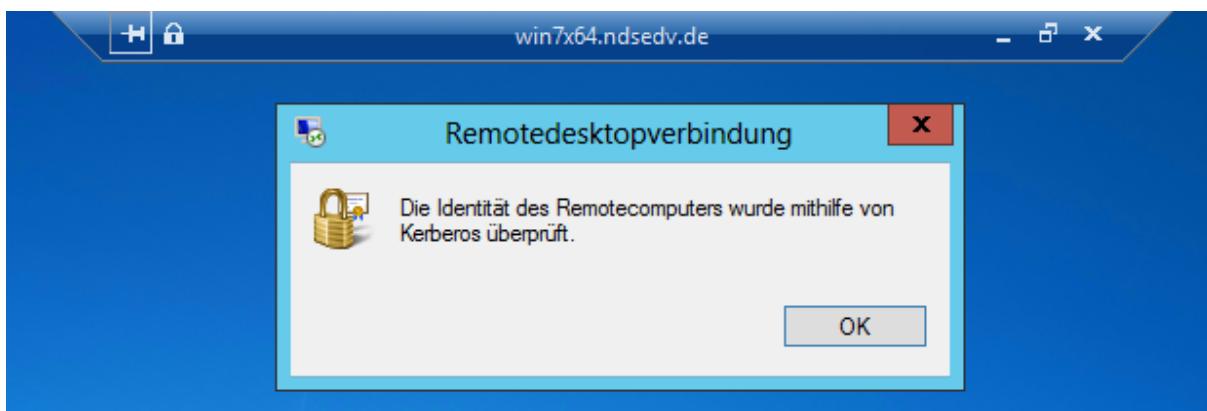


RDP-tcp – Zertifikat manuell per Powershell zuweisen

Die Ausgangslage ist, dass der Client bereits über ein Computerzertifikat verfügt sowie TLS1.2 aktiv ist.



Genutzt wird aber immer noch das selbstsignierte Maschinen Zertifikat.



RDP-tcp – Zertifikat manuell per Powershell zuweisen

Mit diesem Befehl kann man das aktuelle Zertifikat auslesen:

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
Datei Bearbeiten Anzeigen Debug Hilfe
Unbenannt1.ps1
1 wmic /namespace:\\root\cimv2\TerminalServices PATH Win32_TSGeneralSetting Get SSLCertificateSHA1Hash
2 wmic /namespace:\\root\cimv2\TerminalServices PATH Win32_TSGeneralSetting Set SSLCertificateSHA1Hash=hash

PS C:\Users\NDS\Desktop> wmic /namespace:\\root\cimv2\TerminalServices PATH Win32_TSGeneralSetting Get SSLCertificateSHA1Hash
SSLCertificateSHA1Hash
36736EBBB562A8A877E1D79DA476B6186B5083A2
36736EBBB562A8A877E1D79DA476B6186B5083A2

Befehl 1) Überprüfen welches Zertifikat zugewiesen ist
Befehl 2) Ein Zertifikat zuweisen

Abgeschlossen
```

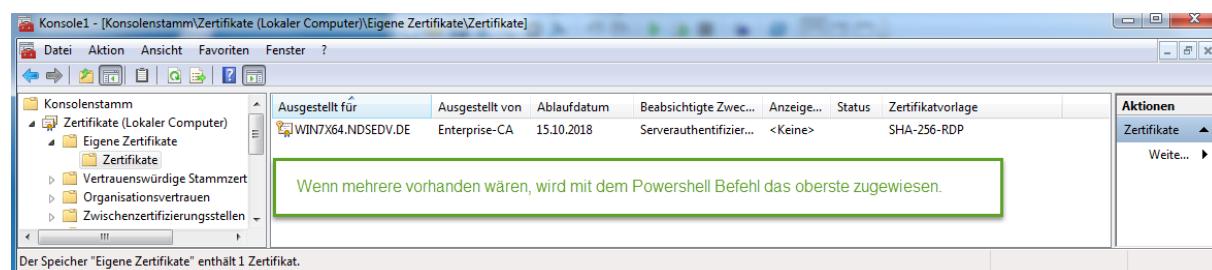
Mithilfe der Powershell weisen wir dem RDP-TCP Protokoll das erste aufgeführte Computerzertifikat zu.

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
Datei Bearbeiten Anzeigen Debug Hilfe
CertRDP.ps1
1 $sts = gwmi -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp'"
2 $thumb = (gci -path cert:/LocalMachine/My | select -first 1).Thumbprint
3 $wmi -path $sts.__path -argument @{SSLCertificateSHA1Hash=$thumb}

PS C:\Users\NDS\Desktop> C:\Users\NDS\Desktop\CertRDP.ps1

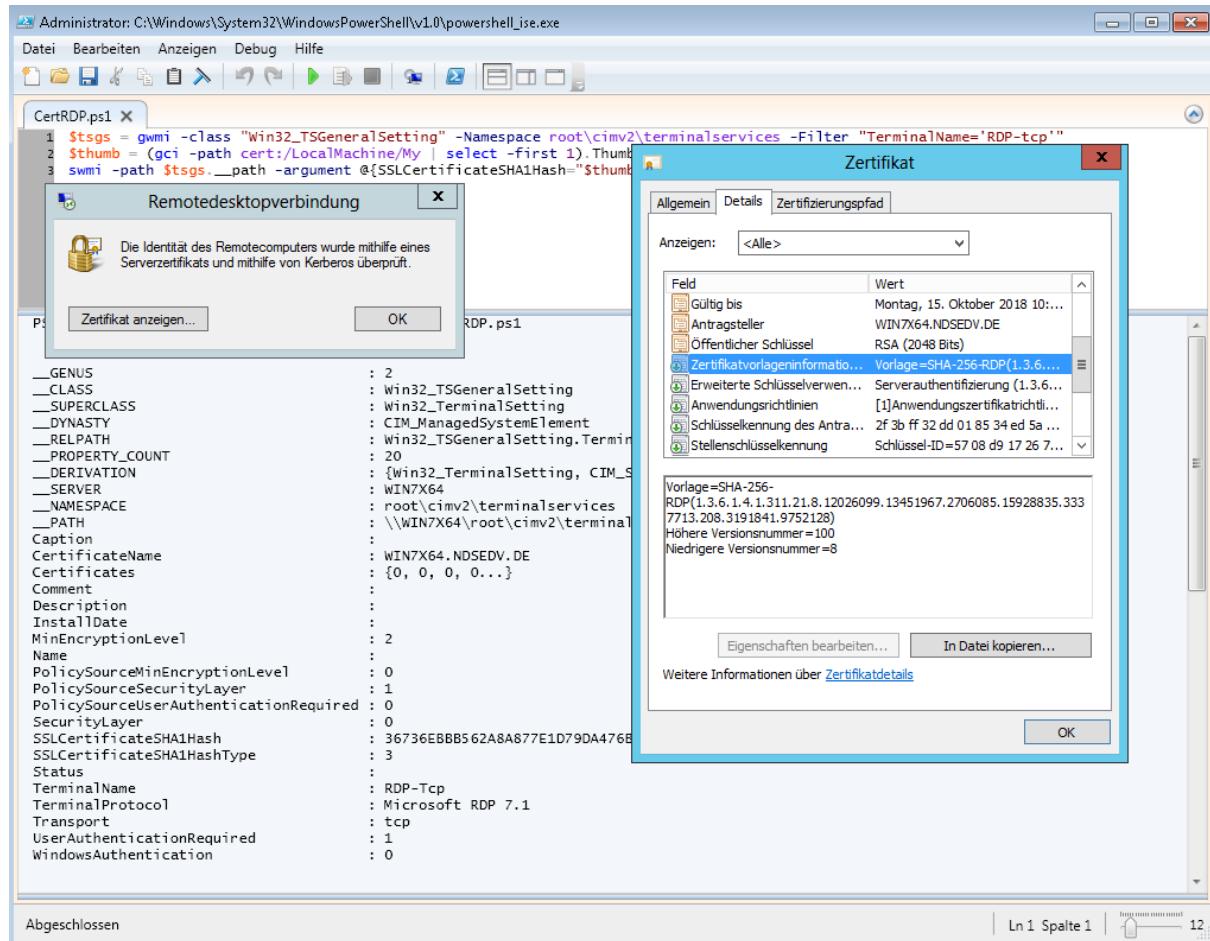
__GENUS
__CLASS
__SUPERCLASS
__DYNASTY
__RELPATH
__PROPERTY_COUNT
__DERIVATION
__SERVER
__NAMESPACE
__PATH
Caption
CertificateName : WIN7X64.NDSEDV.DE ← Red Arrow
Certificates
Comment
Description
InstallDate
MinEncryptionLevel
Name
PolicySourceMinEncryptionLevel : 0
PolicySourceSecurityLayer : 1
PolicySourceUserAuthenticationRequired : 0
SecurityLayer : 0
SSLCertificateSHA1Hash : 36736EBBB562A8A877E1D79DA476B6186B5083A2
SSLCertificateSHA1HashType : 3
Status
TerminalName : RDP-Tcp
TerminalProtocol : Microsoft RDP 7.1
Transport : tcp
UserAuthenticationRequired : 1
WindowsAuthentication : 0

Abgeschlossen
```



RDP-tcp – Zertifikat manuell per Powershell zuweisen

Erneuter Versuch einer RDP Verbindung.



Powershell Skript:

```
$tsgs = gwmi -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices  
-Filter "TerminalName='RDP-tcp'"  
$thumb = (gci -path cert:/LocalMachine/My | select -first 1).Thumbprint  
swmi -path $tsgs.__path -argument @{SSLCertificateSHA1Hash="$thumb"}
```

oder das letzte in der Auflistung:

```
$tsgs = gwmi -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices  
-Filter "TerminalName='RDP-tcp'"  
$thumb = (gci -path cert:/LocalMachine/My | select -Last 1).Thumbprint  
swmi -path $tsgs.__path -argument @{SSLCertificateSHA1Hash="$thumb"}
```

oder per Thumbprint zuweisen:

```
$path = (Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace  
root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp").__path  
  
Set-WmiInstance -Path $path -argument  
@{SSLCertificateSHA1Hash="B7A2E65FBC40CDFADC57D283AC4A0508CC58E566"}
```

oder per CMD importieren und zuweisen:

```
certutil -importpfx rdp.pfx  
wmic /namespace:\\root\cimv2\TerminalServices PATH Win32_TSGeneralSetting Set  
SSLCertificateSHA1Hash=B7A2E65FBC40CDFADC57D283AC4A0508CC58E566
```

RDP-tcp – Zertifikat manuell per Powershell zuweisen

Die vorhandenen Zertifikate auslesen:

```
Set-Location Cert:\CurrentUser\My  
Get-ChildItem | Format-Table Subject, Thumbprint -AutoSize
```

The screenshot shows a Windows PowerShell ISE window titled "Windows PowerShell ISE". A script file named "RDP CERT.ps1" is open. The code within the file is:

```
Set-Location Cert:\CurrentUser\My  
Get-ChildItem | Format-Table Subject, Thumbprint -AutoSize
```

When run, the output shows a table with two columns: "Subject" and "Thumbprint". The "Subject" column displays the certificate details, and the "Thumbprint" column displays a redacted (blurred) string of characters.

Subject	Thumbprint
OU=Symantec Trust Network, OU=Persona Not Validated, OU=S/MIME, E=team@nds-edv.de, CN=Persona Not Validated - J... CN=joernwalter.de, E=mai1@joernwalter.de, CN=mai1@joernwalter.de	[REDACTED]