



## **Konfiguration von EFS über Registry Keys sowie weiteren mitgelieferten Tools**

## INHALT

Festlegung des Verschlüsselungsalgorithmus.....	3
Verschlüsselungsoption im Kontextmenü aktivieren.....	4
EFS deaktivieren .....	5
Support Tools.....	6
EFSinfo .....	6
Cipher .....	7
EFS Zertifikat manuell ändern.....	8
Backup des EFS - Zertifikates.....	8
Linktipps .....	9

## FESTLEGUNG DES VERSCHLÜSSELUNGALGORITHMUS

Da ab XP SP1 der AES 256 Algorithmus verwendet wird, muss, um Abwärtskompatibilität zwischen den verschiedenen Windows-Versionen zu gewährleisten, eine Adaptierung der Registry durchgeführt werden. Vor einer Änderung des Standard-Algorithmus sollten alle bereits verschlüsselten Dateien entschlüsselt werden.

Lokalisieren Sie im Registry Editor (regedit) den Schlüssel

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\EFS**

Erstellen Sie einen neuen DWORD Eintrag mit dem Namen AlgorithmID (New / DWORD value) und setzen diesen auf den entsprechenden Hexadezimalwert.

3DES	0x6603
DESX	0x6604
AES-256	0x6610

Danach ist ein Restart des Systems notwendig.

## VERSCHLÜSSELUNGSOPTION IM KONTEXTMENÜ AKTIVIEREN

Um im Kontextmenü, etwa im Windows-Explorer, die Option Verschlüsseln oder Entschlüsseln angeboten zu bekommen, ist eine Adaptierung der Registry notwendig.

Lokalisieren Sie im Registry Editor (regedit) den Schlüssel

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Explorer\Advanced**

Erstellen Sie einen neuen DWORD Eintrag mit dem Namen **EncryptionContextMenu** (New / DWORD value) und setzen diesen auf den Wert 1.

## EFS DEAKTIVIEREN

Da EFS normalerweise aktiviert ist, steht diese Option auch jedem zur Verfügung. Eine Deaktivierung von EFS kann über eine Gruppenrichtlinie oder über einen Registry Eintrag vorgenommen werden.

Lokalisieren Sie im Registry Editor (regedit) den Schlüssel

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\EFS**

Erstellen Sie einen neuen DWORD Eintrag mit dem Namen **EfsConfiguration** (New / DWORD value) und setzen diesen auf den Wert 1.

In einer Domäne lässt sich EFS über eine Gruppenrichtlinie deaktivieren. Eigenschaften von ..Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien öffentlicher Schlüssel\Verschlüsselndes Dateisystem kann die Verwendung von EFS ausgeschlossen werden.

## SUPPORT TOOLS

Als mitgelieferte Tools sind das Kommandozeilenprogramm Cipher und das Supporttool EFSinfo zu nennen

### EFSINFO

Mit EFSinfo lassen sich zu einer verschlüsselten Datei einige Informationen finden.

<code>/u</code>	Zeigt Benutzerinformationen an.
<code>/r</code>	Zeigt Recovery Agent Information an.
<code>/c</code>	Zeigt den Hash-Wert (Thumbprint) des verwendeten Zertifikates an
<code>/i</code>	Erzwingt die Durchführung des Befehls bei Fehlermeldungen
<code>/k</code>	Zeigt Schlüsselinformationen an
<code>/y</code>	Zeigt die Hash-Wert (Thumbprint) des aktuellen EFS Zertifikates am Rechner an.
<code>/?</code>	Zeigt die Hilfe an

## CIPHER

Cipher ist ein Kommandozeilentool, mit dem einige Operationen im Zusammenhang mit EFS durchgeführt werden können.

Einige gängige Parameter, mit der Cipher verwendet werden kann:

/?	zeigt eine komplette Liste aller möglichen Parameter an.
/e	verschlüsselt das angegebene Verzeichnis
/d	entschlüsselt das angegebene Verzeichnis
/s:verzeichnis	führt das Kommando unter Verzeichnis und dessen Unterordner aus, jedoch ohne Dateien zu verändern
/a	führt das Kommando an angegebene Dateien und Dateien in angegebenen Verzeichnissen aus
/k	erstellt einen neues EFS-Schlüsselpaar und EFS-Zertifikat für den aktuellen Nutzer
/r	erstellt einen Recovery Agent Schlüssel und ein dementsprechendes Zertifikat; beide werden in eine PFX-Datei gespeichert, während das Zertifikat alleine in eine CER-Datei kommt
/u	erneuert die EFS-Verschlüsselung des Nutzers oder des Wiederherstellungsagenten (Recovery Agent) an jeder Datei mit dem aktuellen Zertifikat; sinnvoll nach Cipher /K – oder manueller Änderung des EFS-Zertifikats.
/u /n	zeigt jede verschlüsselte Datei auf lokalen Platten an, ohne Änderungen vorzunehmen. Die Ausführung von /u kann eine längere Zeit beanspruchen.
/w	ist eine „Wipe Funktion – damit werden nicht belegte Datenbereiche permanent überschrieben – sinnvoll ist diese Funktion vor allem, da bei einer EFS Verschlüsselung eigentlich eine neue Datei erzeugt wird und die Klartextdatei bloß gelöscht wird.

### ACHTUNG:

Cipher /k enrolled eine neues EFS-Zertifikat und wenn im Certificate Store ein Zertifikat dieses Users mit Schlüsselverwendung EFS schon vorhanden ist, wird dieses aus dem Certificate Store ohne Rückfrage entfernt!

Dieses Zertifikat muss aus dem hoffentlich existierenden Backup wieder importiert werden.

## EFS ZERTIFIKAT MANUELL ÄNDERN

Um das für EFS zu verwendende Zertifikat zu ändern, muss der Hash-Wert des Zertifikates in der Registry geändert werden. Der SHA-1 Hash-Wert ist als Thumbprint Wert im „Certificate Viewer“ ersichtlich.

Lokalisieren Sie im Registry Editor (regedit) den Schlüssel

`HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\EFS\CurrentKeys`

Ändern Sie neuen BINARY Eintrag mit dem Namen `CertificateHash` auf den entsprechenden Hash-Wert des neu zu verwendenden Zertifikates.

## BACKUP DES EFS - ZERTIFIKATES

Sinnvoll erscheint es, das EFS-Zertifikat aus dem Windows-Zertifikatsspeicher zu (inklusive privatem Schlüssel) zu exportieren und sicher zu hinterlegen. Neben dem schon erwähnten Problem bei „cipher /k“ kann auch der Verlust des Windows-Passwortes schwerwiegende Folgen haben.

Alle Private Keys zu Zertifikaten im Certificate Store, und noch einiges mehr, liegen verschlüsselt vor. Die Verschlüsselung erfolgt mit einem Master-Key, der auch regelmäßig (60 Tage) im Hintergrund geändert wird. Der Master-Key ist seinerseits verschlüsselt mit einem vom Benutzer – Passwort abgeleiteten Schlüssel.

Bei Änderungen des Passwortes durch den Benutzer wird der Master-Key umgeschlüsselt. Wird das Passwort von einem Administrator zurückgesetzt, geschieht dies NICHT, und nach einer Anmeldung mit dem neuen Passwort kann auf keine privaten Schlüssel etc. zugegriffen werden. Microsoft sieht dies als Schutz vor böswilligen Administratoren. Setzt der Benutzer das Passwort gleich wieder auf sein ursprüngliches zurück, ist für ihn der Zugriff wieder möglich. Problematisch ist dies, wenn die Rücksetzung notwendig war, weil der Benutzer sein Passwort vergessen hat.

Eine Passwort Reset Disk könnte helfen, allerdings nicht, wenn der Rechner einer Domäne angehört, denn ein Backup von Domänen-Passwörter kann nicht mit einer Passwort Reset Disk geschehen.

Der Einsatz von EFS ist unbedingt notwendig Recovery Agents zu verwenden und um den Aufwand bei Passwortrücksetzungen nicht zu vervielfachen, ist zusätzlich der Einsatz eines **Smart Card Logon** empfehlenswert. Dort hängt der Schutz des Master-Keys nicht am Passwort. Das EFS-Zertifikat kann aber nicht auf eine Smart Card installiert werden.

## LINKTIPPS

EFS in Windows Server2003 – How To

<http://support.microsoft.com/default.aspx?scid=kb;en-us;324897>

Bestimmung des EFS - Verschlüsselungsalgorithmus

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B329741>

[http://www.microsoft.com/technet/prodtechnol/winxpro/reskit/prnb\\_efs\\_cbhn.asp](http://www.microsoft.com/technet/prodtechnol/winxpro/reskit/prnb_efs_cbhn.asp)

Verschlüsseln / Entschlüsseln im Kontext-Menü

<http://support.microsoft.com/default.aspx?scid=kb;en-us;241121>

<http://www.microsoft.com/WindowsXP/expertzone/tips/july02/keam.asp>

Third Party CA für EFS

<http://support.microsoft.com/default.aspx?scid=kb;en-us;273856>

Schlüsselverschlüssler – Sicherheit des Master Keys

<http://www.kes.info/aktuell/akheft/artikel1.htm>

Cipher

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/cipher.asp>

### ANMERKUNG:

unter FEK wird dort und bei der Hilfe zum Cipher-Befehl nicht der symmetrische Schlüssel verstanden, sondern das komplette EFS-Schlüsselpaar

CRYPTAS it-Security & Media GmbH  
Modecenterstrasse 22/B2  
A-1030 Wien, Austria  
T +43 (1) 798 96 96 – 0  
F +43 (1) 798 96 96 – 99  
info@cryptas.com

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)  
[www.cryptasmedia.com](http://www.cryptasmedia.com)