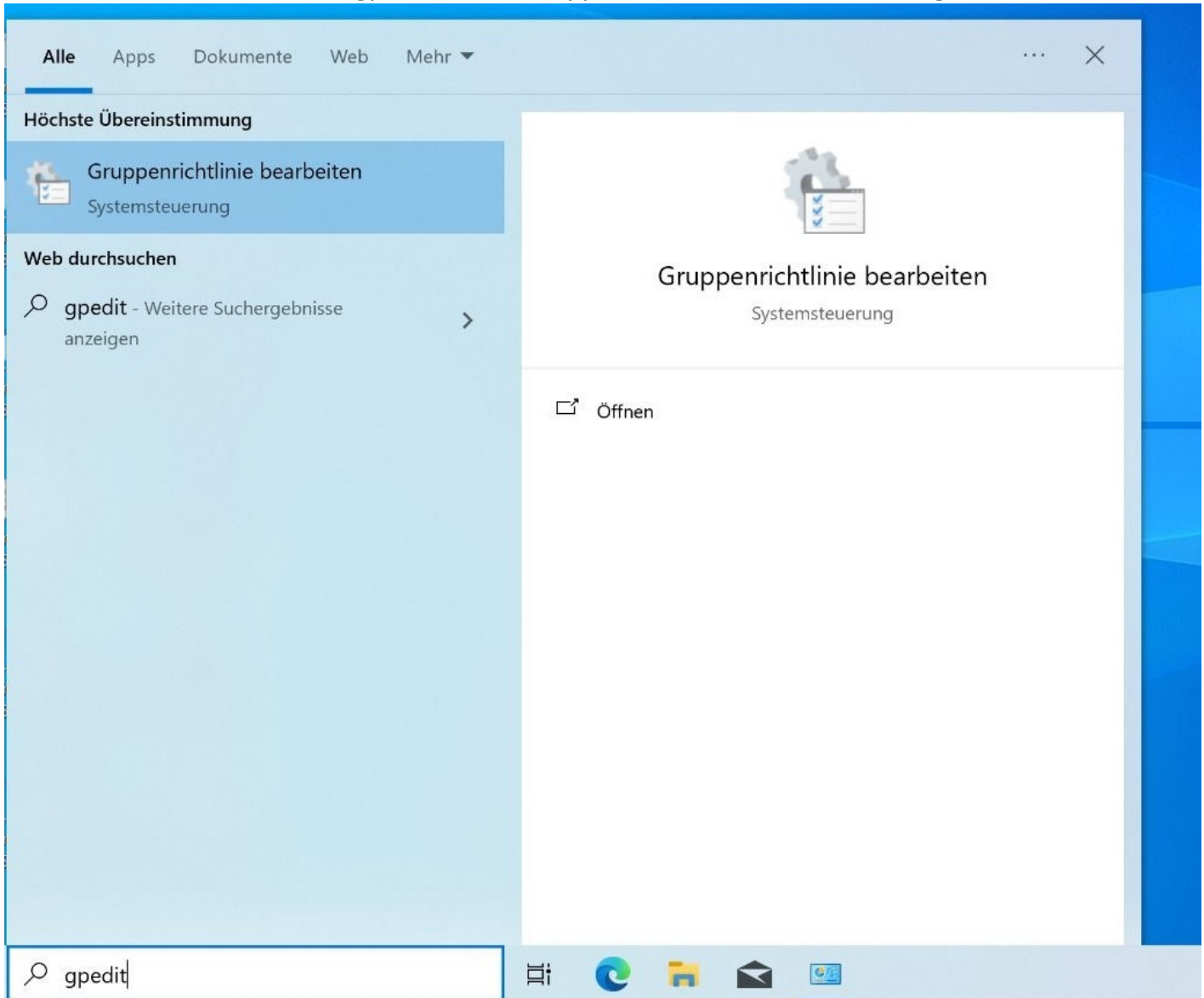
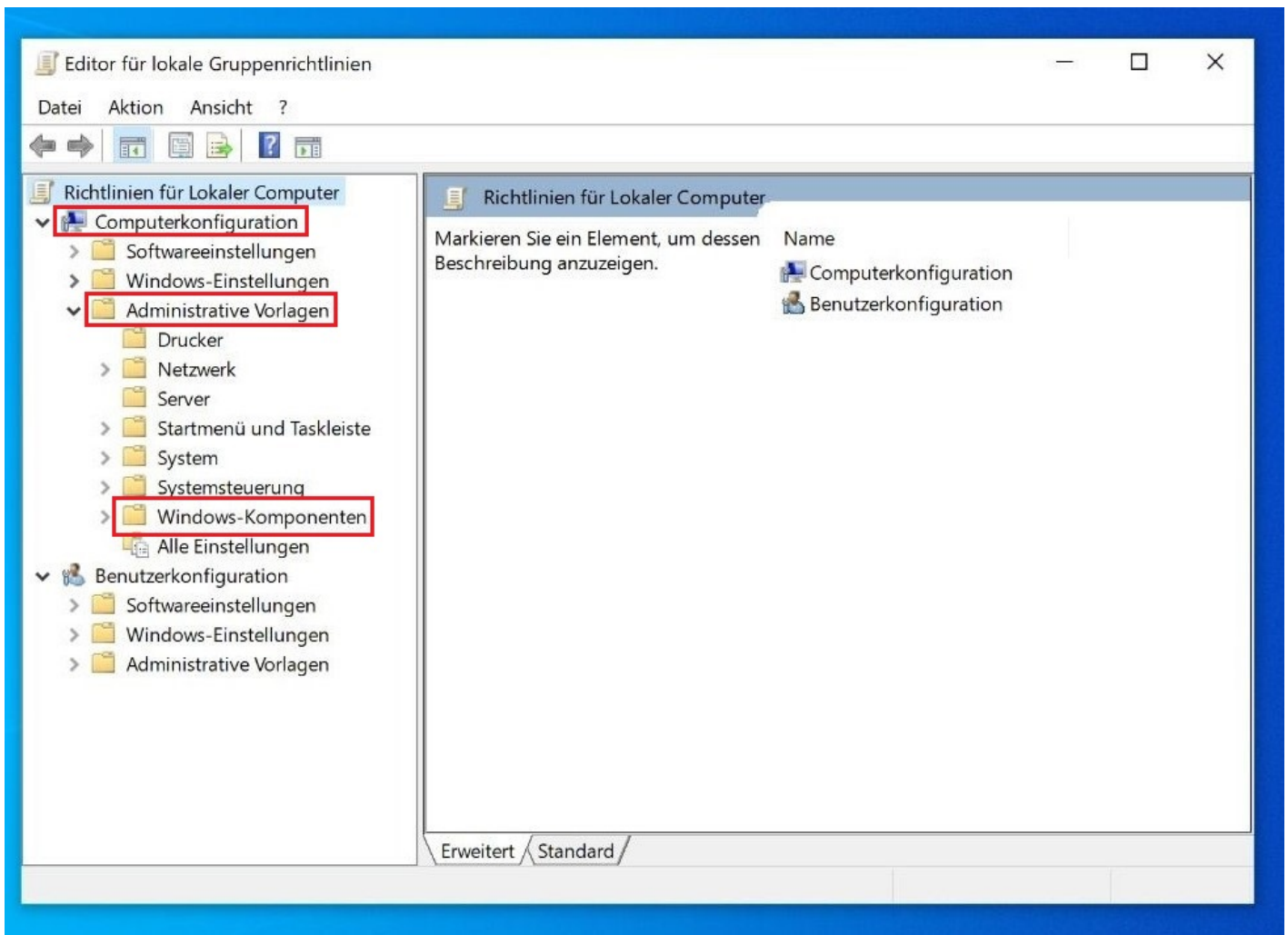


Bitlocker Pin einrichten

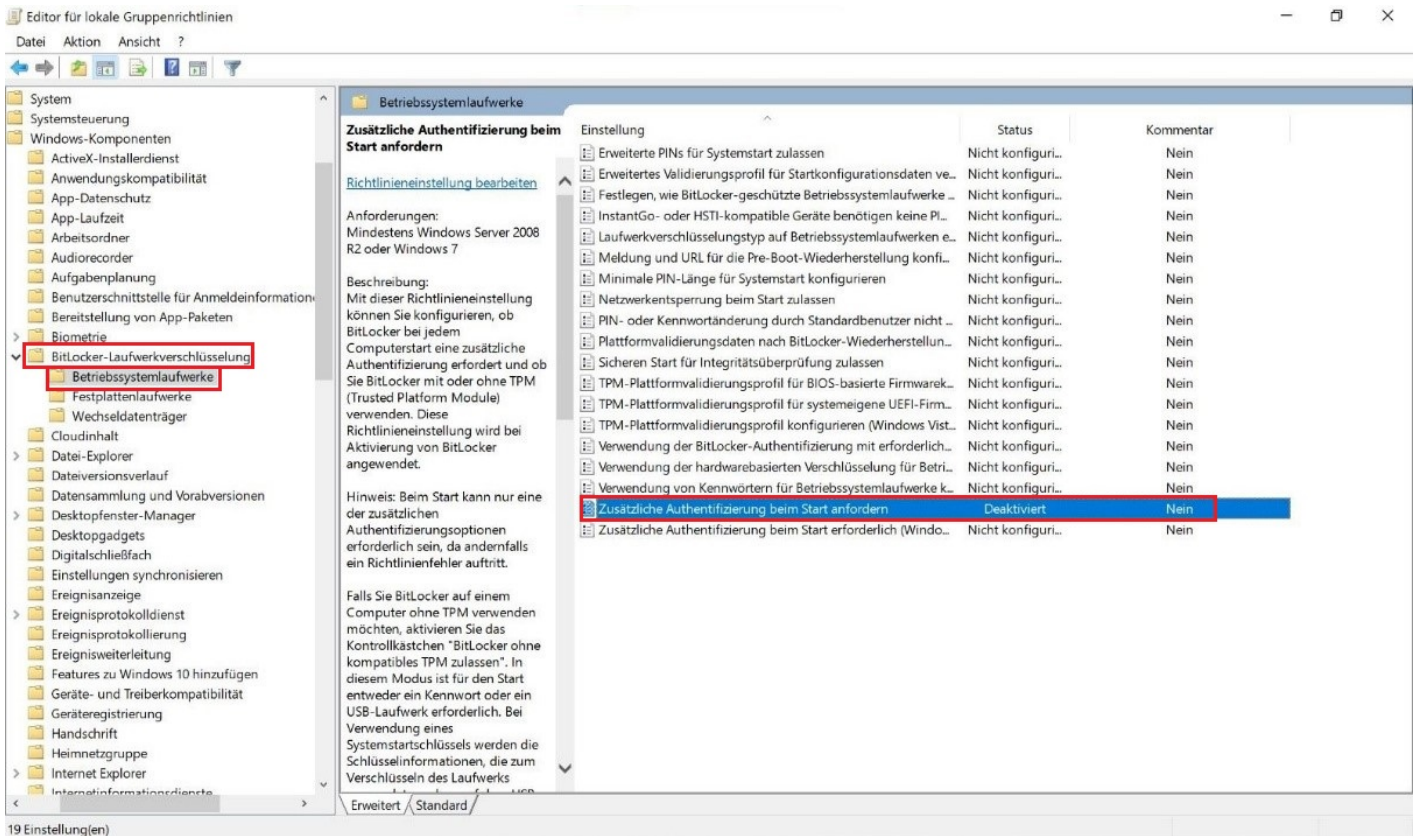
Schritt 1: In die Suchleiste „gpedit“ oder „Gruppenrichtlinie bearbeiten“ eingeben.



Schritt 2: Das Fenster "Editor für lokale Gruppenrichtlinien" öffnet sich. Dort Navigiert man zu "Computerkonfiguration" -> "Administrative Vorlagen" -> "Windows-Komponenten" ->



"Bitlocker-Laufwerksverschlüsselung" -> "Betriebssystemlaufwerke" -> doppelklick auf "Zusätzliche Authentifizierung beim Start anfordern"



Schritt 3: Es öffnet sich folgendes Fenster. Das Modul oben links auf "Aktiviert" setzen und in den Optionen „Start Pin bei TPM erforderlich“ auswählen und mit "OK" bestätigen.

Zusätzliche Authentifizierung beim Start anfordern

Zusätzliche Authentifizierung beim Start anfordern Vorherige Einstellung Nächste Einstellung

☐ Nicht konfiguriert
 ☒ **Aktiviert**
☐ Deaktiviert

Kommentar:

Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7

Optionen:

☐ BitLocker ohne kompatibles TPM zulassen (hierfür ein Kennwort oder ein USB-Flashlaufwerk mit Systemstartschlüssel erforderlich)
 Einstellungen für Computer mit einem TPM:
 TPM-Start konfigurieren: **TPM zulassen**
 TPM-Systemstart-PIN konfigurieren:
 Start-PIN bei TPM erforderlich
 TPM-Systemstartschlüssel konfigurieren:
 Systemstartschlüssel bei TPM zulassen
 TPM-Systemstartschlüssel und -PIN konfigurieren:
 Systemstartschlüssel und PIN bei TPM zulassen

Hilfe:

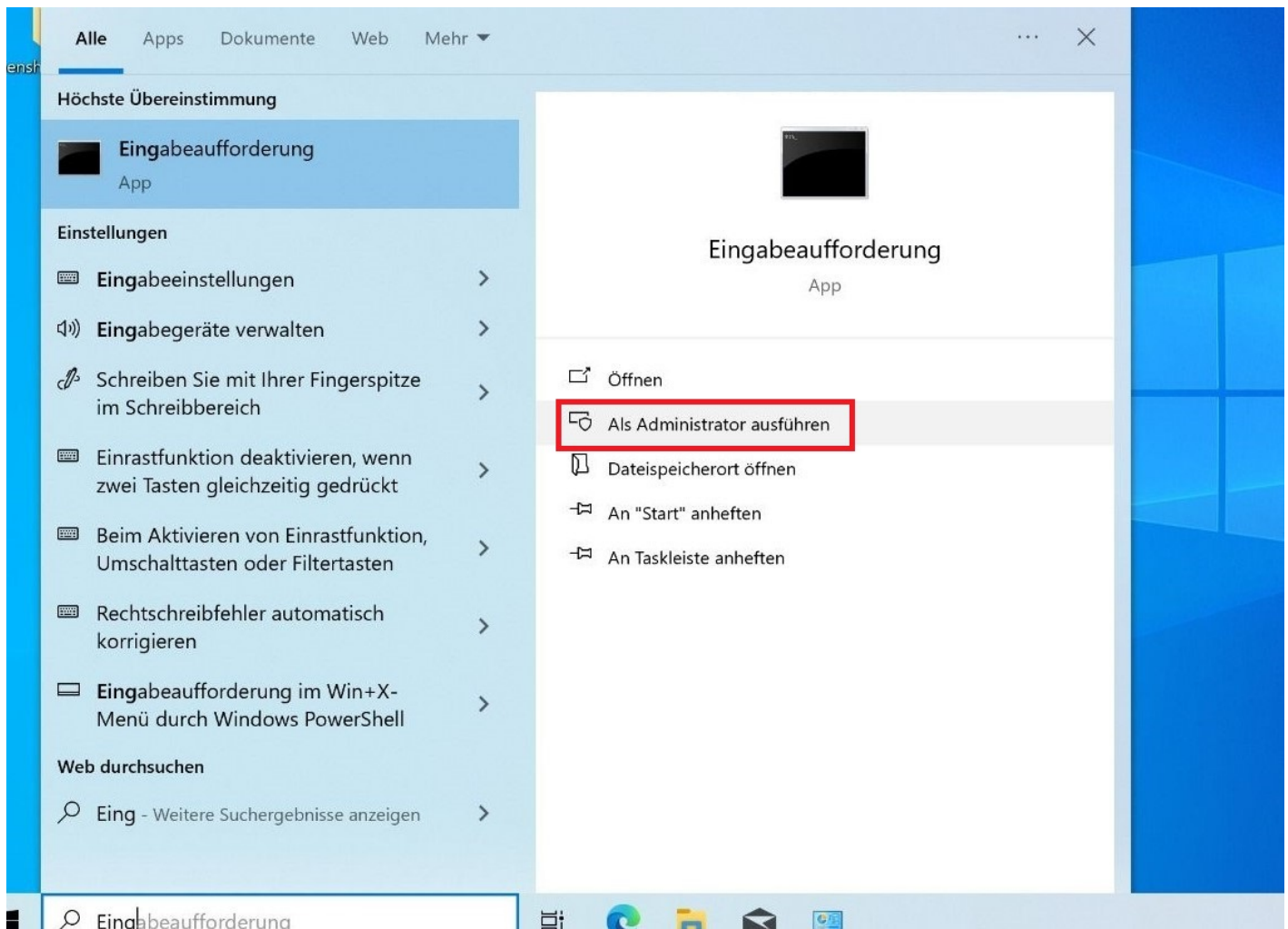
Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob BitLocker bei jedem Computerstart eine zusätzliche Authentifizierung erfordert und ob Sie BitLocker mit oder ohne TPM (Trusted Platform Module) verwenden. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.

Hinweis: Beim Start kann nur eine der zusätzlichen Authentifizierungsoptionen erforderlich sein, da andernfalls ein Richtlinienfehler auftritt.

Falls Sie BitLocker auf einem Computer ohne TPM verwenden möchten, aktivieren Sie das Kontrollkästchen "BitLocker ohne kompatibles TPM zulassen". In diesem Modus ist für den Start entweder ein Kennwort oder ein USB-Laufwerk erforderlich. Bei Verwendung eines Systemstartschlüssels werden die Schlüsselinformationen, die zum Verschlüsseln des Laufwerks verwendet werden, auf dem USB-Laufwerk gespeichert, wodurch ein USB-Stick entsteht. Wenn der USB-Stick eingesteckt wird, wird der Zugriff auf das Laufwerk authentifiziert, und es kann auf das

OK Abbrechen Übernehmen

Schritt 4: Anschließend muss eine PIN vergeben werden. Dazu starten wir in die Eingabeaufforderung. Dafür im Suchfeld "cmd" eingeben. GANZ WICHTIG! Als Administrator ausführen.

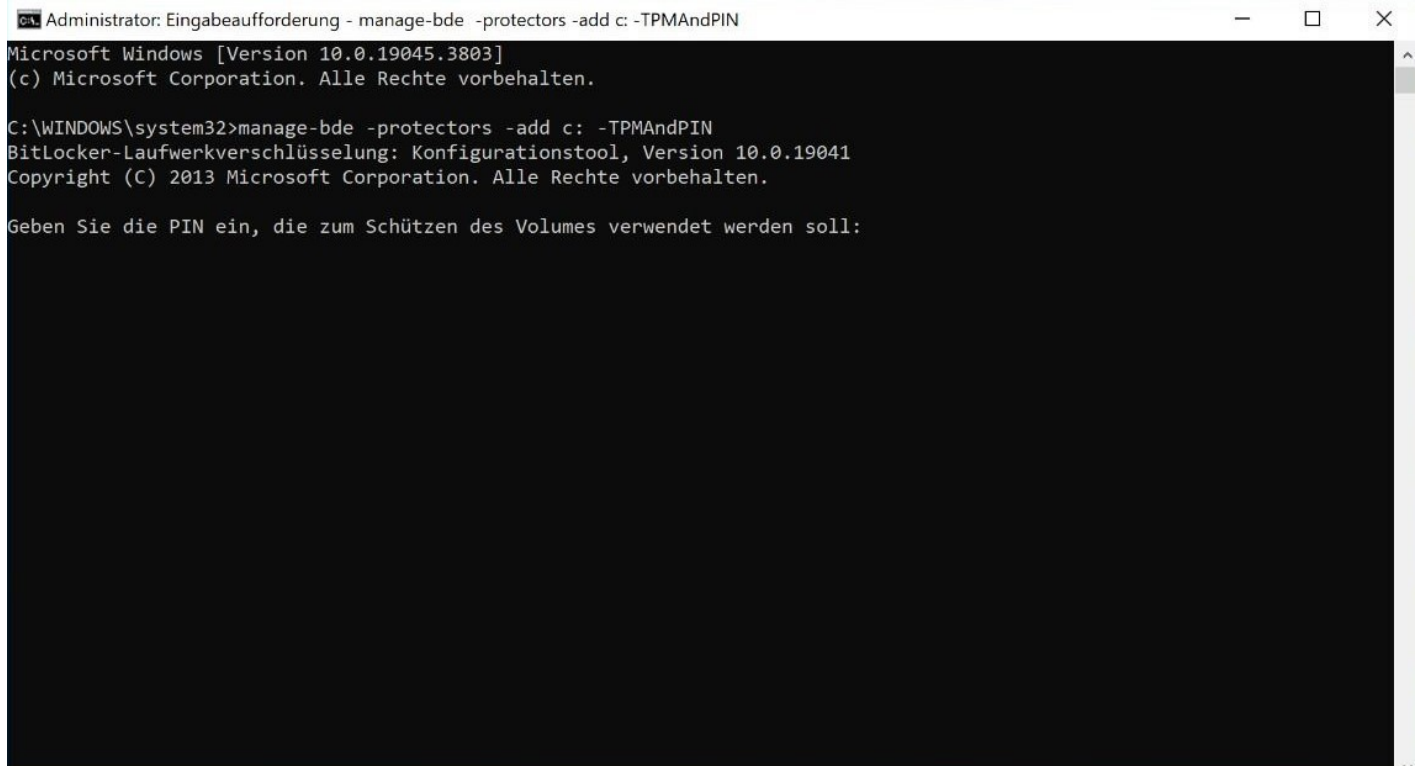


Schritt 5: Folgenden Befehl eingeben: *manage-bde -protectors -add C: -TPMAndPIN*

(C: ist der Laufwerksbuchstabe, bei mehreren Laufwerken ist auf die Bezeichnung zu achten.)

In der Oberen Zeile ist das Ganze aufgelistet Hinter C:\Windows\system32>.....

Das Ganze wird dann mit Enter bestätigt. ACHTUNG: DIE EINGABE DER PIN WIRD NICHT ANGEZEIGT

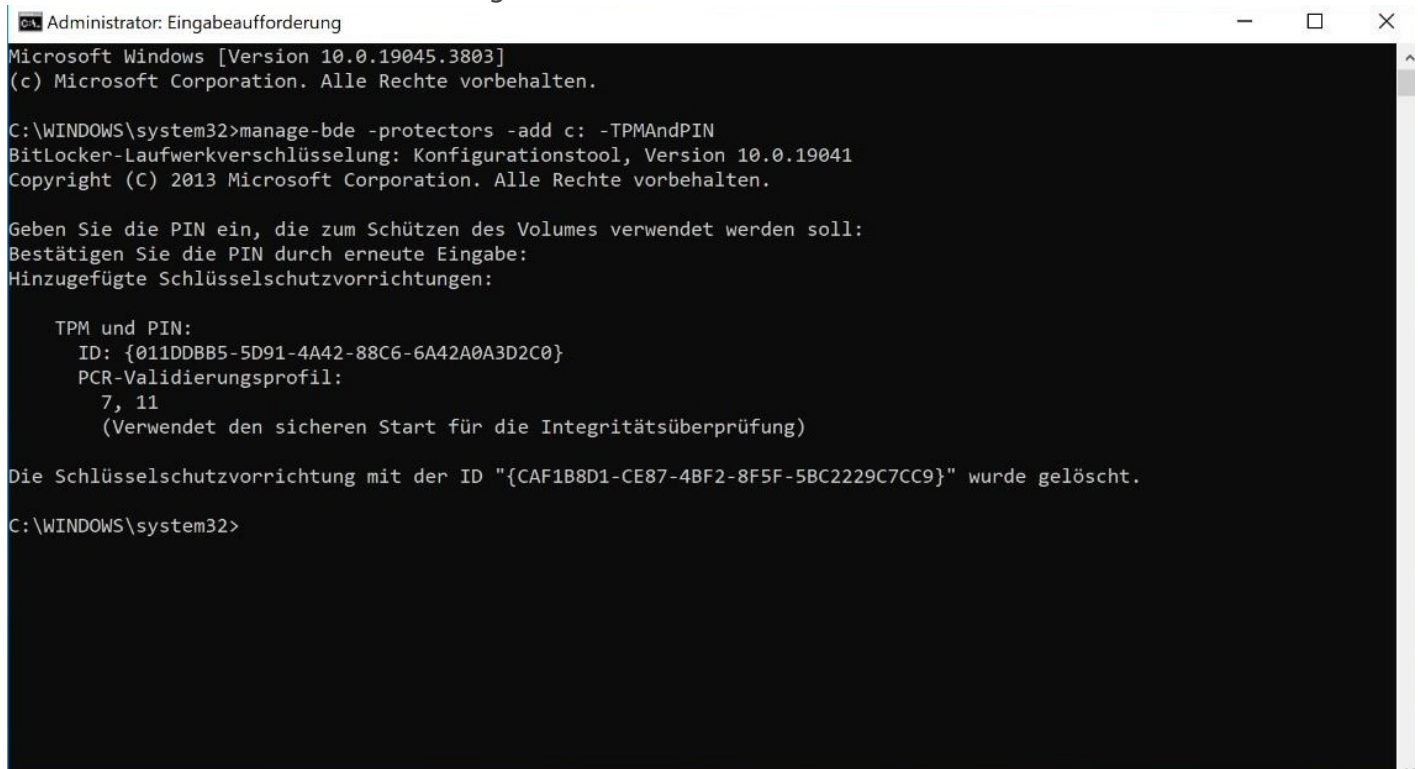


```
Administrator: Eingabeaufforderung - manage-bde -protectors -add c: -TPMAndPIN
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

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

Geben Sie die PIN ein, die zum Schützen des Volumes verwendet werden soll:
```

Schritt 6: Nun wird der PIN erzeugt.



```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

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

Geben Sie die PIN ein, die zum Schützen des Volumes verwendet werden soll:
Bestätigen Sie die PIN durch erneute Eingabe:
Hinzugefügte Schlüsselschutzvorrichtungen:

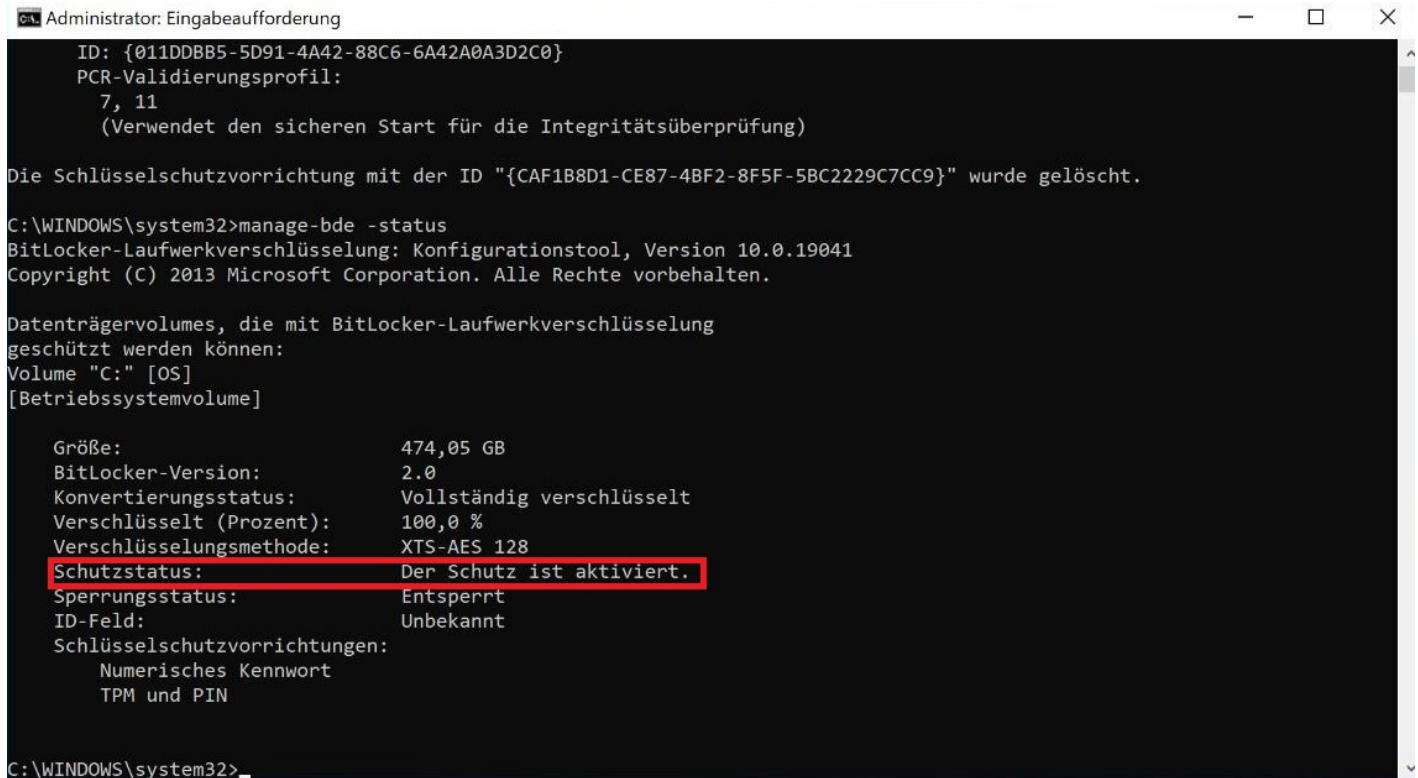
    TPM und PIN:
        ID: {011DDBB5-5D91-4A42-88C6-6A42A0A3D2C0}
        PCR-Validierungsprofil:
            7, 11
            (Verwendet den sicheren Start für die Integritätsüberprüfung)

Die Schlüsselschutzvorrichtung mit der ID "{CAF1B8D1-CE87-4BF2-8F5F-5BC2229C7CC9}" wurde gelöscht.

C:\WINDOWS\system32>
```

Schritt 7: Um zu überprüfen ob der Schutz aktiviert ist, gibt man folgenden Befehl ein: *manage-bde -status*

Bei einer erfolgreichen Einrichtung steht unter Schutzstatus „Der Schutz ist aktiviert“.



```
Administrator: Eingabeaufforderung
ID: {011DDBB5-5D91-4A42-88C6-6A42A0A3D2C0}
PCR-Validierungsprofil:
    7, 11
    (Verwendet den sicheren Start für die Integritätsüberprüfung)

Die Schlüsselschutzvorrichtung mit der ID "{CAF1B8D1-CE87-4BF2-8F5F-5BC2229C7CC9}" wurde gelöscht.

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

Datenträgervolumes, die mit BitLocker-Laufwerkverschlüsselung
geschützt werden können:
Volume "C:" [OS]
[Betriebssystemvolumen]

Größe:                474,05 GB
BitLocker-Version:     2.0
Konvertierungsstatus:  Vollständig verschlüsselt
Verschlüsselt (Prozent): 100,0 %
Verschlüsselungsmethode: XTS-AES 128
Schutzstatus:          Der Schutz ist aktiviert.
Sperrungsstatus:       Entsperrt
ID-Feld:               Unbekannt
Schlüsselschutzvorrichtungen:
    Numerisches Kennwort
    TPM und PIN

C:\WINDOWS\system32>
```

Revision #4

Created 8 May 2024 13:41:11 by Robert Hoffmeister

Updated 29 May 2024 10:04:43 by Dennis Lukas