Verschlüsselung mit bitlocker

1. automatisch
2. manuell bei Anwesenheit im Institut – Systempartition
3. manuell bei Anwesenheit im Institut - Datenpartition
4. manuell außerhalb des KIT (z.B. im Home Office) – Systempartition
5. manuell außerhalb des KIT - Datenpartition

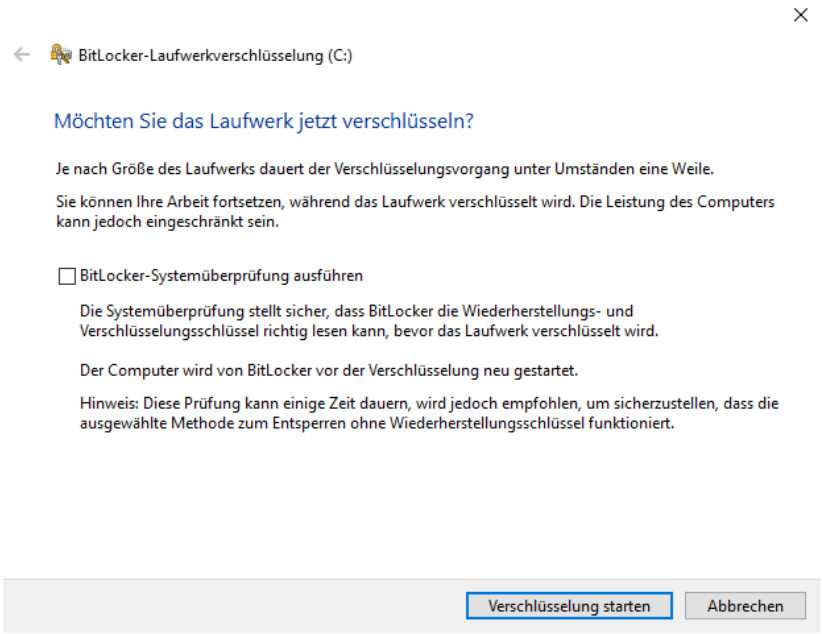
Ergänzende Hinweise findet man am Ende des Dokuments.

1. **automatisch**:
   Dies ist der einfachste Weg. Es wird nur die Systempartition verschlüsselt, evtl. weitere vorhandene Datenpartitionen müssen aber manuell verschlüsselt werden (siehe unter 3.).
   Der Rechner muss kabelgebunden im KIT-LAN hängen (kein WLAN und kein VPN).

   a. kurze Meldung an mich (Rechner muss in eine spezielle OU (Organisationseinheit) im AD verschoben werden)
   b. Rechner im KIT kabelgebunden ins LAN hängen
   c. Rechner im KIT-LAN neu starten (wecken aus Ruhemodus reicht nicht). Der Neustart muss evtl. zweimal durchgeführt werden.
   d. Nach dem 2. Boot im KIT-LAN erfolgt eine automatische Verschlüsselung der Systempartition.

2. **Manuelle Verschlüsselung der Systempartition im Institut**:
   Der Rechner hängt kabelgebunden im KIT-LAN. Der Anwender muss über ein lokales Administrator-Konto verfügen

   a. Rechner im KIT-LAN neu starten (wecken aus dem Ruhemodus reicht nicht)
   b. Datei-Explorer öffnen
   c. Rechtsklick auf die Systempartition (normalerweise ist dies C:)
   d. Im Kontextmenü „Bitlocker aktivieren“ auswählen, Administratorkonto eingeben.
   e. es erscheint folgendes Fenster:

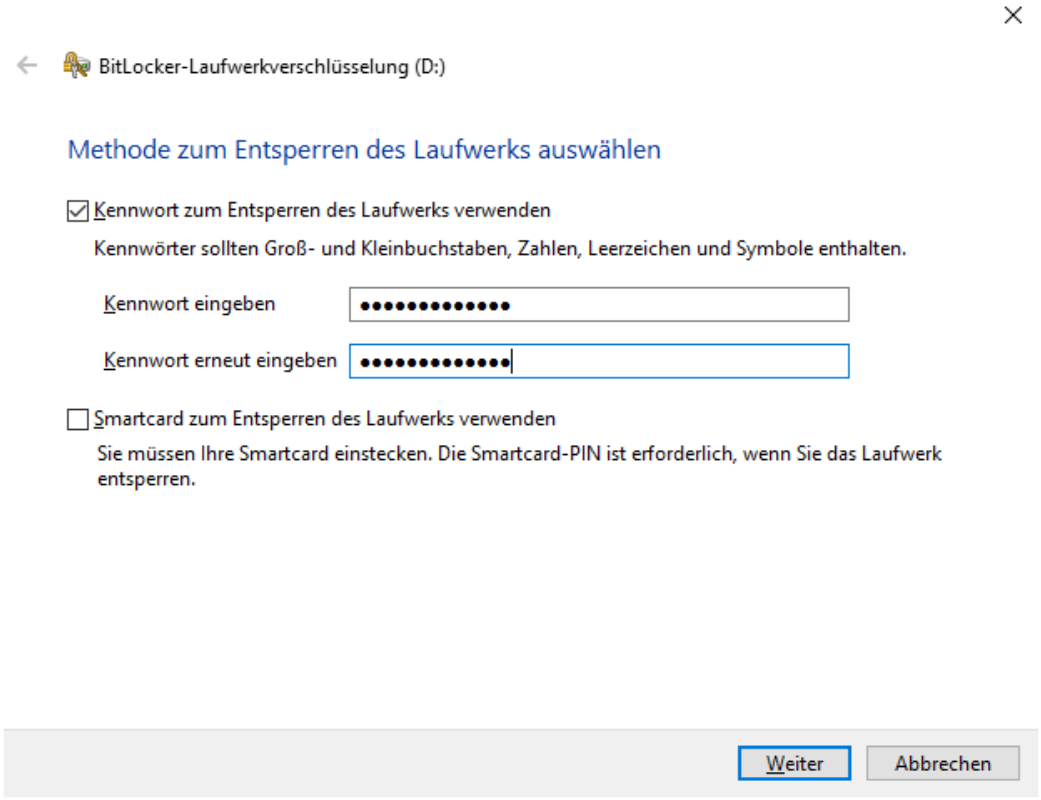


   die Bitlocker-Systemüberprüfung kann ausgewählt werden.

f. auf „Verschlüsselung starten“ klicken. Ohne „Systemüberprüfung“ startet die Verschlüsselung direkt, mit Systemüberprüfung muss der Rechner noch einmal neu gestartet werden und wird erst nach dem Neustart verschlüsselt.

3. **manuelle Verschlüsselung einer Datenpartition im Institut**:
Der Rechner hängt kabelgebunden im KIT-LAN. Der Anwender muss über ein lokales Administrator-Konto verfügen

   a. Rechner im KIT-LAN neu starten (wecken aus dem Ruhemodus reicht nicht), sofern nicht bereits die Systempartition verschlüsselt wurde.
   b. Datei-Explorer öffnen
   c. Rechtsklick auf die Datenpartition
   d. Im Kontextmenü „Bitlocker aktivieren“ auswählen, Administratorkonto eingeben.
   e. Kennwort für die Entschlüsselung eingeben:



   f. Der Schlüssel wird automatisch im AD abgelegt, man kann ihn aber auch für sich selbst speichern. Wenn man den Schlüssel speichert oder druckt, für einen sicheren Ablageort sorgen.
   g. Verschlüsselung starten

4. **Manuelle Verschlüsselung der Systempartition von zu Hause / außerhalb des KIT-Netzes**:
Der Anwender muss über ein lokales Administrator-Konto verfügen.

   a. VPN-Verbindung ins KIT herstellen
   b. CMD-Fenster öffnen (z.B. indem im Suchfeld cmd eingegeben und dann Enter gedrückt wird).
   c. im CMD-Fenster den Befehl „gpupdate /force“ eingeben. Nach einer Weile sollten zwei „erfolgreich“ Meldungen angezeigt werden

```
U:\>gpupdate /force
Die Richtlinie wird aktualisiert...

Die Aktualisierung der Computerrichtlinie wurde erfolgreich abgeschlossen.
Die Aktualisierung der Benutzerrichtlinie wurde erfolgreich abgeschlossen.
```

Erscheint stattdessen eine Fehlermeldung, bitte zuerst prüfen, ob die VPN-Verbindung aktiv ist (OpenVPN-Symbol ist grün?) und wenn ja, den Befehl nochmal durchführen. Sollte danach immer noch eine Fehlermeldung erscheinen, diese bitte an mich weitergeben und die Verschlüsselung nicht fortsetzen.

d. Nach erfolgreicher Aktualisierung der Richtlinien muss der Rechner neu gestartet werden.

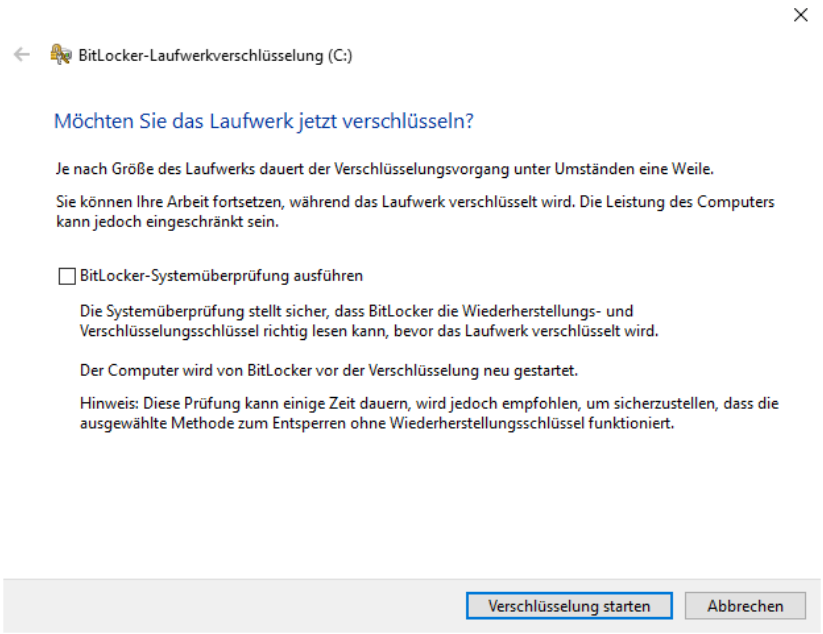
e. Nach dem Neustart wieder eine VPN-Verbindung herstellen.

f. Datei-Explorer öffnen

g. Rechtsklick auf die Systempartition (normalerweise ist dies C:)

h. Im Kontextmenü „Bitlocker aktivieren“ auswählen, Administratorkonto eingeben.

i. es erscheint folgendes Fenster:



die Bitlocker-Systemüberprüfung kann ausgewählt werden.

j. auf „Verschlüsselung starten“ klicken. Ohne „Systemüberprüfung“ startet die Verschlüsselung direkt, mit Systemüberprüfung muss der Rechner noch einmal neu gestartet werden und wird erst nach dem Neustart verschlüsselt

5. **Manuelle Verschlüsselung einer Datenpartition außerhalb des KIT-Netzes:**
Der Anwender muss über ein lokales Administrator-Konto verfügen.

a. VPN-Verbindung ins KIT herstellen

b. nur nötig, wenn nicht bereits die Systempartition nach Anleitung verschlüsselt wurde: CMD-Fenster öffnen (z.B. indem im Suchfeld cmd eingegeben und dann Enter gedrückt wird).

c. nur nötig, wenn nicht bereits die Systempartition nach Anleitung verschlüsselt wurde: im CMD-Fenster den Befehl „gpupdate /force“ eingeben. Nach einer Weile sollten zwei „erfolgreich“ Meldungen angezeigt werden

```
U:\>gpupdate /force
Die Richtlinie wird aktualisiert...

Die Aktualisierung der Computerrichtlinie wurde erfolgreich abgeschlossen.
Die Aktualisierung der Benutzerrichtlinie wurde erfolgreich abgeschlossen.
```

Erscheint stattdessen eine Fehlermeldung, bitte zuerst prüfen, ob die VPN-Verbindung aktiv ist (OpenVPN-Symbol ist grün?) und wenn ja, den Befehl nochmal durchführen. Sollte danach immer noch eine Fehlermeldung erscheinen, diese bitte an mich weitergeben und die Verschlüsselung nicht fortsetzen.

d. nur nötig, wenn nicht bereits die Systempartition nach Anleitung verschlüsselt wurde: nach erfolgreicher Aktualisierung der Richtlinien muss der Rechner neu gestartet werden.

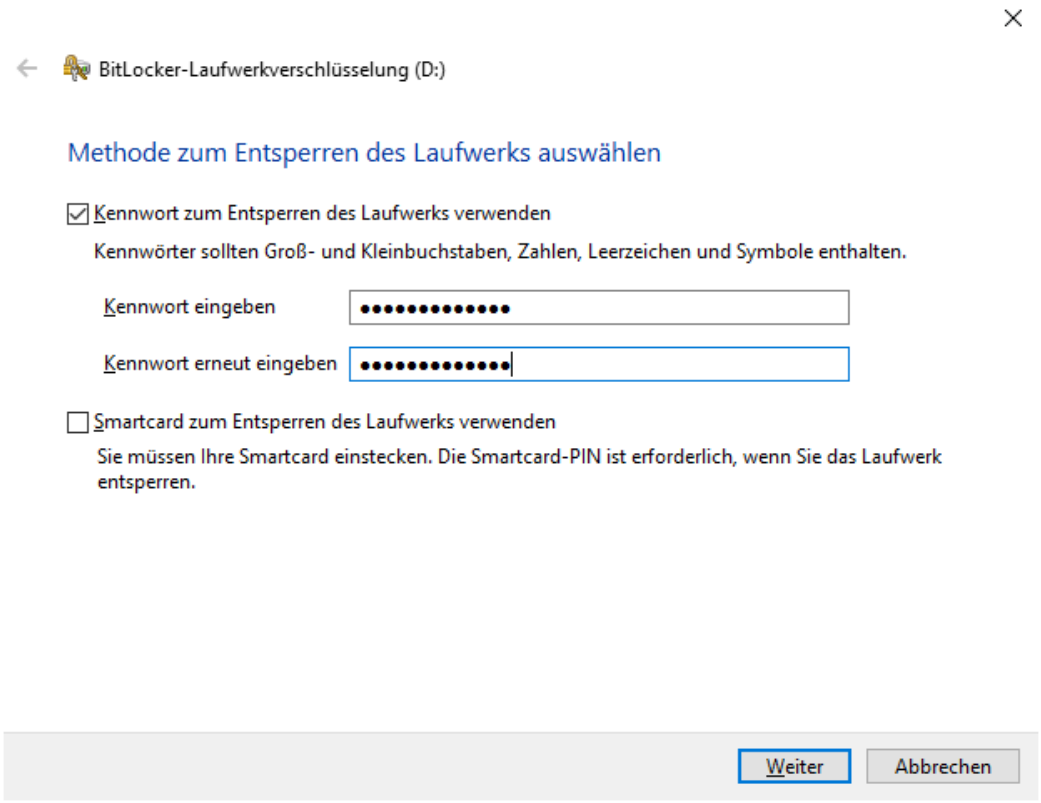
e. nur nötig, wenn nicht bereits die Systempartition nach Anleitung verschlüsselt wurde: nach dem Neustart wieder eine VPN-Verbindung herstellen.

f. Datei-Explorer öffnen

g. Rechtsklick auf die Datenpartition

h. im Kontextmenü „Bitlocker aktivieren“ auswählen, Administratorkonto eingeben.

i. Kennwort für die Entschlüsselung eingeben:

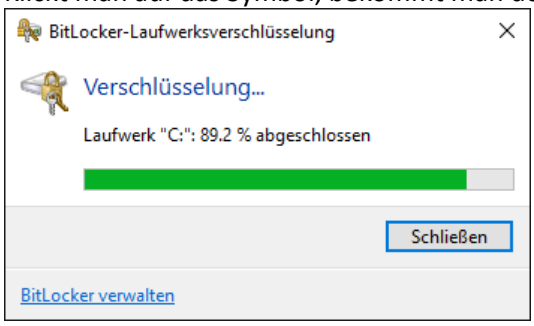


j. Der Schlüssel wird automatisch im AD abgelegt, man kann ihn aber auch für sich selbst speichern. Wenn man den Schlüssel speichert oder druckt, für einen sicheren Ablageort sorgen.

k. Verschlüsselung starten

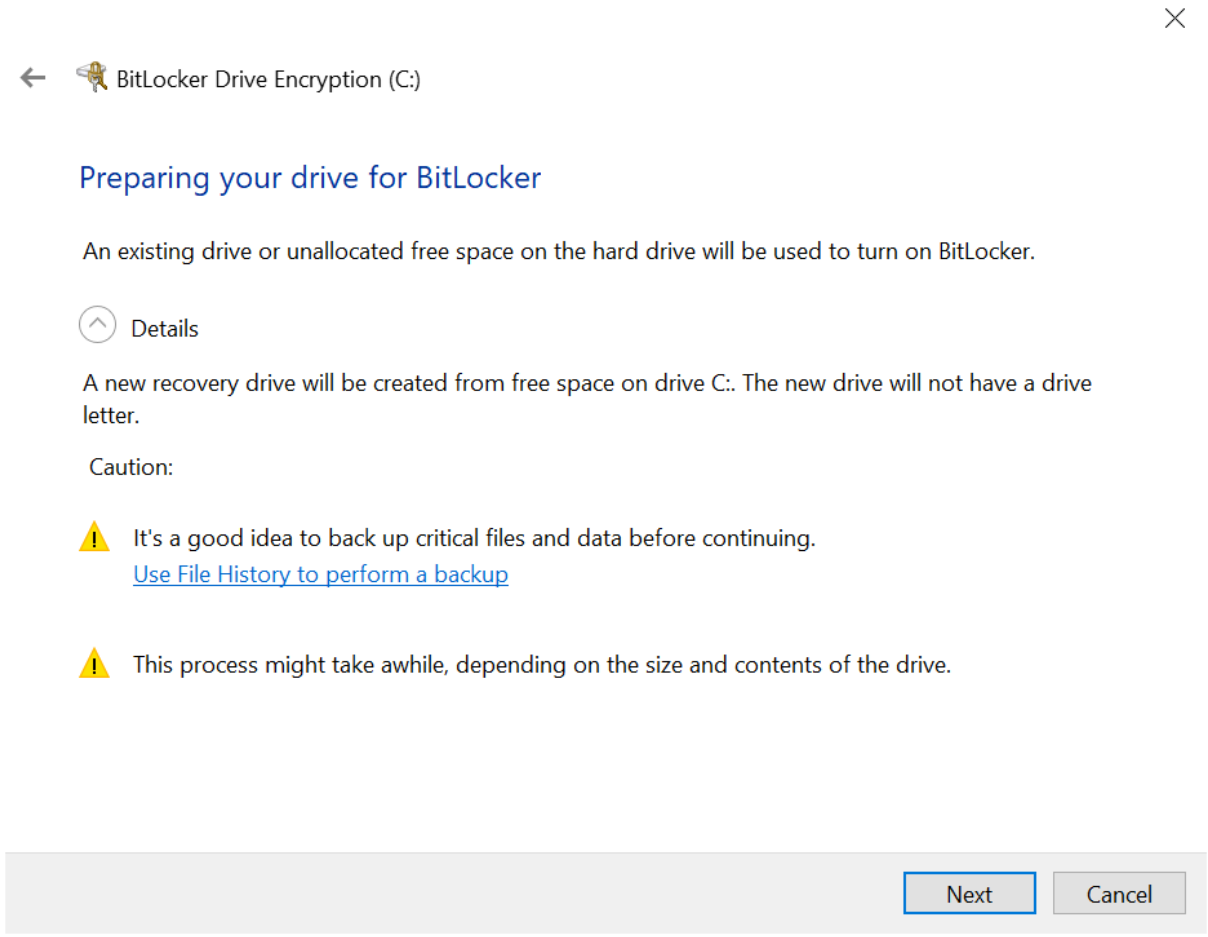
Weitere Hinweise:

- **Während des Verschlüsselung-Prozesses** erscheint in der Taskleiste ein Symbol:
  Klickt man auf das Symbol, bekommt man den Status angezeigt:



- Zu Beginn der Verschlüsselung kann eine Meldung erscheinen, dass **TPM aktiviert** werden müsse. Durch Klick auf weiter wird dies evtl. automatisch durchgeführt. Es kann aber auch sein, dass man dies im BIOS des Rechners manuell aktivieren muss. Gern bin ich behilflich bei der Suche, wo im jeweiligen BIOS diese Einstellung zu finden ist.

- Im manuellen Prozess kann ein weiteres Fenster erscheinen, das die Notwendigkeit **einer weiteren Wiederherstellungspartition** mitteilt, weshalb das Laufwerk C: verkleinert werden müsse. Diese ist ca. 1GB groß, kann und sollte also akzeptiert werden, da nur mit dieser Wiederherstellungspartition eine Verschlüsselung möglich ist.
  Leider habe ich aktuell nur eine englische Version dieses Fensters vorliegen:



- Nach der Verschlüsselung einer **Datenpartition** kann man diese beim Systemstart auch **automatisch entsperren** lassen (ansonsten wir nach jedem Systemstart beim ersten Zugriff auf die Datenpartition das beim Verschlüsseln eingegebene password verlangt).
  - Datei Explorer starten
  - Rechtsklick auf die verschlüsselte Datenpartition
  - Bitlocker verwalten auswählen
  - „automatische Entsperrung aktivieren“ anklicken:

An dieser Stelle kann die automatische Entsperrung auch wieder deaktiviert werden.

- Nach Rücksprache mit mir ist der **automatische Weg auch im Home Office** möglich.

- **Die Verschlüsselung ist für den Benutzer transparent**. Solange die Systemplatte nicht ausgebaut wird, wird sie beim Bootvorgang automatisch entschlüsselt. Sollte jemand die Platte ausbauen (müssen) und von anderer Stelle auf die Platte zugreifen müssen, wird der Schlüssel erforderlich.

- Es kann vorkommen, dass **beim Booten nach dem Schlüssel gefragt** wird. Dies kann z.B. dann der Fall sein, wenn zwischendurch von einem anderen Gerät versucht wurde zu booten. In diesem Fall reicht es normalerweise, wenn der Rechner einfach nochmal gebootet wird.

- Der Schlüssel kann von jedem auch selbst abgespeichert werden:
  - Datei Explorer starten
  - Rechtsklick auf die Partition, von der der Schlüssel gespeichert werden soll
  - Bitlocker verwalten auswählen
  - Wiederherstellungsschlüssel sichern auswählen

  - Anmeldedaten eines Admin-Kontos eingeben
  - Gewünschte Speichermöglichkeit auswählen. In jedem Fall muss der Speicherort sicher gegen fremden Zugriff sein.

- Im IMK-ASF sorgt eine GPO (Gruppenrichtlinie) dafür, dass bei einer Festplattenverschlüsselung der Schlüssel im AD (Active Directory) abgelegt wird.