

04.12.2020

aktualisiert am 18.11.2023

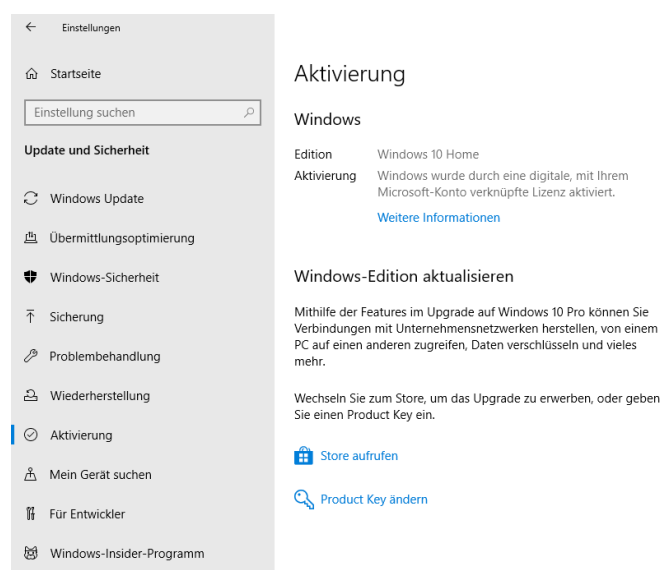
BitLocker-Installationsanleitung

Das Aktivieren der Festplattenverschlüsselung mit BitLocker unter Windows ist einfacher als es klingt. Doch für Nutzer von Windows Home ist es mit 145 € nicht ganz billig. Getestet habe ich BitLocker unter Windows 10 und 11, es funktioniert aber auch unter Windows 8. Allerdings werden für Windows 8 seit Januar 2023 keine aktuellen Sicherheitsupdates mehr ausgeliefert, so dass es (oder eine noch ältere Windows-Version) sich auf einem Praxisrechner verbietet.

Ratsam ist zunächst, alle Daten vom Computer auf einer (möglichst mit dem Verfahren AES-256 verschlüsselten) externen Festplatte, SD-Karte oder einem USB-Stick zu sichern. Bei der Installation von Windows Pro und BitLocker geht selten etwas schief. Falls doch, sind dann aber keine Daten verloren. Um herauszufinden, welche Edition von Windows auf dem Rechner läuft, klickt man auf Windows-Symbol => Einstellungen (das Zahnrad-Symbol) => System => Info (dafür ganz nach unten scrollen) oder man klickt im Windows-Explorer mit der rechten Maustaste auf »Dieser PC« und anschließend mit der linken Maustaste auf »Eigenschaften«. Die Windows-Edition findet man auch, indem man die Windows-Logo-Taste + Pause (neben F12) drückt oder indem man die Windows-Logo-Taste + r drückt und dann msinfo32 öffnet.

Sollte dort »Windows Home« stehen, muss als Voraussetzung für den Einsatz von BitLocker zunächst das kostenpflichtige Upgrade auf Windows Pro durchgeführt werden. Dazu muss der Computer mit dem Internet verbunden sein. In Windows 10 wählt man Windows-Symbol => Einstellungen => Update und Sicherheit => Aktivierung => Store aufrufen. In Windows 11 wählt man Windows-Symbol => Einstellungen => System => Aktivierung => Windows-Edition aktualisieren => Store öffnen.

Dort klickt man auf die Schaltfläche »Kaufen« bzw. »Abrufen für 145,00 €« und muss sich zunächst in ein bestehendes Microsoft-Konto einloggen oder ein neues Microsoft-Konto erstellen. Darin kann zwischen

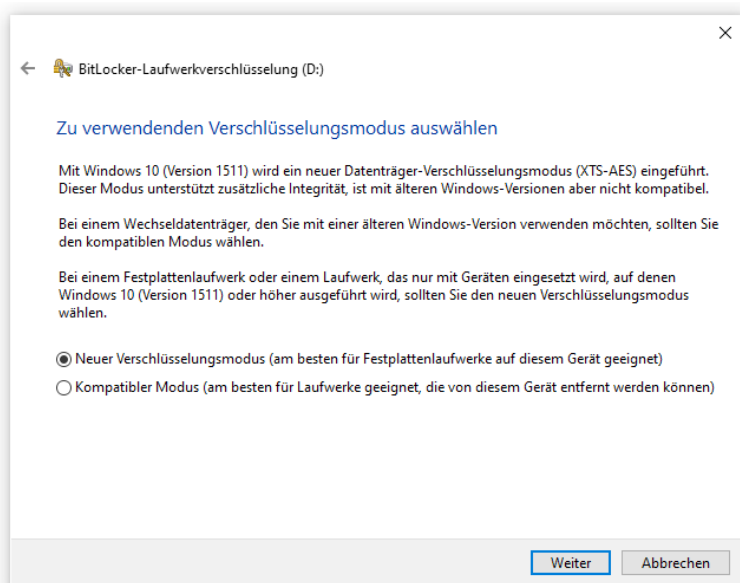


verschiedenen Zahlungsmethoden gewählt werden: Kreditkarte, PayPal¹, Sofortüberweisung² oder Giropay³. Hatte man schon zuvor im Microsoft-Konto eine Zahlungsmethode eingerichtet, wird sie automatisch mit dem Kaufpreis belastet. Ich habe einmal PayPal und einmal Giropay getestet. Dabei habe ich keine Probleme gefunden außer jenem, dass PayPal neben Microsoft dann schon die zweite Firma ist, die diese Zahlung in den USA verarbeitet.

Nach erfolgreichem Kauf klickt man im Microsoft Store auf »Installieren« und bejaht die fürsorgliche Rückfrage, ob man tatsächlich von allen Dateien Sicherungskopien gemacht hat. Die Installation von Windows Pro dauert wenige Augenblicke. Nach einem Neustart meldet Windows: »Erfolgreich! Das war schon alles. Der PC kann jetzt verwendet werden.«

BitLocker einrichten

Externe Datenträger können Sie auch dann mit BitLocker verschlüsseln, wenn die Verschlüsselung der internen Festplatte des Computers nicht eingerichtet ist (und umgekehrt). BitLocker hat jedoch nur die 128-Bit-Verschlüsselung voreingestellt. Deshalb ist es ratsam, in jedem Fall zuerst BitLocker einzurichten. Sollten Sie beim Verschlüsseln eines externen Datenträgers die folgende Nachfrage erhalten, ist BitLocker noch nicht vollständig eingerichtet:



Vor der Einrichtung von BitLocker stellen sich mehrere Glaubens- und Geschmacksfragen. Die erste Frage ist jene für oder wider den in den meisten aktuellen Rechnern verbauten TPM-Chip⁴ (Trusted Platform Module). Auch ohne eingebautes TPM lässt sich BitLocker verwenden. Umgekehrt habe ich leider keine Methode gefunden, wie bei einem funktionierenden TPM BitLocker davon abgehalten werden kann, es zu benutzen. Entsprechende Kenntnisse oder entsprechenden Mut vorausgesetzt, können Sie jedoch versuchen, das TPM im BIOS Ihres Computers zu deaktivieren. Dazu müssen Sie direkt nach dem Start des Rechners und noch bevor

¹ <https://de.wikipedia.org/wiki/PayPal>

² <https://de.wikipedia.org/wiki/Sofort%C3%BCberweisung>

³ <https://de.wikipedia.org/wiki/Giropay>

⁴ https://de.wikipedia.org/wiki/Trusted_Platform_Module

Windows hochfährt, entweder die Taste F2 oder die Taste F10 gedrückt halten. Dann öffnen sich die BIOS-Einstellungen, wo das TPM meist unter dem Punkt »Security« verzeichnet ist.

Für die Verwendung des TPM spricht, dass mit diesem Chip die Festplatte nur dann wieder entschlüsselt werden kann, wenn die Hardware des Rechners unverändert ist. Würde man eine Kopie aller mit BitLocker verschlüsselten Daten auf einem anderen Rechner anlegen, um dort die Verschlüsselung zu brechen, ließe der TPM-Chip den Versuch scheitern. Gegen den TPM-Chip spricht, dass dessen Manipulation durch die NSA oder andere staatliche Stellen nicht auszuschließen ist. Diese könnten dann selbst die Festplatte entschlüsseln oder deren Entschlüsselung durch den Besitzer verhindern. Ist das TPM defekt, besteht das Risiko, dass der Computer nicht mehr startet. Die Hersteller der freien Verschlüsselungssoftware VeraCrypt kritisieren das TPM als »völlig überflüssig«⁵.

Ob der Rechner über ein TPM verfügt, finden Sie heraus, indem Sie in einem Benutzerkonto mit Administratorrechten die Windows-Logo-Taste + r drücken und tpm.msc öffnen. Dort steht unter »Status«, ob das TPM vorhanden und einsatzbereit ist.

Nicht zu empfehlen ist die Authentifizierung von BitLocker allein über das TPM, weil einige Angriffe auf die verschlüsselten Daten dann trotzdem möglich wären. So lautet die zweite Entscheidung, was entweder als alleinige Authentifizierung ohne TPM oder als zweiter Authentifizierungsfaktor zusätzlich zum TPM-Chip gewählt werden soll: Passwort oder Schlüsseldatei?

Vor- und zugleich Nachteil des Passwortes ist, dass es nicht aufgeschrieben werden muss. Was man im Gedächtnis hat, kann zwar nicht ausgespäht, wohl aber vergessen werden. Das Passwort ist weniger komplex als die Schlüsseldatei und deshalb leichter durch Probieren zu finden. Bei jedem Start des Rechners muss es eingegeben werden. Wie ein Hacker beim Durchprobieren von BitLocker-Passwörtern vorgeht, zeigt dieses Video⁶.

Vor- und zugleich Nachteil der Schlüsseldatei ist deren Länge. Um sich diese Information zu merken, müsste man ein Gedächtniskünstler sein. Deshalb wird die Schlüsseldatei auf einem USB-Stick oder einer SD-Karte abgelegt. Diese externen Speicher dürfen jeweils beliebige weitere, von BitLocker unabhängige Daten enthalten. Bei jedem Einschalten muss der Datenträger mit der Schlüsseldatei mit dem Rechner verbunden sein. Bis zum nächsten Einschalten kann man ihn dann wieder entfernen.

Eine Entscheidungshilfe zu der Frage TPM-Chip, Passwort und/oder Schlüsseldatei bietet dieser Artikel⁷ (auf Englisch). Microsoft empfiehlt die Kombination aus TPM-Chip und Passwort. Ich bevorzuge die Schlüsseldatei auf USB-Stick, gezwungenermaßen mit TPM, das sich auf meinen Computern bisher nicht abschalten ließ.

Vor dem Einrichten von BitLocker kann eine dritte Entscheidung getroffen werden. Die Verschlüsselungsstärke von BitLocker ist auf 128 Bit voreingestellt. Sie kann problemlos auf 256 Bit erhöht werden, ohne dass es die Schnelligkeit des Rechners merklich bremst.

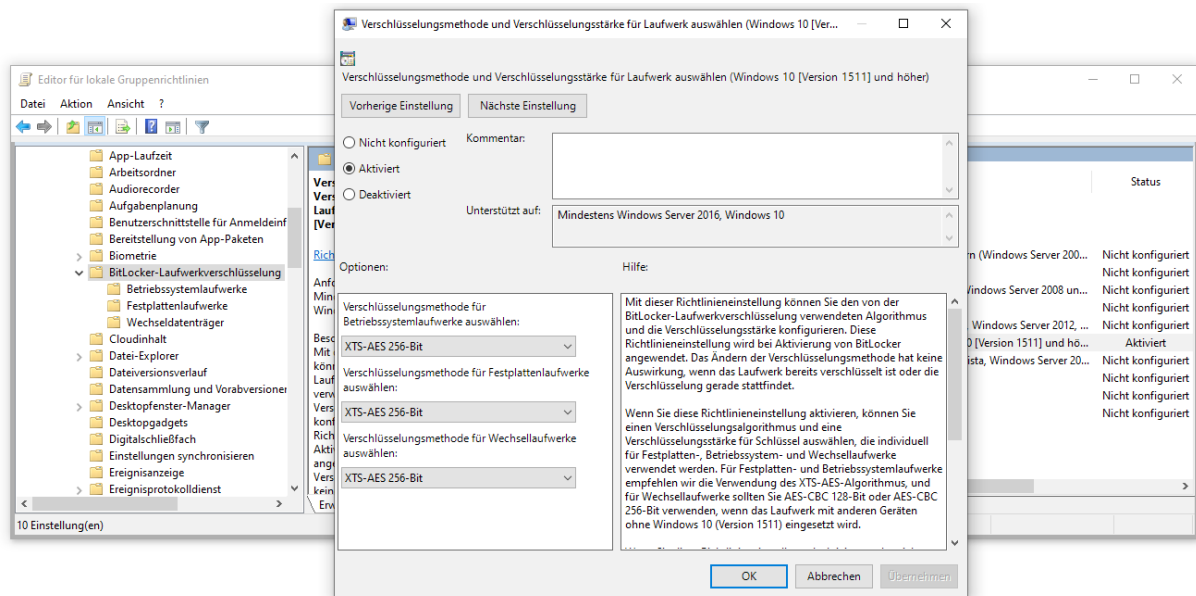
Um die Installation durchzuführen, müssen wir Windows mitteilen, wie wir uns hinsichtlich TPM-Chip, Passwort oder Schlüsseldatei und Verschlüsselungsstärke entschieden haben. Das

⁵ https://en.wikipedia.org/wiki/Trusted_Platform_Module#Reception

⁶ <https://www.youtube.com/watch?v=gue6suh7ZIM>

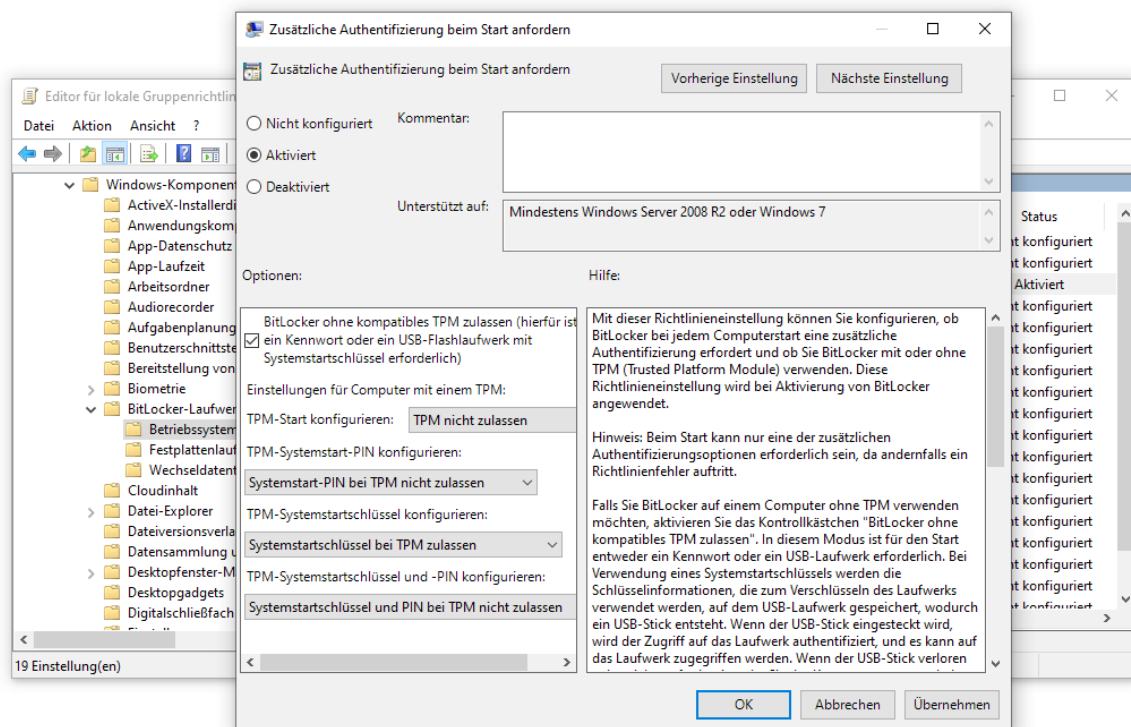
⁷ [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/ee706531\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/ee706531(v=ws.10))

geschieht in den sogenannten Gruppenrichtlinien. Um dorthin zu gelangen, drückt man die Windows-Logo-Taste + r, öffnet gpedit.msc und klickt sich durch bis zum Unterordner Richtlinien für Lokaler Computer => Computerkonfiguration => Administrative Vorlagen => Windows-Komponenten => BitLocker-Laufwerkverschlüsselung. (Bitte nicht nach unten in die Benutzerkonfiguration verrutschen, wo es auch Administrative Vorlagen gibt.)



Im Unterordner BitLocker-Laufwerkverschlüsselung angekommen, stehen auf der rechten Seite mehrere Einträge mit dem Namen »Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen«. Der passende Eintrag ist der für Windows-Version 1511 und höher. Ist man sich nicht sicher, können auch alle Einträge bearbeitet werden. Nach Doppelklick auf den Eintrag muss die Option »Aktiviert« und darunter die gewünschte Kombination aus Verschlüsselungsmethode und Verschlüsselungsstärke gewählt werden, beispielsweise XTS-AES 256-Bit. Möchten Sie mit BitLocker verschlüsselte externe Datenträger noch unter Windows 8 benutzen, wählen Sie bei »Verschlüsselungsmethode für Wechsellaufwerke auswählen« AES-CBC 256-Bit, sonst wählen Sie auch hier XTS-AES 256-Bit.

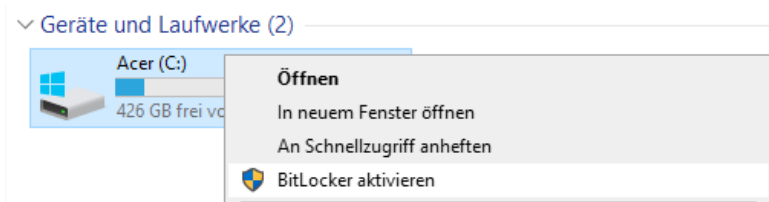
Zurück auf der linken Seite wählt man den Unterordner »Betriebssystemlaufwerke« und doppelklickt auf der rechten Seite auf den Eintrag »Zusätzliche Authentifizierung beim Start anfordern«. Auch hier muss wieder die Option »Aktiviert« gewählt werden. Verfügt der Computer über keinen TPM-Chip, muss das Häkchen bei »BitLocker ohne kompatibles TPM zulassen« gesetzt sein. Andererseits hindert das Setzen dieses Häkchens BitLocker nicht an der Benutzung eines vorhandenen TPM.



Die nachfolgenden Einstellungen zu Passwort (PIN) und Schlüsseldatei können entsprechend den eigenen Wünschen gesetzt werden. Dieses Fenster kann jetzt wieder geschlossen werden.

BitLocker auf interner Festplatte aktivieren

Es geht weiter im Windows-Explorer, wo man mit der rechten Maustaste auf das Betriebssystem-Laufwerk (meist C:) klickt, »BitLocker aktivieren« wählt und die Laufwerksverschlüsselung startet. Will man den Systemstartschlüssel auf USB-Stick oder SD-Karte nutzen, sollte der externe Datenträger jetzt schon angeschlossen sein.

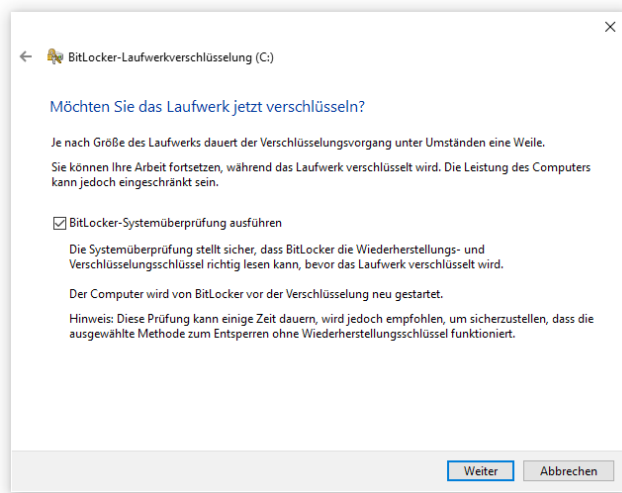


Hat man sich für das Anlegen eines Systemstartschlüssels entschieden, fragt Windows, auf welchem USB-Laufwerk er gespeichert werden soll. Anschließend bittet Sie Windows, einen Wiederherstellungsschlüssel zu sichern. Tun Sie das am besten sowohl als Datei auf einem externen Laufwerk als auch als Ausdruck auf Papier.

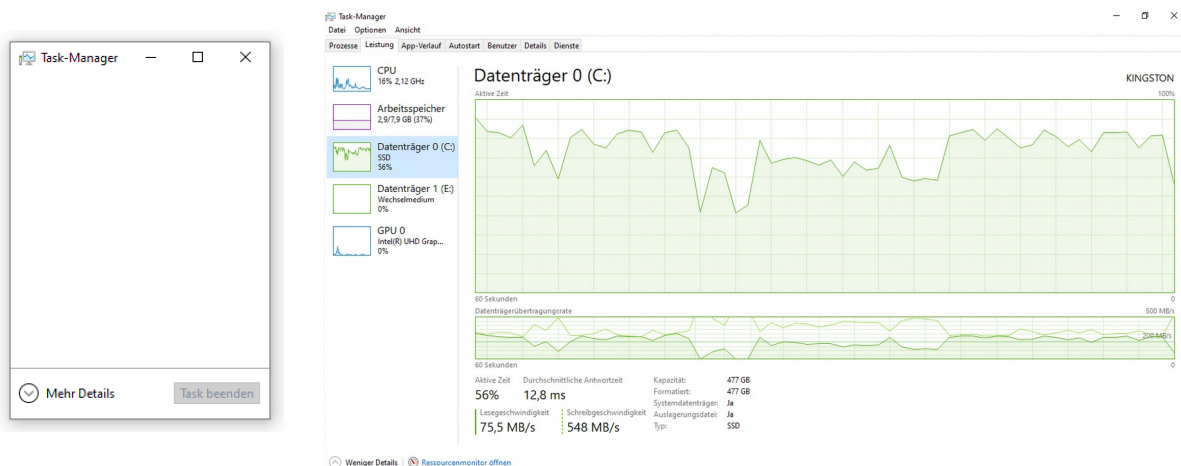
Während der Systemstartschlüssel ein 256-Bit AES-Schlüssel ist, handelt es sich beim Wiederherstellungsschlüssel um eine 48-stellige Dezimalzahl. Der Taschenrechner verrät uns, dass der Logarithmus zur Basis 2 von $10^{48} = 159,4$ ist. Selbst wenn wir das aufrunden, hat der Wiederherstellungsschlüssel also nur einen Informationsgehalt von 160 Bit. Wer sich für den Fall, dass alle Kopien des Systemstartschlüssels verloren gehen, auf regelmäßige Sicherungskopien der Daten verlassen möchte, kann den Wiederherstellungsschlüssel wieder löschen. Mehr dazu später.

Dass dieselben Daten parallel mit mehreren Schlüsseln oder Kennwörtern verschlüsselt zu sein scheinen, funktioniert deshalb, weil der eigentliche 256-Bit AES-Schlüssel für die Daten dem Benutzer gegenüber gar nicht auftaucht. Statt dessen wird dieser Schlüssel einmal mit dem Systemstartschlüssel verschlüsselt, ein andermal mit dem Kennwort verschlüsselt und einmal mit dem Wiederherstellungsschlüssel verschlüsselt jeweils auf dem Datenträger abgelegt.

Nun wählen Sie bitte noch »Gesamtes Laufwerk verschlüsseln«. So können Sie nicht in die Gefahr geraten, dass sich auf den unverschlüsselten Teilen des Datenträgers vielleicht doch noch alte Daten befinden, die für einen Angreifer lesbar bleiben. Schließlich wählen Sie noch die BitLocker-Systemüberprüfung aus. Anschließend fordert Windows Sie zum Neustart des Computers auf.

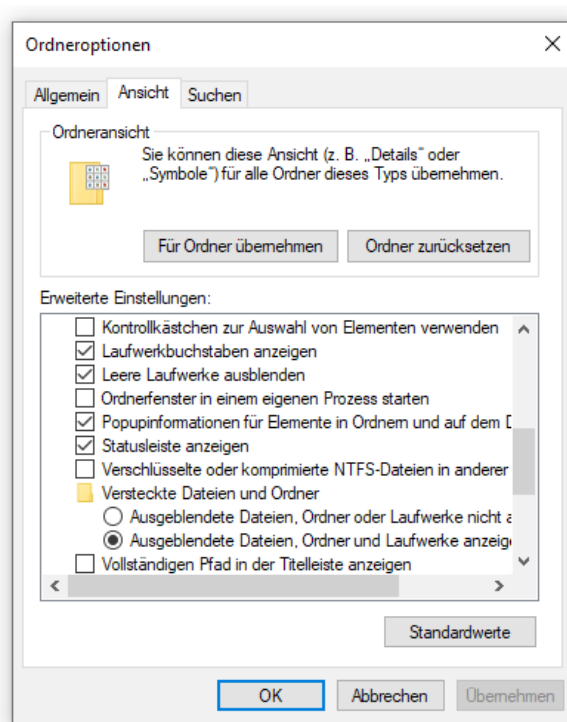


Nach dem Neustart bemerkt man zunächst nichts und man könnte meinen, die Laufwerksverschlüsselung habe nicht funktioniert. Gewissheit verschaffen kann man sich, indem man mit Strg + Alt + Entf den Taskmanager startet. Dort muss man auf Mehr Details => Leistung klicken um zu sehen, dass Windows tatsächlich mit dem zu verschlüsselnden Datenträger arbeitet.



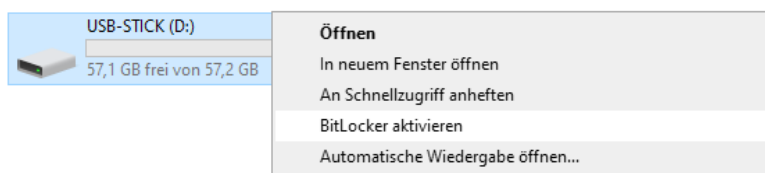
Je nach Größe des Laufwerks dauert der Verschlüsselungsvorgang zwischen wenigen Minuten und einer Stunde. Sie können derweil mit dem Computer weiter arbeiten.

Von der Datei mit dem Systemstartschlüssel sollte man sich mehrere Sicherungskopien anfertigen und sie gut verwahren. Sucht man die Schlüsseldatei auf dem USB-Stick (oder der SD-Karte), sieht man zunächst nichts, da sie als Systemdatei gekennzeichnet ist und Systemdateien von Windows normalerweise nicht angezeigt werden. Das lässt sich ändern, indem man im Windows-Explorer auf Datei => Optionen => Ansicht geht und das Häkchen bei »Geschützte Systemdateien ausblenden (empfohlen)« entfernt. In derselben Liste weiter unten muss außerdem »Ausgeblendete Dateien, Ordner und Laufwerke anzeigen« markiert werden. Jetzt wird im Windows-Explorer die Schlüsseldatei mit angezeigt, deren Name auf *.BEK (für BitLocker Encryption Key) endet. Nicht passieren darf es, dass USB-Stick bzw. SD-Karte und damit die Schlüsseldatei gemeinsam mit dem verschlüsselten Rechner in die Hände Unbefugter geraten.



BitLocker auf externem Datenträger aktivieren

Um einen externen Datenträger mit BitLocker zu verschlüsseln, beginnt man wieder im Windows-Explorer und klickt mit der rechten Maustaste auf das zu verschlüsselnde Laufwerk.



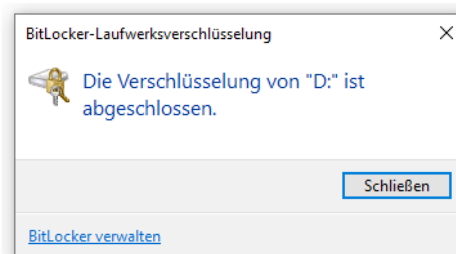
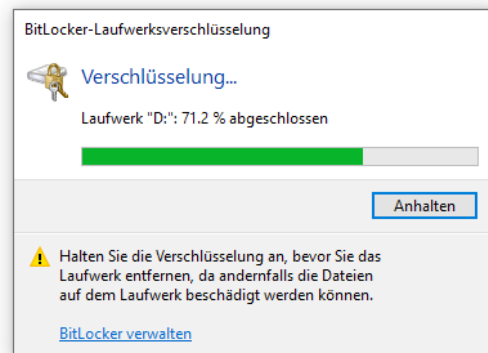
Anschließend muss ein sehr sicheres Passwort gewählt werden. Geriete der Datenträger (oder eine Kopie der darauf befindlichen Daten) in die Hände eines Angreifers, hat dieser alle Zeit der Welt, um mögliche Passwörter durchzuprobieren. Es ist nicht übertrieben, ein Passwort mit einer zufälligen Kombination von Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen zu erfinden und es 40 bis 50 Zeichen lang zu machen. Das entspricht dann ungefähr dem Informationsgehalt eines 256-Bit Schlüssels.

Dann sichern Sie bitte den Wiederherstellungsschlüssel, wählen »Gesamtes Laufwerk verschlüsseln« und warten, bis die Verschlüsselung abgeschlossen ist.

Zum Erzeugen und Speichern des Passwortes empfehle ich einen Passwortmanager, z.B. KeePassXC⁸. Von dort kann das Passwort in die Zwischenablage kopiert und in BitLocker eingefügt werden. In umgekehrter Richtung können Sie den Wiederherstellungsschlüssel

⁸ <https://keepassxc.org>

(besonders den für die interne Festplatte) mit in den Passwortmanager eintragen, damit er nicht als einzelne Textdatei oder auf einem Blatt Papier verloren geht.



Der Konsolen-Befehl manage-bde

In allen aktuellen Windows-Versionen (einschließlich Windows Home) funktioniert der Befehl `manage-bde`. Bde steht hier für »BitLocker device encryption« – BitLocker-Geräteverschlüsselung. Dieser Befehl zeigt Informationen über verschlüsselte Laufwerke an und kann die Verschlüsselungsstärke durch das Löschen nicht benötigter Wiederherstellungsschlüssel erhöhen. Dazu muss die Windows-Eingabeaufforderung (oder die Windows PowerShell) im Administratormodus gestartet werden.

Die Eingabeaufforderung können Sie wie folgt im Administratormodus öffnen:

- Rechtsklick auf das Windows-Symbol => Suchen => den Begriff Eingabeaufforderung oder `cmd` ganz oder teilweise eingeben und in den Suchergebnissen Als Administrator ausführen anklicken und den folgenden Dialog mit Ja bestätigen *oder*
- Linksklick auf das Windows-Symbol => Windows-System => Klick mit der rechten Maustaste auf Eingabeaufforderung, dann Mehr => Als Administrator ausführen und den folgenden Dialog mit Ja bestätigen *oder*
- Windows-Taste + r drücken, `cmd` eingeben und die Tastenkombination Strg + Umschalttaste gedrückt halten, während Sie den Dialog mit OK bestätigen. Auch hier müssen Sie wieder den folgenden Dialog mit Ja bestätigen.

Die jeweils einzugebenden Befehle lauten für die Laufwerksinformationen

```
manage-bde -status [Laufwerksbuchstabe:]
```

zum Löschen des Wiederherstellungsschlüssels

```
manage-bde -protectors -delete [Laufwerksbuchstabe:] -type recoverypassword
```

und zum Löschen des externen Schlüssels

```
manage-bde -protectors -delete [Laufwerksbuchstabe:] -type externalkey
```


Nun ist der Schlüssel zu den (hoffentlich regelmäßig sicherungskopierten) Daten nur noch mit dem (hoffentlich sehr sicheren) Kennwort verschlüsselt.

```
Administrator: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.630]
(c) 2019 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>manage-bde -status d:
BitLocker-Laufwerkverschlüsselung: Konfigurationstool, Version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

Volume "D:" [USB-STICK]
[Datenvolume]

Größe: 57,28 GB
BitLocker-Version: 2.0
Konvertierungsstatus: Vollständig verschlüsselt
Verschlüsselt (Prozent): 100,0 %
Verschlüsselungsmethode: XTS-AES 256
Schutzstatus: Der Schutz ist aktiviert.
Sperrungsstatus: Entsperrt
ID-Feld: Unbekannt
Automatische Entsperrung: Deaktiviert
Schlüsselschutzvorrichtungen:
    Kennwort
    Numerisches Kennwort

C:\WINDOWS\system32>manage-bde -protectors -delete d: -type recoverypassword
BitLocker-Laufwerkverschlüsselung: Konfigurationstool, Version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

Volume "D:" [USB-STICK]
Schlüsselschutzvorrichtungen vom Typ "Numerisches Kennwort"

Numerisches Kennwort:
ID: {26459F9C-C767-41BA-814C-0520942908F4}
Kennwort:
112343-103466-436832-520256-713460-065120-404129-112178

Die Schlüsselschutzvorrichtung mit der ID "{26459F9C-C767-41BA-814C-0520942908F4}" wurde gelöscht.

C:\WINDOWS\system32>
```

Vom Löschen des Wiederherstellungsschlüssels »Numerisches Kennwort« für ein Betriebssystem-Laufwerk rate ich ab, weil im Fehlerfall die Wiederherstellung des kompletten Betriebssystems aus Sicherungskopien schwieriger ist.

Unter »Schlüsselschutzvorrichtungen« sind anschließend »Kennwort« und gegebenenfalls »Externer Schlüssel (Erforderlich zur automatischen Entsperrung)« verzeichnet.

Möchten Sie ein kompliziertes Kennwort nicht nach jedem Einlegen des externen Datenträgers neu eingeben, können Sie mit der Option »Auf diesem PC automatisch entsperren« den jeweiligen Computer einen Extra-Schlüssel zur Umgehung des Kennwortes anlegen lassen:

BitLocker (D:)

Geben Sie das Kennwort ein, um dieses Laufwerk zu entsperren.

.....

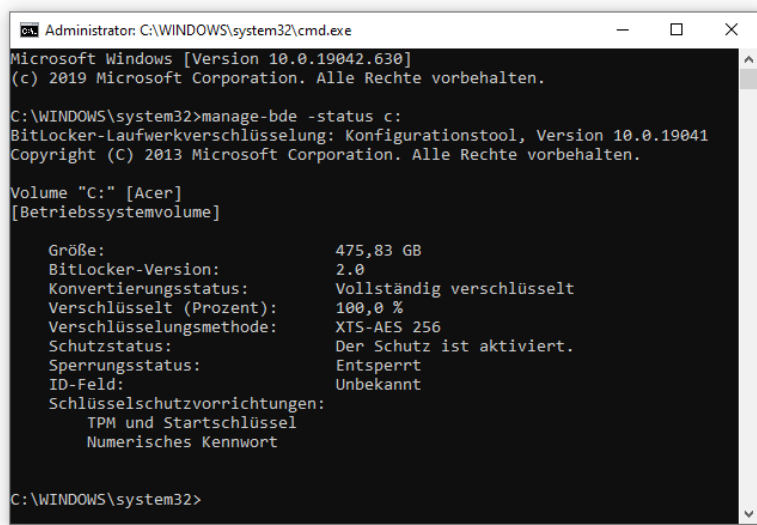
[Weniger Optionen](#)

[Wiederherstellungsschlüssel eingeben](#)

Auf diesem PC automatisch entsperren

[Entsperren](#)

Die BitLocker-Informationen für eine interne Festplatte können folgendermaßen aussehen:



```
Administrator: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.630]
(c) 2019 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>manage-bde -status c:
BitLocker-Laufwerkverschlüsselung: Konfigurationstool, Version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

Volume "C:" [Acer]
[Betriebssystemvolumen]

Größe:                475,83 GB
BitLocker-Version:    2.0
Konvertierungsstatus: Vollständig verschlüsselt
Verschlüsselt (Prozent): 100,0 %
Verschlüsselungsmethode: XTS-AES 256
Schutzstatus:         Der Schutz ist aktiviert.
Sperrungsstatus:     Entsperrt
ID-Feld:              Unbekannt
Schlüsselschutzvorrichtungen:
    TPM und Startschlüssel
    Numerisches Kennwort

C:\WINDOWS\system32>
```