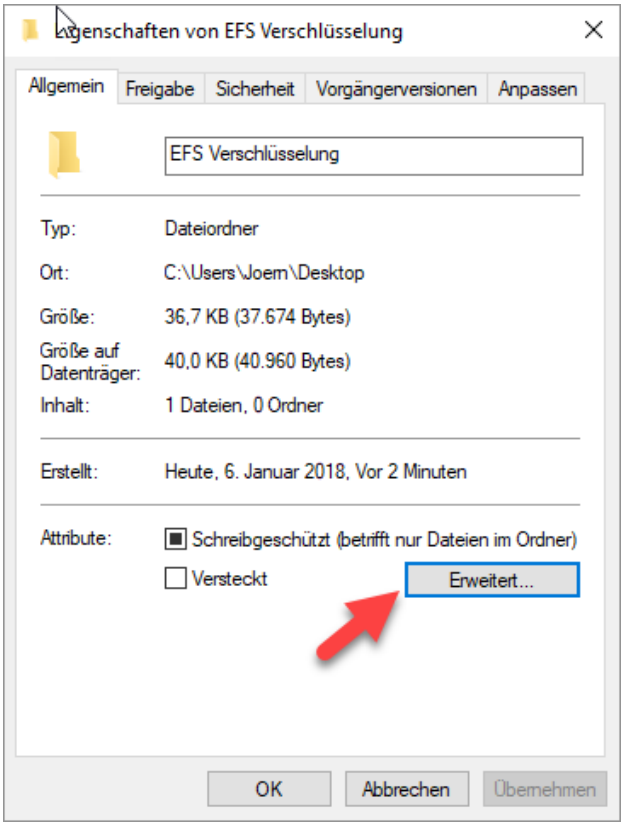
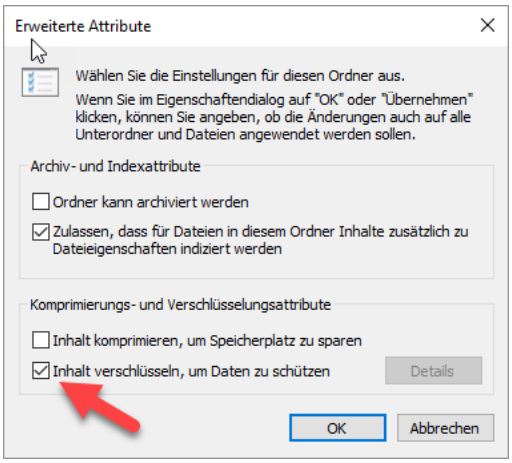
Windows EFS Verschlüsselung

Unter Windows 10 Pro können wir Daten mittels des EFS (Encrypting File System) schnell und sicher verschlüsseln. Die Umsetzung ist in weniger als 5 Minuten erledigt. Nach der Aktivierung wird auf dem System ein selbstsigniertes Zertifikat erzeugt. Dieses Zertifikat besteht aus 2 Teilen und zwar einem öffentlichen Schlüssel und einem privaten Schlüssel. Der öffentliche Schlüssel verschlüsselt die Daten und der private Schlüssel entschlüsselt die Daten wieder. Wir sprechen hier also von einem Schlüsselpaar. Zur Demonstration erstelle ich auf meinem Desktop einen neuen Ordner und nenne diesen EFS Verschlüsselung.

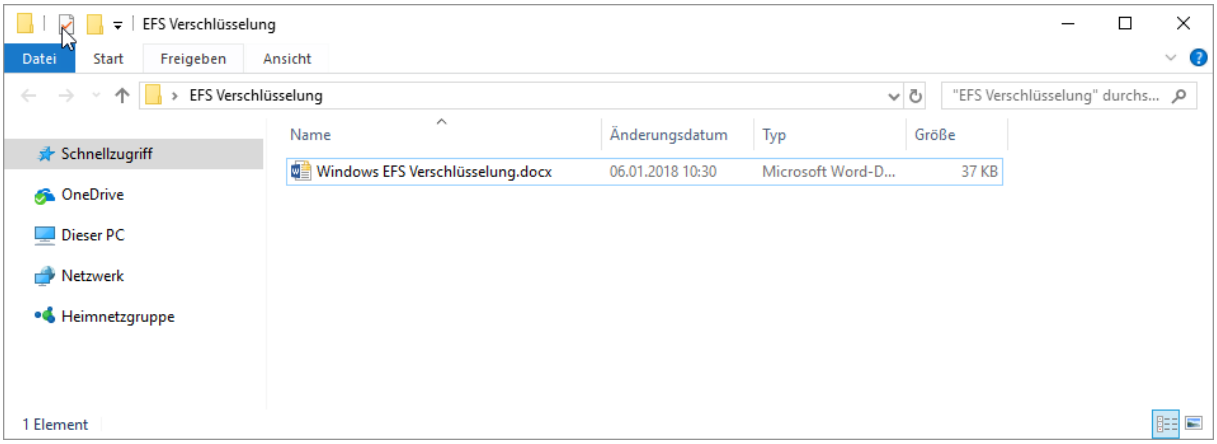
Mit einem Rechtsklick auf den Ordner öffne ich die Eigenschaften. Über den Reiter Allgemein > Erweitert öffnen wir die Ansicht der erweiterten Attribute.



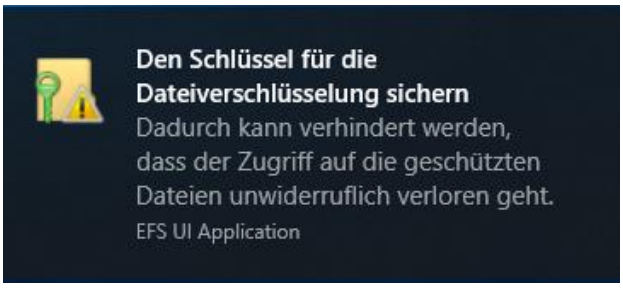
Ich setze den Haken in „Inhalt verschlüsseln, um Daten zu schützen"



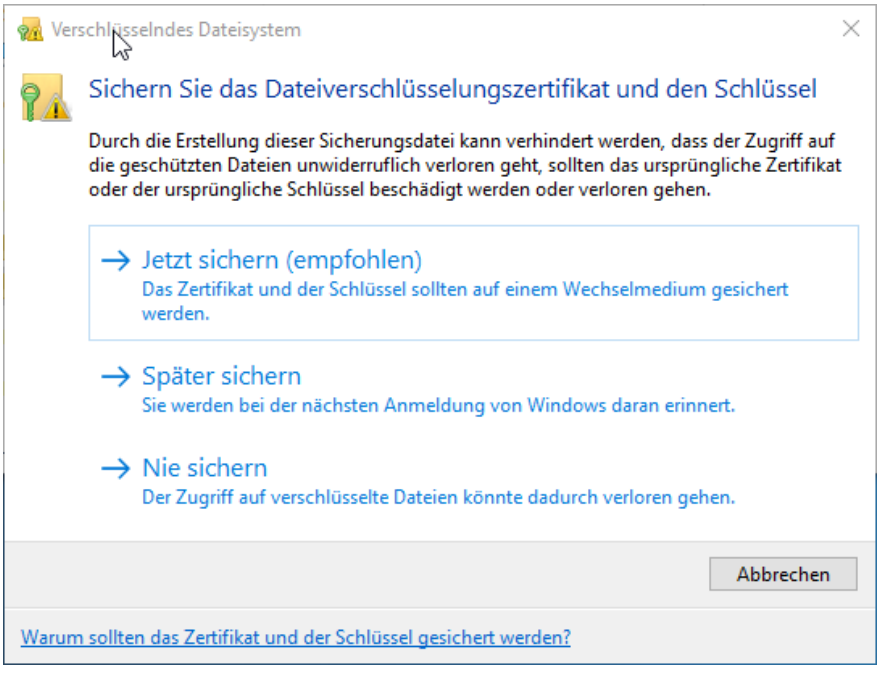
Mit OK bestätige ich nun die Veränderung des Attributes und diese wirkt sich somit auf den ganzen Ordner aus. Sobald ich nun neue Dateien erstelle und bereits Dateien enthalten waren, werden diese verschlüsselt. Das erkennen wir an dem Schloßsymbol.



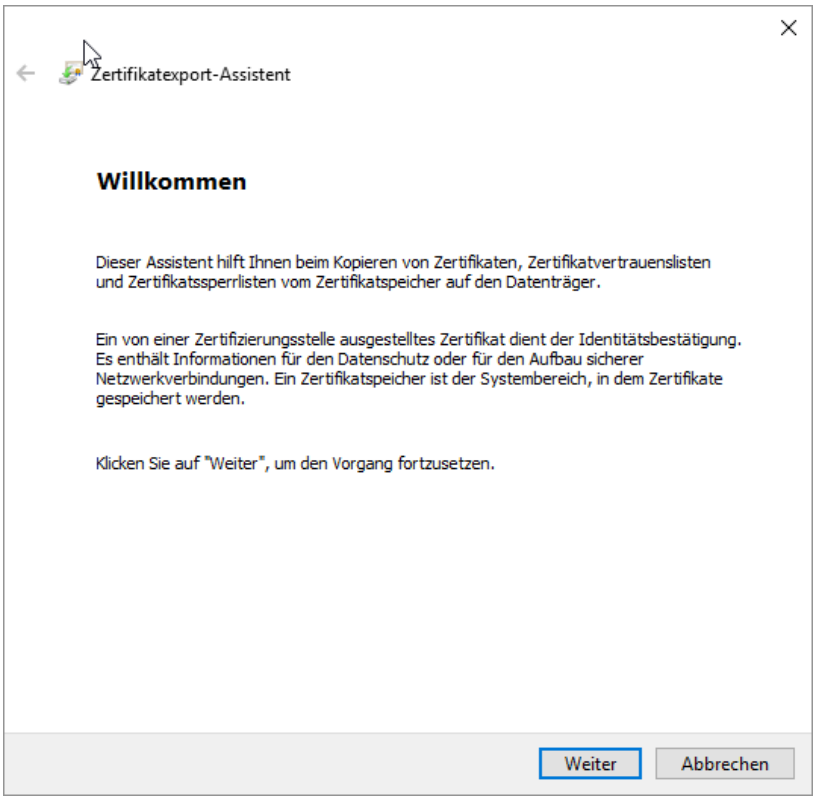
Nachdem nun die Verschlüsselung aktiviert wurde, werden wir vom System aufgefordert, das Zertifikat mit dem die Daten nun verschlüsselt wurden, zu sichern. Die Sicherung des Zertifikats stellt sicher, dass wir auch nach einem Wechsel, Neuinstallation des Systems oder nach dem Kopieren auf einem anderen Computer auf unsere Daten zugreifen können.



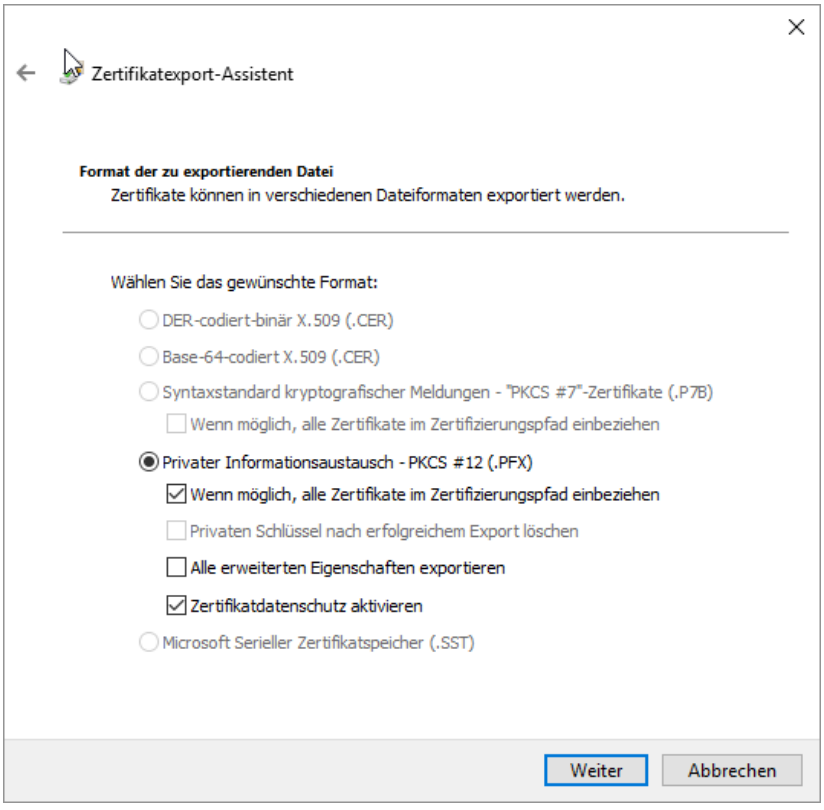
Das Zertifikat können wir über mehrere Wege sichern. Entweder über den Assistenten…



Der Assistent startet.

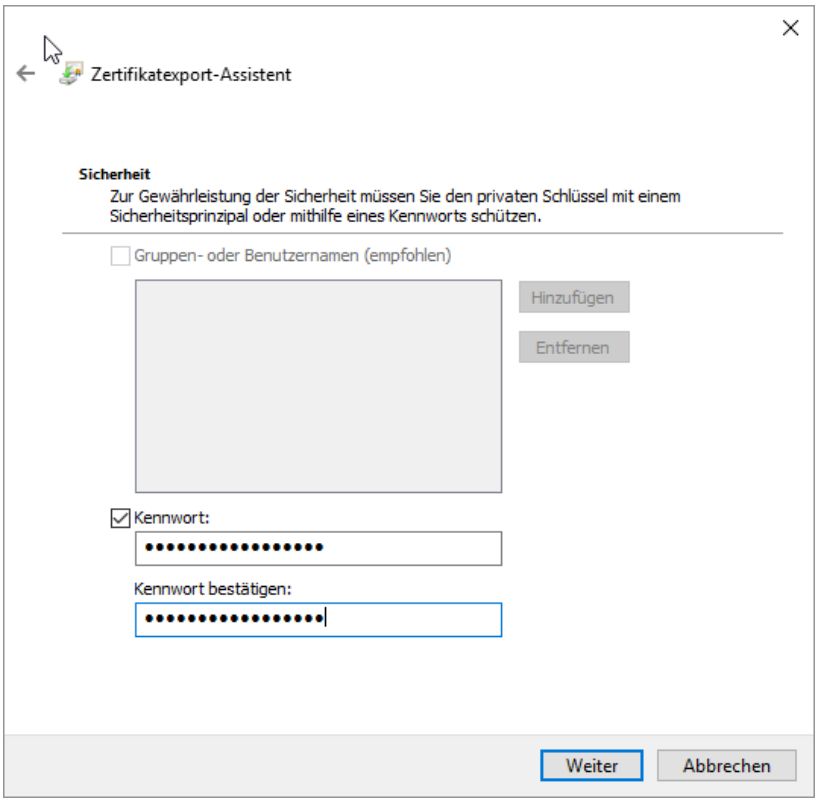


Die Einstellungen werden übernommen.

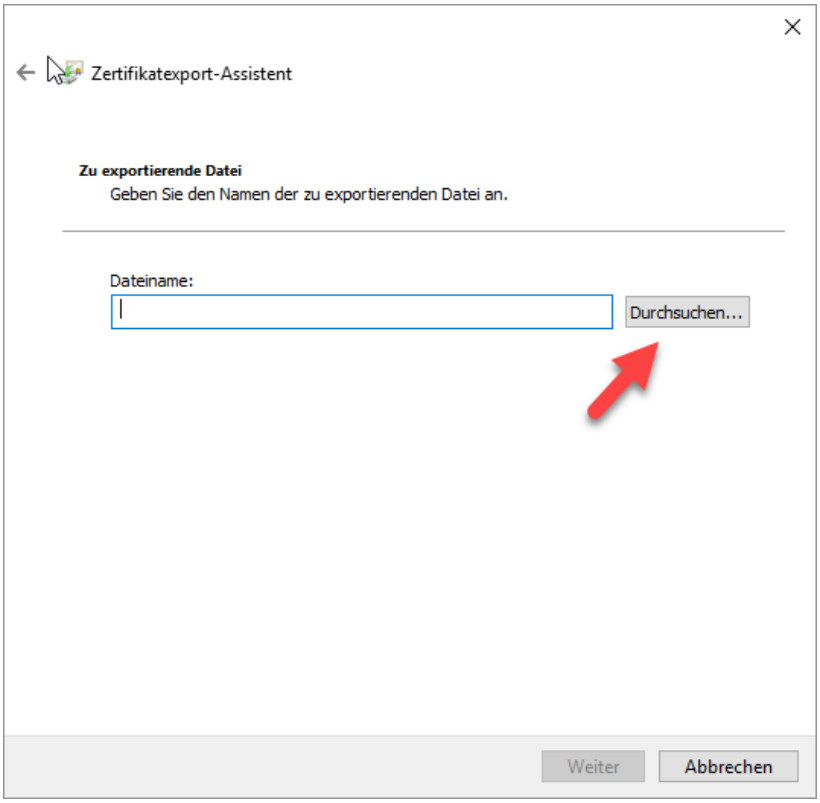


Windows EFS Verschlüsselung

Vergeben ein starkes mindestens 12-stelliges Passwort.

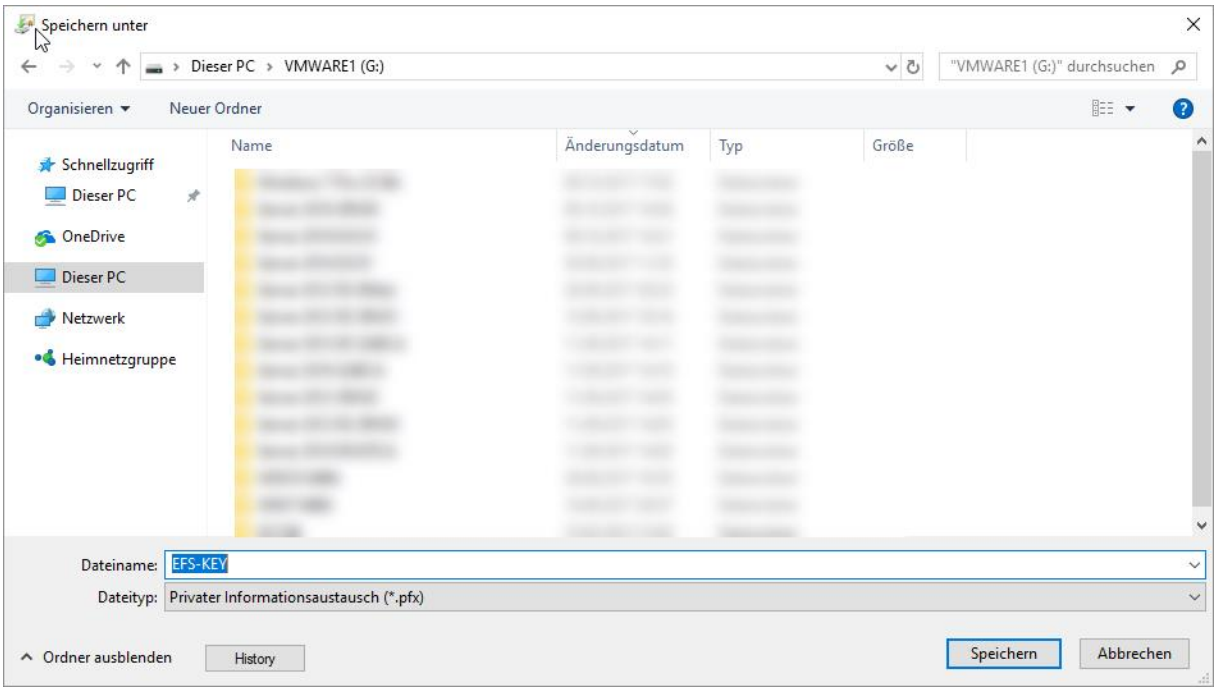


Und speichern das Zertifikat (Schlüsselpaar) an einen sicheren Ort. Bitte an 2 verschiedenen Orten ablegen, gerne noch zusätzlich auf einen USB-Stick.

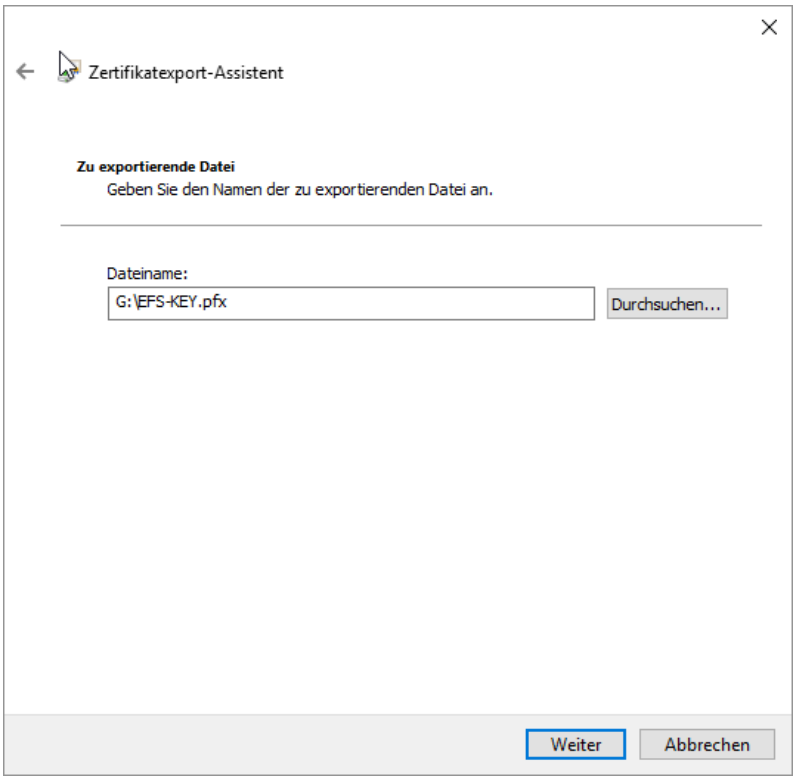


Windows EFS Verschlüsselung

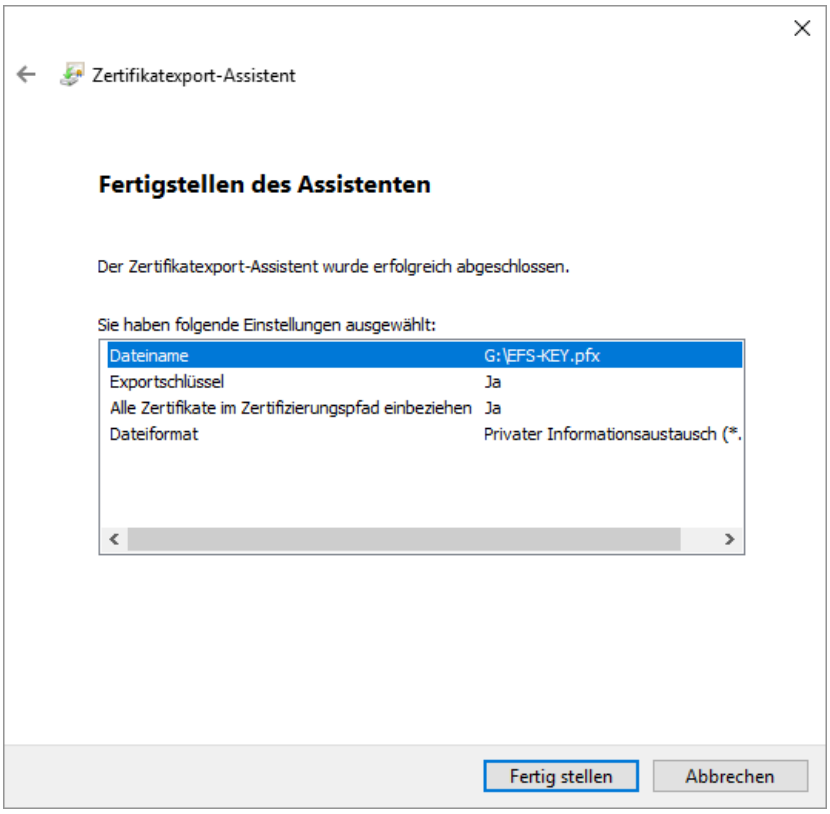
Ziel auswählen…



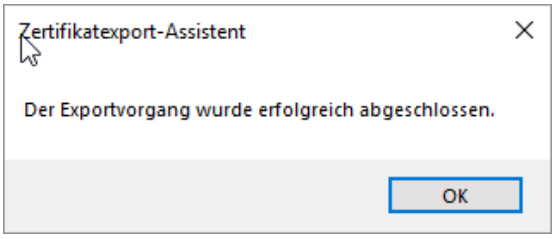
…mit > Weiter den Speicherort bestätigen.



Mit „Fertig stellen“ schließen wir den Vorgang ab.

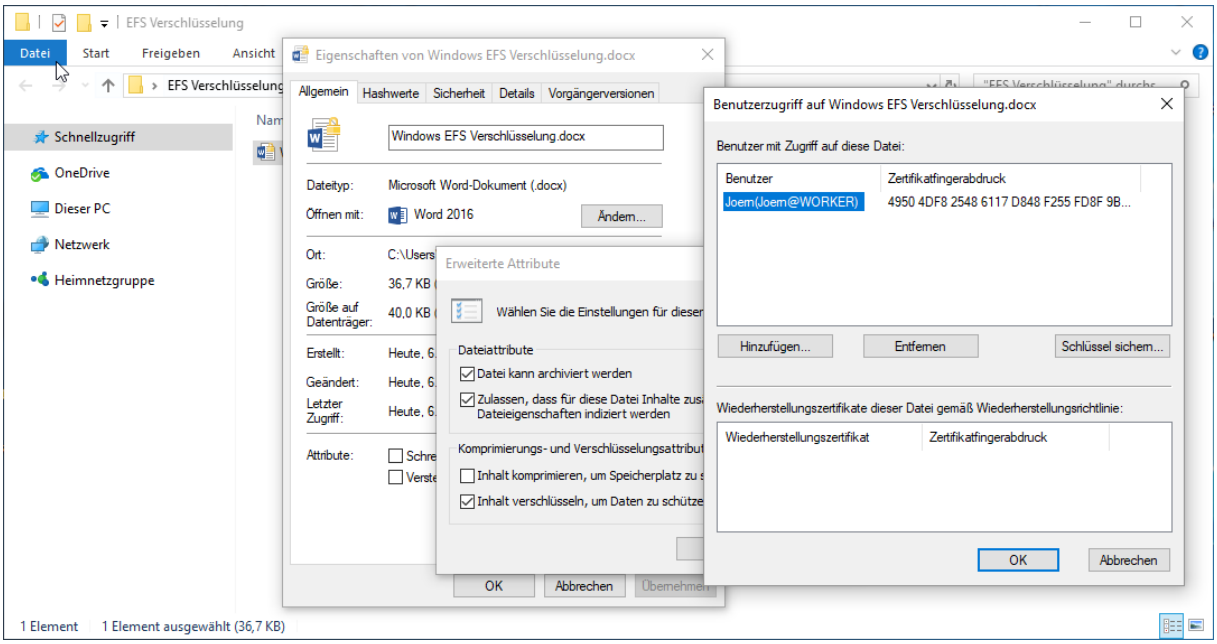


Das Schlüsselpaar wurde erfolgreich exportiert.

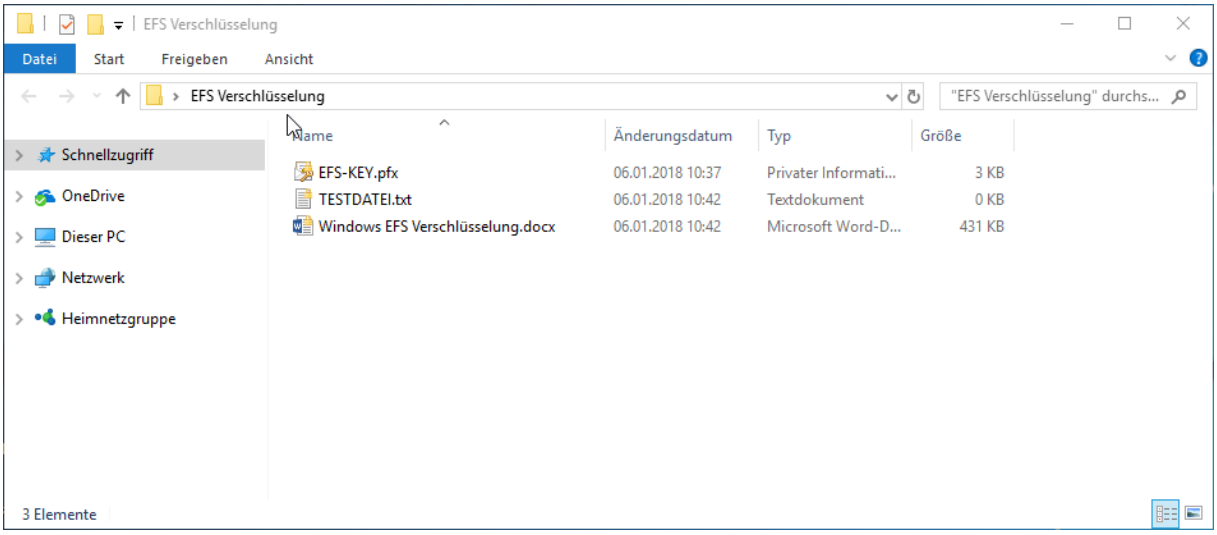


Windows EFS Verschlüsselung

…oder Rechtsklick auf den Ordner > Erweitert > Details > Schlüssel sichern…



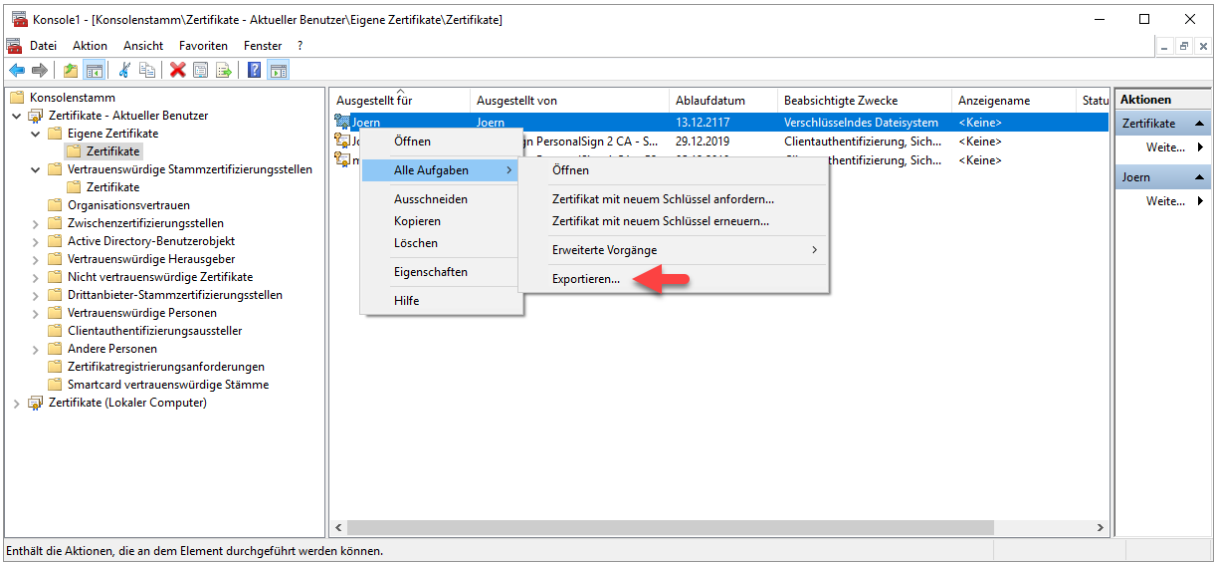
Die Datei EFS-KEY.pfx enthält den öffentlichen sowie den privaten Schlüssel.



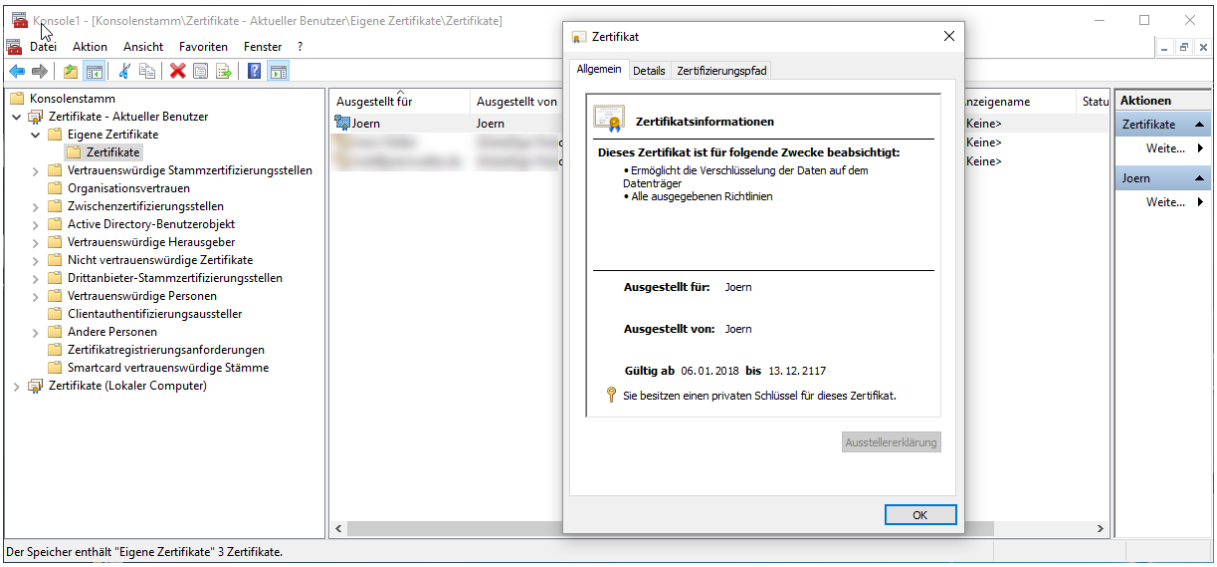
Windows EFS Verschlüsselung

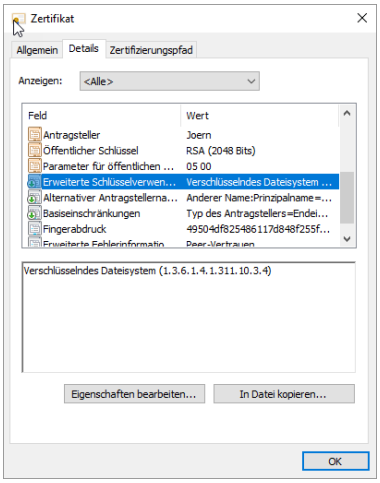
Eine weitere Möglichkeit wäre der Zugriff auf das Zertifikat über die MMC.

CMD > MMC > Datei > Snap-in hinzufügen > Zertifikate > Aktueller Benutzer
Zertifikat anklicken > Rechtsklick > Alle Aufgaben > Exportieren



Ein Doppelklick auf das Zertifikat öffnet die Eigenschaften.





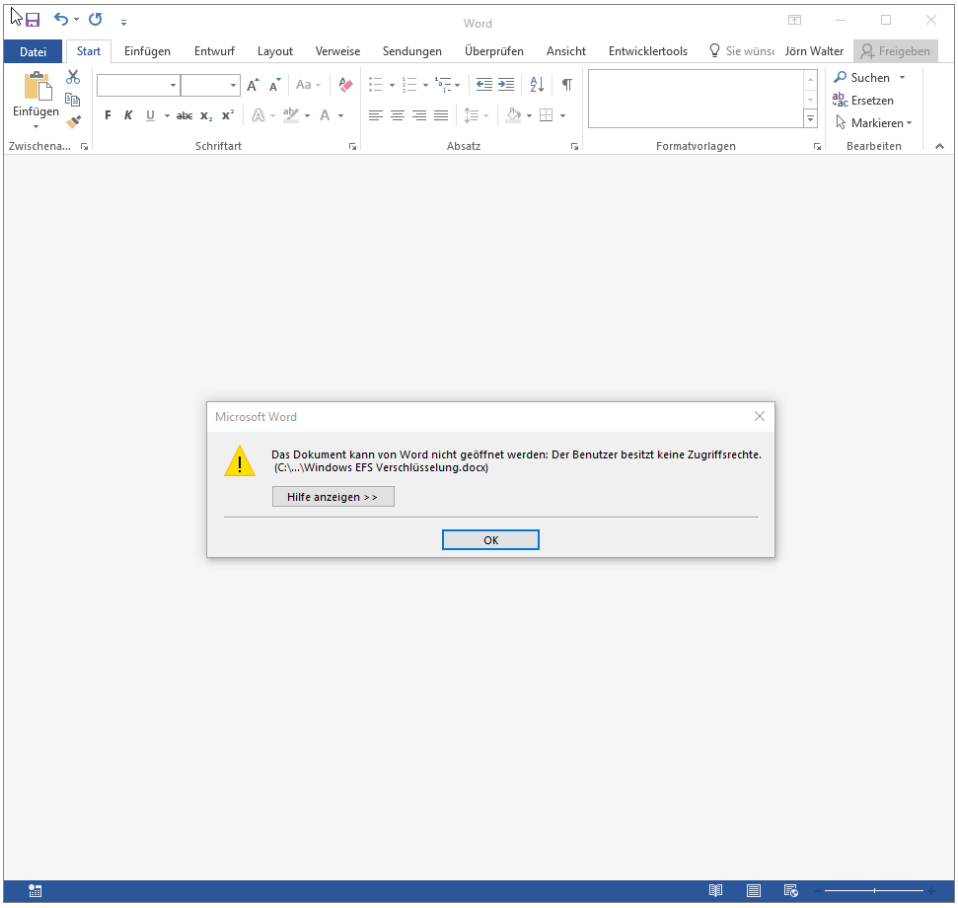
Erstellt von Jörn Walter **06.01.2018 / 29.12.2019**

Sollte das System nun neu aufgesetzt werden, muss nur noch das Zertifikat mit einem Doppelklick importiert werden. Nach dem Import sind die Daten wieder im Zugriff und können bearbeitet werden.

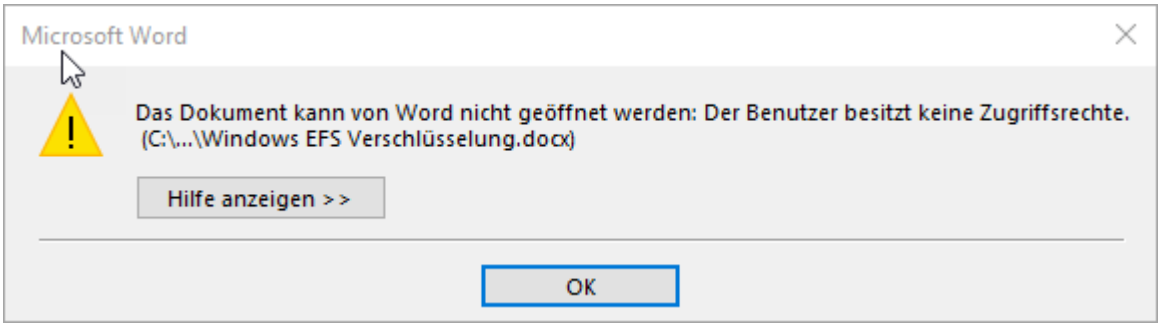
Zur Veranschaulichung werde ich das Zertifikat über die MMC löschen und nach einem Neustart des Systems versuchen die Daten zu öffnen.

Der Neustart ist erfolgt und ich versuche nun diese Anleitung die sich in dem verschlüsselten Ordner befand zu öffnen.

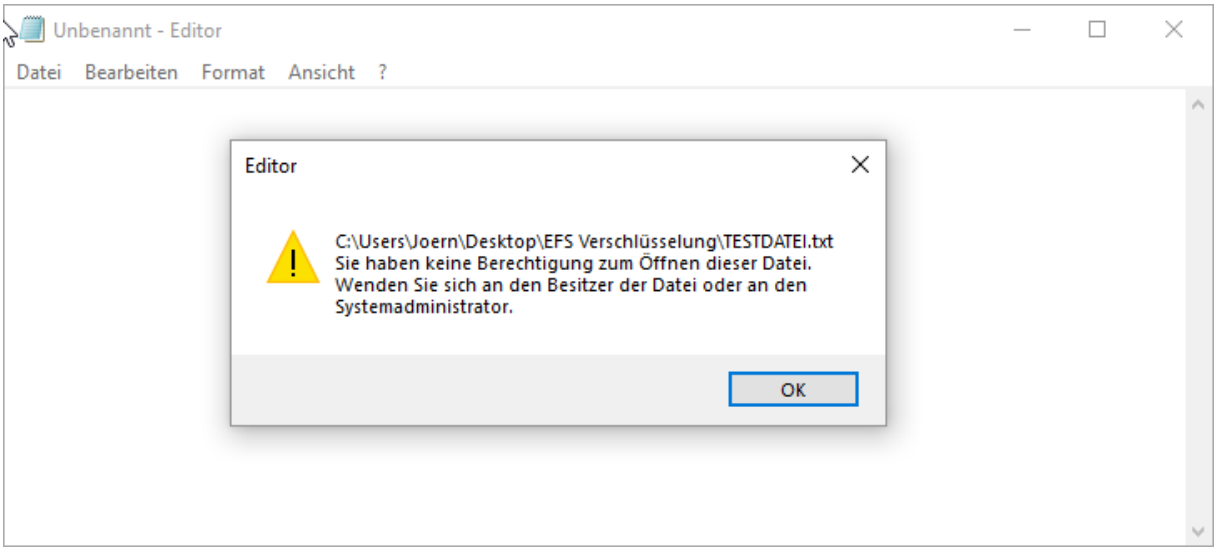
Der Versuch scheitert, nach kurzer Zeit. Warum nach kurzer Zeit? Auf dem System wird nach dem Zertifikat zum Öffnen der Datei gesucht.



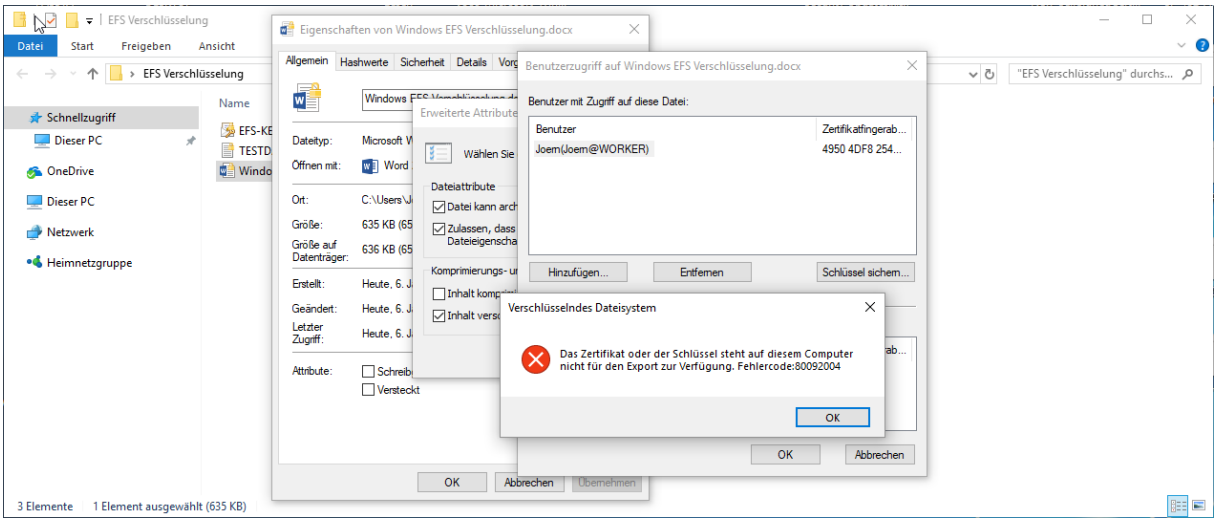
Die Fehlermeldung etwas näher betrachtet: Es fehlen schlicht weg die Rechte! Und das recht zum Öffnen der Datei hätten wir, wenn der private Schlüssel vorhanden wäre.



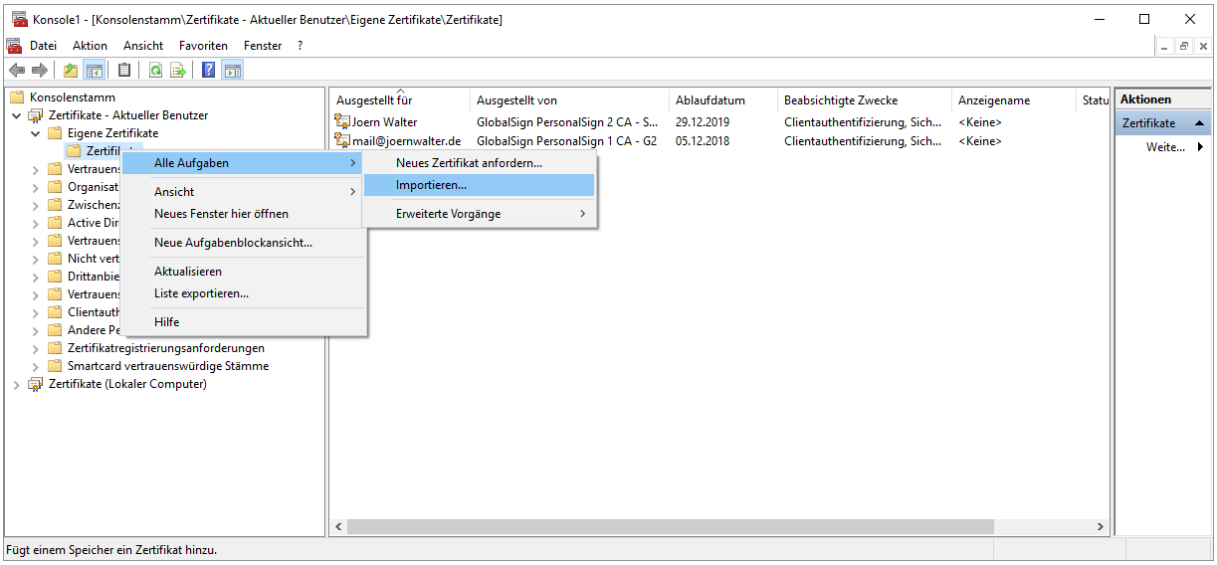
Auch der Versuch die TESTDATEI.TXT zu öffnen scheitert.



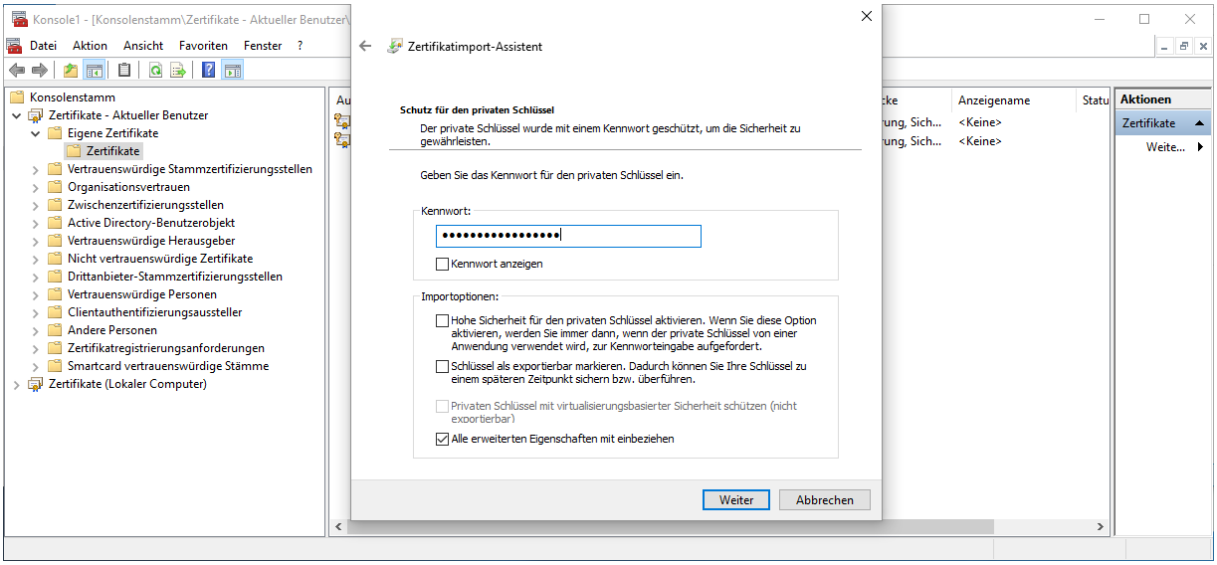
Die Eigenschaften der verschlüsselten Dateien sagen aus, dass das Zertifikat zum Entschlüsseln fehlt.



Treten wir nun den Gegenbeweis an. Ich importiere das gesicherte Zertifikat wieder über die MMC oder durch einen Doppelklick.

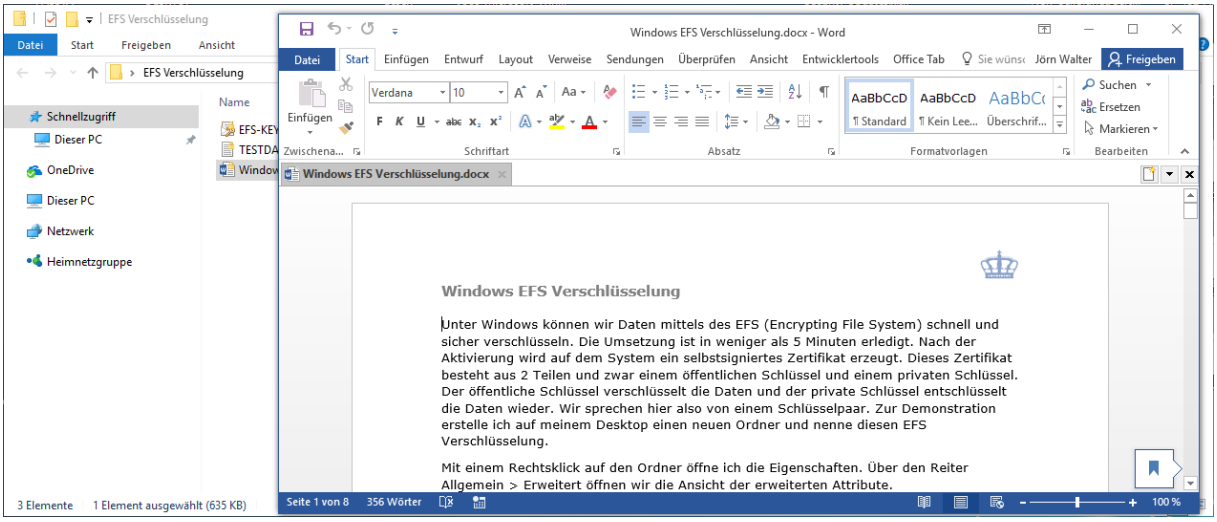


Geben das sichere Passwort ein um den Importvorgang überhaupt durchführen zu können.



Windows EFS Verschlüsselung

Nachdem das Zertifikat wieder auf dem System vorhanden ist, sind die Dateien wieder im Zugriff.



CMD One-Liner mit Cipher:

Kommen wir nun zur Powershell. Über die Powershell setzen wir den Befehl Cipher zur Verschlüsselung ein.

Möchten wir eine einzelne Datei verschlüsseln, dann lautet der Befehl:

cipher /A /E Dateiname

Möchten wir mehrere einzelne Dateien verschlüsseln, dann lautet der Befehl:

cipher /A /E Dateiname1 Dateinam2 Dateiname3

Möchten wir eine einzelne Datei wieder entschlüsseln, dann lautet der Befehl:

cipher /D Dateiname

Möchten wir mehrere einzelne Dateien wieder entschlüsseln, dann lautet der Befehl:

cipher /D Dateiname1 Dateinam2 Dateiname3

Möchten wir einen ganzen Ordner verschlüsseln, dann lautet der Befehl:

cipher /E OrdnerPfad

Möchten wir alle Dateien in einem Ordner verschlüsseln, dann lautet der Befehl:

cipher /E OrdnerPfad*

Möchten wir bestimmte Dateien in einem Ordner verschlüsseln, dann lautet der Befehl:

cipher /E E:docx*

Möchten wir bestimmte Dateien in einem Ordner rekursiv verschlüsseln, dann lautet der Befehl:

cipher /E /S:OrdnerPfad

Zum Entschlüsseln aller Dateien in Ordner und Unterordnern, dann lautet der Befehl:

cipher /A /E / S: OrdnerPfad

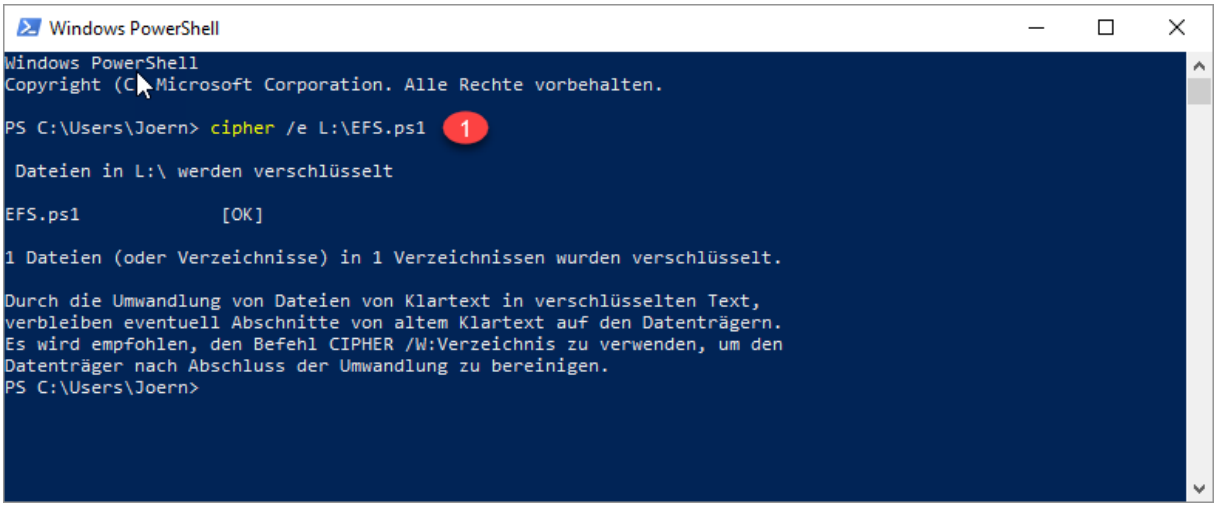
Windows EFS Verschlüsselung

Zum Entschlüsseln aller Dateien und Ordner und Unterordnern, dann lautet der Befehl:

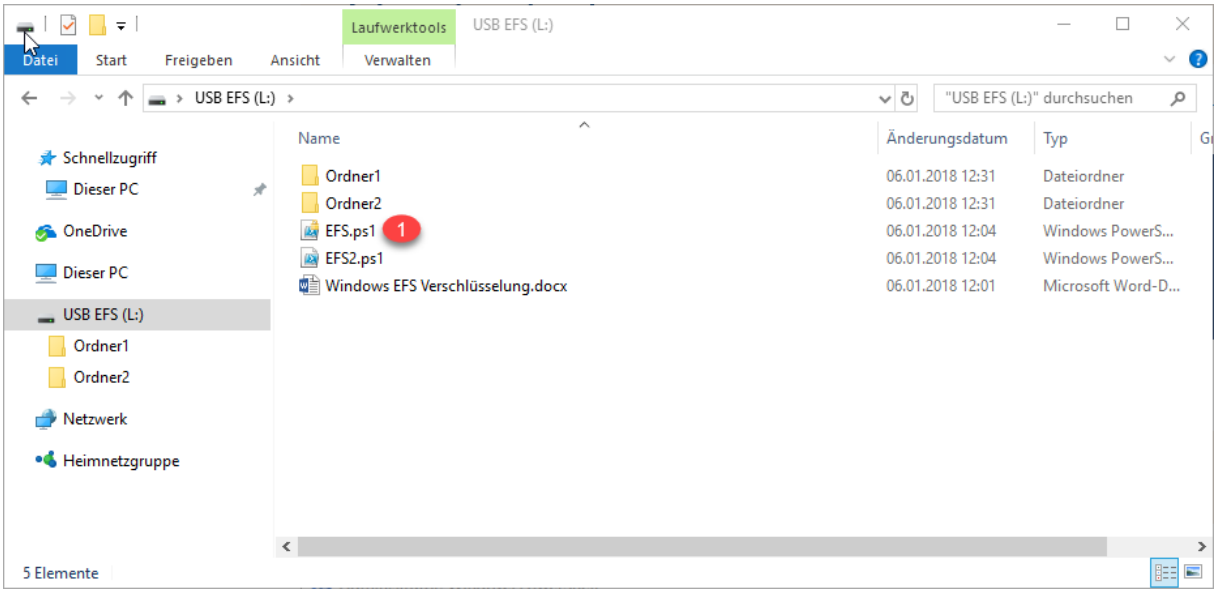
cipher /D Dateiname

Beispielanwendung:

Wir verwenden das erste Mal die Dateiverschlüsselung. Ein Zertifikat wird angelegt, die Datei wird verschlüsselt, das Zertifikat muss gesichert werden. Das ist der gleiche Ablauf wie am Anfang der Doku bereits beschrieben.

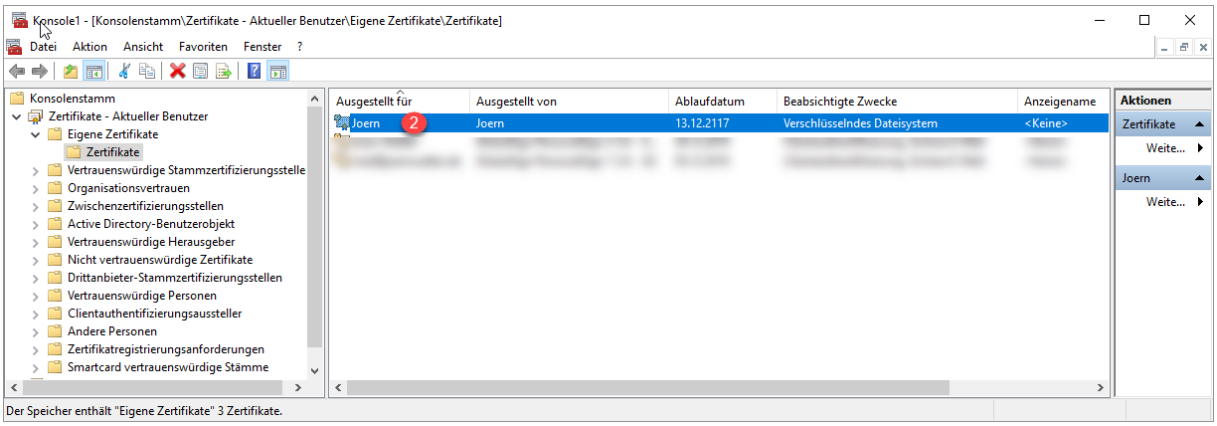


1) Die Datei wurde verschlüsselt:

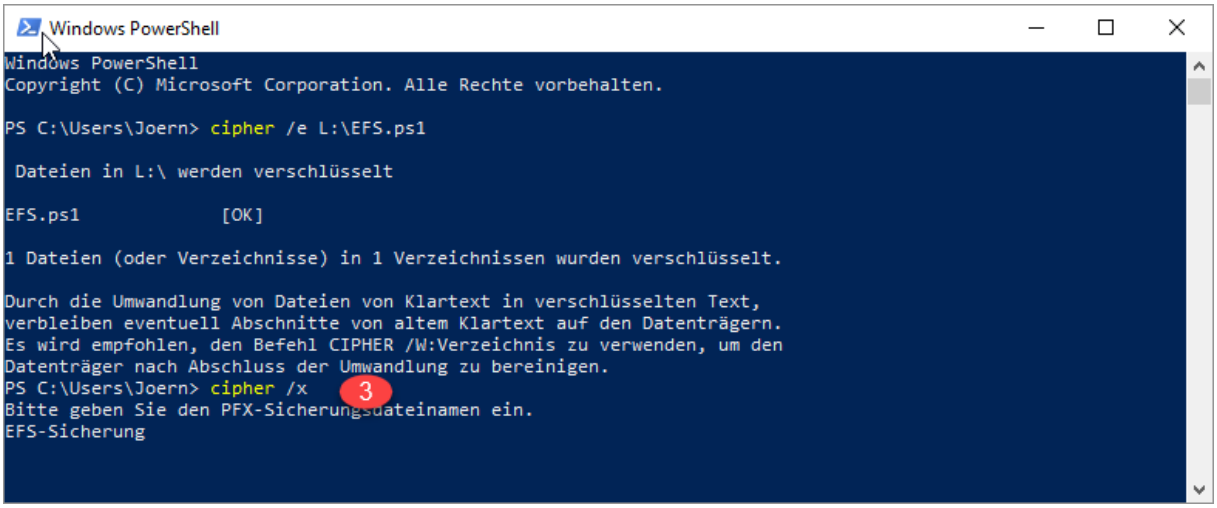


Windows EFS Verschlüsselung

2) Das Zertifikat wurde angelegt:



3) Das Zertifikat muss gesichert werden:



Powershell One-Liner mit FileEncryption:

Get-Item L:\EFS.ps1 | Enable-FileEncryption
Get-Item L:\EFS.ps1,L:\EFS2.ps1 | Enable-FileEncryption

Get-Item L:\EFS.ps1 | Disable-FileEncryption
Get-Item L:\EFS.ps1,L:\EFS2.ps1 | Disable-FileEncryption

Get-ChildItem L:\Ordner1 | Enable-FileEncryption
Get-ChildItem L:\Ordner1,L:\Ordner2 | Enable-FileEncryption

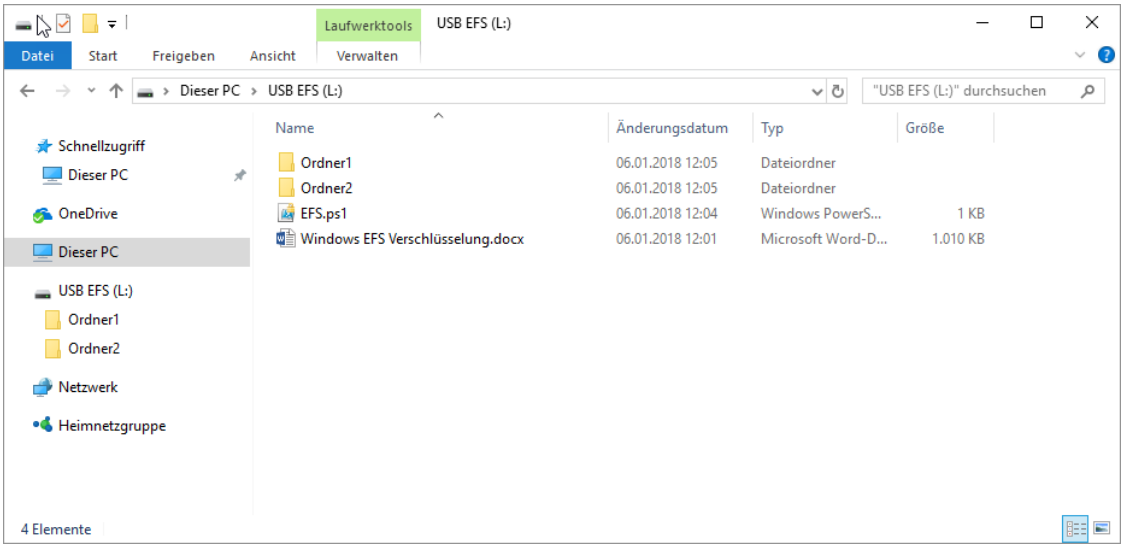
Get-ChildItem L:\Ordner1 | Disable-FileEncryption
Get-ChildItem L:\Ordner1,L:\Ordner2 | Disable-FileEncryption

Windows EFS Verschlüsselung

Powershell-Skript:

Setzen wir nun ein Skript zum Verschlüsseln und entschlüsseln ein.

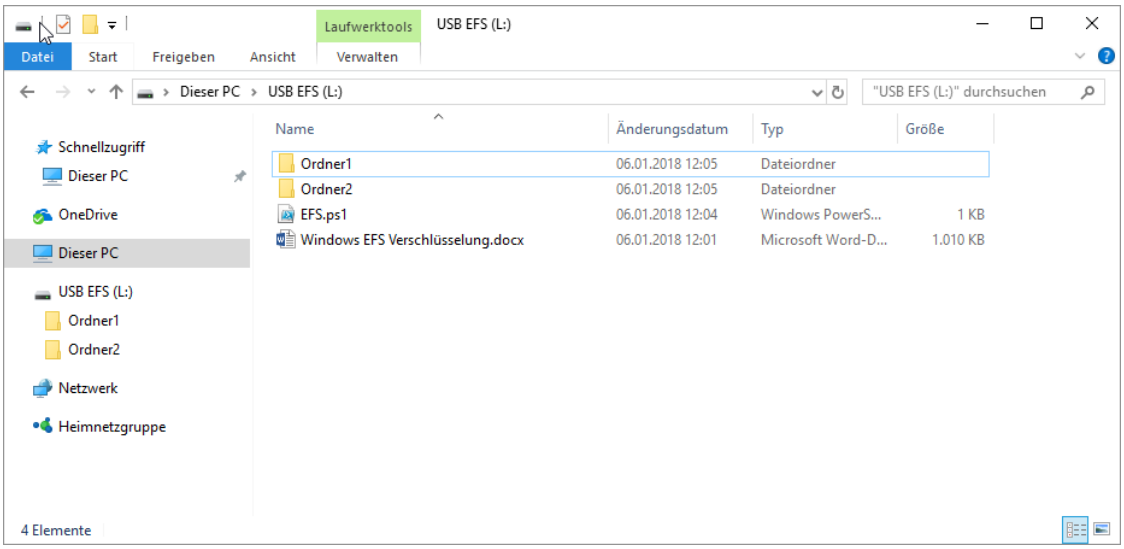
```
# Verschlüsseln einer Datei oder Dateien im Ordner
function Enable-FileEncryption
{
	[OutputType([void])]
	[CmdletBinding()]
	param
	(
		[Parameter(Mandatory,ValueFromPipeline)]
		[ValidateNotNullOrEmpty()]
		[System.IO.FileInfo]$File
	)
	begin {
		$ErrorActionPreference = 'Stop'
	}
	process {
		try
		{
			$File.Encrypt()
		}
		catch
		{
			$PSCmdlet.ThrowTerminatingError($_)
		}
	}
}
# Get-ChildItem -Path 'L:\Ordner1' | Enable-FileEncryption
Get-Item -Path 'L:\EFS.PS1' | Enable-FileEncryption
```




```
# Entschlüsseln
function Disable-FileEncryption
{
	[OutputType([void])]
	[CmdletBinding()]
	param
	(
		[Parameter(Mandatory, ValueFromPipeline)]
		[ValidateNotNullOrEmpty()]
		[System.IO.FileInfo]$File
	)
	begin {
		$ErrorActionPreference = 'Stop'
	}
	process {
		try
		{
			$File.Decrypt()
		}
		catch
```

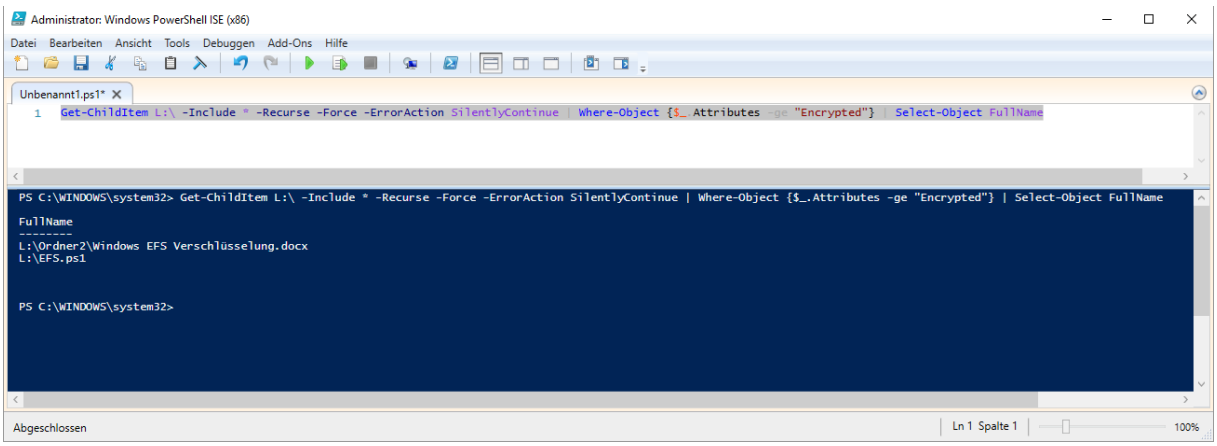
Windows EFS Verschlüsselung

```
                {
                        $PSCmdlet.ThrowTerminatingError($_)
                }
        }
}
# Get-ChildItem -Path 'L:\Ordner1' | Disable-FileEncryption
Get-Item -Path 'L:\EFS.PS1' | Disable-FileEncryption
```



Auf einem Laufwerk nach verschlüsselten Dateien suchen. Das geht mit der Powershell schnell und einfach. Dazu setzen wir diesen Befehl ab. Wir suchen nach Dateien mit dem Attribut **Encrypted**.

```
Get-ChildItem L:\ -Include * -Recurse -Force -ErrorAction SilentlyContinue | Where-Object {$_.Attributes -ge "Encrypted"} | Select-Object FullName
```



In Kurzversion:

```
GCI L:\ * -r -fo -ea silentlycontinue | ? {$_.attributes -ge "encrypted"} | select fullname
```

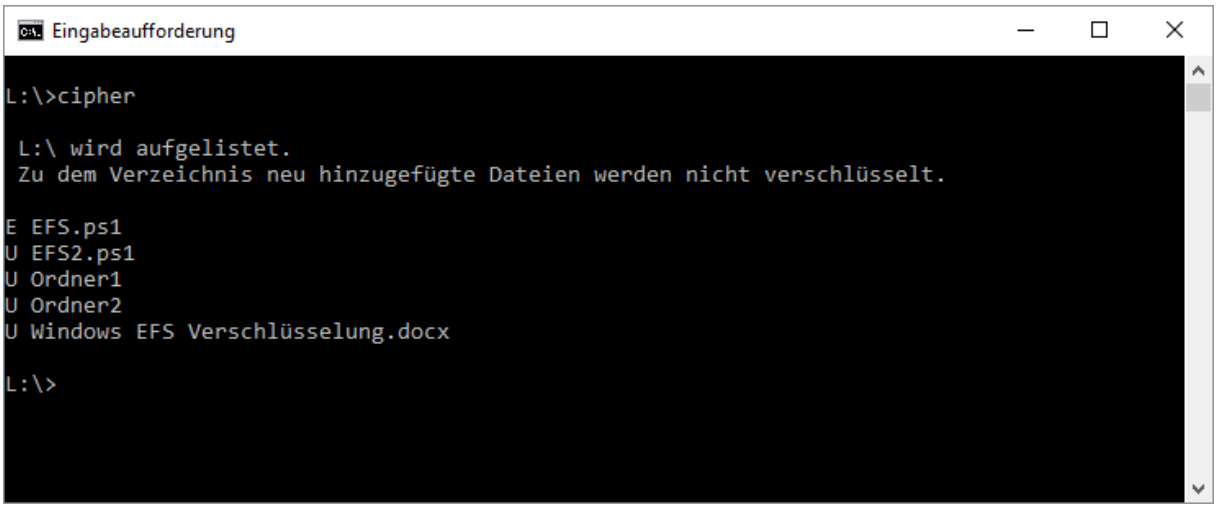
Normale Dateisuche rekursiv:

```
Get-ChildItem L:\ -Include EFS.ps1 -Recurse -Force -ErrorAction SilentlyContinue | Select-Object FullName
```

```
GCI L:\EFS.ps1 -r -fo -ea silentlycontinue | select fullname
```

Windows EFS Verschlüsselung

Nur mit dem Befehl Cipher können wir den Status abfragen:

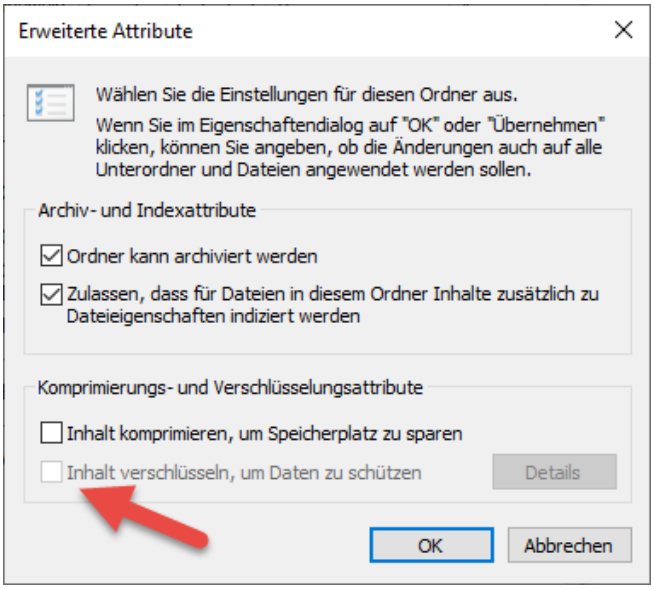


Optional:

EFS schaltet man auf die Weise komplett ab.

Windows Registry Editor Version 5.00

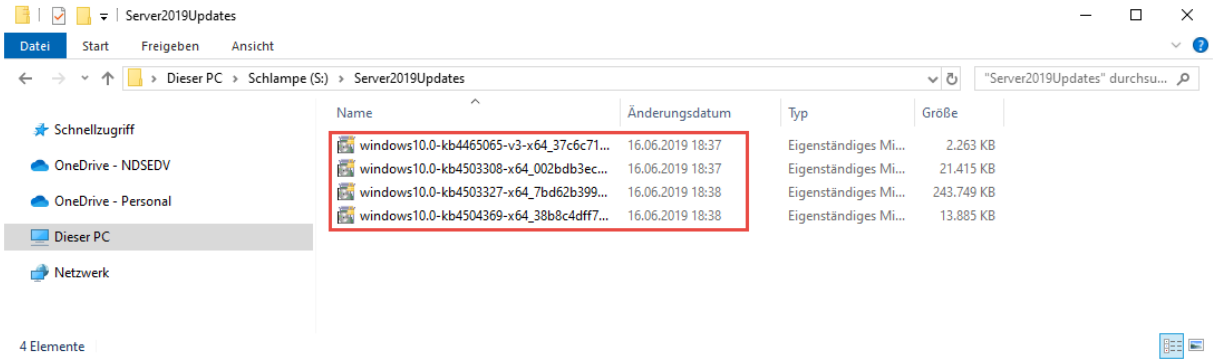
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies]
"NtfsDisableEncryption"=dword:00000001



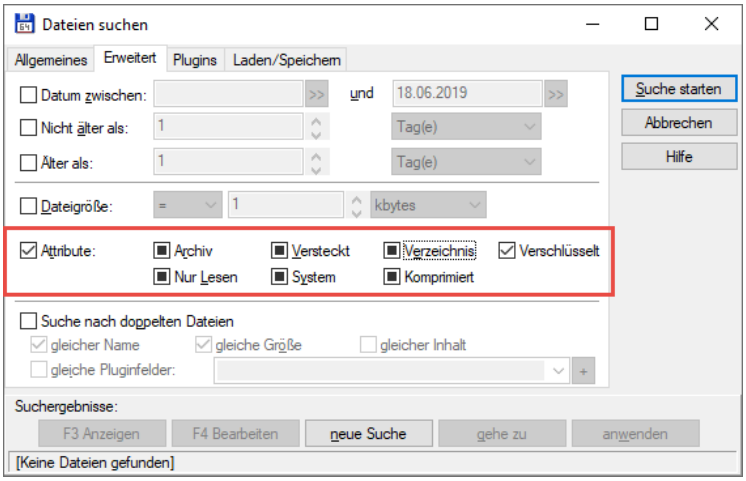
Windows EFS Verschlüsselung

Nur nach verschlüsselten Dateien suchen. Das geht sehr gut mit dem Total Commander.

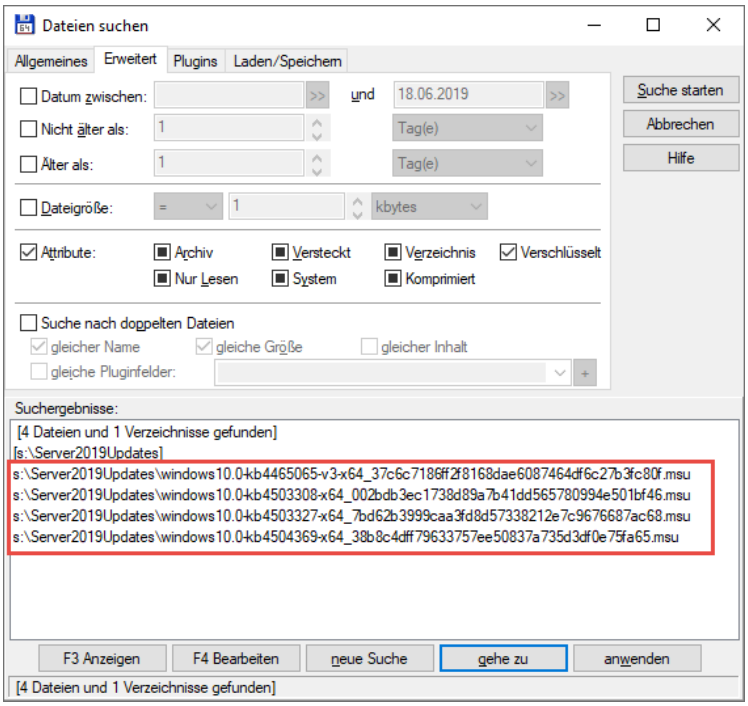
Das sind meine einzigen verschlüsselten Dateien unter dem Laufwerk S:\



Geben das Verzeichnis S:\ an und wechsle zum TAB > Erweitert. Dort markiere ich meine Optionen wie abgebildet.



Im Ergebnis sind das meine 4 Dateien.



Erstellt von Jörn Walter **06.01.2018 / 29.12.2019**