

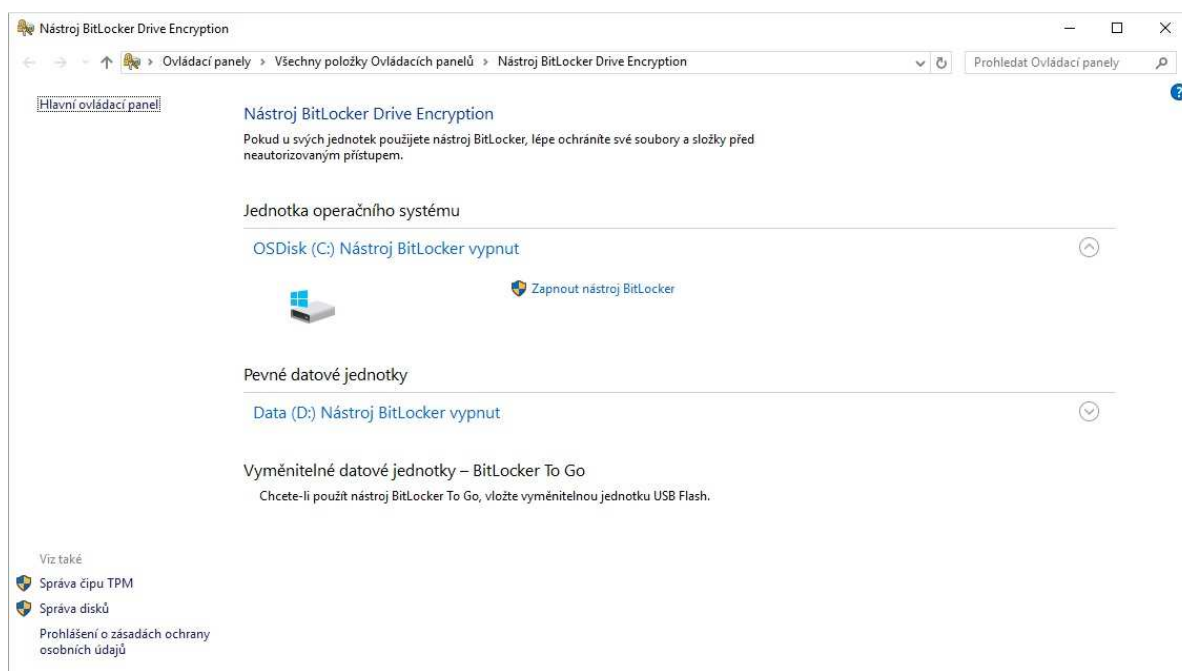
## Šifrování systémového disku C: a datového disku D: ve standardním image

verze 001 ze dne 12.12.2018

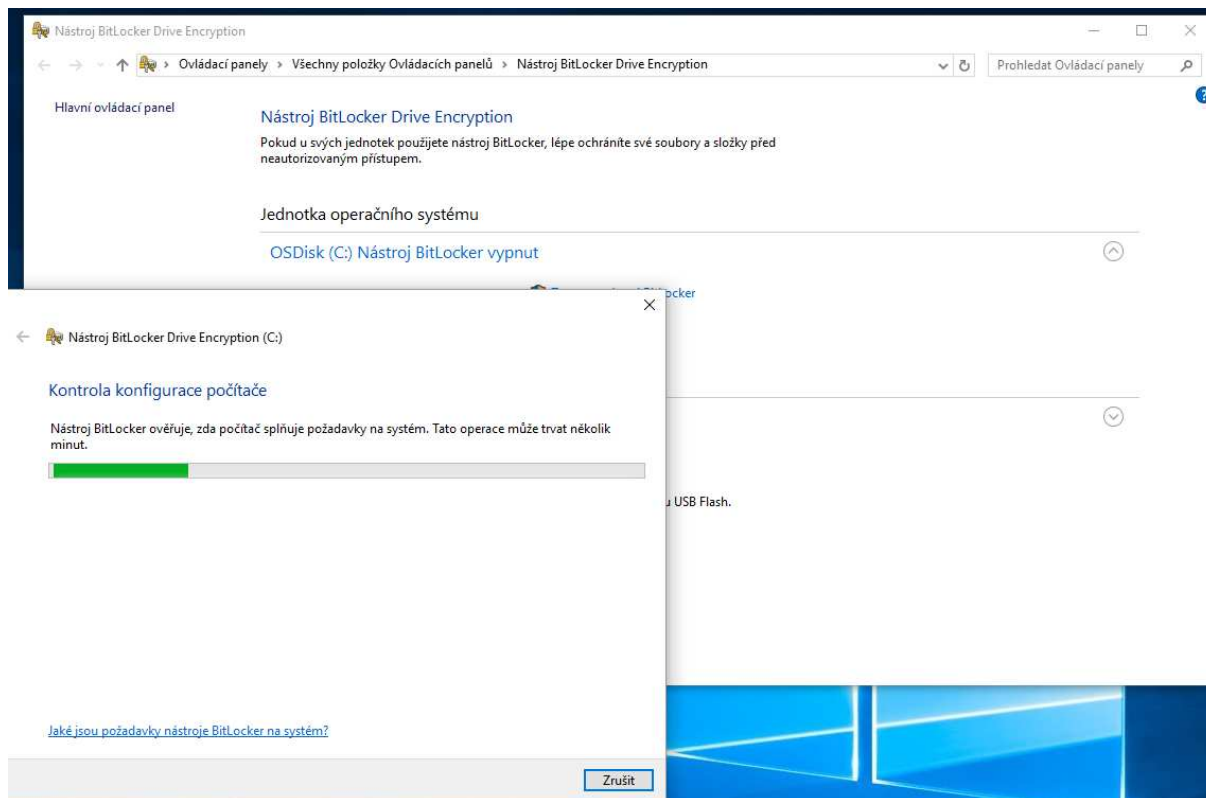
Microsoft nabízí pro šifrování disků v systému Windows 10 nástroj BitLocker. Funguje relativně jednoduše a provozní zatížení systému je nepatrné. V rámci VŠE jsme pro Vás připravili návod, jak zašifrovat data na stanici (notebooku), která má standardní image. Při postupování pomocí tohoto návodu je při zapomenutí klíče nebo poškození hardware možné rozšifrování Helpdeskem CI. Pro šifrování je nutné být administrátorem systému a být připojen v síti VŠE, a to z důvodů, že se do síťového prostředí uloží klíč, který je nutný pro rozšifrování disku.

Před vlastním šifrováním doporučuje aktuální data zálohovat, a to buď na přenosný disk nebo přes aplikaci Microsoft OneDrive nebo do ownCloudu Cesnetu.

Přes volbu Start najdeme volbu *Spravovat nástroj BitLocker*

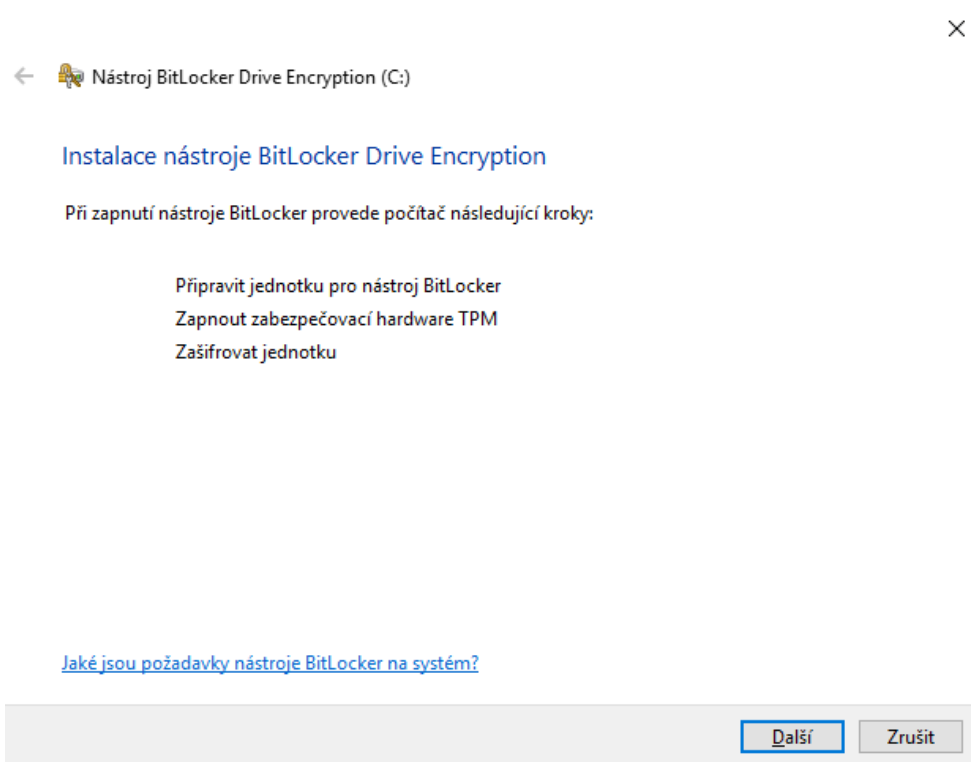


U disku C – zapneme volbu *Zapnout nástroj BitLocker*, bude probíhat kontrola konfigurace počítače.

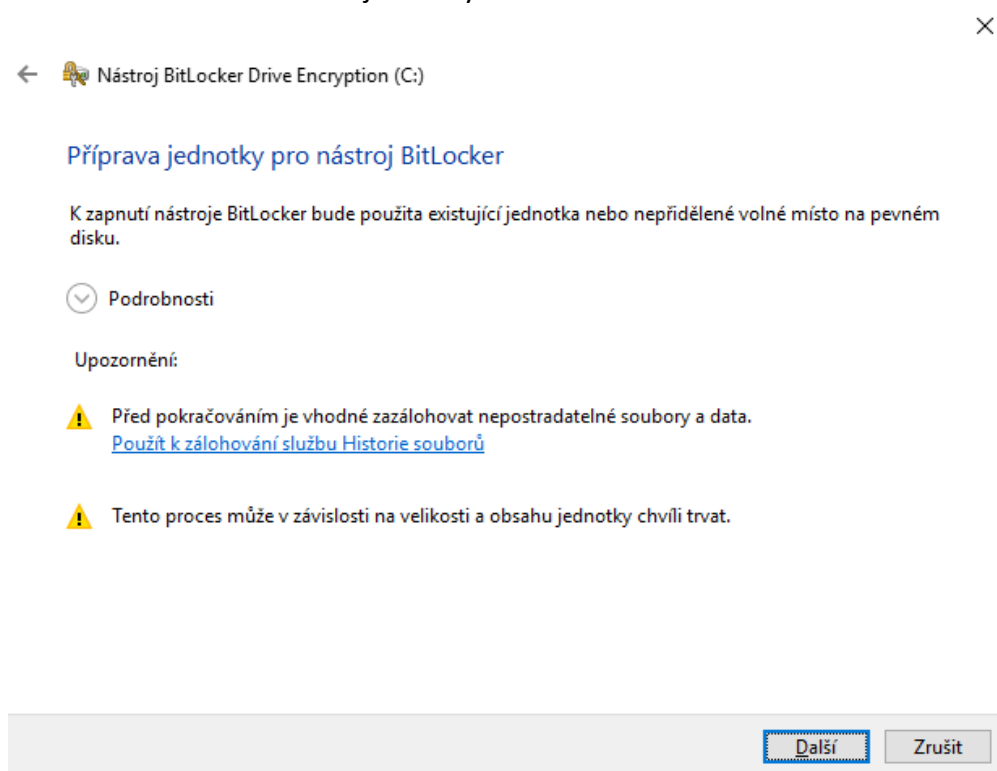


Vlastní instalace nástroje BitLocker bude provedena v několika krocích. Zde může nastat odchylka podle konfigurace počítače.

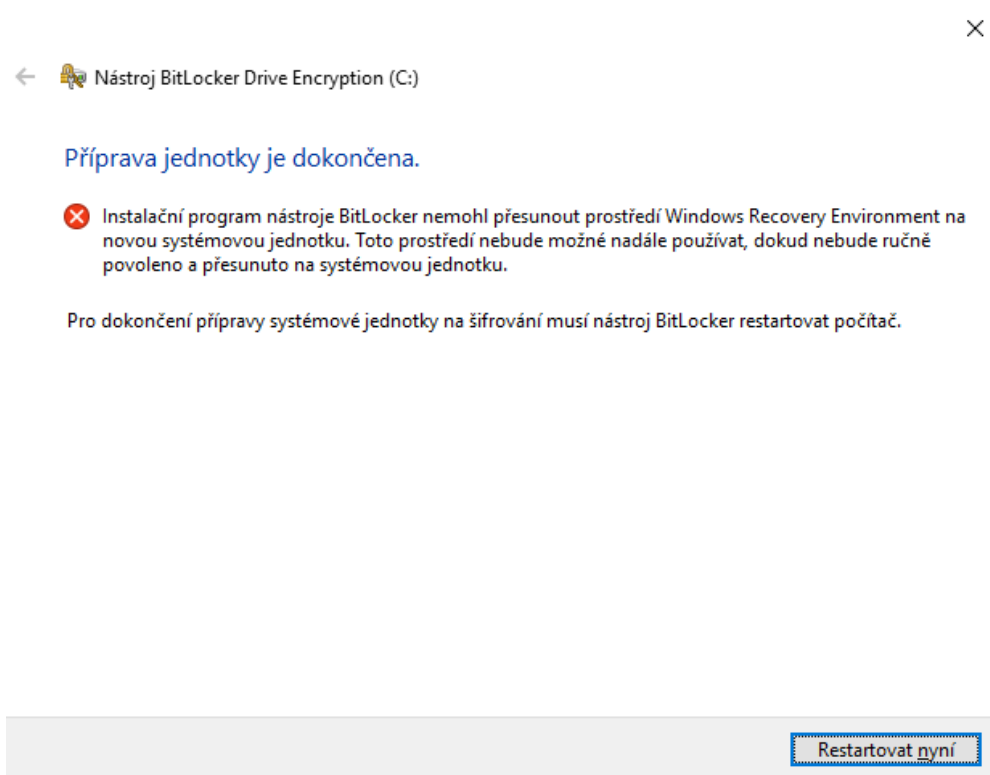
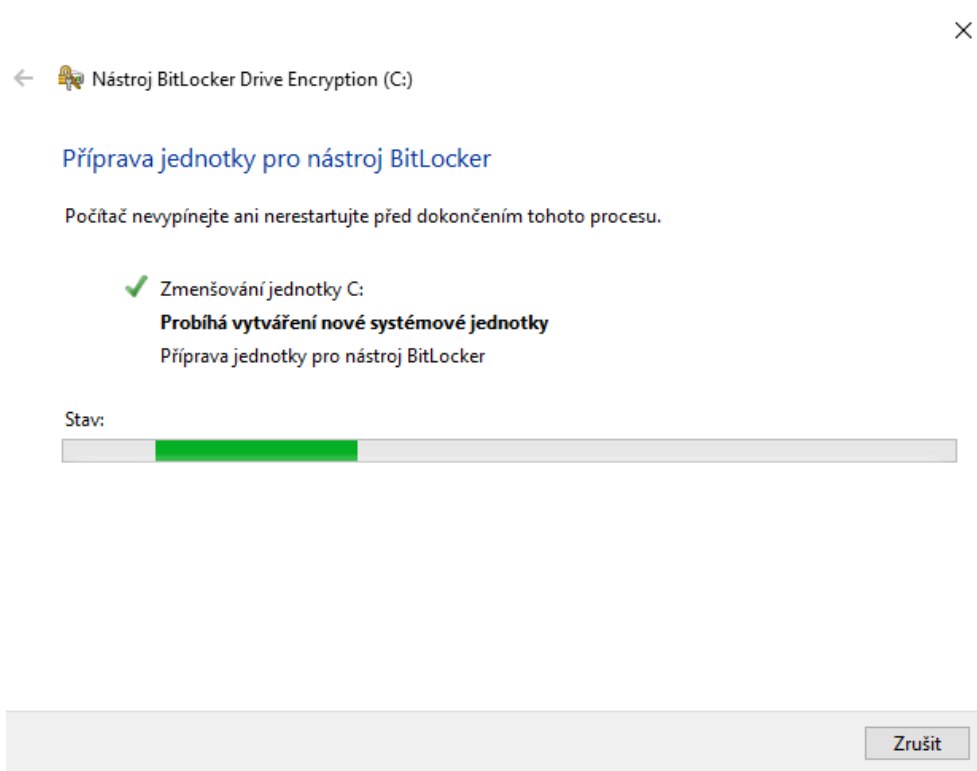
Před vlastním zašifrování je nutné aktivovat TPM čip, který bývá součástí počítačů a notebooků, vlastní aktivace TPM čipu se provede instalační utilitou sama, ale bude se vyžadovat součinnost ze strany uživatele. Na některých starších počítačích může být potřeba zapnout TPM v BIOSu (provede na požádání Helpdesk) Jednotlivé kroky popisu následující dialogové okno, kde stiskneme tlačítko *Další*



Jsme znovu varování, že je nutné data zálohovat a systém nás informuje, což že doba šifrování závisí na velikosti a obsahu jednotky.




Disk C je upraven, tak aby se na disku vytvořila část pro zavedení systému, která nesmí být šifrována, a tudíž se musí jednat o jiný oddíl než oddíl s operačním systémem. Jeho velikost je malá cca do 350 MB.



Po restartu by průvodce sám měl naběhnout do dialogového okna *Nástroj BitLocker Drive Encryption (C:)*. Stiskneme tlačítko *Další*. Systém bude zapínat TPM čip, a tak opět musíme restartovat.



←  Nástroj BitLocker Drive Encryption (C:)

### Zapnout zabezpečovací hardware TPM

Před zapnutím hardwaru TPM pro tento počítač vyjměte všechny disky CD, DVD nebo jednotky USB Flash a restartujte počítač.

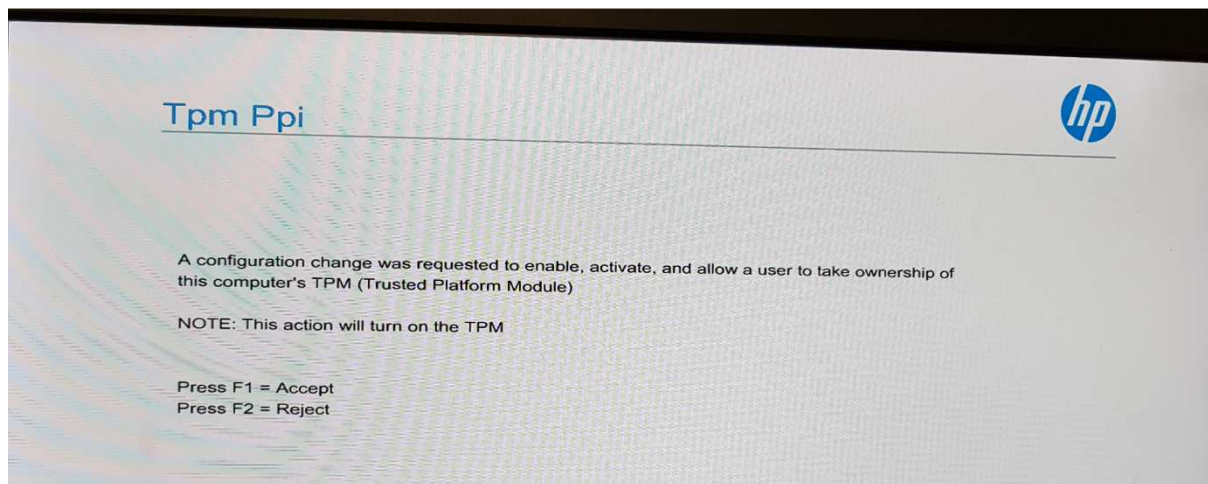
Po restartování počítače postupujte podle pokynů k zapnutí čipu TPM.

[Co je čip TPM?](#)

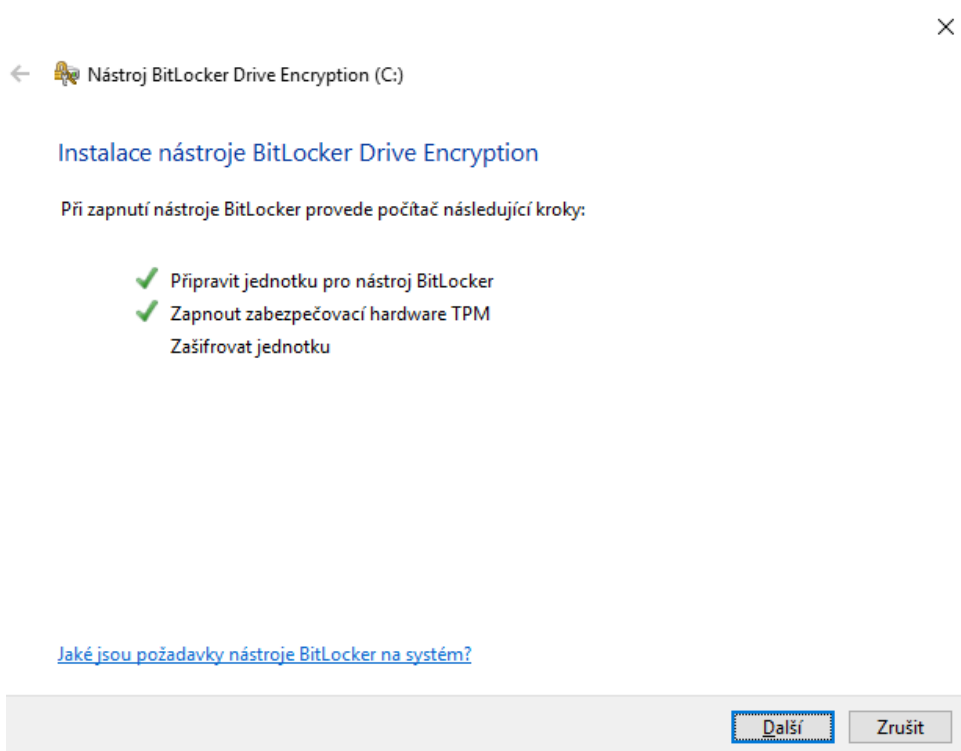
[Restartovat](#)

[Zrušit](#)

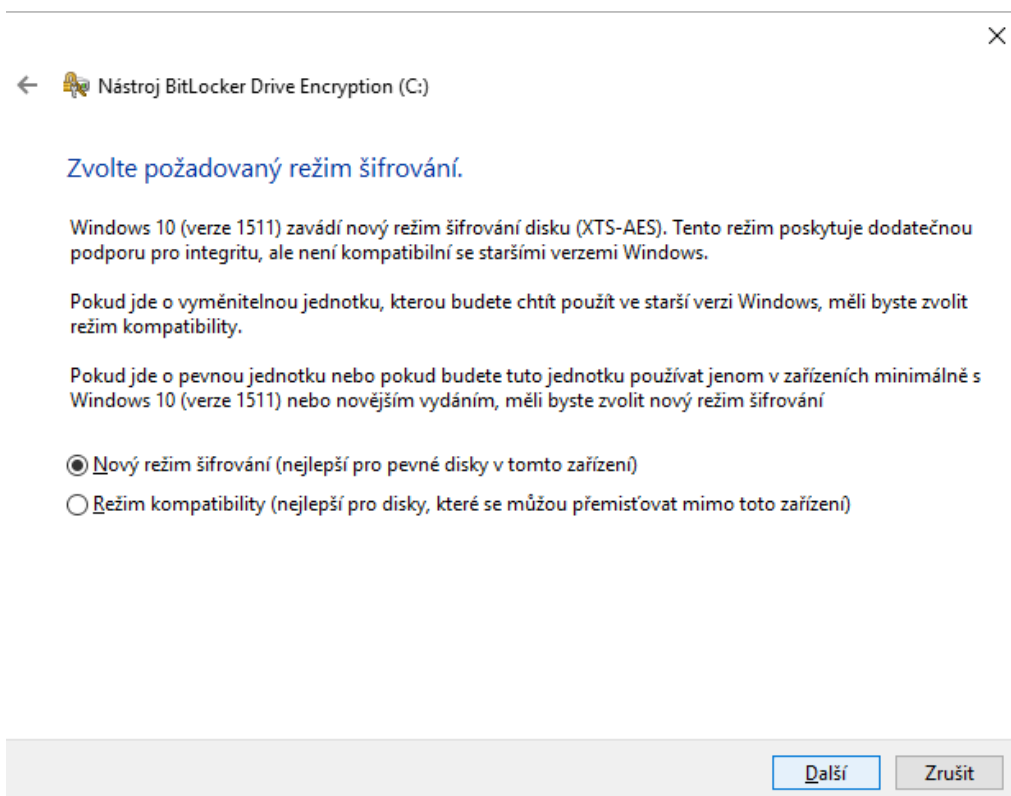
Je pravděpodobné, že pro vlastní aktivaci TPM čipu, budete muset být součinni. Např. na All-in-One od HP je nutná akceptace přes klávesu F1.



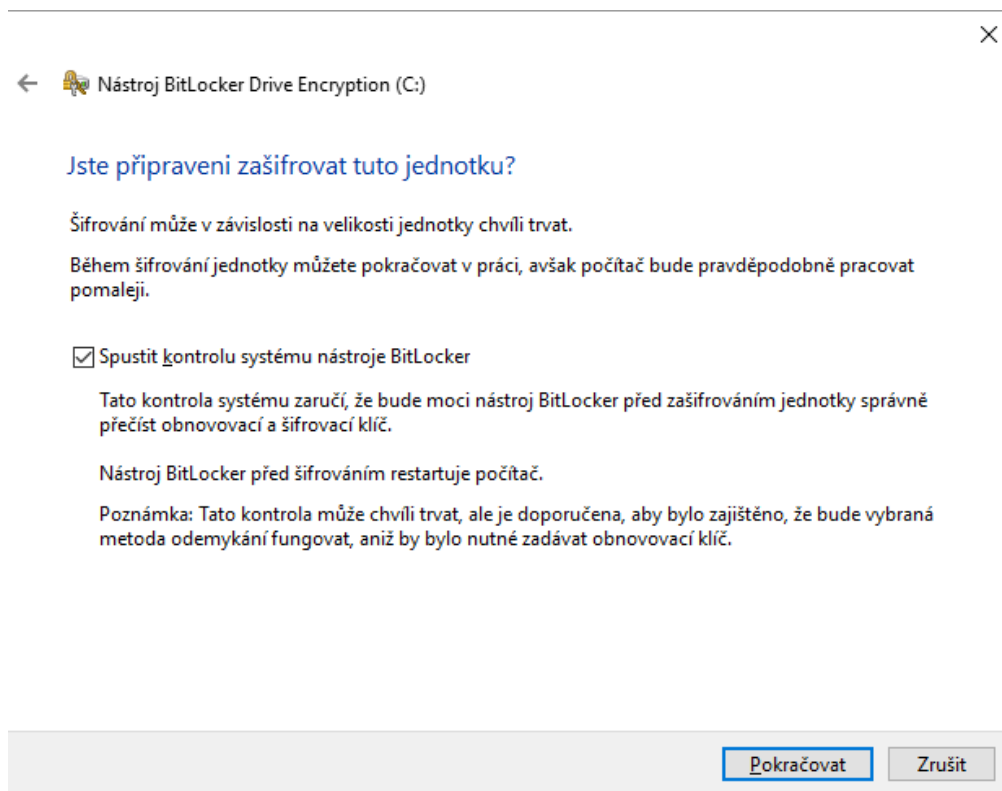
Opět se vrátím do průvodce, kde jsme splnili dva z požadovaných bodů a můžeme přistoupit na vlastní šifrování jednotky. Pokračujeme volbou *Další*.



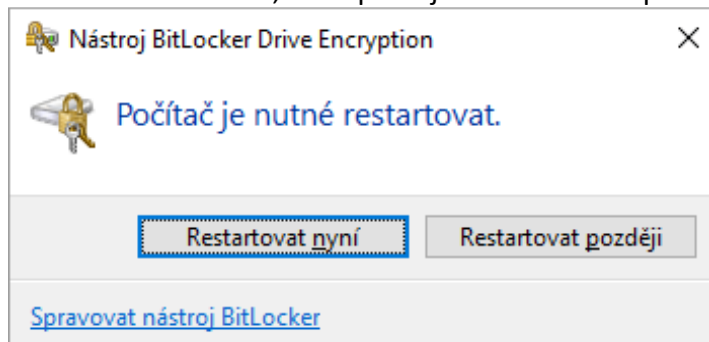
Při šifrování jsme dotázáni na režim šifrování. Od verze Windows 10 volíme nový šifrovací algoritmus XTS-AES



V posledním kroku můžeme zvolit, aby se provedla systémová kontrola (testuje se práce s klíči v TPM a další), jinak se hned spustí šifrování disku a při nějakých komplikacích ho již nemusíme rozšifrovat.

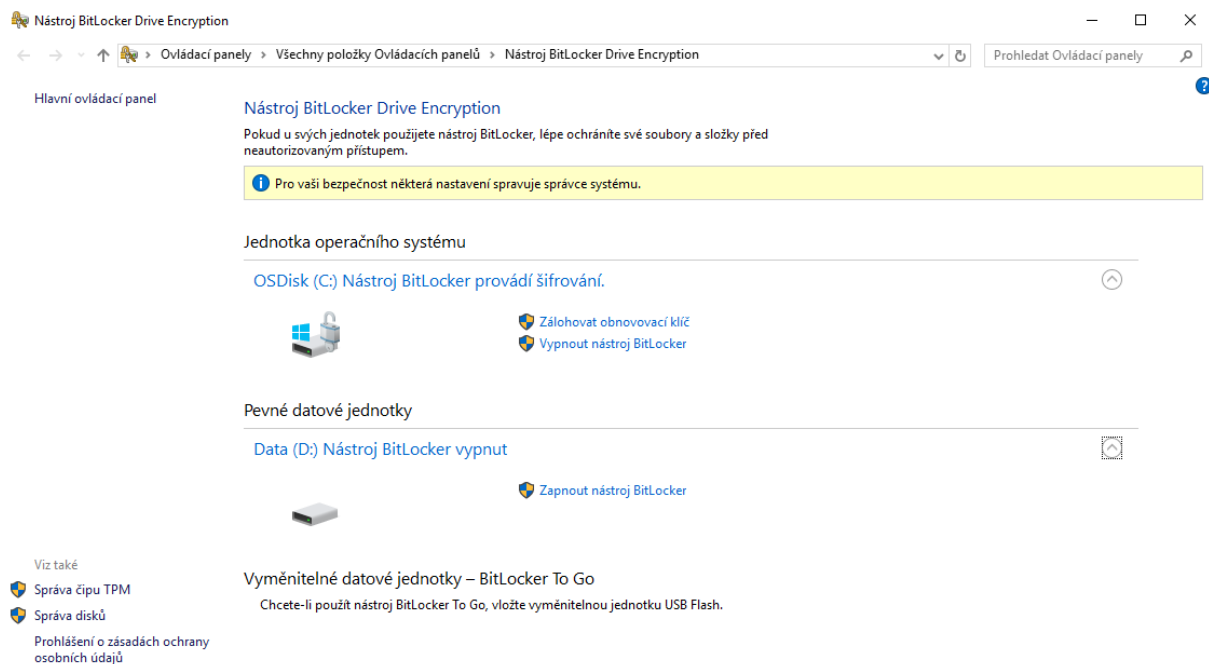


Po volbě Pokračovat, se dopravujeme k Restartu počítače.

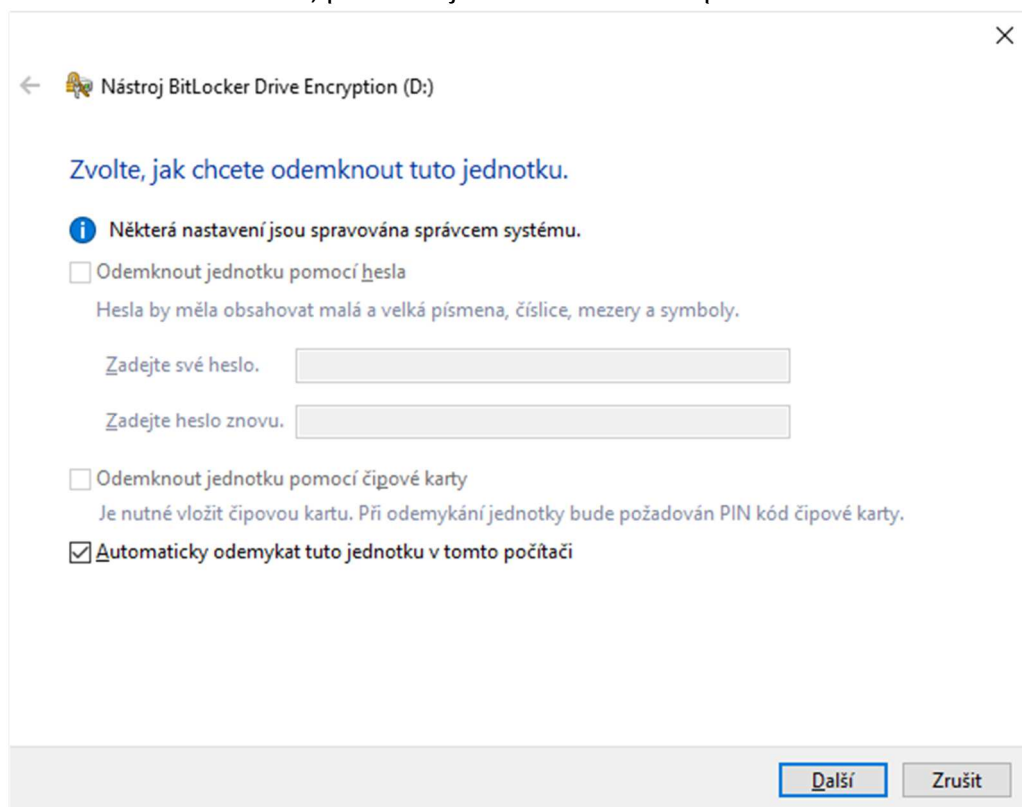


Tímto se zašifruje disk C, informace o šifrovacím klíči se uloží do TPM čipu a do objektu počítač v Active Directory.

Abychom zašifrovali i úložiště dokumentů – potřebujeme zašifrovat i disk D. Znovu tedy musíme zavolat nástroj Bitlocker. Poté, co se nám zobrazí utilita, uvidíme, že disk C je již zašifrován (je totiž dostupná volba *Vypnout nástroj BitLocker*), zatímco u disku D máme volbu *Zapnout nástroj Bitlocker*, kterou není zavoláme.




Objeví se okno, v kterém jsou omezené možnosti (nastavené správcem systému). Jedinou dostupnou volbou je nyní volba *Automaticky odemknout tuto jednotku v tomto počítači*. Zaškrtnete-li tuto volbu, pak se objeví tlačítko *Další* v průvodci



Volíme opět režim šifrování pro disk D.





←  Nástroj BitLocker Drive Encryption (D:)

### Zvolte požadovaný režim šifrování.

Windows 10 (verze 1511) zavádí nový režim šifrování disku (XTS-AES). Tento režim poskytuje dodatečnou podporu pro integritu, ale není kompatibilní se staršími verzemi Windows.

Pokud jde o vyměnitelnou jednotku, kterou budete chtít použít ve starší verzi Windows, měli byste zvolit režim kompatibility.

Pokud jde o pevnou jednotku nebo pokud budete tuto jednotku používat jenom v zařízeních minimálně s Windows 10 (verze 1511) nebo novějším vydáním, měli byste zvolit nový režim šifrování

- Nový režim šifrování** (nejlepší pro pevné disky v tomto zařízení)
- Režim kompatibility** (nejlepší pro disky, které se mohou přemísťovat mimo toto zařízení)

Další

Zrušit

Tlačítkem *Zahájit šifrování* v následujícím okně zahájíme šifrování disku D.



←  Nástroj BitLocker Drive Encryption (D:)

### Jste připraveni zašifrovat tuto jednotku?

Jednotka se v tomto počítači automaticky odemkne.

Šifrování může v závislosti na velikosti jednotky chvíli trvat.

Soubory budou chráněny až po dokončení šifrování.

Zahájit šifrování

Zrušit

O dokončení šifrování jste informováni následujícím dialogovým oknem.

Šifrování D: bylo dokončeno.

Zavřít

[Spravovat nástroj BitLocker](#)

Pokud zavoláte opětovně **Nástroj pro BitLocker**, uvidíte, že zašifrovány jsou oba disky.

Nástroj BitLocker Drive Encryption

Ovládací panely > Všechny položky Ovládacích panelů > Nástroj BitLocker Drive Encryption

Hlavní ovládací panel

**Nástroj BitLocker Drive Encryption**

Pokud u svých jednotek použijete nástroj BitLocker, lépe ochráníte své soubory a složky před neautorizovaným přístupem.

Pro vaši bezpečnost některá nastavení spravuje správce systému.

Jednotka operačního systému

OSDisk (C:) Nástroj BitLocker zapnut

- Pozastavit ochranu
- Zálohovat obnovovací klíč
- Vypnout nástroj BitLocker

Pevné datové jednotky

Data (D:) Nástroj BitLocker zapnut

- Zálohovat obnovovací klíč
- Vypnout automatické odemknutí
- Vypnout nástroj BitLocker

Viz také

- Správa čipu TPM
- Správa disků
- Prohlášení o zásadách ochrany osobních údajů

Vyměnitelné datové jednotky – BitLocker To Go

Chcete-li použít nástroj BitLocker To Go, vložte vyměnitelnou jednotku USB Flash.

Doporučujeme na počítač vhodným způsobem poznamenat jméno počítače (popis ikonky počítače na ploše ve formátu „Počítač VSE-xxxx“, kde xxxx je pětimístné číslo). Tento údaj je třeba v případě poškození počítače pro rozšifrování disku mimo původní počítač. Bez znalosti jména může být obtížné nalezení správného dešifrovacího klíče v AD.