

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.

📕 kigenschaft	ten von EFS Vers	chlüsselung	×			
Allgemein Frei	igabe Sicherheit	Vorgängerversionen	Anpassen			
	EFS Verschlüsse	EFS Verschlüsselung				
Тур:	Dateiordner					
Ort:	C:\Users\Joem\	Desktop				
Größe:	36,7 KB (37.674	Bytes)				
Größe auf Datenträger:	40,0 KB (40.960 Bytes)					
Inhalt:	1 Dateien, 0 Ordner					
Erstellt:	Heute, 6. Januar 2018, Vor 2 Minuten					
Attribute:	Schreibgesch	ützt (betrifft nur Dateie	n im Ordner)			
	Versteckt	Erw	eitert			
	ОК	Abbrechen	Übernehmen			

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

Erweite	rte Attribute	×			
	Wählen Sie die Einstellungen für diesen Ordner aus. Wenn Sie im Eigenschaftendialog auf "OK" oder "Übernehmen" klicken, können Sie angeben, ob die Änderungen auch auf alle Unterordner und Dateien angewendet werden sollen.				
Archiv	- und Indexattribute				
Or	dner kann archiviert werden				
Zulassen, dass für Dateien in diesem Ordner Inhalte zusätzlich zu Dateieigenschaften indiziert werden					
Kompr	imierungs- und Verschlüsselungsattribute				
🗌 Ini	halt komprimieren, um Speicherplatz zu sparen				
Inhalt verschlüsseln, um Daten zu schützen Details					
	OK Abbrecher	n			



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.

📙   💦 📙 🗧   EFS Verschlüsselung	9					_		×
Datei Start Freigeben A	nsicht							~ 🕐
$\leftarrow \rightarrow \checkmark \uparrow $ 🕞 $\rightarrow$ EFS Verschlü	sselung		~	œ	FS Verso	chlüsselung"	durchs	P
🕹 Schnellzugriff	Name	Änderungsdatum	Тур	Größe				
Schneizugini	📄 Windows EFS Verschlüsselung.docx	06.01.2018 10:30	Microsoft Word-D	3	37 KB			
A OneDrive								
💻 Dieser PC								
💣 Netzwerk								
•� Heimnetzgruppe								
1 Element							E	==

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.

<ul> <li>Zertifikatexport-Assistent</li> </ul>	×
Willkommen	
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Zertifikatspeicher auf den Datenträger.	
Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.	
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.	
Weiter Abbrech	en

Die Einstellungen werden übernommen.

← 😺 Zertifikatexport-Assistent	×
Format der zu exportierenden Datei Zertifikate können in verschiedenen Dateiformaten exportiert werden.	
Wählen Sie das gewünschte Format:	
O DER-codiert-binär X.509 (.CER)	
Base-64-codiert X.509 (.CER)	
○ Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)	
Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen	
Privater Informationsaustausch - PKCS #12 (.PFX)	
🗹 Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen	
Privaten Schlüssel nach erfolgreichem Export löschen	
Alle erweiterten Eigenschaften exportieren	
Zertifikatdatenschutz aktivieren	
Microsoft Serieller Zertifikatspeicher (.SST)	
Weiter Abbrech	en



Vergeben ein starkes mindestens 12-stelliges Passwort.

÷ 🦆	Zertifikatexport-Assistent	
2	Sicherheit Zur Gewährleistung der Sicherheit müssen Sie den privaten Schlüssel mit e	inem
	Gruppen- oder Benutzernamen (empfohlen)	
	Hinzufügen	
	Entfernen	
	✓ Kennwort:	
	Kennwort bestätigen:	
	••••••	

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

	$\times$
← 뒏 Zertifikatexport-Assistent	
Zu exportierende Datei	
Geben Sie den Namen der zu exportierenden Datei an.	
	_
Dateiname:	
Weiter Abbrechen	



Ziel auswählen...

→ * ↑ → Dieser PC → VMWARE	E1 (G:)			5 ~	"VMWARE1 (G:)" durchsuchen	٩
ganisieren 👻 Neuer Ordner						?
<ul> <li>Schnellzugriff</li> <li>Dieser PC</li> <li>OneDrive</li> <li>Dieser PC</li> <li>Netzwerk</li> <li>Heimnetzgruppe</li> </ul>		Änderungsdatum	Тур	Größe		
Dateiname: EFS-KEY						`
Dateityp: Privater Informationsausta	ausch (*.pfx)					~

...mit > Weiter den Speicherort bestätigen.

		$\times$
~	Zertifikatexport-Assistent	
	Zu exportierende Datei Geben Sie den Namen der zu exportierenden Datei an.	
	Dateiname:	_
	G:\EFS-KEY.pfx Durchsuchen	
	Weiter Abbrechen	



Mit "Fertig stellen" schließen wir den Vorgang ab.

÷	Ş	Zertifikatexport-Assistent		×
		Fertigstellen des Assistenten		
		Der Zertifikatexport-Assistent wurde erfolgreich ab	geschlossen.	
		Sie haben folgende Einstellungen ausgewählt:		
		Dateiname	G:\EFS-KEY.pfx	
		Exportschlüssel	Ja	
		Alle Zertifikate im Zertifizierungspfad einbeziehen	Ja	
		Dateiformat	Privater Informationsaustausch (*.	
		<	>	
			Fertig stellen Abbrec	hen

Das Schlüsselpaar wurde erfolgreich exportiert.

Zertifikatexport-Assistent	×
Der Exportvorgang wurde erfolgreich abgeschlossen.	
ОК	



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

📕 📔 📑 🗧 🛛 EFS Verschlüsselung			- 🗆 X
Datei Start Freigeben Ansicht	📑 Eigenschaften von	Windows EFS Verschlüsselung.docx	× 🔹 🗸 🗸 🗸 🗸
← 🦂 → ↑ 📴 → EFS Verschlüsselung Nam	Allgemein Hashwerte	Sicherheit Details Vorgängerversionen	Benutzerzugriff auf Windows EFS Verschlüsselung.docx
🖈 Schnellzugriff	Window	vs EFS Verschlüsselung.docx	Benutzer mit Zugriff auf diese Datei:
🏂 OneDrive	Dateityp: Microso	ft Word-Dokument (.docx)	Benutzer Zertifikatfingerabdruck
📃 Dieser PC	Öffnen mit: 💽 Wo	ord 2016 Åndem	Joem(Joem@WORKER) 4950 4DF8 2548 6117 D848 F255 FD8F 9B
💣 Netzwerk	Ort: C:\User	s Envoitarte Attribute	
• <b>4</b> Heimnetzgruppe	Größe: 36,7 KB		
	Größe auf 40,0 KB Datenträger:	Wählen Sie die Einstellungen für dieser	
	Erstellt: Heute,	Dateiattribute	Hinzufügen Entfernen Schlüssel sichem
	Geändert: Heute,	Datei kann archiviert werden	
	Zugriff: Heute,	Dateieigenschaften indiziert werden	Wiederherstellungszertfikate dieser Datei gemäß Wiederherstellungsrichtlinie:
	Attribute: Schr	e Komprimierungs- und Verschlüsselungsattribut	vviedemerstellungszertifikat Zertifikatfingeraboruck
	Vers	Inhalt komprimieren, um Speicherplatz zu s	
			OK Abbrechen
		OK Abbrechen Übernehme	
1 Element 1 Element ausgewählt (36,7 KB)			

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

📙   🛃 🚽 =   EFS Verschlüsselur	ng				_		$\times$
Datei Start Freigeben	Ansicht						~ 🕐
← → ✓ ↑ 📑 → EFS Verschl	üsselung		~	ප "EFS V	erschlüsselung	" durchs	. , <b>р</b>
	ame ^	Änderungsdatum	Тур	Größe			
> 📌 Schnellzugriff	😼 EFS-KEY.pfx	06.01.2018 10:37	Privater Informati	3 K	В		
> 痜 OneDrive	TESTDATEI.txt	06.01.2018 10:42	Textdokument	0 K	В		
> 💻 Dieser PC	📄 Windows EFS Verschlüsselung.docx	06.01.2018 10:42	Microsoft Word-D	431 K	В		
> 🎒 Netzwerk							
> 🔩 Heimnetzgruppe							
							_
3 Elemente							:== 🖿



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.

🚪 Konsole1 - [Konsolenstamm\Zertifikate - Aktueller Benu	tzer\Eigene Zertifikate\Zertif	fikate]					-		×
Datei Aktion Ansicht Favoriten Fenster ?			🔲 Zertifi	kat	×			- é	F X
			Allgemein	Details Zertifizierungspfad					
<ul> <li>Konsolenstamm</li> <li>Eigene Zertifikate</li> <li>Eigene Zertifikate</li> <li>Vertrauenswürdige Stammzertifizierungsstellen</li> <li>Organisationsvertrauen</li> <li>Zvischenzerfifizierungsstellen</li> <li>Active Directory-Benutzerobjekt</li> <li>Vertrauenswürdige Herausgeber</li> <li>Nicht vertrauenswürdige Personen</li> <li>Drittanbieter-Stammzertifizierungsstellen</li> <li>Andere Personen</li> <li>Zertifikate gistrierungsanforderungen</li> <li>Santarda vertrauenswürdige Stämme</li> <li>Zertifikate (Lokaler Computer)</li> </ul>	Ausgestellt für	Ausgestellt von Joern c	Aligemein Diese	Details       Zertifizierungspfad         Zertifizierungspfad         zertifizierungspfad         eszertifikat ist für folgende Zwecke beabsichtigt:         • Emsäglicht de Verschlüsselung der Daten auf dem Datenväger         • Alle ausgegebenen Richtlinien         Ausgestellt für:       Joern         Ausgestellt von:       Joern         Gültig ab       06.01.2018       bis         Sie besitzen einen privaten Schlüssel für dieses Zertifikat.		nzeigename Keine> Keine> Keine>	Statu	Aktionen Zertifikate Weite Joern Weite	
	<	_		ОК			>		
Der Speicher enthält "Eigene Zertifikate" 3 Zertifikate.									

gemen	- Cer under ungopr		
zeigen:	<alle></alle>	$\checkmark$	
Feld		Wert	^
📋 Antrags	teller	Joern	
Öffentli	cher Schlüssel	RSA (2048 Bits)	
Parame	ter für öffentlichen	05 00	
Erweiter	rte Schlüsselverwen	Verschlüsselndes Dateisystem	
🗊 Alternat	iver Antragstellerna	Anderer Name:Prinzipalname=	
Basisein	schränkungen	Typ des Antragstellers=Endei	
Fingeral	odruck	49504df825486117d848f255f	
Frweiter	te Fehlerinformatio	Peer-Vertrauen	
		To Datai Justiana	

Erstellt von Jörn Walter



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.

Microsoft	t Word	
!	Das Dokument kann von Word nicht geöffnet werden: Der Benutzer besitzt keine Zugriffsrechte. (C:\\Windows EFS Verschlüsselung.docx) Hilfe anzeigen >>	
	ОК	

Auch der Versuch die TESTDATEI.TXT zu öffnen scheitert.

Unk 🥼	benannt - Editor	r			_	$\times$
Datei	Bearbeiten Fo	ormat Ansi	cht ?			
						^
		Editor		×		
			C:\Users\Joern\Desktop\EFS Verschlüsselung\TESTDATEI.txt Sie haben keine Berechtigung zum Öffnen dieser Datei. Wenden Sie sich an den Besitzer der Datei oder an den Systemadministrator.			
			ОК			
						~

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.

<ul> <li>Konsolel - [Konsolenstamm\Zertifikate - Aktueller Benutze</li> <li>Datei Aktion Ansicht Favoriten Fenster ?</li> <li>Total Aktion Ansicht Favoriten Fenster ?</li> <li>Konsolenstamm</li> <li>Zertifikate - Aktueller Benutzer</li> <li>Eigene Zertifikate</li> <li>Vetrauenswürdige Stammzertifizierungsstellen</li> <li>Zotsich zertifikate</li> <li>Vetrauenswürdige Herausgeber</li> <li>Nith vetrauenswürdige Personen</li> <li>Zithi vetrauenswürdige Personen</li> <li>Zettifikate Personen</li> <li>Zettifikate (Lokaler Computer)</li> <li>Zettifikate (Lokaler Computer)</li> </ul>		X ske Anzz ung, Sich <kei< th=""><th>eigename Statu Akti ine&gt; Zerti</th><th>] × _ ₽ × onen fikate ▲ Weite ►</th></kei<>	eigename Statu Akti ine> Zerti	] × _ ₽ × onen fikate ▲ Weite ►
<ul> <li>&gt; ☐ Extended galacteringaniteringaniteringen</li> <li>&gt; ☐ Stamme</li> <li>&gt; ☐ Zertifikate (Lokaler Computer)</li> </ul>	Ghlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern Dzw. überführen.       Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht excortierbar)       ✓ Alle erweiterten Eigenschaften mit einbeziehen       Weiter     Abbrechen		>	



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

📑 📔 🔄 🔻 🕴 EFS Verschlüsselung	<u></u>	Windows EFS Verschlüsselung.docx - Word 📼 —	
Datei Start Freigeben Ansicht			
← → ✓ ↑ ►> EFS Verschlüsselung	Datei Start Einfü	en Entwurf Layout Verweise Sendungen Überprüfen Ansicht Entwicklertools Office Tab ♀ Sie wüns⊲ Jörn Walter	A Freigeben
Name	e Kerdana	・10 ・A A A A A A A A A A A A A A A A A A A	Suchen ×
📌 Schnellzugriff	Einfügen F K	🗓 🗸 əbəc 🗙 🗴 🕺 🖌 📲 🛫 📥 🗧 🧮 🖅 🖉 🖉 🐨 🔛 🛪 🕺 T Standard 🛛 Kein Lee Überschrif 🤤 🦷	Madiana
🛄 Dieser PC 🛛 🖈 📑	FS-KEY - V		Warkieren *
	ESTDA Zwischena 🕞	Schriftart 12 Absatz 12 Formatvorlagen 12	Bearbeiten 🔺
AneDrive 🔤 V	Vindov 💼 Windows EFS Versch	üsselung.docx ×	<u> </u>
Dieser PC			<b>▲</b>
Netzwerk			
• Heimnetzgruppe			
3.11			
		Windows EFS Verschlüsselung	
		Inter Windows können wir Daten mittels des EES (Encrynting Eile 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	
		verschlusselung.	
		Mit einem Rechtsklick auf den Ordner öffne ich die Eigenschaften. Über den Reiter	
		Allgemein > Erweitert öffnen wir die Ansicht der erweiterten Attribute.	
3 Elemente 1 Element ausgewählt (635 KB)	Seite 1 von 8 356 Wört	r 🕼 🖩 🖪 🗟	+     100 % 📲

## **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:

<mark>cipher /A /E Dateiname</mark>

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:

#### <mark>cipher /D Dateiname</mark>

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

Erstellt von Jörn Walter



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:

🔫   🗹 🛄 =	Laufwerktools USB EFS (L:)		– 🗆 X
Datei Start Freigeben	Ansicht Verwalten		~ 😮
$\leftarrow$ $\rightarrow$ $\checkmark$ $\Uparrow$ $\blacksquare$ $\rightarrow$ USB EFS (L:	) >	✓ ひ "USB EFS (L:	)" durchsuchen 🔎
📌 Schnellzugriff	Name	Änderungsdatum	Тур Gi
💻 Dieser PC 🛛 🖈	Ordner1	06.01.2018 12:31	Dateiordner
	Ordner2	06.01.2018 12:31	Dateiordner
heDrive 🌀	🙀 EFS.ps1	06.01.2018 12:04	Windows PowerS
Dieser BC	🙀 EFS2.ps1	06.01.2018 12:04	Windows PowerS
Jeser PC	🖬 Windows EFS Verschlüsselung.docx	06.01.2018 12:01	Microsoft Word-D
USB EFS (L:)			
Ordner1			
Ordner2			
💣 Netzwerk			
• <b>4</b> Heimnetzgruppe			
	<		>
5 Elemente			



2) Das Zertifikat wurde angelegt:

🚟 Konsole1 - [Konsolenstamm\Zertifikate - Aktueller Ber	nutze	r\Eigene Zertifikate\Zerti	fikate]			-	
a Datei Aktion Ansicht Favoriten Fenster ?							- 8 ×
🗢 🔶 📶 🦨 🖬 🗙 🖾 🗟 🖬							
Konsolenstamm	۱ A	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Anzeigename	Aktionen
V 🙀 Zertifikate - Aktueller Benutzer	1	Joern 🙆	Joern	13.12.2117	Verschlüsselndes Dateisystem	<keine></keine>	Zertifikate 🔺
Zertifikate	0			_			Weite 🕨
> C Vertrauenswürdige Stammzertifizierungsstelle							Joern 🔺
Organisationsvertrauen     Twicchenzertifizierungsstellen							Weite 🕨
Active Directory-Benutzerobiekt							
> Vertrauenswürdige Herausgeber							
> 📔 Nicht vertrauenswürdige Zertifikate							
> 🧮 Drittanbieter-Stammzertifizierungsstellen							
> iii Vertrauenswürdige Personen							
> Clientauthentifizierungsaussteller							
> 🦰 Andere Personen							
> Zertifikatregistrierungsanforderungen							
> Smartcard vertrauenswürdige Stämme	-    -						
< >	<					>	
Der Speicher enthält "Eigene Zertifikate" 3 Zertifikate.							

#### 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



## **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

- [; · · · ·	Laufwerktools USB EFS (L:)		-	n x
Datei Start Freigeben	Ansicht Verwalten			~ ?
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow$ Dieser PC	> USB EFS (L:)		✓ ひ "USB EFS (L:)" durchsuch	en 🔎
★ Schnellzugriff Dieser PC	Name	Änderungsdatum 06.01.2018 12:05	Typ Größe Dateiordner	
S OneDrive	<ul> <li>Grane 2</li> <li>EFS.ps1</li> <li>Windows EFS Verschlüsselung.docx</li> </ul>	06.01.2018 12:03 06.01.2018 12:04 06.01.2018 12:01	Windows PowerS 1 KB Microsoft Word-D 1.010 KB	
USB EFS (L:) Ordner1 Ordner2				
💣 Netzwerk				
4 Elemente				

# # Entschlüsseln

{

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



{ } } # Get-ChildItem - Get-Item -Path 'L	<pre>\$PSCmdlet.ThrowTerm Path 'L:\Ordner1'   D' :\EFS.PS1'   Disable-I</pre>	iinatingError( isable-FileEn FileEncryptio	(\$_) cryption n		
	Laufwerktools USB EFS (L:)			- 0	×
Datei Start Freigeben	Ansicht Verwalten				~ 🕐
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare$ > Dieser PC	> USB EFS (L:)		U" ٽ	SB EFS (L:)" durchsuchen	Q
	Name	Änderungsdatum	Тур	Größe	
Schnellzugriff	Ordner1	06.01.2018 12:05	Dateiordner		
Dieser PC 🖈	Grdner2	06.01.2018 12:05	Dateiordner		
즑 OneDrive	EFS.ps1	06.01.2018 12:04	Windows PowerS	1 KB	
💻 Dieser PC	Windows EFS Verschlüsselung.docx	06.01.2018 12:01	Microsoft Word-D	1.010 KB	
USB EFS (L:)					
Ordner1					
Ordner?					
orancie					
💣 Netzwerk					
•4 Heimnetzgruppe					
4 Elemente					

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

Administrator: Windows PowerShell ISE (x86)		×
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe		
Unbenannt1.ps1* X		
1 Get-ChildItem L:\ -Include * -Recurse -Force -ErrorAction SilentlyContinue   Where-Object {\$ Attributes -ge "Encrypted"}   Select-Object FullName		$\sim$
		>
PS C:\wINDOWS\system32> Get-ChildItem L:\ -Include * -Recurse -Force -ErrorAction SilentlyContinue   Where-Object {\$Attributes -ge "Encrypted"}   Select-Object F	ullName	^
FullName		
L:\ordner2\Windows EFS Verschlüsselung.docx		
L:\EFS.ps1		
PS C:\WINDOWS\system32>		
		~
		>
Abgeschlossen   Ln 1 Spatte 1		100%

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



Nur mit dem Befehl Cipher können wir den Status abfragen:

Eingabeaufforderung	_	×
L:\>cipher		^
L:\ wird aufgelistet. Zu dem Verzeichnis neu hinzugefügte Dateien werden nicht verschlüsselt.		
E EFS.ps1 U EFS2.ps1 U Ordner1 U Ordner2 U Windows EFS Verschlüsselung.docx		
L:\>		
		$\sim$

## **Optional:**

EFS schaltet man auf die Weise komplett ab.

Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Policies] "NtfsDisableEncryption"=dword:0000001

Erweiterte Attribute	×							
Wählen Sie die Einstellungen für diesen Ordner aus. Wenn Sie im Eigenschaftendialog auf "OK" oder "Übernehmen" klicken, können Sie angeben, ob die Änderungen auch auf alle Unterordner und Dateien angewendet werden sollen.								
Archiv- und Indexattribute								
Ordner kann archiviert werden								
Zulassen, dass für Dateien in diesem Ordner Inhalte zusätzlich zu Dateieigenschaften indiziert werden								
Komprimierungs- und Verschlüsselungsattribute								
Inhalt komprimieren, um Speicherplatz zu sparen								
Inhalt verschlüsseln, um Daten zu schützen Details								
OK Abbreche	n							



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

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

📑   🔄 📙 🖛   Server2019Updates					-		×
Datei Start Freigeben Ansicht							~ 🕐
← → ~ ↑ 📙 → Dieser PC → Schlampe (	S:) > Server2019Updates			∨ Ö ~	erver2019Updates" o	lurchsu	. ,o
3 o L H W	Name	Änderungsdatum	Тур	Größe			
✤ Schnellzugriff ● OneDrive - NDSEDV	im windows10.0-kb4465065-v3-x64_37c6c71	16.06.2019 18:37	Eigenständiges Mi	2.263 KB			
OneDrive - NDSEDV	📷 windows10.0-kb4503308-x64_002bdb3ec	16.06.2019 18:37	Eigenständiges Mi	21.415 KB			
OneDrive - Personal	📷 windows10.0-kb4503327-x64_7bd62b399	16.06.2019 18:38	Eigenständiges Mi	243.749 KB			
	is windows10.0-kb4504369-x64_38b8c4dff7	16.06.2019 18:38	Eigenständiges Mi	13.885 KB			
🔜 Dieser PC							
💣 Netzwerk							
4 Elemente							1335 <b>B</b>

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

🔡 Dateien suchen								_		×
Allgemeines Erweiter	t Plugins	Laden/Spe	ichem							
Datum <u>z</u> wischen:			>>	und	18. <mark>06</mark> .	2019		>>	Suche	starten
Nicht <u>ä</u> lter als:	1		0		Tag(e)		$\sim$		Abbre	chen
Alter als:	1		$\hat{\mathbf{x}}$		Tag(e)	)	$\sim$		Hil	fe
Dateigröße:	= ~	1		0 kł	ytes	$\sim$				
Attribute: Archiv IIVersteckt IVerzeichnis Verschlüsselt IINur Lesen IIISystem IIKomprimiert										
Suche nach dogpelten Dateien         ✓ gleicher Name       ✓ gleiche Größe         gleicher Pluginfelder:       ✓ +										
Suchergebnisse:						_				
F3 Anzeigen F4 Bearbeiten neue Suche gehe zu anwenden										
Keine Dateien gefund	ienj									

Im Ergebnis sind das meine 4 Dateien.

🔛 Dateien s	uchen									_	П	×
an Dutcien s		-										~
Allgemeines	Erweitert	Plugins	Laden/Spe	eichem	1							
Datum <u>z</u> wis	schen:			>>	und	18.06.2	019		>>		Suche	starten
Nicht <u>ä</u> lter	als: 1			$\hat{\mathbf{C}}$		Tag(e)		~			Abbre	chen
Älter als:	1			$\odot$		Tag(e)		$\sim$			Hi	fe
Dateigröße	: =	- v	1		0 kl	oytes	$\sim$					
Attribute:		Archiv		erstec	kt	V <u>e</u> rzei	chnis	<mark>∕ V</mark> e	rschlü	sselt		
		Nur <u>L</u> es	en 🔳 S	ystem		Kompr	imiert					
Suche nac	<b>h doppel</b> Name	ten Dateie	<b>n</b> leiche Gr <u>ö</u> ße	;		jleicher In	halt					
	e:	ar.								+		
[4 Dateien und	1 Verzei	chnisse ge	funden]									
[s:\Server2019	Updates]											_
s:\Server2019l s:\Server2019l	Jpdates\v	windows1	0.0-kb44650 0.0-kb45033	65-v3- 08-v6/	-x64_37 4 002br	c6c7186	f2f8168 8d89a0	Bdae60	37464d 56578(	ff6c27	7b3fc80f.ms 501bf46.ms	9U 81
s:\Server2019	Jpdates\	windows1	0.0-kb45033	27-x64	4_7bd62	2b3999ca	a3fd8d	573382	12e7c	96766	687ac68.ms	su
s:\Server2019l	Jpdates∖≀	windows1	0.0-kb45043	69-x64	4_38b8d	:4dff 7963	3757ee	e50837a	a735d3	3df0e7	75fa65.msu	
F3 Anz	eigen	F4 Be	earbeiten	n	eue Su	che	ge	ehe zu		a	in <u>w</u> enden	
[4 Dateien und	1 Verzei	chnisse ge	funden]									