# Datenverschlüsselung

*mit Microsoft Bitlocker Drive Encryption (BDE) und TrueCrypt*

***Thomas Reinwart***

## Microsoft Bitlocker

Seit Windows Vista bietet Microsoft mit Bitlocker eine Verschlüsselung der Festplatte (HDD/SSD) in seinem Betriebssystem an. Auch in den Folgeprodukten Windows 7, Windows Server und auch in Windows 8 gibt es natürlich weiterhin diese Möglichkeit. Allerdings war der Bitlocker in alten Windows Versionen erst ab der Enterprise und Ultimate Editionen enthalten, die Home Editions waren ausgenommen.

Daten auf Windows RT-PCs werden mit einer Geräteverschlüsselung geschützt, die auf BitLocker-Technologie basiert. Daten auf Windows 8-PCs und auf Wechseldatenträgern werden mit BitLocker und BitLocker To Go geschützt.

### Wie funktioniert das?

Es handelt sich dabei um eine Verschlüsslung einer HDD/SSD, genauer gesagt einer Partition, die Daten sind ohne das Wissen des Zugangsschlüssels unbrauchbar. Bitlocker kann logische Partitionen verschlüsseln. Somit lassen sich auch Partitionen, die aus mehreren Festplatten bestehen, verschlüsseln. Die Verschlüsselung selber basiert auf 128 Bit AES. Prozessoren haben eine AES Hardwarebeschleunigung integriert damit dies von der Geschwindigkeit her nicht merkliche Auswirkung hat.

### Warum sollte man das nutzen?

Bei Verlust des Rechners sind die Daten also geschützt, es gibt einzig den materiellen Verlust des Gerätes, nicht aber den heiklen Verlust sensibler Daten.

Nicht nur der Verlust, auch die Herausgabe eines Computers stellt ein Datenproblem dar: Im Falle einer noch bestehenden Garantie eines Computers darf dieser nicht geöffnet werden um die Festplatte zu entnehmen / tauschen und seine Daten nicht in fremde Hände zu geben. Alternativ kann man nun alles von Rechner löschen (und dabei nichts vergessen) und nach der Reparatur (falls ich denselben Rechner mit denselben unveränderten Daten wieder erhalten sollte) wird alles zurücksichern bzw. neu installieren – oder eben die Daten verschlüsseln und das Passwort / Recovery Key nicht hergeben.

### Authentifizierungsmöglichkeiten

Bitlocker unterstützt ein Trusted Platform Modul (TPM), TPM mit PIN, eine Schlüsseldatei (Passkey) auf einem USB-Stick, TPM mit USB-Stick und eine Kombination aus TPM, PIN und Passkey.

Um Zugang zu den Daten zu erhalten, gibt es mehrere Möglichkeiten, die Authentifizierung beim Bootvorgang bekannt zu geben. Im Falle des Verlust es Zugangscodes gibt es auch einen Recovery Key, den man sicher aufbewahrt.

Zwar bietet das NTFS Filesystem auch eine Verschlüsselung von einzelnen Ordnern an, diese sind dann mit der SID eines Users verbunden, es handelt sich um primitive Kryptisierung einzelner Bereiche eines Mediums im Gegensatz zu einer kompletten Verschlüsselung des Mediums.

### Mehrere Festplatten in Verwendung (intern oder extern)

Bitlocker unterstützt mehrere Festplatten gleichzeitig, also Boot/System als auch Daten Festplatten. Sind mehre interne HDDs verschlüsselt, bietet Bitlocker eine AutoUnlock Funktion an, damit muss nach Eingabe es ersten Passworts der ersten HDD nicht alle weiteren Schlüssel bekanntgegeben werden. Das funktioniert deshalb, da bei AutoUnlock die weiteren Keys auf der ersten Platte gespeichert werden.

### Partition zusätzlich extern sichern – ist das möglich?

Bei einer Datensicherung werden die Daten unverschlüsselt auf ein Zielmedium übertragen. Wird das Zielmedium ebenfalls verschlüsselt, dann ist das Backup auch geschützt.

Bei einer Sicherung der Partition mit Acronis (Version 2013 für Windows 8) und dem Zurücksichern der Partition sind die Daten anschließend unverschlüsselt. Hier muss Bitlocker wieder aktiviert werden. Hat der Rechner mehrere HDDs mit Bitlocker in Verwendung, funktioniert nach dem Restore der ersten Partition auch die AutoUnlock Möglichkeit der zweiten Festplatte nicht mehr, das der Key ursprünglich auf der ersten (boot) HDD hinterlegt war. Somit muss der Key neu bekanntgegeben werden.

Wiederherstellung des Keys für die AutoUnlock Funktion auf CMD Ebene:

***Liste der Laufwerke mit Bitlocker Zuordnung***

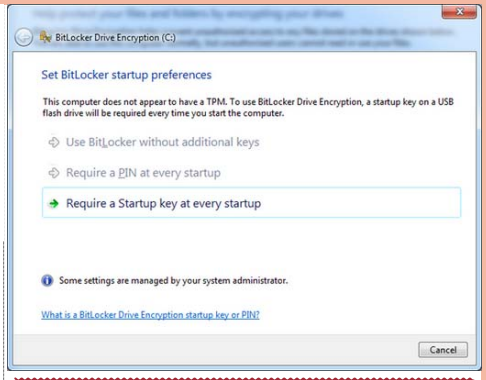
*manage-bde –status*

***Wenn in der Ausgabe erscheint: Data Error CRC Check***

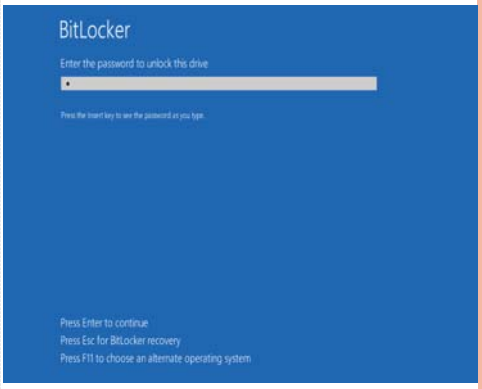
*manage-bde –autounlock –clearallkeys C:*

*manage-bde –autounlock –enable D:*

Nach bzw. beim Reboot des Systems wird der Key auf C: neu erstellt und AutoUnlock funktioniert wieder.

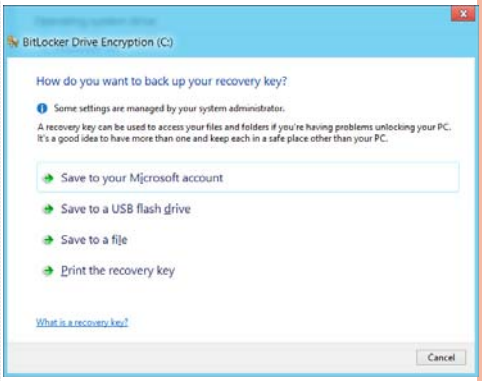



Einrichtung von Bitlocker

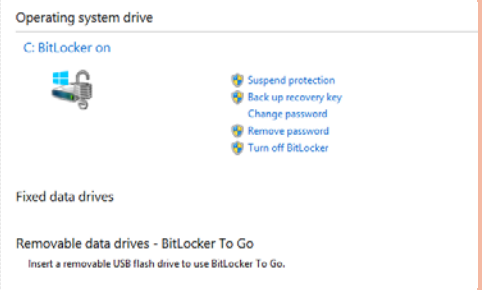



Eingabe des Bitlocker Passwords beim Bootvorgang bzw. der Recovery Möglichekeit bei Verlust des Passwords.


Explorer Anzeige eines Laufwerks mit Bitlocker

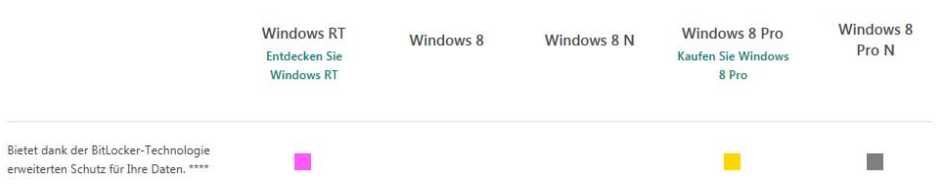



Aufbewahrungsmöglichkeiten des Recovery Keys




Auch können externe Festplatten und USB Sticks verschlüsselt werden.

Bei Windows 8 ist Bitlocker bei RT und der der Pro Version integriert:



## Alternative: TrueCrypt

Eine OpenSource Variante bietet dazu TrueCrypt an. Unterstützt wird hier Windows 7/Vista/XP (Windows 8 noch nicht), aber auch Linux und MAC. TrueCrypt bietet mehr Einstellungsmöglichkeiten als Bitlocker, darunter fällt unter anderen die Auswahl des Encryption Algorithmus. Es bietet keine Möglichkeit eine Partition wiederherstellen, sollte man das Passwort verlegt haben. Aber es gibt die Möglichkeit eine Rescue Disk zu erstellen.

### Wie sicher ist eine Verschlüsselung überhaupt?

Im Internet wird immer wieder Software angeboten, die einen Zugriff auf verschlüsselte Laufwerke anbieten. Die Technik dahinter funktioniert so, dass versucht wird im RAM des Rechners nach dem Passwort der Verschlüsselung zu suchen. Dazu muss allerdings der Rechner eingeschaltet sein, die verschlüsselte Festplatte gemountet sein, erst dann ist das Passwort im Arbeitsspeicher. Das ist sowohl bei Bitlocker als auch bei TrueCrypt grundsätzlich möglich.

Über die Erfolgsquoten dazu kann ich nichts berichten.

### Performance Microsoft Bitlocker / TrueCrypt

Der Rechner wird durch die Ver- und Entschlüsselung von Daten unwesentlich langsamer, tatsächlich merkt man es nicht. Auf die Akkulaufzeit hat es ebenfalls so gut wie keine Auswirkung. Eine AES Unterstützung des Prozessors bringt Vorteile, diese ist in allen Core i5-Desktop -Prozessoren (und den meisten mobilen Prozessoren) integriert.

### Unterschiede Microsoft Bitlocker / TrueCrypt

Bitlocker ist leider erst ab der Pro Version von Windows 8 dabei. Bitlocker ist bei der Einrichtung benutzerfreundlichen und einfach gehalten, es macht das, was man von einer Verschlüsselung erwartet. Es werden mehrere Authentifizierungsoptionen angeboten.

TrueCrypt unterstützt mehrere Betriebssysteme und es ist OpenSource. Es ist für den Laien im Vergleich zu Bitlocker nicht gleich so rasch bei der Einrichtung zu durchschauen, man muss als Anfänger in der Dokumentation nachlesen um die richtige Auswahl zu treffen. Dafür bietet es aber viel mehr Flexibilität bei der Einrichtung, etwa bei der Auswahl des Algorithmus oder die Anlage versteckter Partitionen.

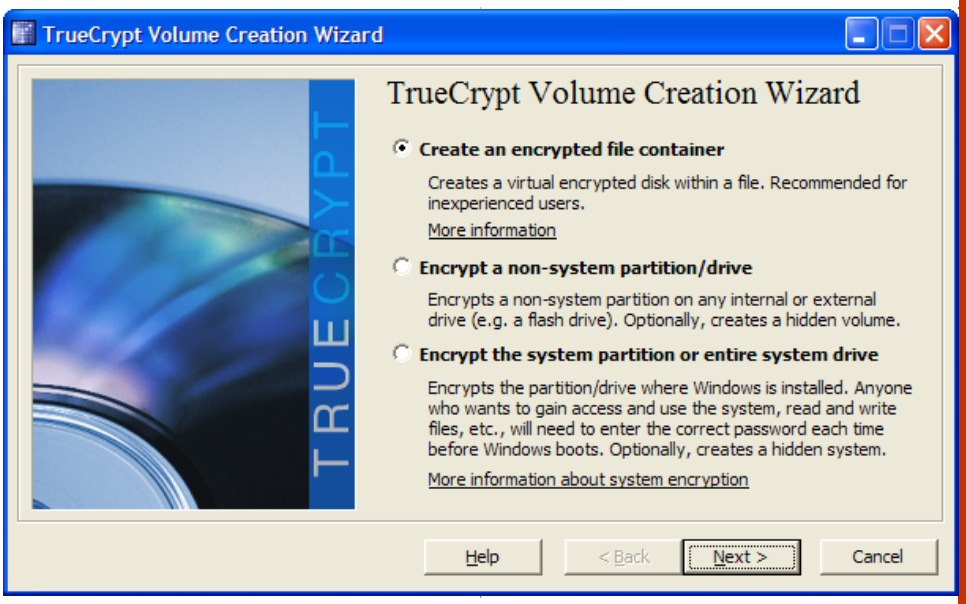
## Fazit

Zumindest auf Windows 8 Pro / RT ist die Möglichkeit für die Nutzung von Verschlüsselung durch Microsoft Bitlocker integriert, es muss keine zusätzliche Software angeschafft und installiert werden. Die Aktivierung des Bitlockers ist nicht sonderlich schwierig, außerdem ist alles mit Wizzards und ausführlicher Beschreibung abgedeckt. Selbst für die Einsteiger Version von Windows oder für alternative Betriebssysteme gib es eine wunderbare Variante mit TrueCrypt, um seine Daten zu schützen.

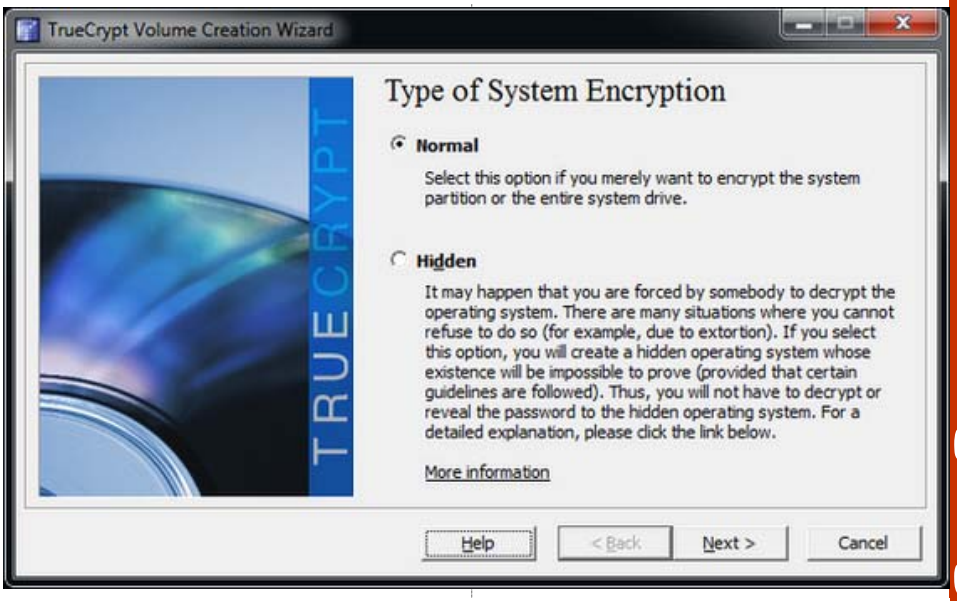
Es ist mir unverständlich, warum noch immer so viele Personen mit mobilen Geräten wie Notebooks, USB Sticks und externe Festplatten unverschlüsselt unterwegs sind und so sorglos damit umgehen. Gleichzeitig liest man häufig, dass immer wieder Daten durch Verlust von Medien abhandenkommen und an falscher Stelle wieder auftauchen, der Aufschrei in den Medien ist demensprechend groß. Die Dunkelziffer ist sicher noch viel höher.

Aber vielleicht hat dies in unserer Facebook Gesellschaft – meine Daten sind auch deine Daten – nicht mehr so einen hohen Stellenwert bei vielen?


Auswahl des Encryption Algorithmus




Auswahl der Partition




Auch versteckte Partitions (Betriebssysteme) können erstellt werden, deren Existenz „verschleiert“ werden soll.