Festplattenverschlüsselung

Allgemeines

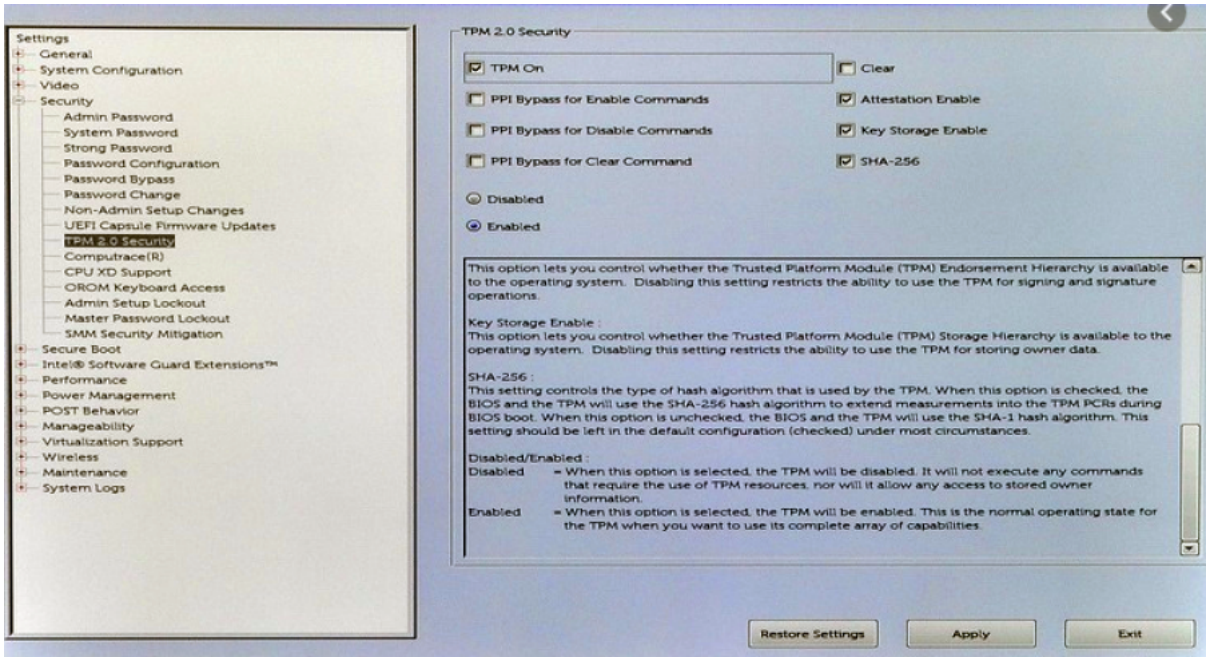
Bitte beachten Sie die den Unterschied zwischen Kennwort, PIN und erweiterter PIN.

- **Kennwort**: Von Kennwörtern wird gesprochen, wenn es sich um eine Authentifizierung des Users gegenüber dem System **ohne Nutzung von TPM** handelt.
- **PIN/Erweiterter PIN**: Von PIN wird gesprochen, wenn es sich um eine Authentifizierung des Users gegenüber dem System **mit Nutzung von TPM** handelt.
  - **Pin:** Zahlen von 0-9
  - **Erweiterter Pin:** Verschiedene Zeichen (Groß- und Kleinbuchstaben, Symbole, Zeichen, Leerzeichen)

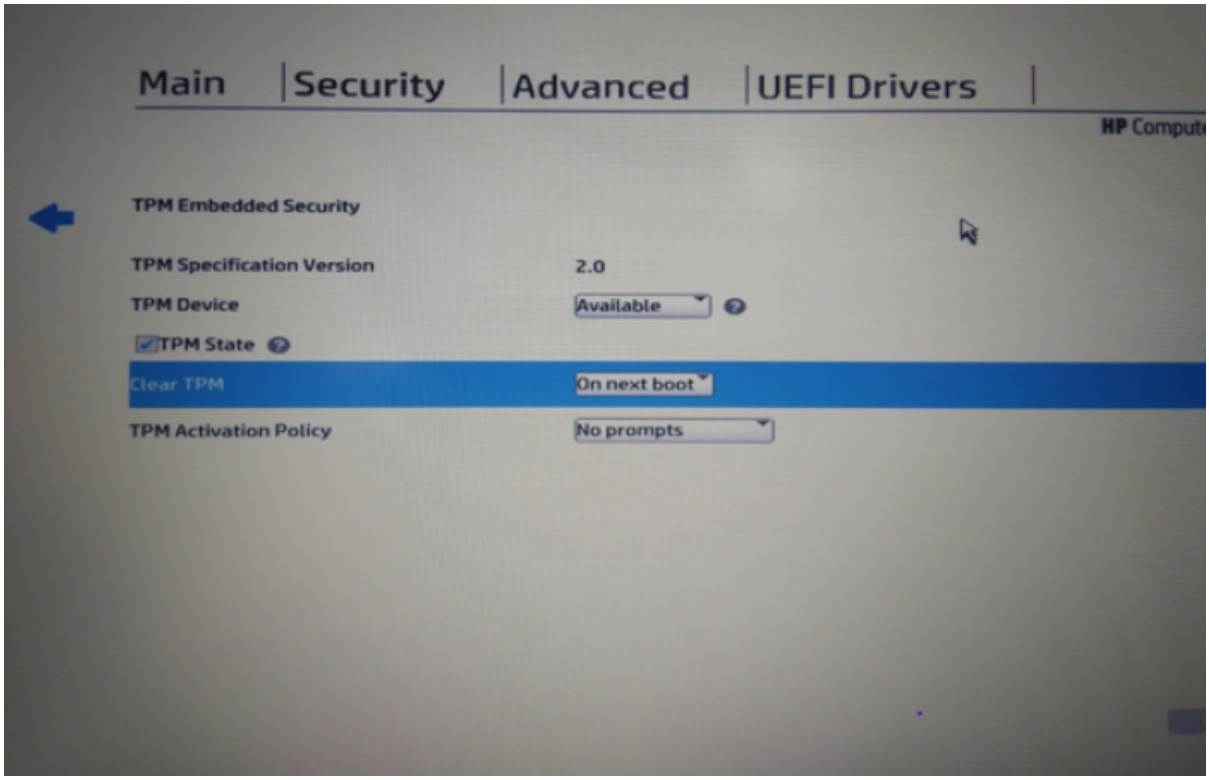
An der Jade Hochschule wird BitLocker für **Systeme ohne Anbindung an das Active-Directory** angeboten - also vorrangig für mobile Geräte.

Vorbereitungen

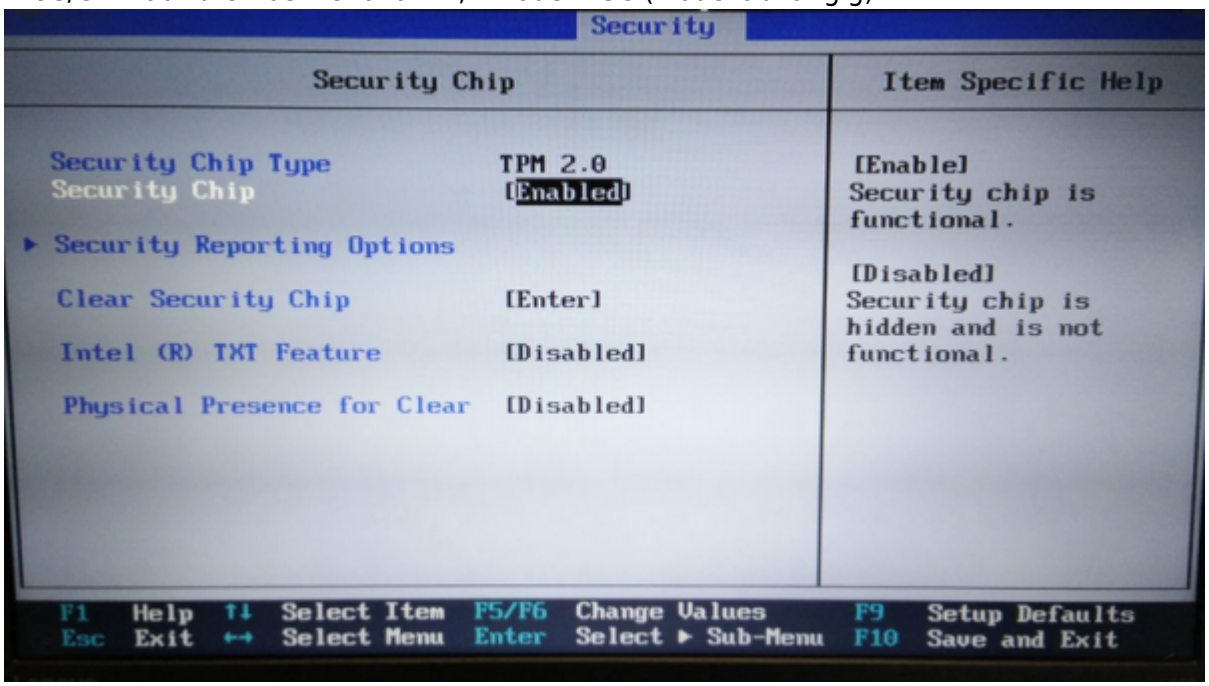
1. Sichern Ihrer persönlichen Daten bzw. des Systems!
2. Wird der Rechner von einer oder mehreren Personen genutzt?
   - Empfehlung bei Einzelnutzung: Entsperrung des Laufwerks durch ein Kennwort (s.u.)
   - Empfehlung bei Nutzung mit mehreren Personen: Entsperrung des Laufwerks mit einem USB-Speicherstick (s.u.)
3. Passwort für lokales Windows-Konto vergeben, falls noch nicht geschehen
4. Betriebssystem auf den neusten Stand aktualisieren (Windows-Update)
5. TPM-Status im BIOS/UEFI überprüfen - **Bitte aktivieren!** Die Abbildungen dienen lediglich als Hilfestellung. Je nach Modell kann die Darstellung im BIOS/UEFI abweichen.
   - BIOS/UEFI aufrufen bei Dell: F2



   - BIOS/UEFI aufrufen bei HP: F10



- BIOS/UEFI aufrufen bei Lenovo: F1, F2 oder ESC (Modellabhängig)



6. Lokale Gruppenrichtlinien für BitLocker anpassen (s.u.)
7. Kennwort/Pin für BitLocker ausdenken/erstellen
8. USB-Stick für Entschlüsselungs-Key bereithalten (nur sehr geringe Speicherkapazität erforderlich)
    - Für die Authentifikation mittels USB-Stick wird eine weiterer USB-Stick benötigt

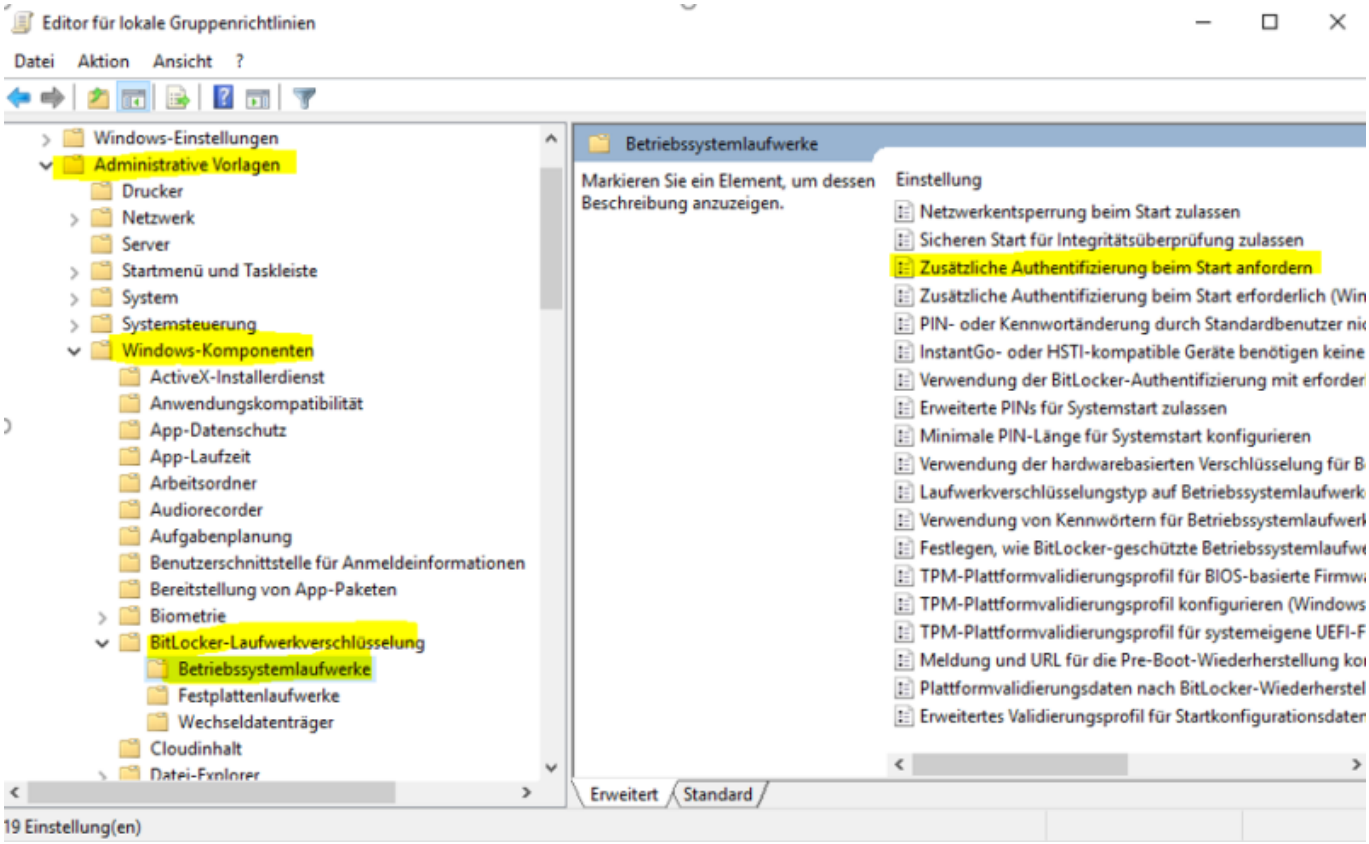
Einrichtung

Anpassung der lokalen Gruppenrichtlinien

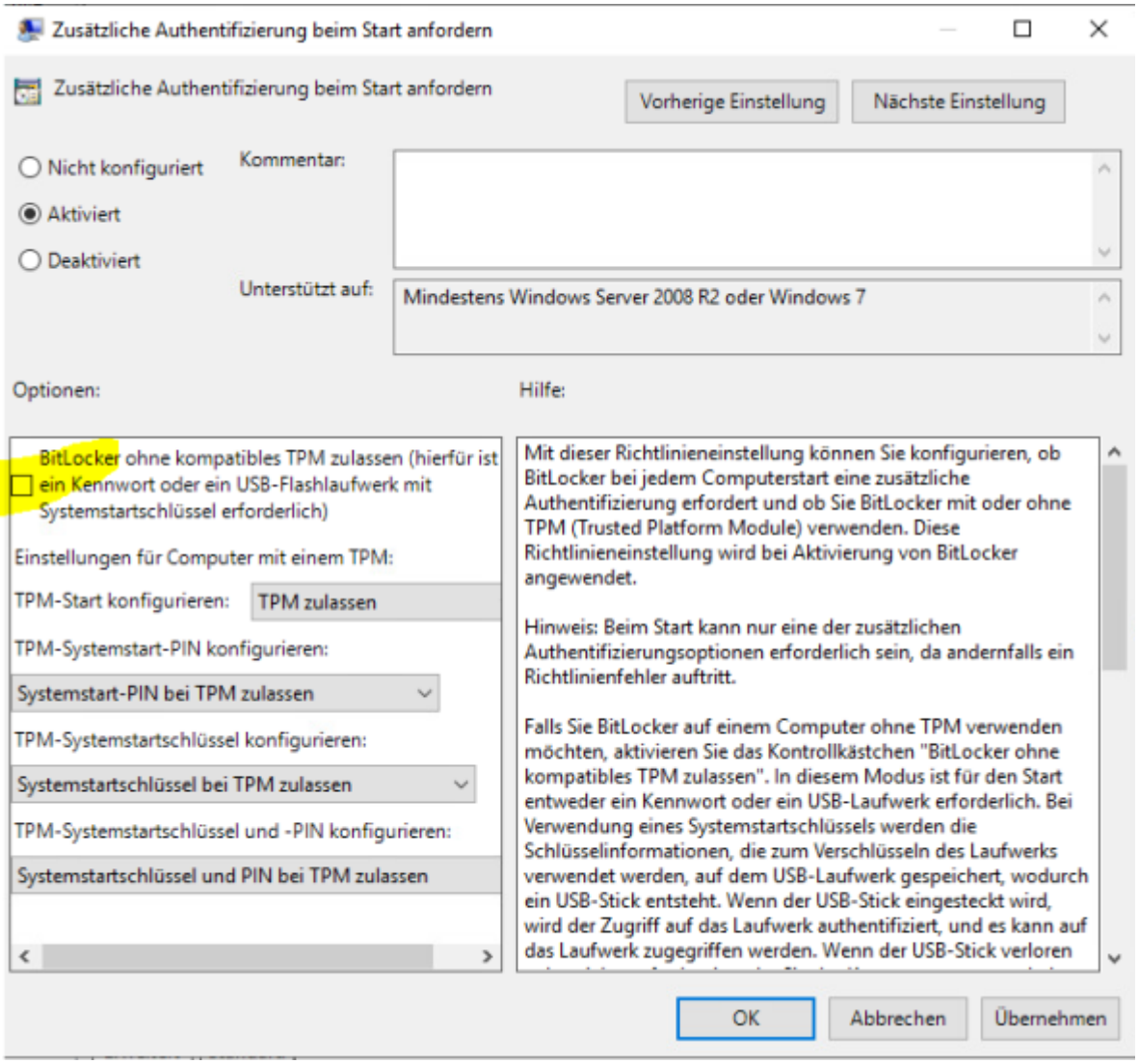
Vorgehensweise:

1. Öffnen Sie die lokalen Gruppenrichtlinien mit Eingabe von gpedit.msc in der Windows Suchmaske. Expandieren Sie anschließend in den Ordner Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → BitLocker Laufwerksverschlüsselung. Anschließend klicken Sie auf Betriebssystemlaufwerke.

2. Unter Betriebssystemlaufwerke öffnen Sie mit einem Doppelklick „Zusätzliche Authentifizierung beim Start anfordern“.

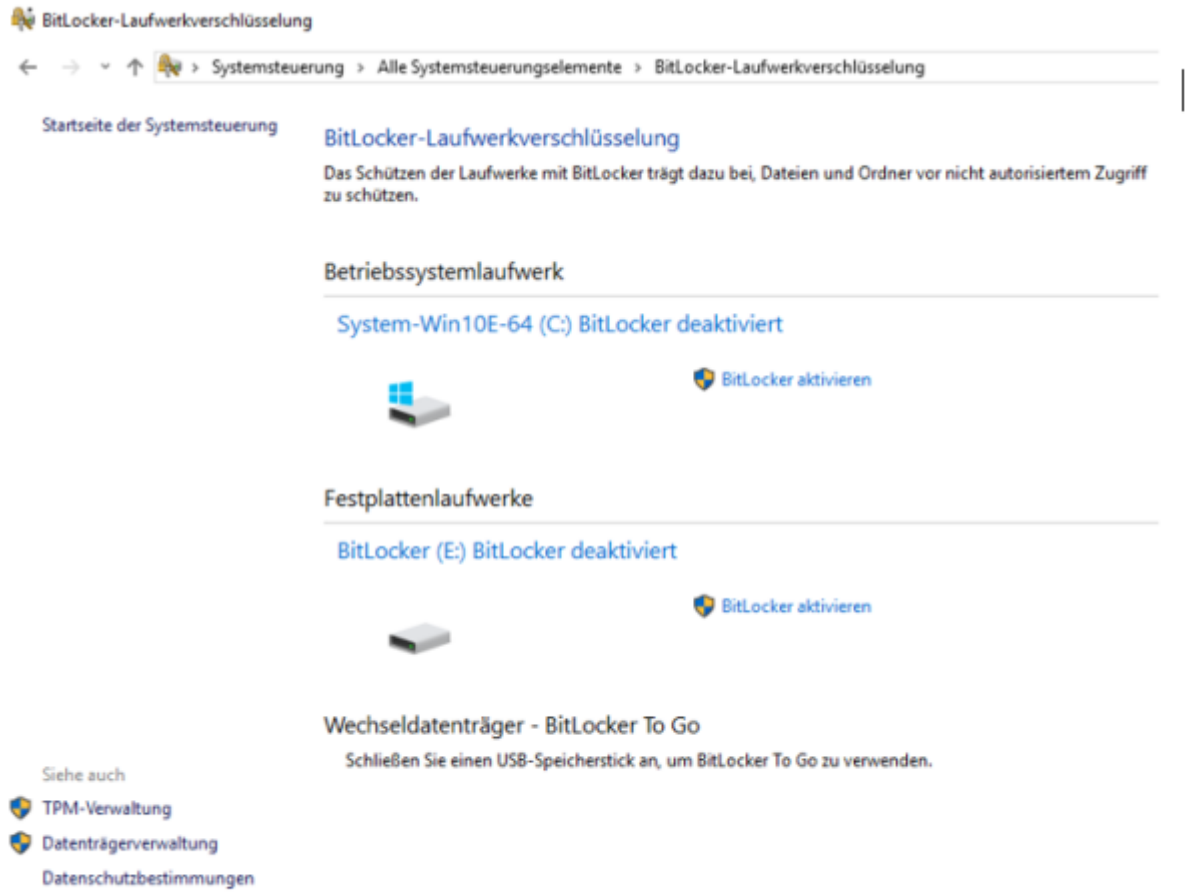


3. Aktivieren Sie die Option und stellen Sie sicher, dass bei „BitLocker ohne kompatibles TPM zulassen (…)“ **kein** Häkchen gesetzt ist. Nun übernehmen Sie die Auswahl und bestätigen mit „OK“.



Verschlüsselung

Öffnen Sie die BitLocker Verwaltung durch Eingabe von „BitLocker verwalten“ in die Windows Suchmaske. Aktivieren Sie BitLocker für das gewünschte Laufwerk in dem Sie auf „**BitLocker aktivieren**“ klicken.



Laufwerk auswählen [Bildquelle: Lennart Thurow]

Hinweis: Bitte beachten Sie, dass bei einer Verschlüsselung der Systemfestplatte ein vorher festgelegtes Kennwort während des Startvorgang des Rechners abgefragt wird. Falls eine Festplatte oder Partition verschlüsselt wird, die lediglich als Datenspeicher fungiert, so erfolgt hier keine Abfrage eines Kennworts.

Festlegen, wie das Laufwerk beim Start entsperrt werden soll

Wählen Sie hier

- USB-Speicherstick anschließen - bei Nutzung mit mehreren Personen
- Pin eingeben - bei Einzelnutzung

Pin zum Entsperren des Laufwerks erstellen

Bedingt durch den Versionsstand von Windows 10 können verschiedene Möglichkeiten angeboten werden, das Laufwerk zu entsperren. Seitens des Hochschulrechenzentrums wird lediglich die Nutzung einer Pin bzw eines Sticks angeboten.

Wie soll der Wiederherstellungsschlüssel gesichert werden

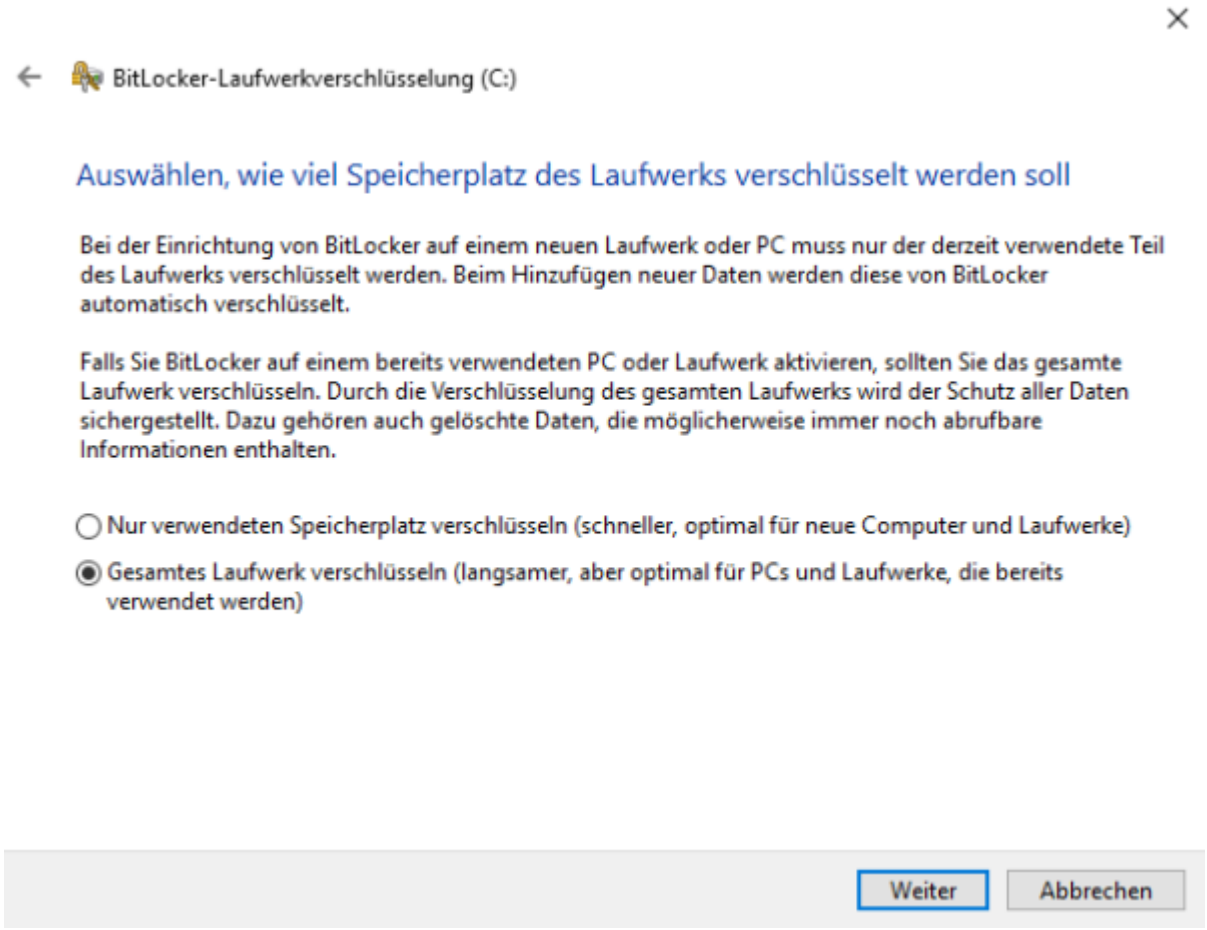
- Möglichkeit 1: Auf USB-Speicherstick speichern
  - Verwenden Sie diesen jedoch nur zur Sicherung des Wiederherstellungsschlüssels, nicht für andere Aufgaben
- Möglichkeit 2: **In Datei speichern (Empfehlung des HRZ)**
  - Speichern Sie die Wiederherstellungsdatei in einem Ort außerhalb Ihres PCs (z.B. Laufwerk Z:\)

- Möglichkeit 3: Wiederherstellungsschlüssel drucken
    - Ausdruck auf Papier

Der Wiederherstellungsschlüssel darf sich niemals auf dem verschlüsselten Gerät befinden. Je nach Version und Versionsstand von Windows 10 kann es vorkommen, dass angeboten wird den Wiederherstellungsschlüssel auf einem Microsoft-Konto zu speichern - wovon wir abraten. Grundsätzlich ist es empfehlenswert den Schlüssel auf einem Medium zu speichern, welches nicht jederzeit erreichbar ist.

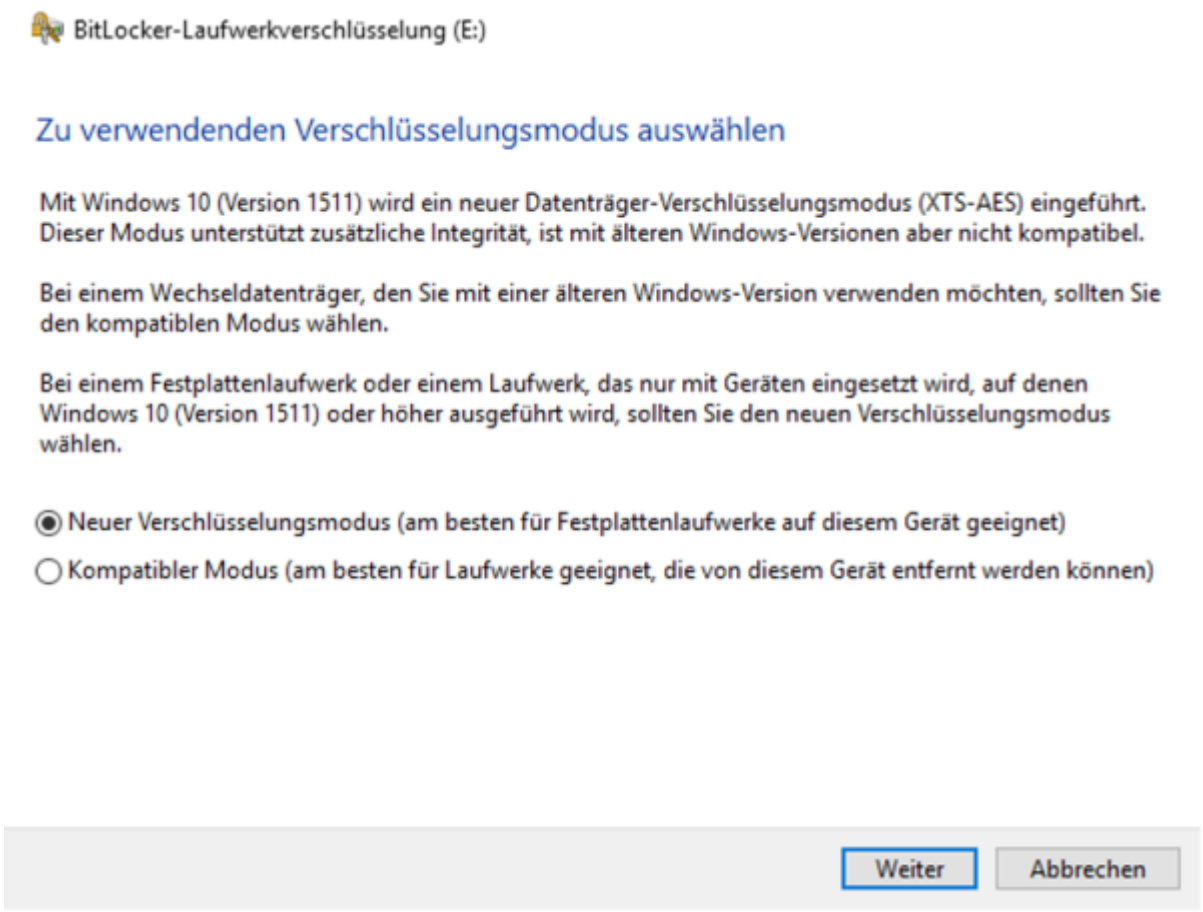
Auswählen, wie viel Speicherplatz des Laufwerks verschlüsselt werden soll

Wählen Sie hier die Option „**Gesamtes Laufwerk verschlüsseln**“



Zu verwendenden Verschlüsselungsmodus auswählen

Wählen Sie hier die Option „**Neuer Verschlüsselungsmodus**“



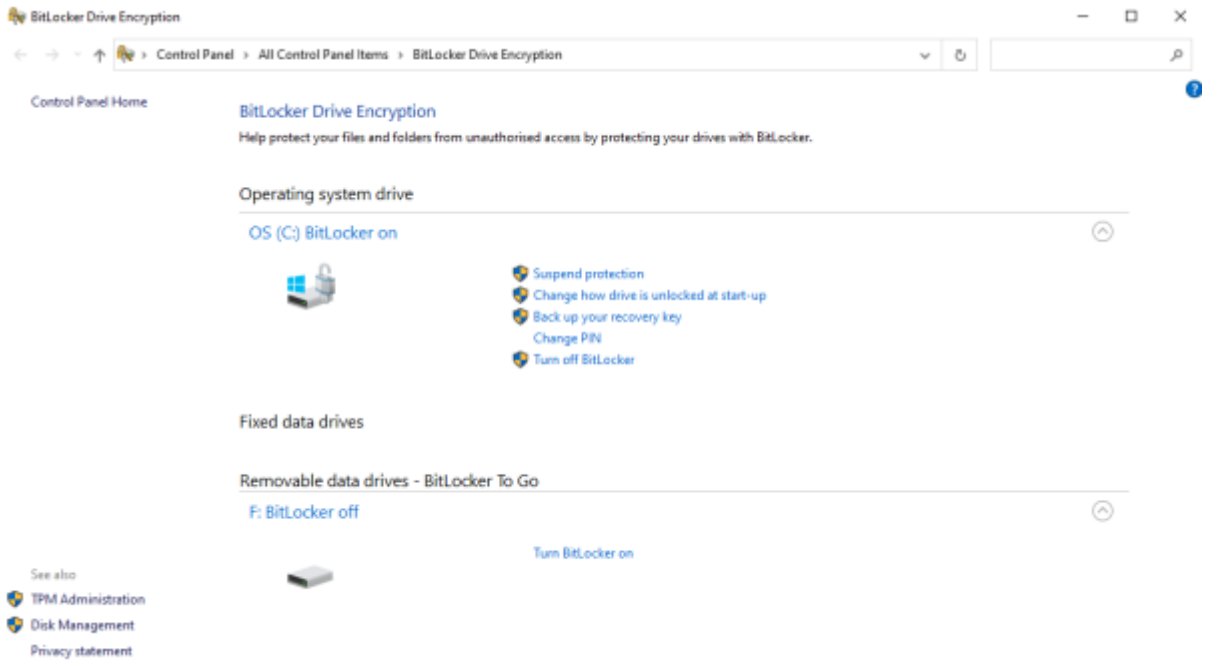
Möchten Sie das Laufwerk jetzt verschlüsseln?

Aktivieren Sie die Option „BitLocker-Systemüberprüfung ausführen“ und folgen Sie den Anweisungen. Der Computer muss dann zur BitLocker-Laufwerksverschlüsselung neu gestartet werden.

Optionen

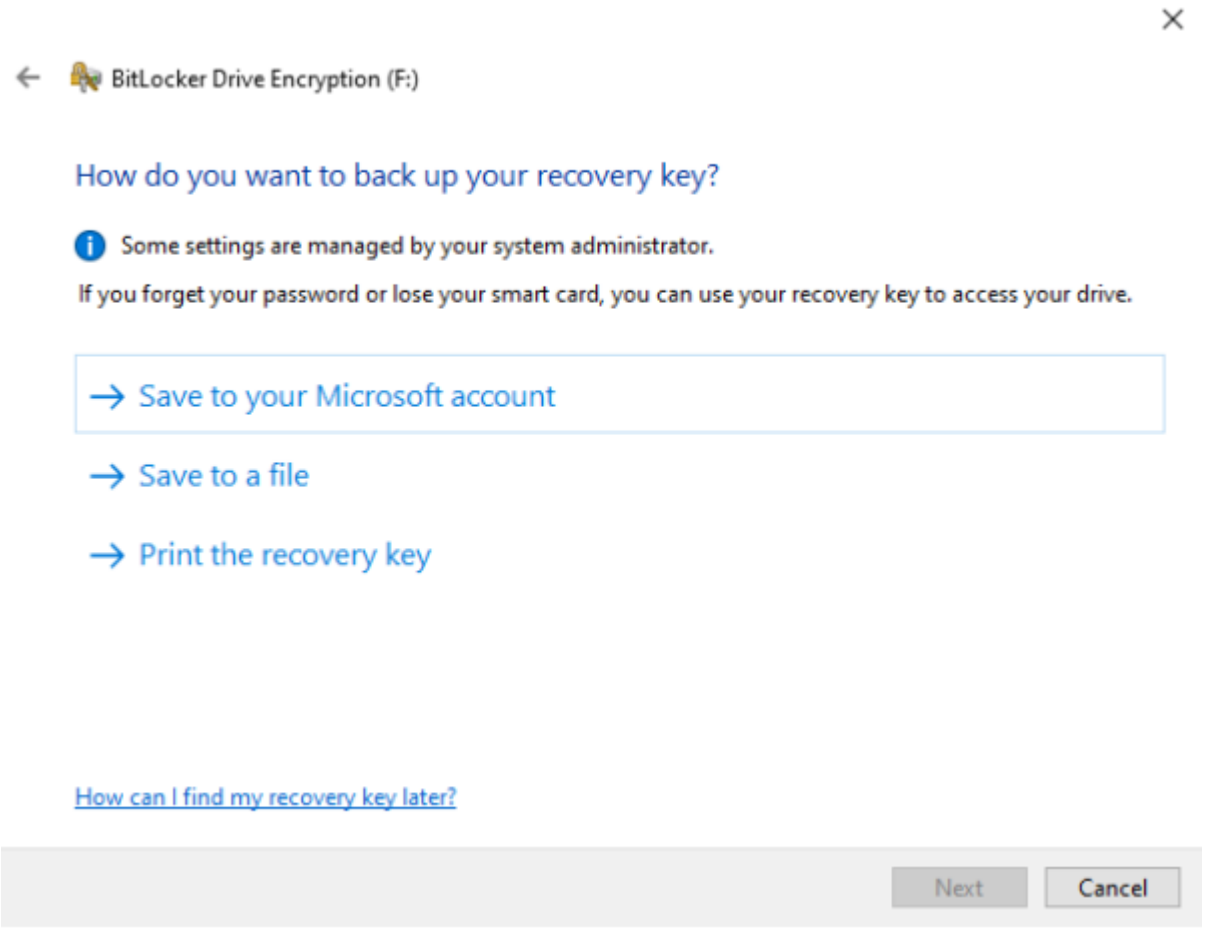
Verschlüsselung von externen Datenträgern

1. Bitlocker auf entsprechenden Laufwerk aktivieren

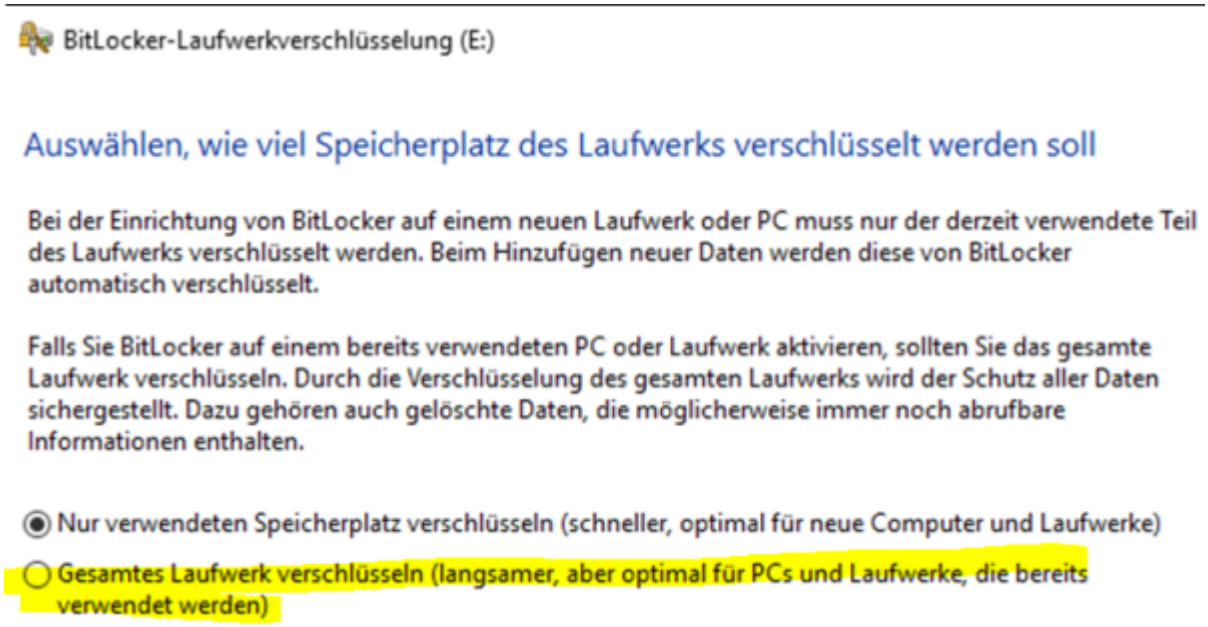


2. Passwort eingeben und auf weiter klicken

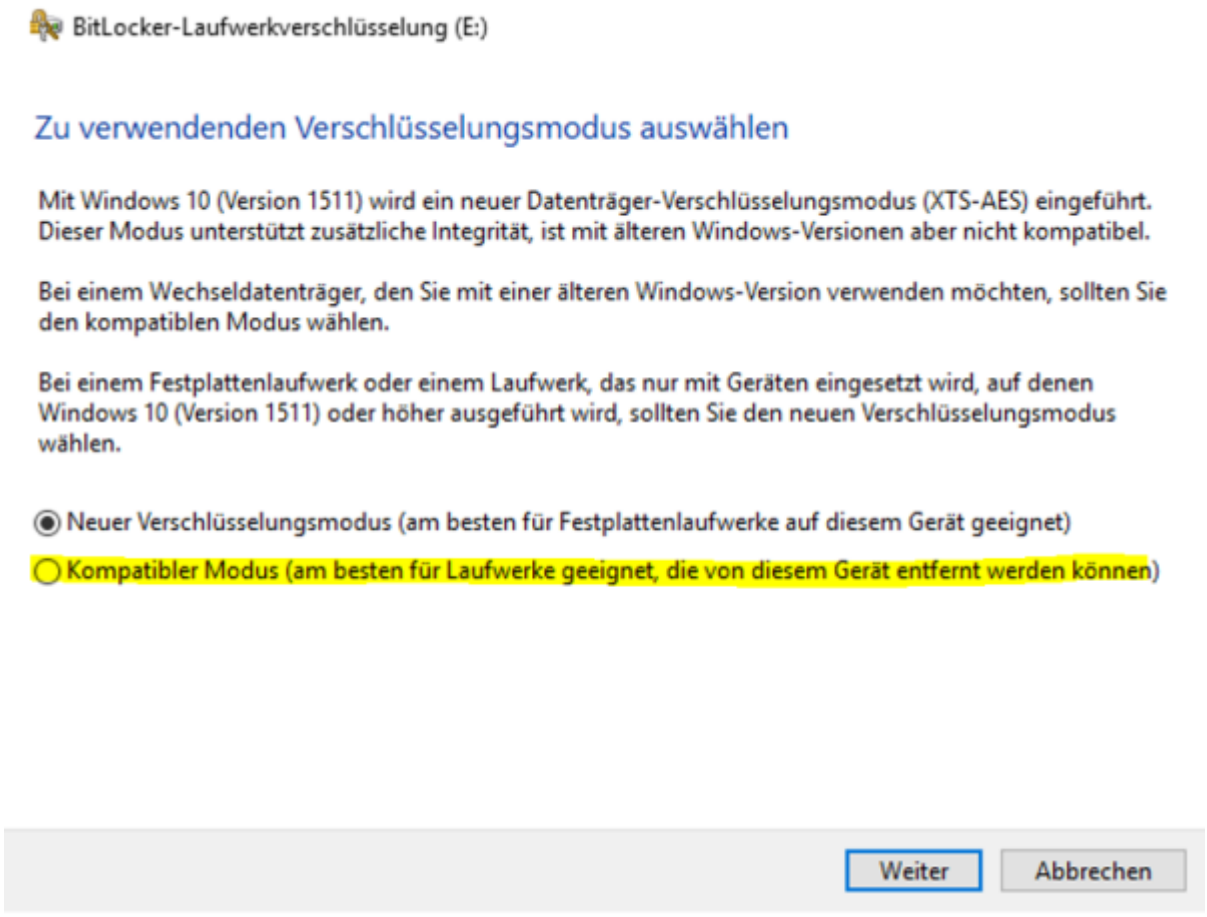
3. Recovery-Key drucken und auf einem externen Datenträger speichern. Dieser Datenspeicher sollte ausschließlich zur Verwahrung des Recovery-Keys dienen. Beachten Sie bitte auch die Möglichkeit unserer Verwahrfunktion unter Laufwerk „x“ **(Siehe Abschnitt: „Wie soll der Wiederherstellungschlüssel gespeichert werden“)**



4. Bitte wählen Sie „gesamtes Laufwerk verschlüsseln“ aus.



5. Wählen Sie bitte den kompatiblen Modus aus.



6. Vorgang bestätigen. Abschließend ist Ihr externer Datenträger verschlüsselt

Entschlüsselung von Laufwerken

Um das Laufwerk zu entschlüsseln müssen Sie auf weitere Optionen klicken und anschließend „Wiederherstellungsschlüssel eingeben“ wählen.

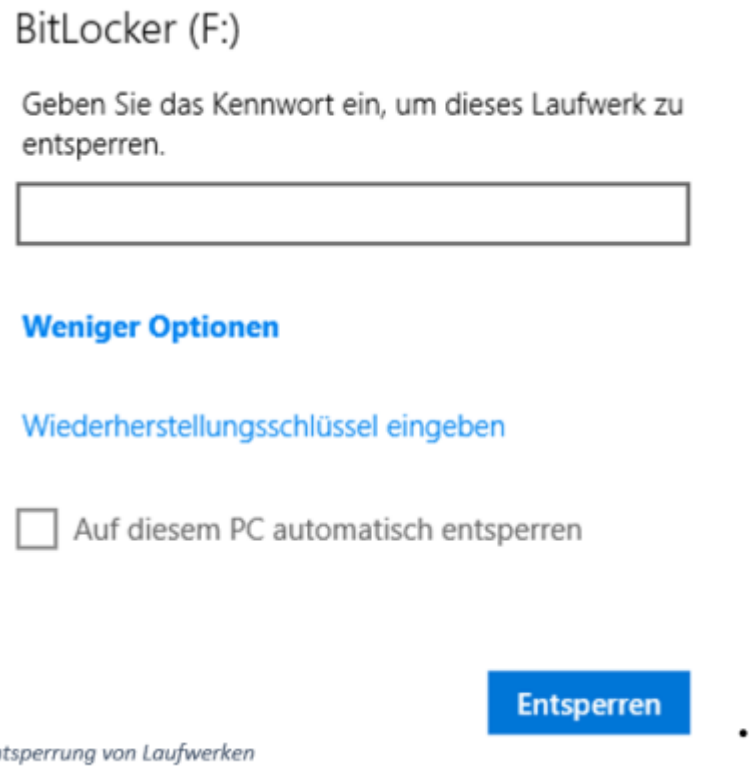
Info: Falls Sie bereits vorher das Kennwort zum Entsperren des Laufwerks eingegeben haben oder das Laufwerk automatisch entsperrt wird, ist bei einer anschließenden Entschlüsselung die Eingabe des Wiederherstellungsschlüssels nicht notwendig und auch nicht möglich*.

BitLocker kann dementsprechend mit Eingabe des Kennwortes komplett deaktiviert werden, ohne dass eine zusätzliche Kennung/Identifizierung notwendig ist. Deaktivierung ist in diesem Fall mit Entschlüsselung gleich zu setzen.

*bezieht sich auf einen Benutzer mit Administratorrechten. Die Deaktivierung von BitLocker kann durch Beschränkung der Rechte eines Standardbenutzers unterbunden werden.

Entsperrung von Laufwerken

- Sie können die automatische Entsperrung eines Laufwerkes aktivieren oder deaktivieren. Hierfür rufen Sie mit Rechtklick auf das Laufwerk „BitLocker verwalten“ auf
- Entsperrung durch Doppelklick auf das Laufwerk und Eingabe des Kennworts (Falls es sich nicht um eine Systempartition handelt)
- Automatische Entsperrung des Laufwerks bei bestimmten Rechnern. Hierfür wird das Häkchen bei „Auf diesem PC automatisch entsperren“ gesetzt und durch Eingabe des Passworts bestätigt



Entsperrung von Laufwerken

Systemstartschlüssel auf mehreren USB-Speichersticks speichern

Öffnen Sie mit Rechtsklick auf einem mit BitLocker geschütztem Laufwerk das Menü „BitLocker verwalten“. Hier kann der Systemstartschlüssel dupliziert werden. Alternativ lässt sich die Datei auch kopieren. Diese ist standardmäßig allerdings als Systemdatei markiert und daher ausgeblendet.

Informationen

Quellen