Anleitung

Bitlocker

Schützen Sie Ihre Daten durch Verschlüsselung

Verschlüsselung von Wechseldatenträgern mit Bitlocker

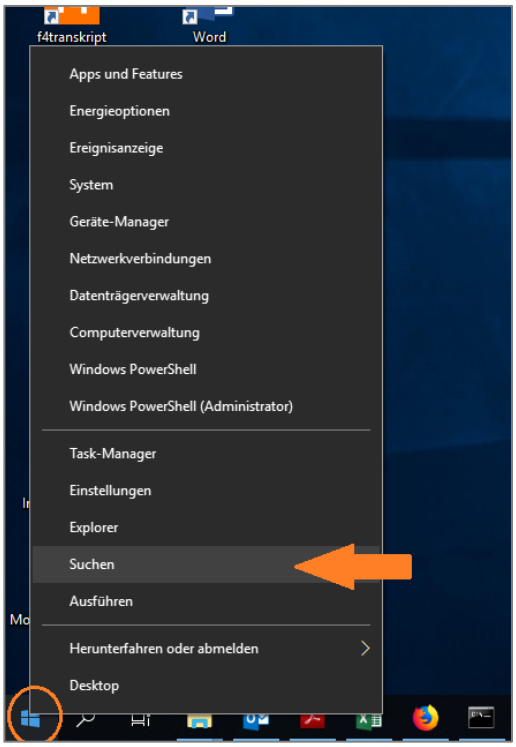
Wechseldatenträger, vor allem USB-sticks, gehen recht häufig verloren, was auch die Gefahr eines unberechtigten Zugriffs durch Dritte mit sich bringt. Auch wenn der Laptop, mit dem der USB-stick verwendet wird, durch Kennwort und sonstige Maßnahmen geschützt ist, gilt dieser Schutz nicht für den Wechseldatenträger. Alle auf ihm befindlichen Daten können ohne weiteres gelesen werden. Das ist eine gravierende Sicherheitslücke, die unbedingt geschlossen werden muß.

Den USB-stick vor unberechtigtem Zugriff zu schützen, ist ganz einfach und erfordert nur einige wenige Handgriffe. Der Schutz besteht darin, die Daten zu verschlüsseln. Im Windows-Betriebssystem ist ein gutes Verschlüsselungsprogramm enthalten: Bitlocker.

1. Arbeitsschritt: Bitlocker starten

Bitlocker kann auf verschiedenen Wegen aufgerufen werden, z.B. über die Systemsteuerung; um die Beschreibung nicht unnötig aufzublähen, wurde auf eine Aufzählung der alternativen Wege verzichtet.

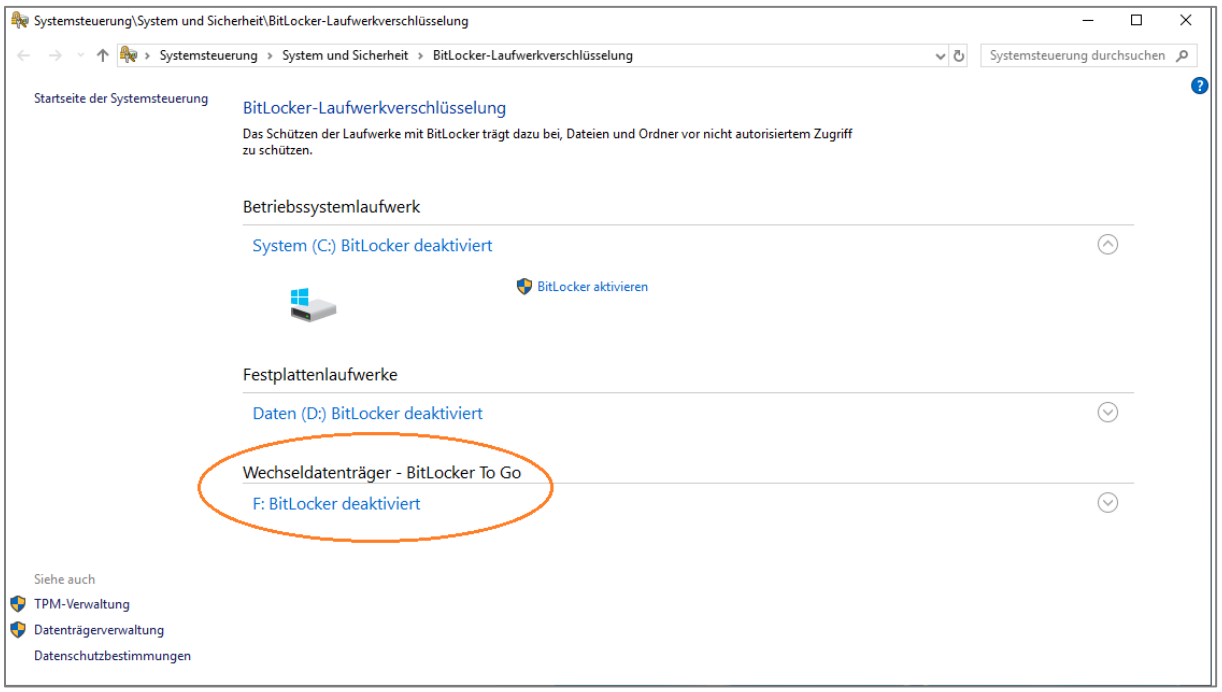
a) Das Windowssymbol links unten in der Startleiste mit der rechten Maustaste anklicken und dort …
b) … den Punkt „Suchen“ auswählen.
c) Im Feld „Suchbegriff hier eingeben“ „Bitlocker“ eintragen.



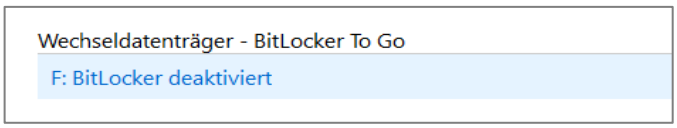
d) Den link „Bitlocker verwalten“ in der rechten Hälfte des Fensters starten.

2. Bitlocker einrichten

a) Wenn Bitlocker das erste Mal gestartet wird, ist noch kein Laufwerk verschlüsselt und Bitlocker überall deaktiviert. Wählen Sie die Option „Wechseldatenträger – Bitlocker To Go“.



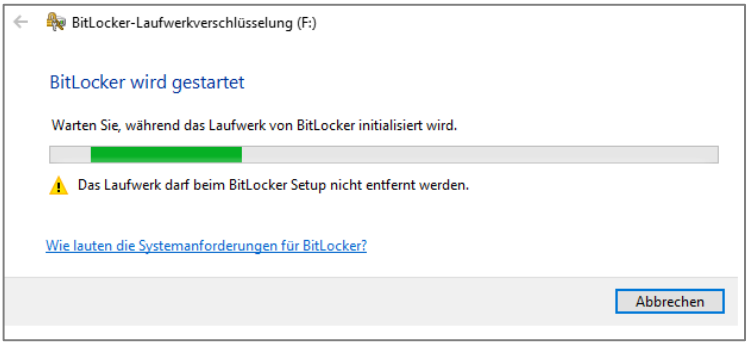
b) Wenn Sie die Maus über den Text „F: Bitlocker deaktiviert“ ziehen, färbt sich das gesamte Feld hellblau.



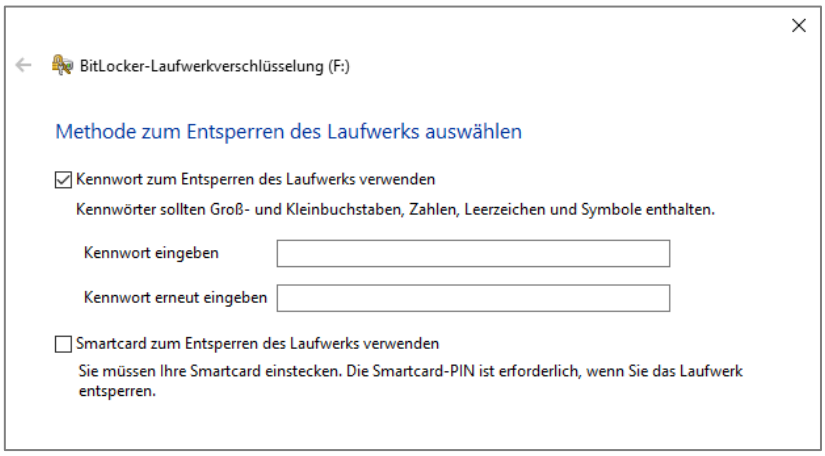
Hinweis: F: steht hier für das Laufwerk des USB-sticks. Bei anderen Computerkonfigurationen kann sich ein davon abweichender Laufwerksbuchstabe ergeben (G: oder E:).

c) Nach einem Mausklick erscheint die Option „Bitlocker aktivieren“.

d) Durch Anklicken der Option „Bitlocker aktivieren“ wird das Laufwerk initialisiert.
Hinweis: dieses Fenster erscheint nur bei USB-sticks, nicht aber beim Verschlüsseln interner Festplatten.



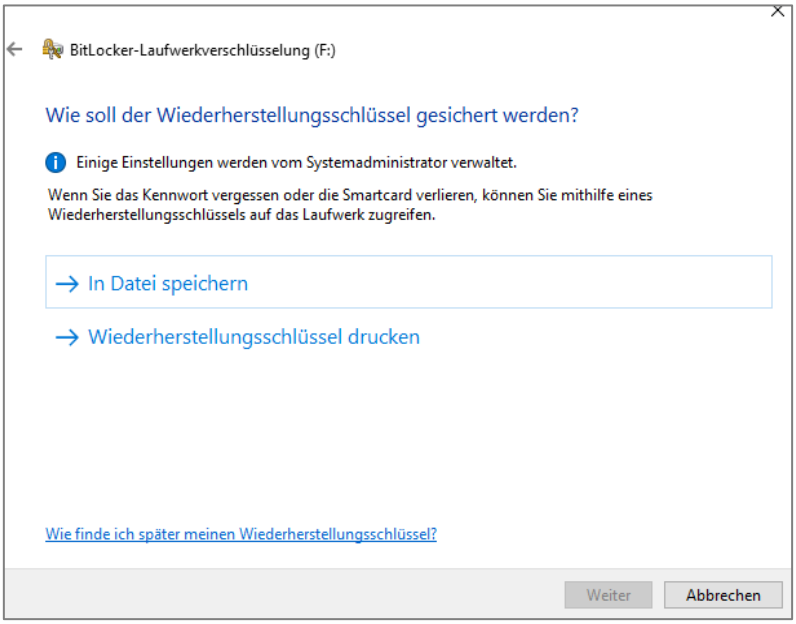
e) Kennworteingabe
Hinweis: Bitte beachten Sie, daß der Schutz Ihrer Daten einzig und allein am Kennwort hängt. Während der Zugriff auf in der Hochschulinfrastruktur gespeicherte Daten zusätzlich noch durch die Benutzerkennung abgesichert wird, steht zwischen Ihren Daten und dem Auge des Kriminellen nur das Kennwort.
→ Legen Sie also bitte besonders großen Wert auf ein komplexes, nicht herausfindbares Kennwort!



f) Wiederherstellungssschlüssel generieren

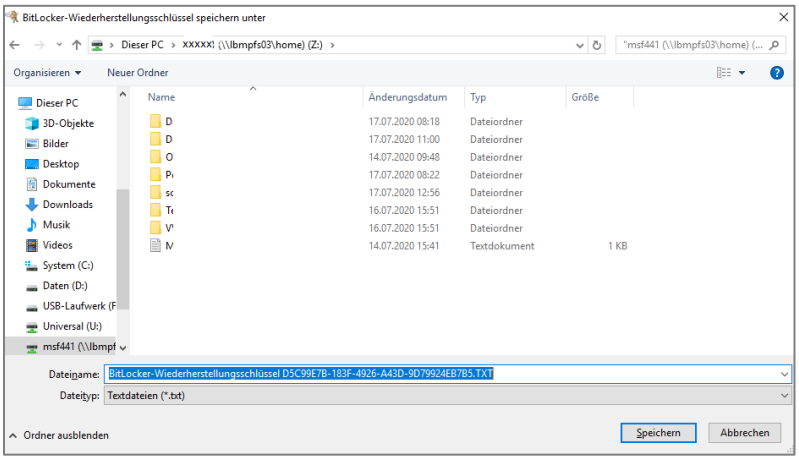
Wenn man das Kennwort für die Anmeldung an der Hochschuldomäne vergessen hat, kann man es sich durch den Benutzerservice zurücksetzen lassen. Ein solches Verfahren ist, wie dies auch bei Bitlocker der Fall ist, nicht für individuell verwaltete Datenbestände möglich. Wenn das Bitlocker-Kennwort vergessen wird, können die verschlüsselten Daten nicht mehr entschlüsselt werden und wären unrettbar verloren. Dieser Gefahr begegnet Bitlocker durch die Generierung eines Wiederherstellungsschlüssels, also einer Art Ersatzkennwort. Falls man das eigentliche Bitlockpaßwort vergessen hat, kann man durch Eingabe des Wiederherstellungsschlüssels wieder auf die Daten auf dem USB-stick zugreifen.

→ Wählen Sie die Option „In Datei speichern“



g) Wiederherstellungssschlüssel abspeichern

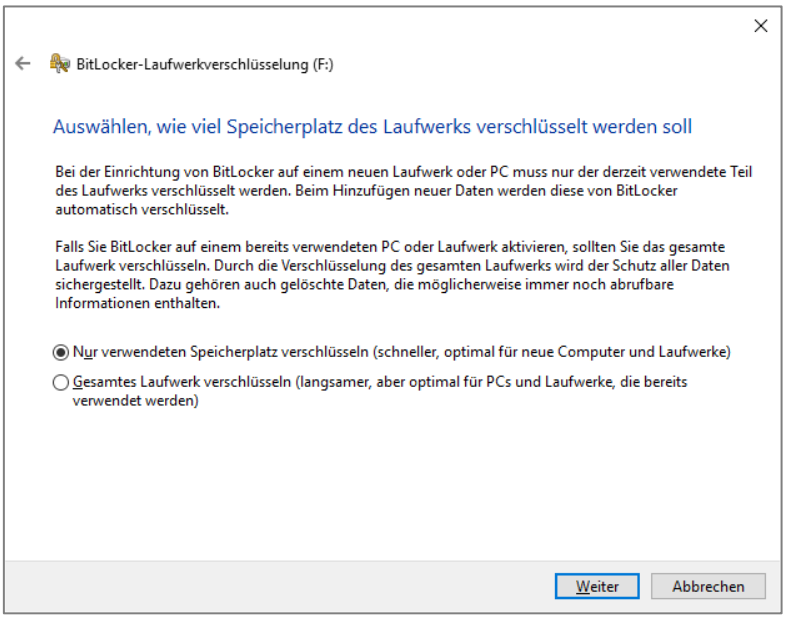
Speichern Sie die Textdatei, die den Wiederherstellungsschlüssel enthält, in einem geeigneten Ordner.



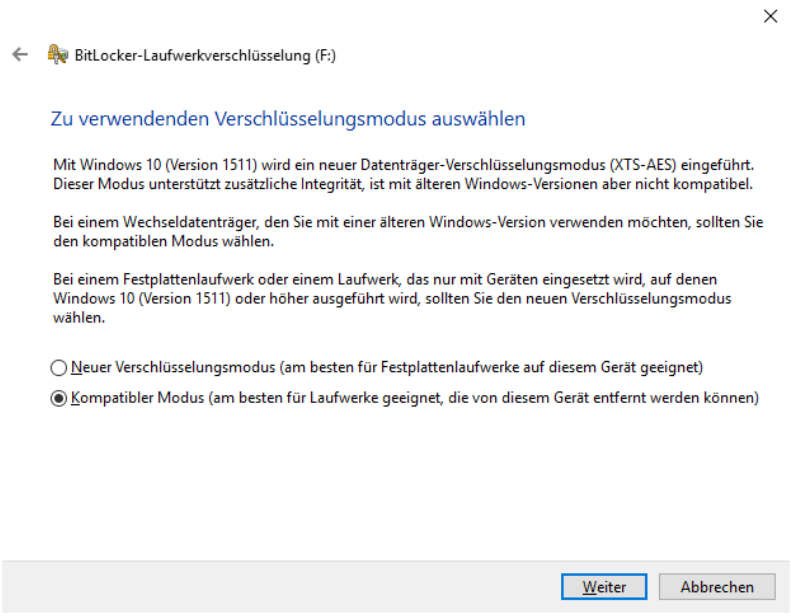
h) Verschlüsselungsmethode wählen

Man muß sich zwischen zwei Methoden entscheiden, je nachdem ob der Datenträger bereits Daten enthält oder noch nicht. Bei einem ganz neuen Datenträger geht die Bitlockereinrichtung sehr schnell, da erst wirklich verschlüsselt wird, wenn Dateien auf dem Datenträger abgelegt werden. Befinden sich bereits Daten auf dem Datenträger, muß dieser komplett, byte für byte, verschlüsselt werden, was ziemlich lange dauert. Zur groben Orientierung: die Verschlüsselung eines 4 GB sticks hat ca. 15 Minuten gebraucht.

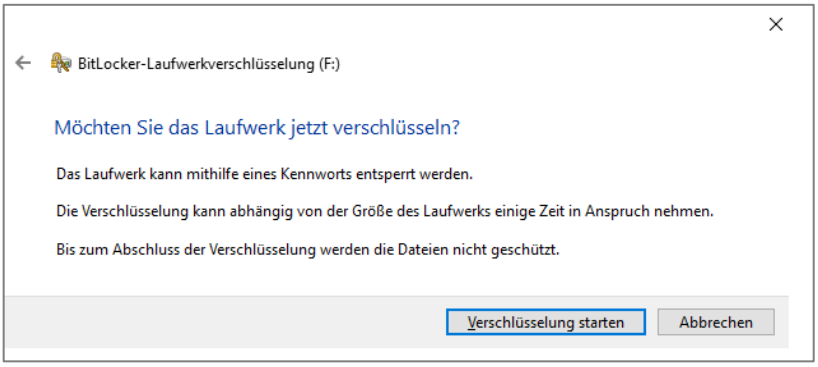
Falls ein USB-stick erst wenige Dateien enthält, empfiehlt es sich daher, diese auf einen anderen Speicherort zu verschieben und nach der Bitlockeinrichtung wieder zurückzuschieben, damit das schnellere Verfahren bei leeren Datenträgern genutzt werden kann.



Im darauffolgenden Fenster beläßt man die Voreinstellung, da diese für Wechseldatenträger am besten geeignet ist.



i) Fertigstellen

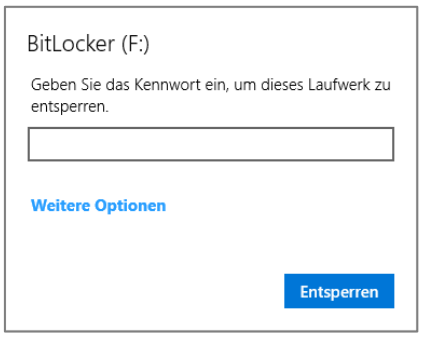


Die Betätigung des Schalters „Verschlüsselung starten“ schließt die Bitlockinstallation ab.

3. Sonstige Tätigkeiten und Hinweise

a) Zugriff auf ein verschlüsseltes Laufwerk

Wenn man ein mit Bitlocker verschlüsseltes Laufwerk anklickt, öffnet sich automatisch das Kennworteingabefenster. Nach Eingabe des Kennworts kann das verschlüsselte Laufwerk wie ein ganz normales Laufwerk genutzt werden. Die Entschlüsselung erfolgt während des Dateizugriffs. Die Arbeit mit der Datei wird durch die Entschlüsselung nicht merklich verzögert.



b) Wiederherstellungsschlüssel ablegen

Je seltener USB-sticks mit schutzwürdigen Daten verwendet werden, desto höher ist die Gefahr des Kennwortvergessens. Darum ist der Wiederherstellungsschlüssel außerordentlich wichtig und darum muß er auch sicher verwahrt werden. Sicher heißt: er sollte nicht von unberechtigten Dritten eingesehen werden können und er sollte zuverlässig zur Verfügung stehen. Das MIT empfiehlt, die Wiederherstellungsschlüssel-Textdatei an die eigene Mailadresse zu schicken und danach die ursprüngliche Schlüsseldatei zu löschen.

c) Wiederherstellungsschlüssel verwenden

In der Wiederherstellungsschlüsseldatei interessiert nur folgender Passus in der Mitte:

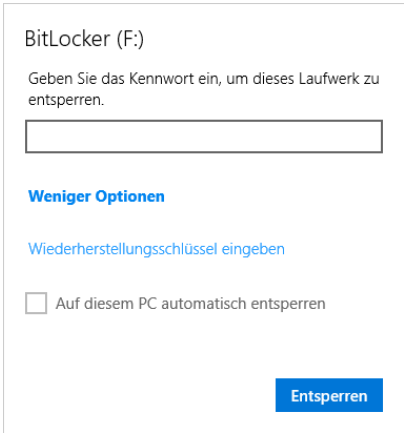
Wiederherstellungsschlüssel:

344661-015147-581853-611545-651408-671418-452378-569921

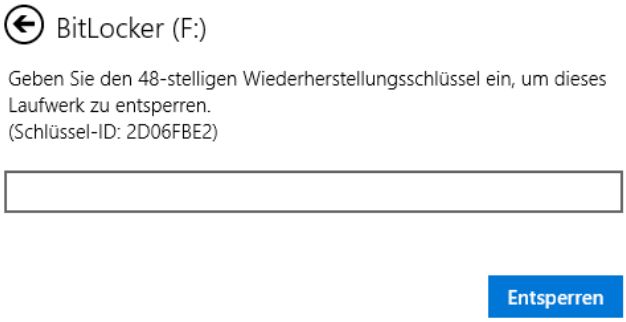
(die genannten Zahlen sind fiktiv)

Die den sogenannten Bezeichner betreffenden Angaben beziehen sich auf in der PH Ludwigsburg nicht praktizierte Ablagevarianten, bei denen Schlüssel sehr vieler Anwender gemeinsam aufbewahrt werden.

- Sie klicken auf das USB-Laufwerk, wodurch sich das unter 3.a) beschriebene Kennworteingabefenster öffnet.



- Sie klicken auf „Weitere Optionen“ und danach auf „Wiederherstellungsschlüssel eingeben“.
- Der Eingabebildschirm für den Wiederherstellungsschlüssel öffnet sich. Man gibt nacheinander die 48 Ziffern ein; die Unterteilung in durch Bindestrich getrennte Sechserblöcke nimmt das System selbständig vor.



- Die Eingabe wird mit dem Schalter „Entsperren“ bestätigt.

c) Keine Verfügbarkeitsgarantie

Hinweis: Bitlocker kann wie jedes andere Verschlüsselungsverfahren Ihre Daten nur vor unberechtigtem Zugriff (Lesen und Verändern) schützen, nicht jedoch die Daten selbst. Die Daten können also durch kriminelles Handeln oder unsachgemäße Handhabung gelöscht oder sonstwie unbrauchbar gemacht werden. Insbesondere kann der Datenträger formatiert werden, ohne daß Bitlocker ein Veto einlegt. Sie sollten daher wichtige Daten niemals ausschließlich auf einem mobilen Datenträger speichern, sondern immer auf den Netzlaufwerken. Der externe Datenträger sollte nur verwendet werden, um Daten mit anderen Personen auszutauschen oder um unabhängig vom Hochschulnetz arbeiten zu können.