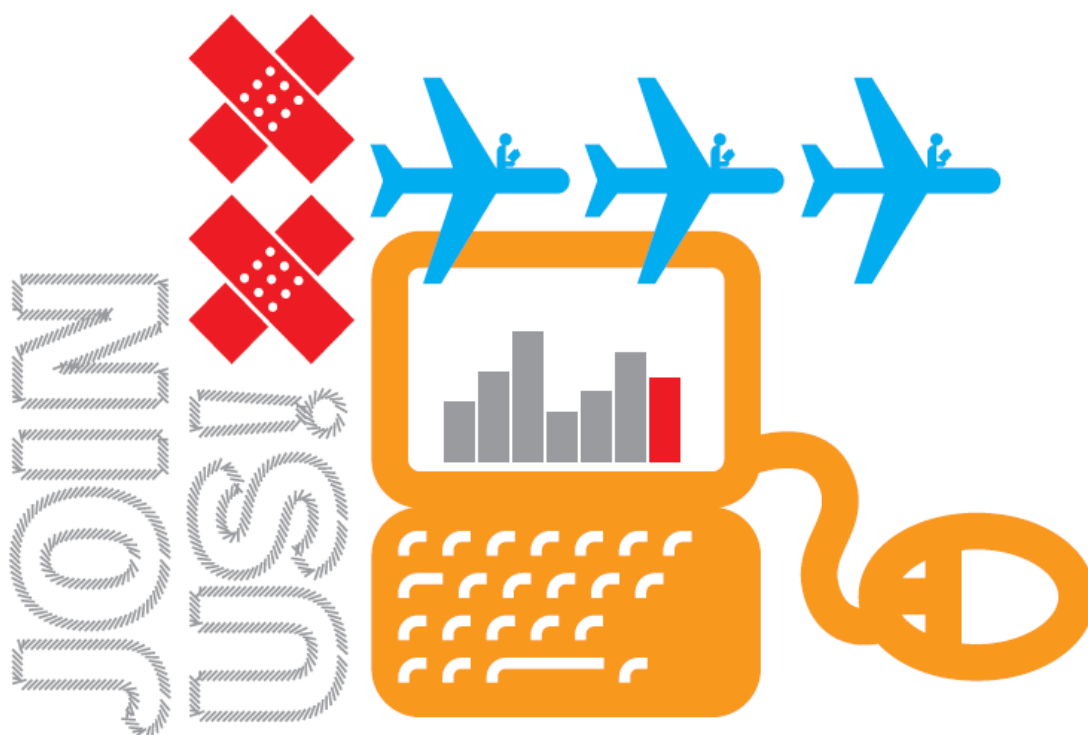


Návod pro šifrování přenosných disků

Vysoká škola
polytechnická
Jihlava

autor: OIKT 2018



Obsah

Varianta 1: BitLocker – šifrování disků	3
Kontrola operačního systému	3
Zašifrování disku	4
Varianta 2: VeraCrypt - použití šifrovaného úložiště	13
Stažení programu VeraCrypt	13
Instalace programu VeraCrypt.....	14
Vytvoření šifrovaného úložiště	18
Otevření šifrovaného úložiště	27
Odpojení šifrovaného úložiště.....	31
Varianta 3: VeraCrypt – šifrování disků	32
Stažení a instalace	32
Zašifrování disku	32
Otevření zašifrovaného disku	43

Varianta 1: BitLocker – šifrování disků

Tento návod slouží pro zašifrování flash disku, externího disku nebo interního disku v počítači. K zašifrování je využito heslo, které by mělo být dostatečně silné a současně zapamatovatelné. Jako minimální délku hesla lze považovat 8 znaků skládajících se z velkých a malých písmen, číslic a speciálních znaků (tečka, podtržítka, pomlčka, apostrof, ampersand a obdobné). Heslo by nemělo být složeno ze jmen a slov, neboť takové je snadno prolomitelné slovníkovým útokem.

Kontrola operačního systému

Pro zašifrování disku je nutné mít v operačním systému nainstalován program BitLocker, který je součástí následujících verzí operačních systémů:

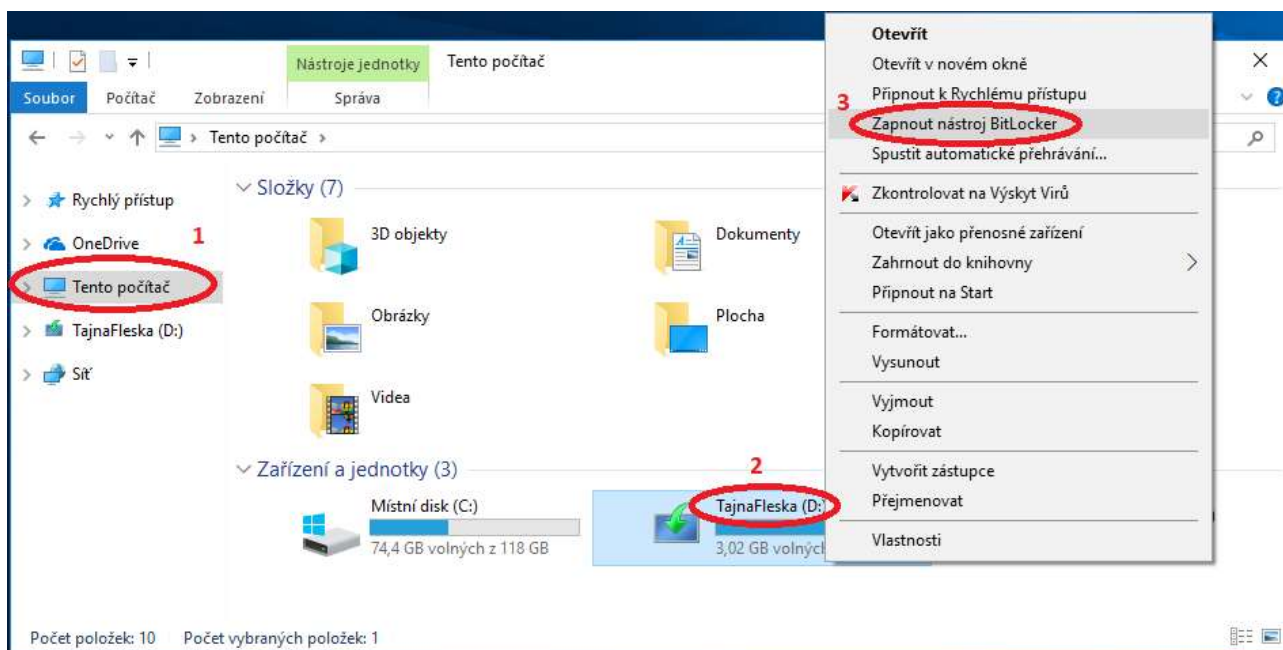
- Windows Vista a Windows 7 ve verzích Ultimate a Enterprise
- Windows 8 a Windows 8.1 ve verzích Pro a Enterprise
- Windows 10 ve verzích Pro, Enterprise a Education

Ostatní verze operačních systémů mohou dovolit otevřít zašifrovaný disk, ale nemusí umožnit jeho vytvoření.

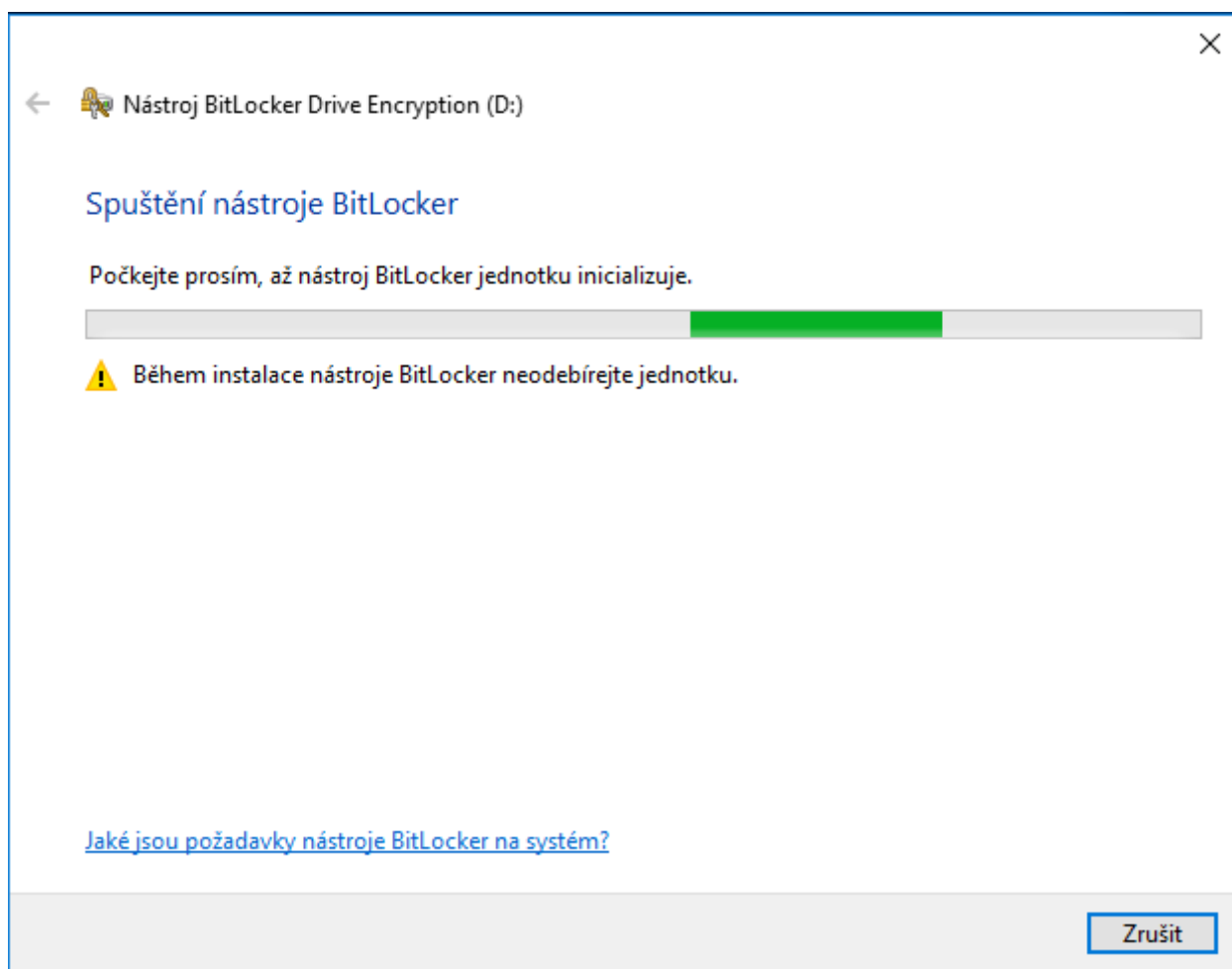
Jestliže ve svém systému program BitLocker nemáte, můžete využít program VeraCrypt. Viz další kapitoly.

Zašifrování disku

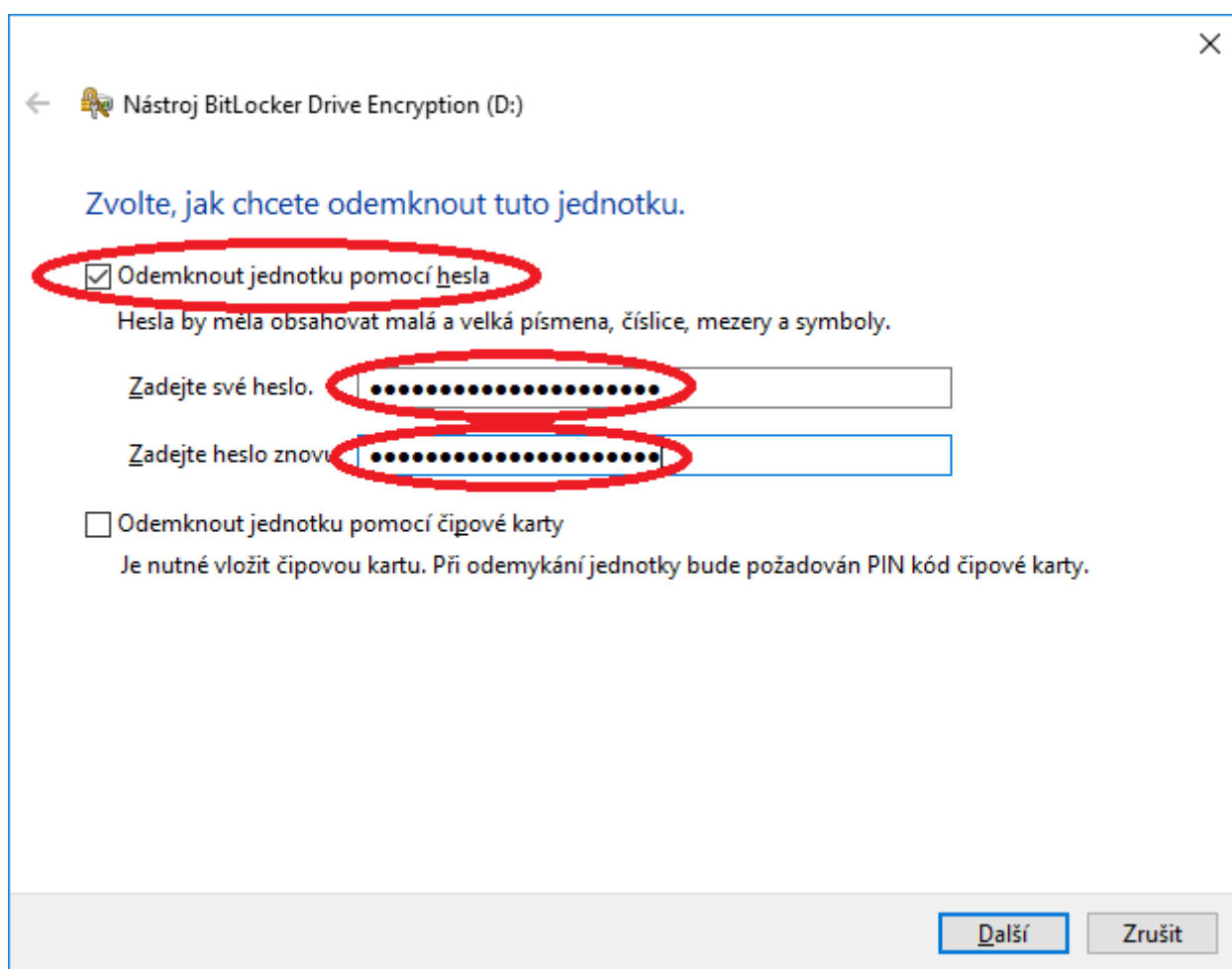
Připojte disk k počítači a klikněte na jeho ikonu pravým tlačítkem. A poté zvolte možnost „Zapnout nástroj BitLocker“.



System inicializuje jednotku.



Zvolte ochranu pomocí hesla a zadejte dostatečně silné a zapamatovatelné heslo.



←  Nástroj BitLocker Drive Encryption (D:)

X

Zvolte, jak chcete odemknout tuto jednotku.

☒ Odemknout jednotku pomocí hesla

Hesla by měla obsahovat malá a velká písmena, číslice, mezery a symboly.

Zadejte své heslo.

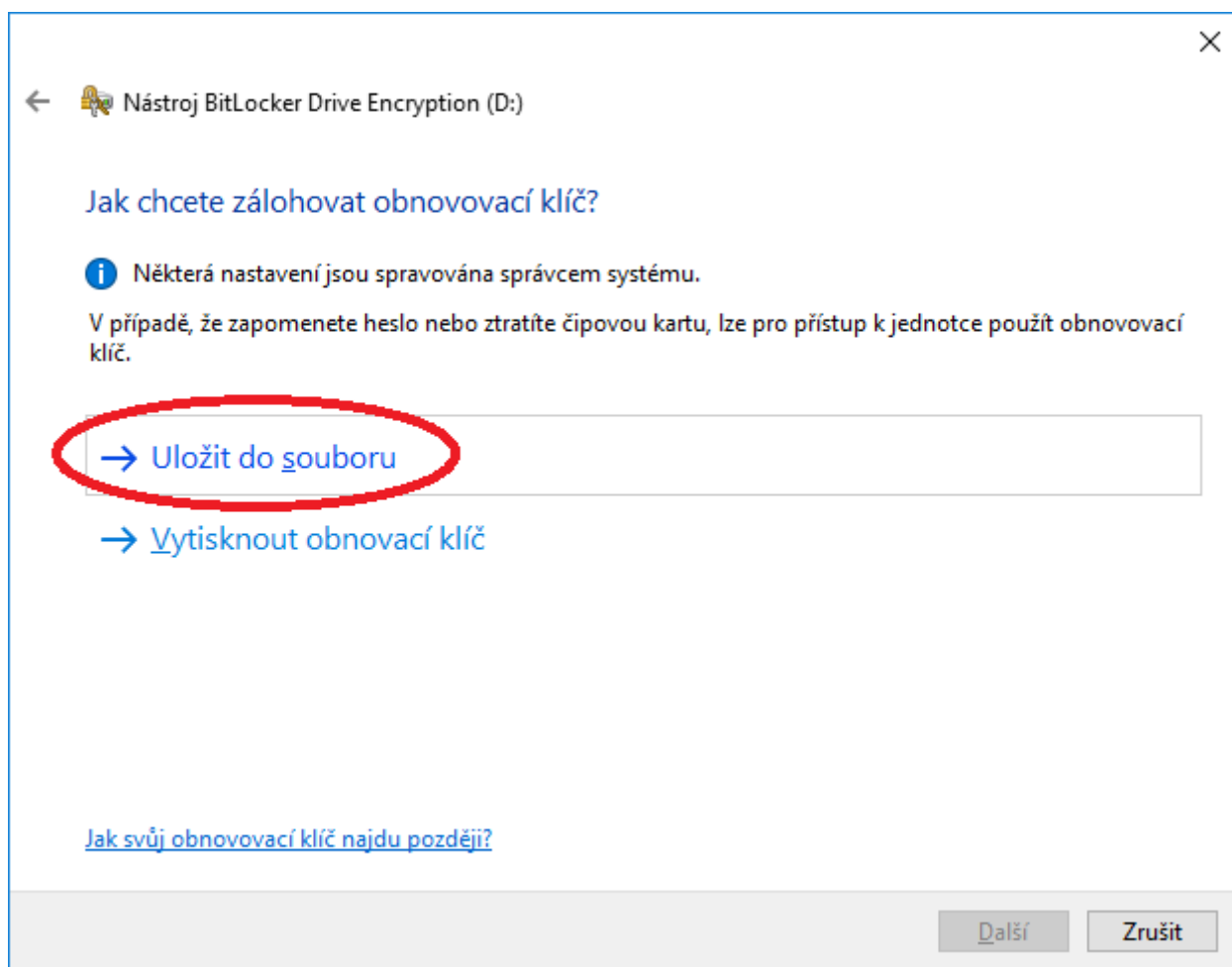
Zadejte heslo znovu

☐ Odemknout jednotku pomocí čipové karty

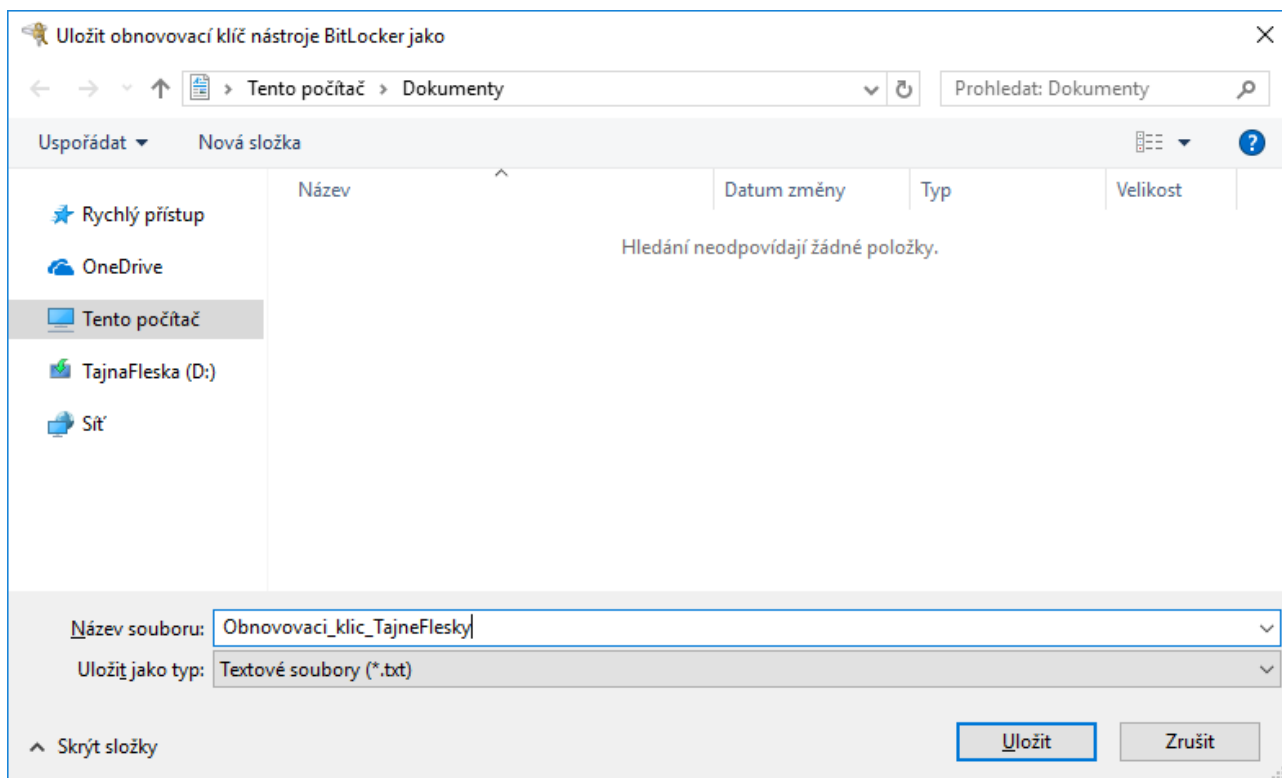
Je nutné vložit čipovou kartu. Při odemykání jednotky bude požadován PIN kód čipové karty.

[Další](#) [Zrušit](#)

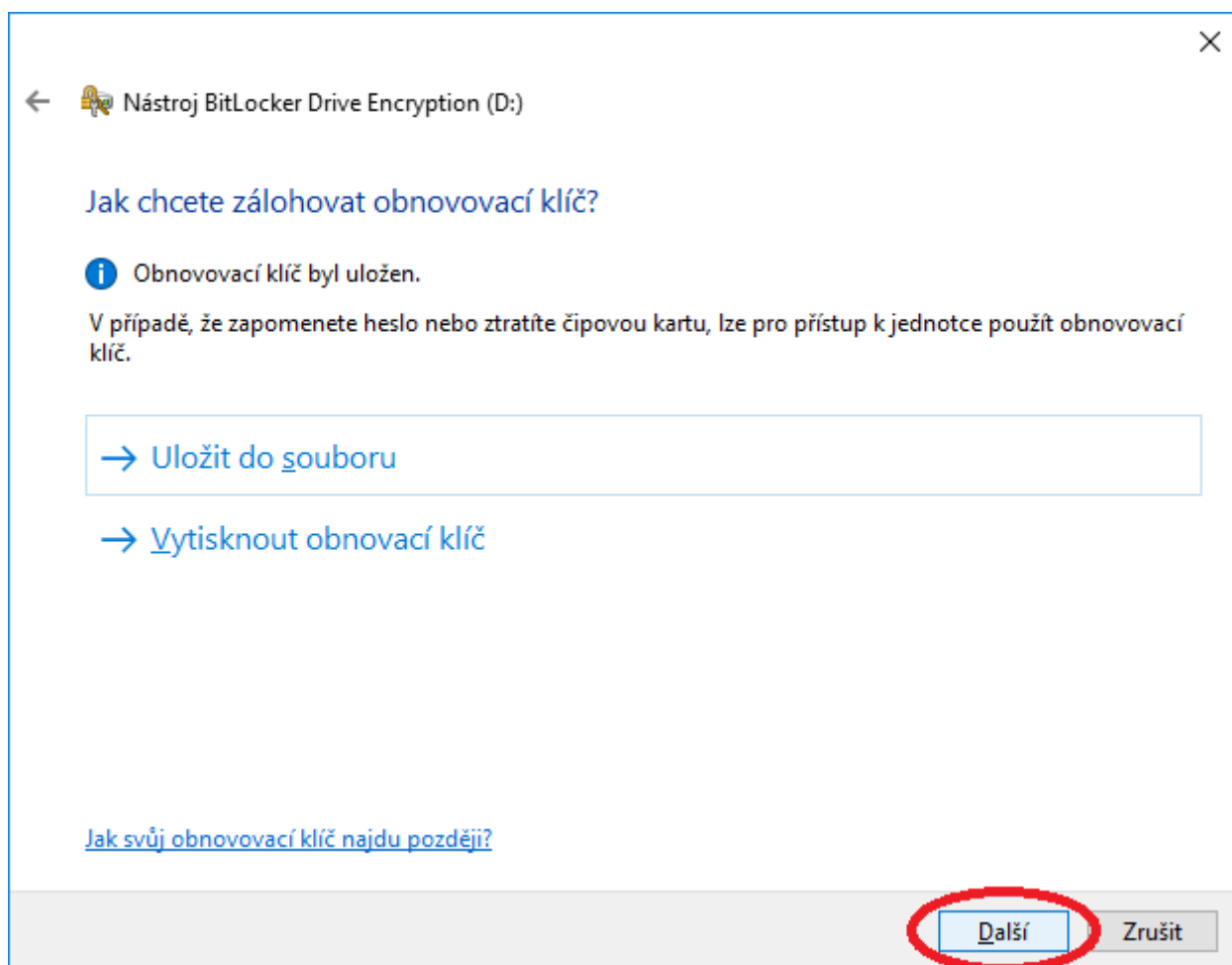
V případě, že heslo zapomenete, je možné data rozšifrovat pomocí obnovovacího klíče. Ten si nyní můžete vytisknout nebo uložit.



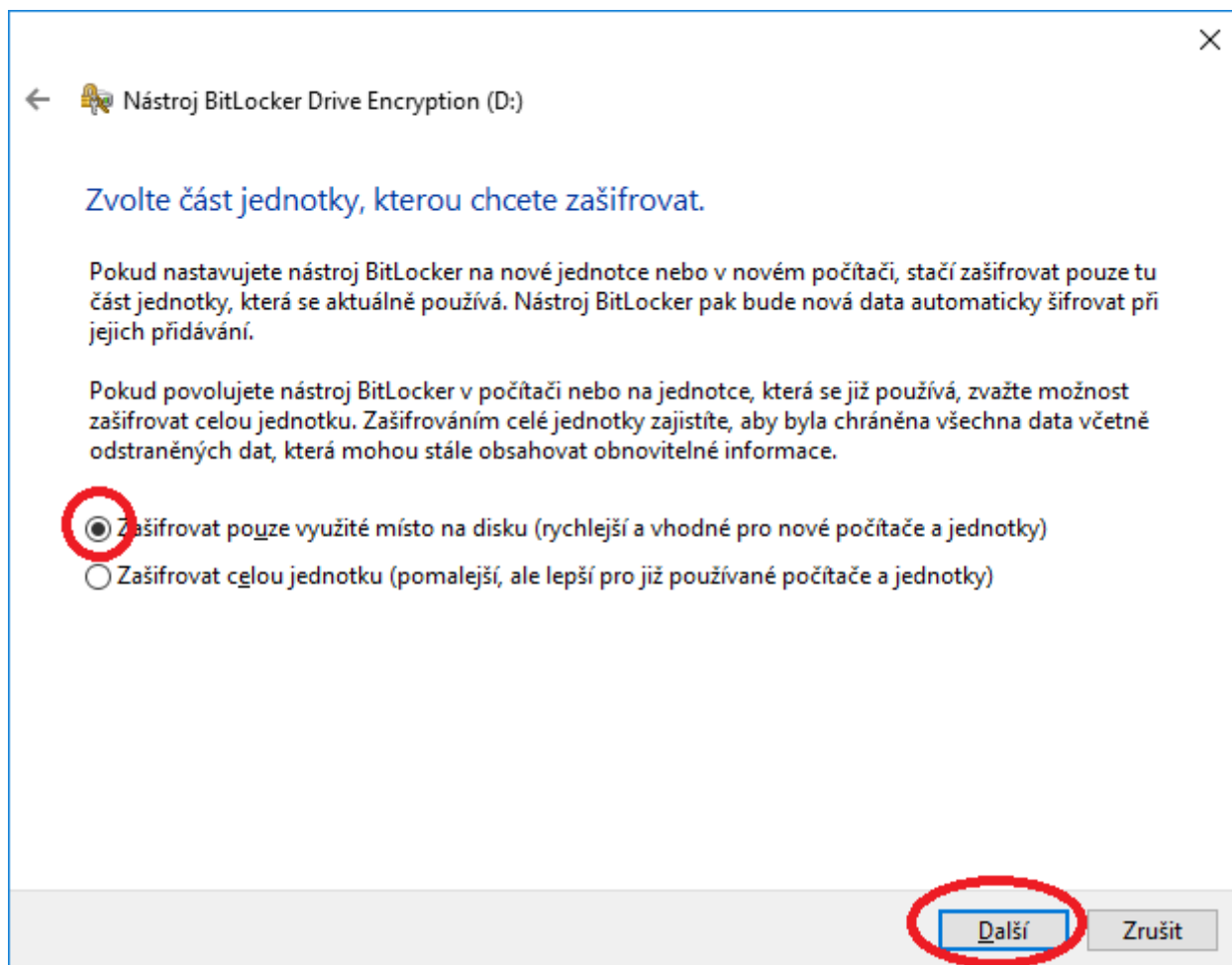
Soubor s obnovovacím klíčem uložte na místo, na kterém jej bude možné i za delší čas nalézt, ale současně se k tomuto souboru nesmí dostat neoprávněné osoby.



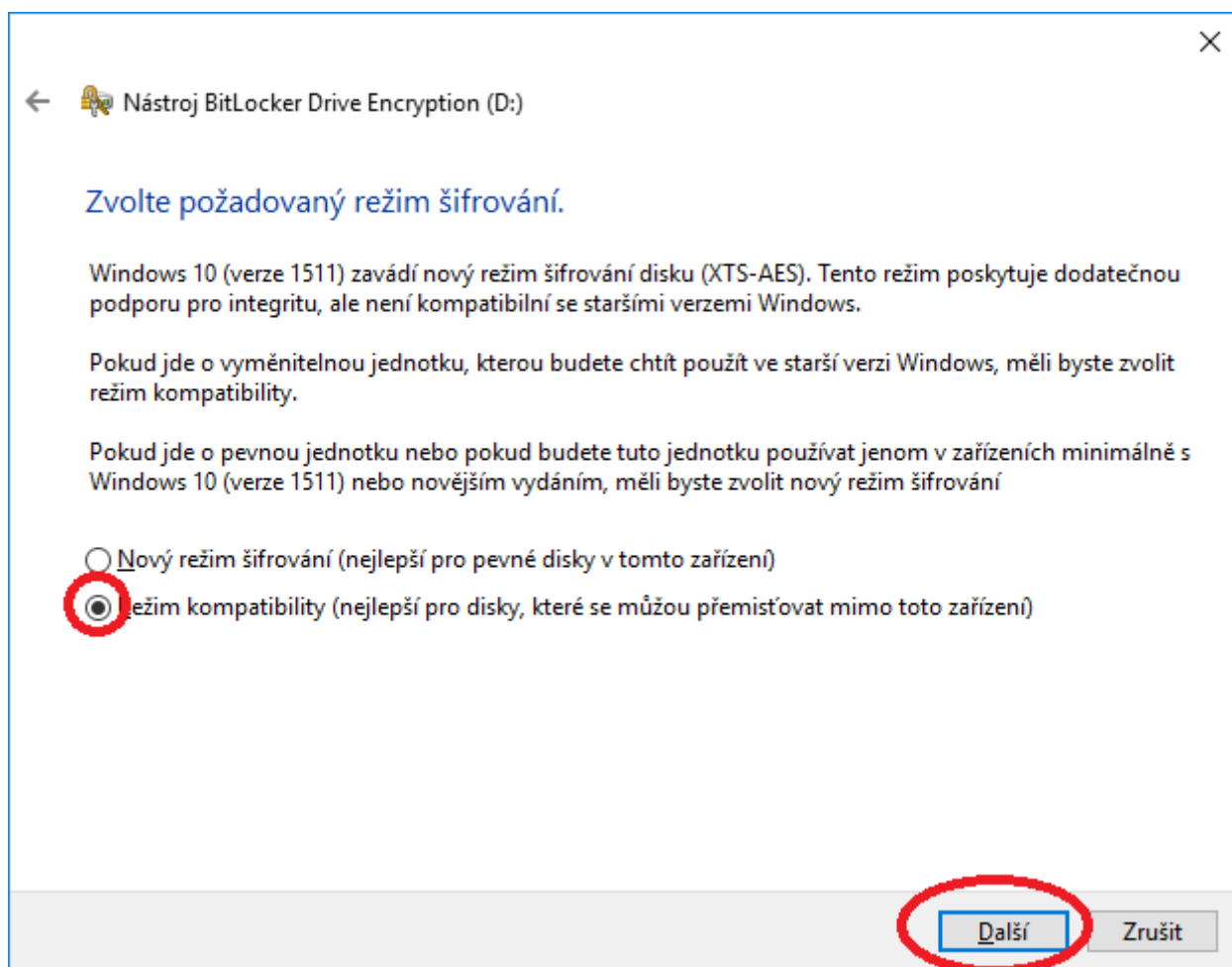
Pokračujte stiskem tlačítka „Další“.



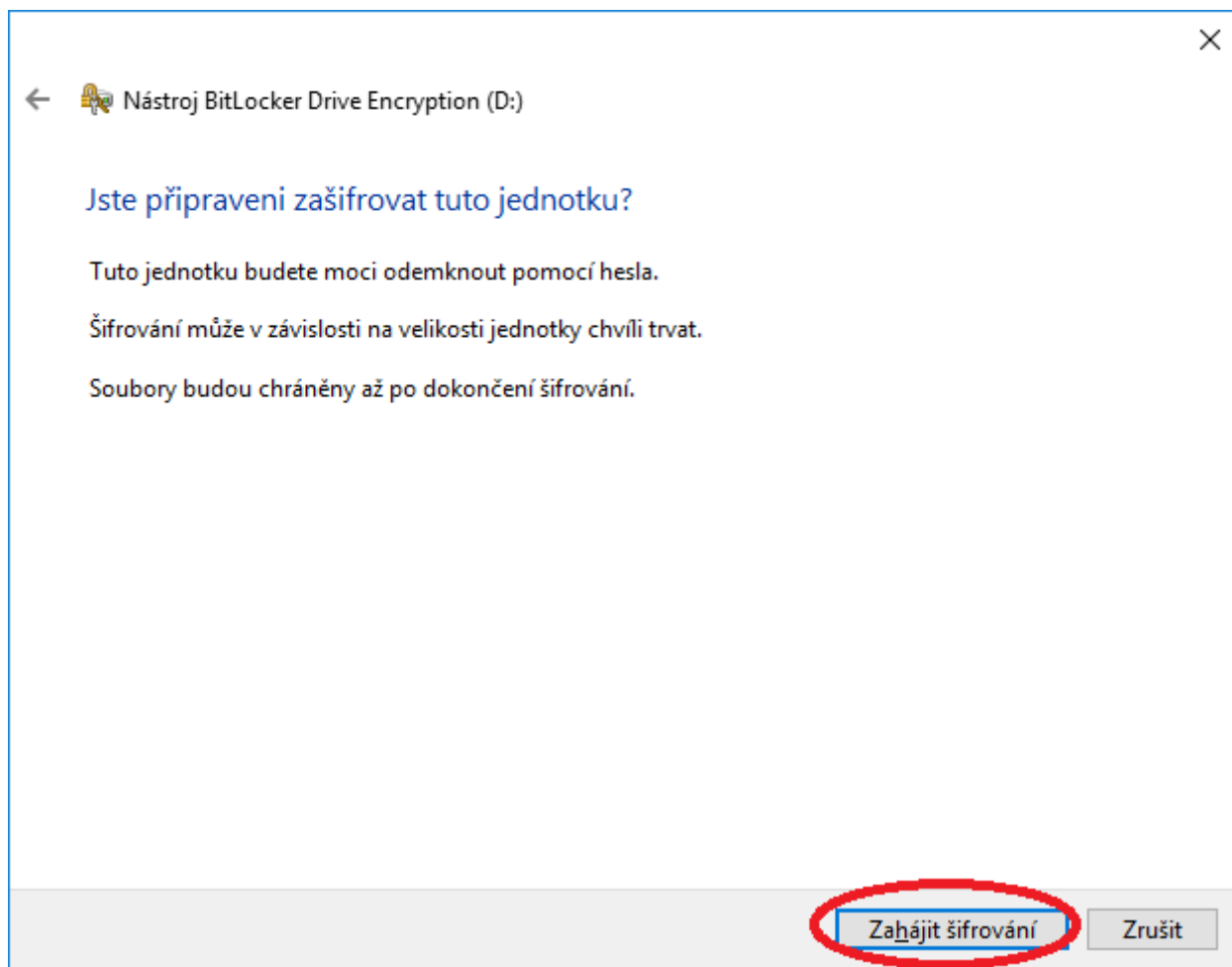
Jestliže se jedná o disk, ze kterého dosud nebyly tajné dokumenty mazány, zvolte první možnost. Pokud se na disku již dříve nacházely tajné soubory a nyní jsou smazány, zvolte druhou možnost, která je pomalejší, ale zajistí, že smazané soubory již nikdo neobnoví.



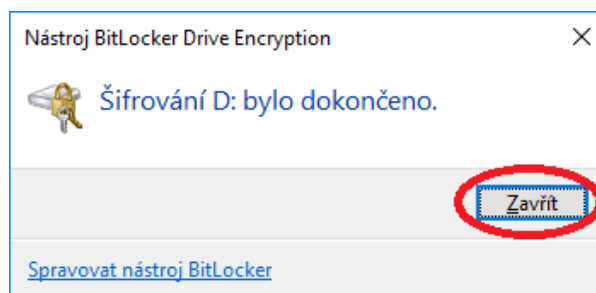
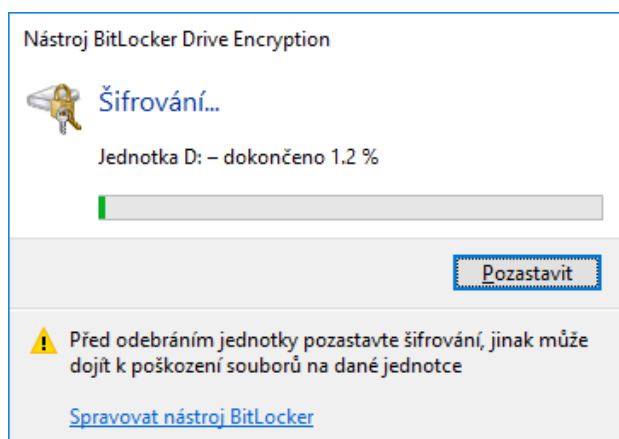
V dalším kroku zvolte režim kompatibility, aby bylo možno disk otevřít i ve starších verzích operačního systému Windows.



Na závěr spusťte šifrování stisknutím tlačítka „Zahájit šifrování“.



Šifrování může trvat v závislosti na množství dat a rychlosti úložiště i několik desítek minut.



Varianta 2: VeraCrypt - použití šifrovaného úložiště

Program VeraCrypt umožňuje vytvořit šifrovaný soubor, jež se po připojení chová jako běžný disk. Po odpojení je možno tento zašifrovaný soubor nakopírovat na externí disk nebo vypálit na CD. Pro rozšifrování souboru na jiném počítači je potřeba znát heslo a mít nainstalovaný program VeraCrypt.

Stažení programu VeraCrypt

Aktuální verzi programu naleznete na adrese:

<https://www.veracrypt.fr/en/Downloads.html>.

Na stránce se nacházejí instalátory pro různé operační systémy. Pro systém Windows je v době psaní tohoto návodu určen soubor „Windows: VeraCrypt Setup 1.22.exe (29.6 MB)“.

Home	Source Code	Downloads	Documentation	Donate	Forums
------	-------------	-----------	---------------	--------	--------

Note to publishers: If you intend to host our files on your server, please instead consider link help us prevent spreading of obsolete versions, which we believe is critical when security is at stake.

[Supported versions of operating systems](#)

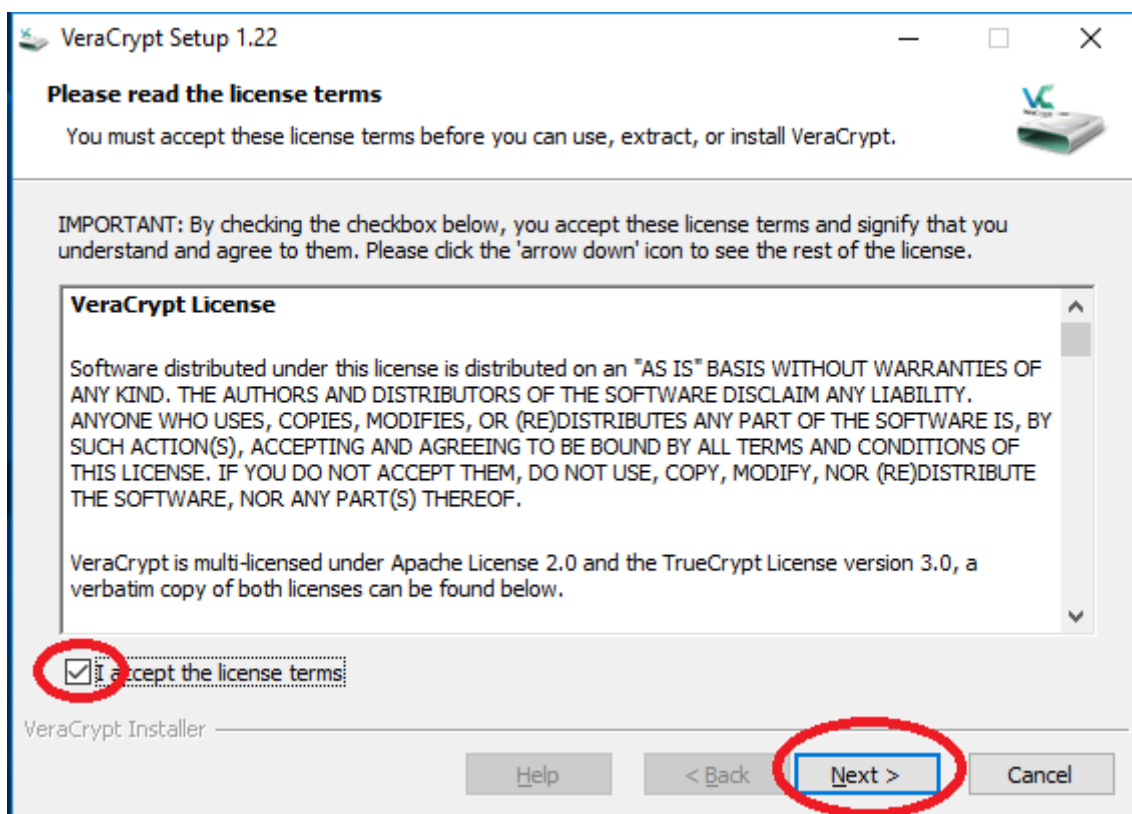
PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x54Fingerprint=993B7D7E8E413809828F0F29EB559C7C54DDD393)

Latest Stable Release - 1.22 (Friday March 30, 2018)

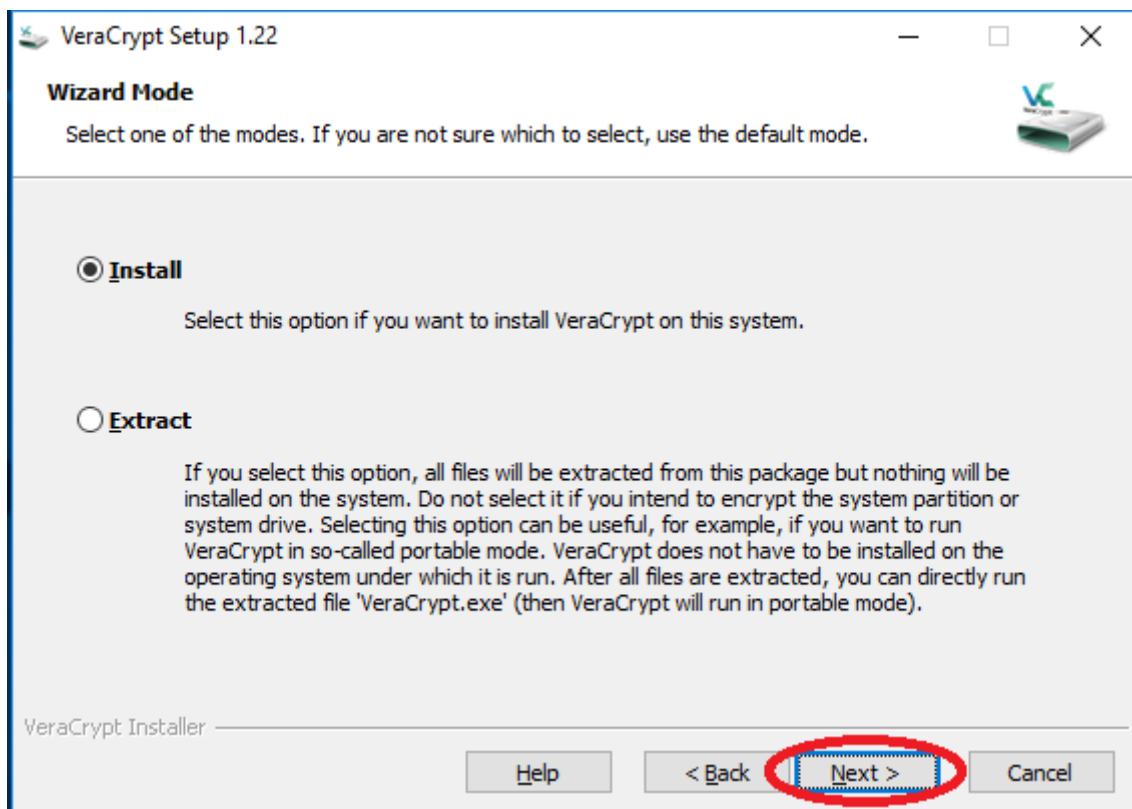
-  **Windows:** [VeraCrypt Setup 1.22.exe \(29.6 MB\)](#) (PGP Signature)
 - Portable version: [VeraCrypt Portable 1.22.exe \(29.4 MB\)](#) (PGP Signature)
-  **Mac OS X:** [VeraCrypt_1.22.dmg \(11.1 MB\)](#) (PGP Signature)
 - [OSXFUSE](#) 2.5 or later must be installed.
-  **Linux:** [veracrypt-1.22-setup.tar.bz2 \(14.6 MB\)](#) (PGP Signature)

Instalace programu VeraCrypt

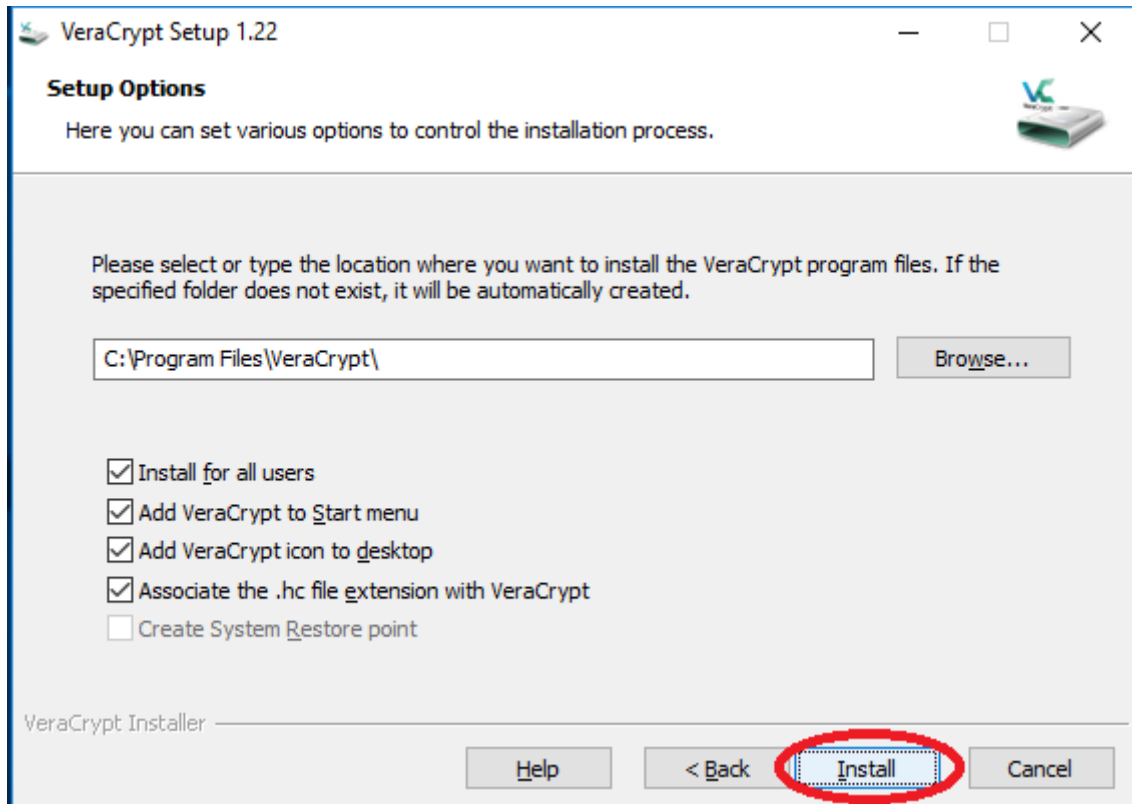
Po stažení spusťte instalátor a potvrďte spuštění s administrátorským oprávněním. Odsouhlaste licenční podmínky a pokračujte tlačítkem „Next >“. Jestliže nemáte administrátorská oprávnění, požádejte o instalaci programu svého správce.



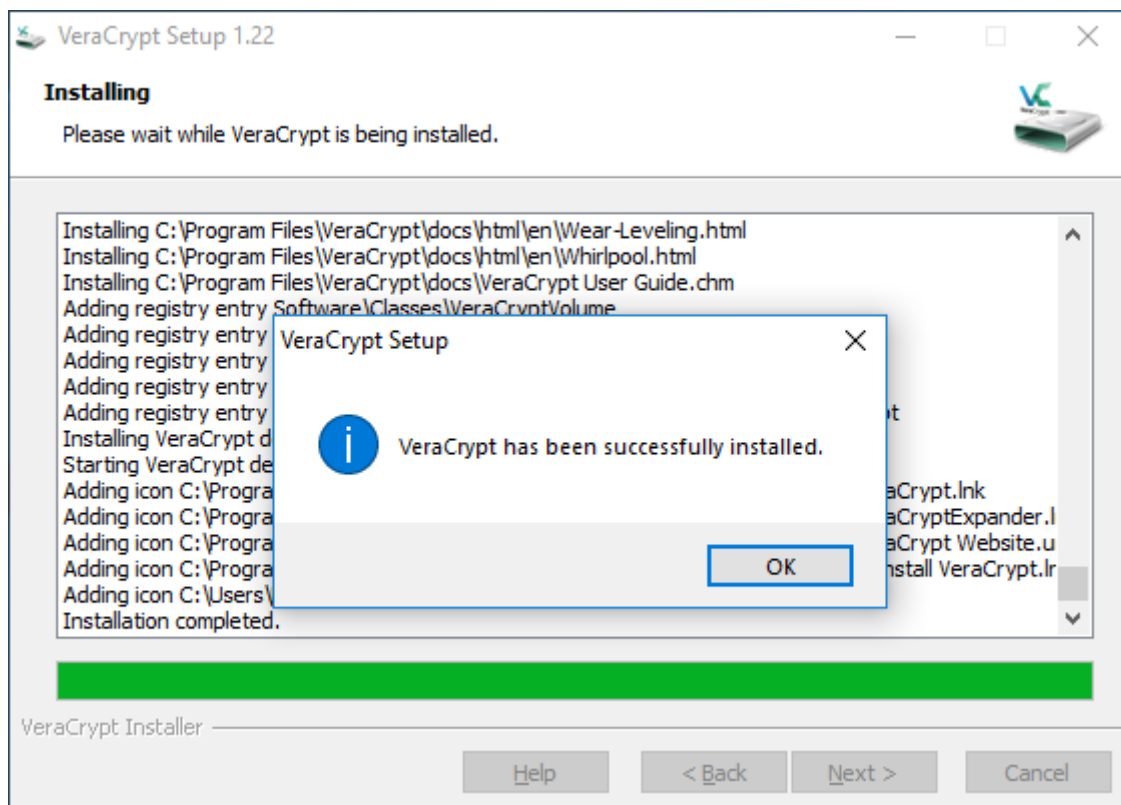
Ponechte vybranou možnost „Install“ a stiskněte „Next >“.



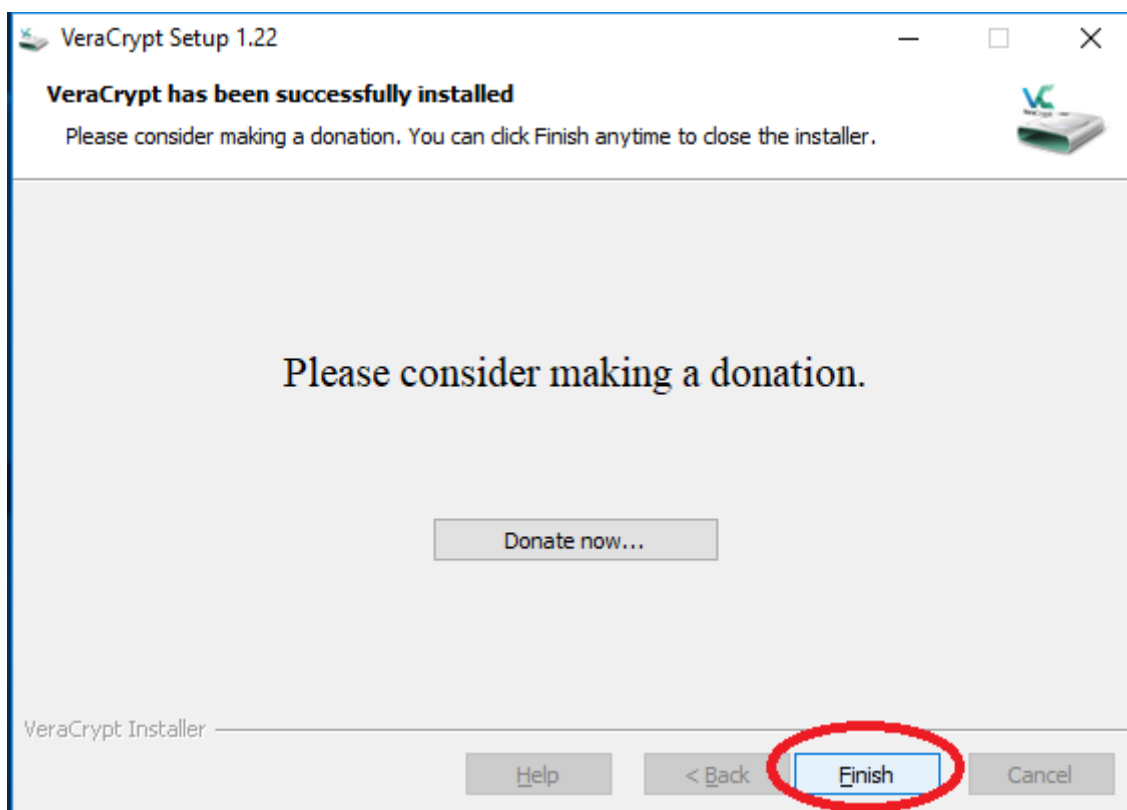
Ponechte výchozí hodnoty a pokračujte na „Install“.



Dokončení instalace potvrďte tlačítkem „OK“.



Stiskněte tlačítko „Finish“.

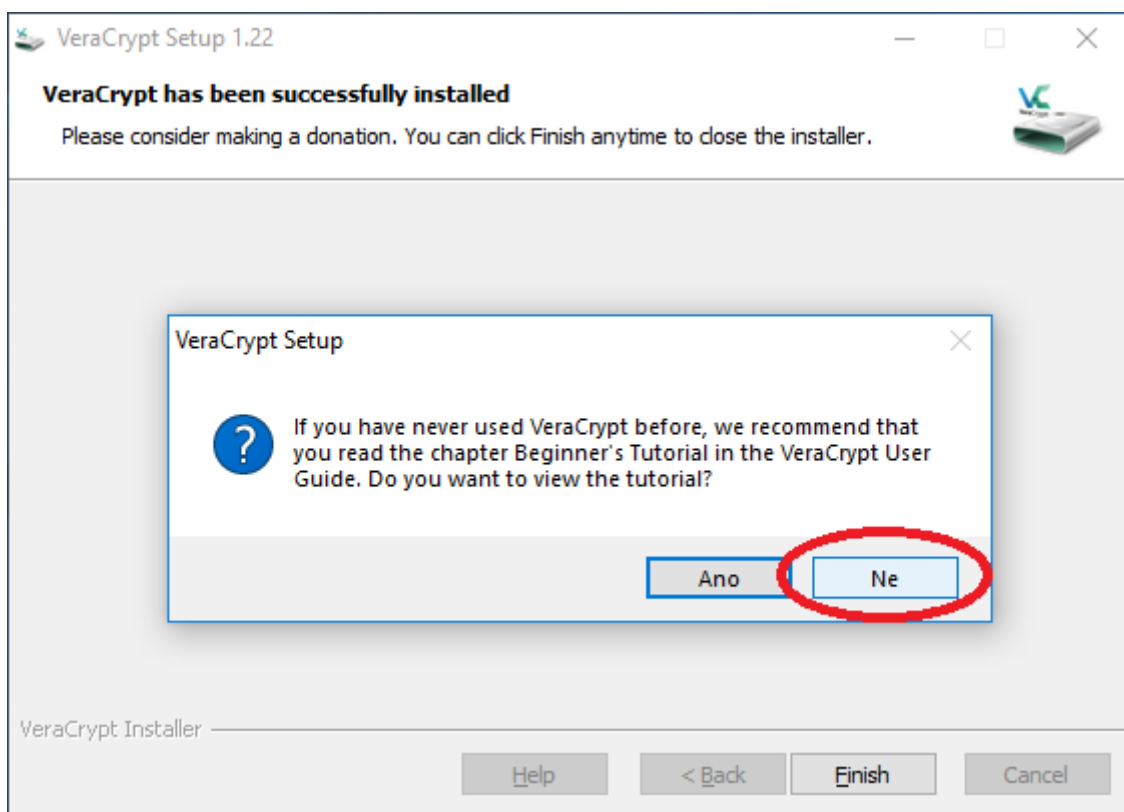


Vysoká škola polytechnická Jihlava

Tolstého 16, 586 01 Jihlava | e-mail: vspj@vspj.cz | tel.: 567 141 111 | fax.: 567 300 727

IČ: 71226401 | DIČ: CZ71226401 | www.vspj.cz

V případě zájmu si můžete nechat zobrazit webovou stránku s tutoriálem na ovládání programu. Není to však nutné a můžete zvolit variantu „Ne“.



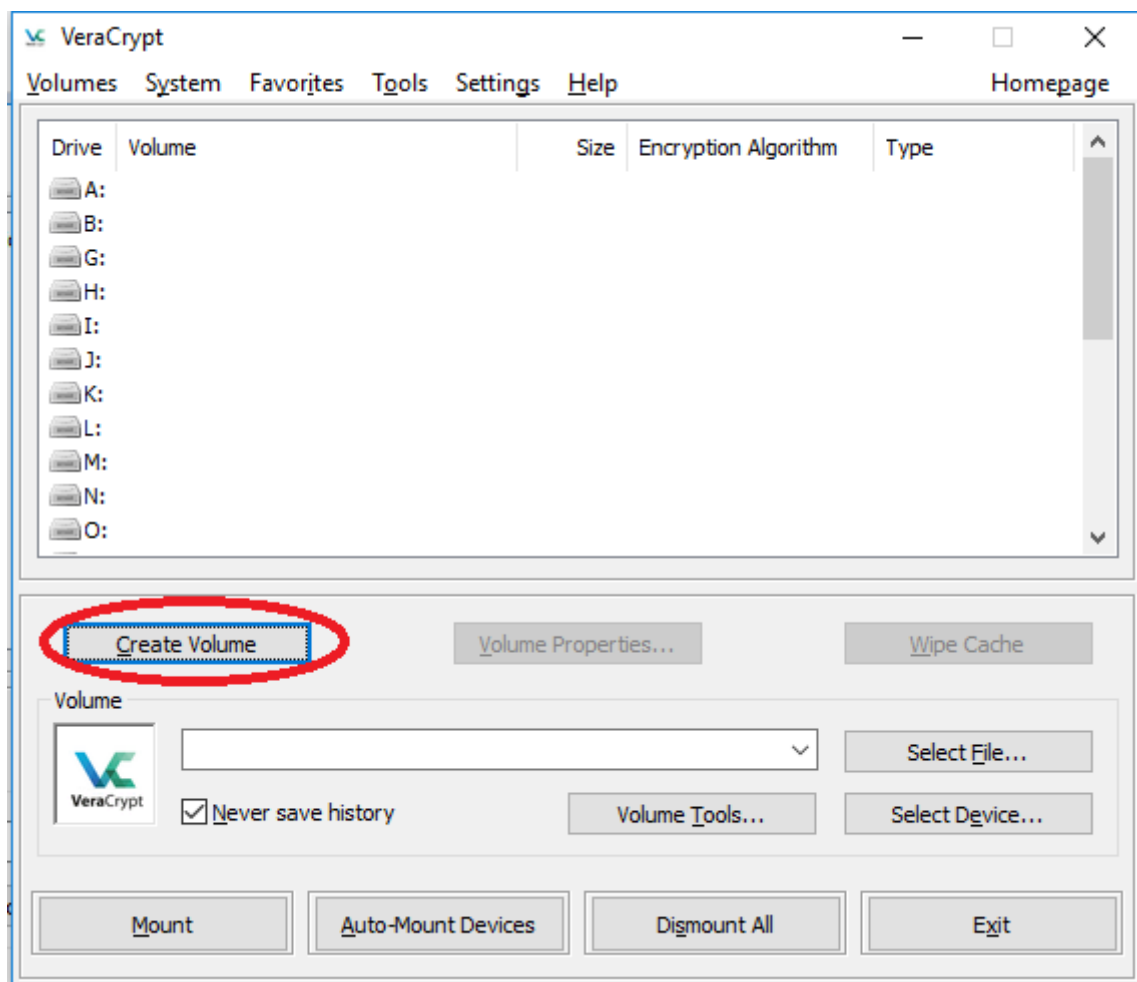
Nyní je instalace dokončena.

Vytvoření šifrovaného úložiště

Po instalaci by se na ploše měla nacházet ikonka programu VeraCrypt. Poklepejte na ni a spusťte aplikaci.



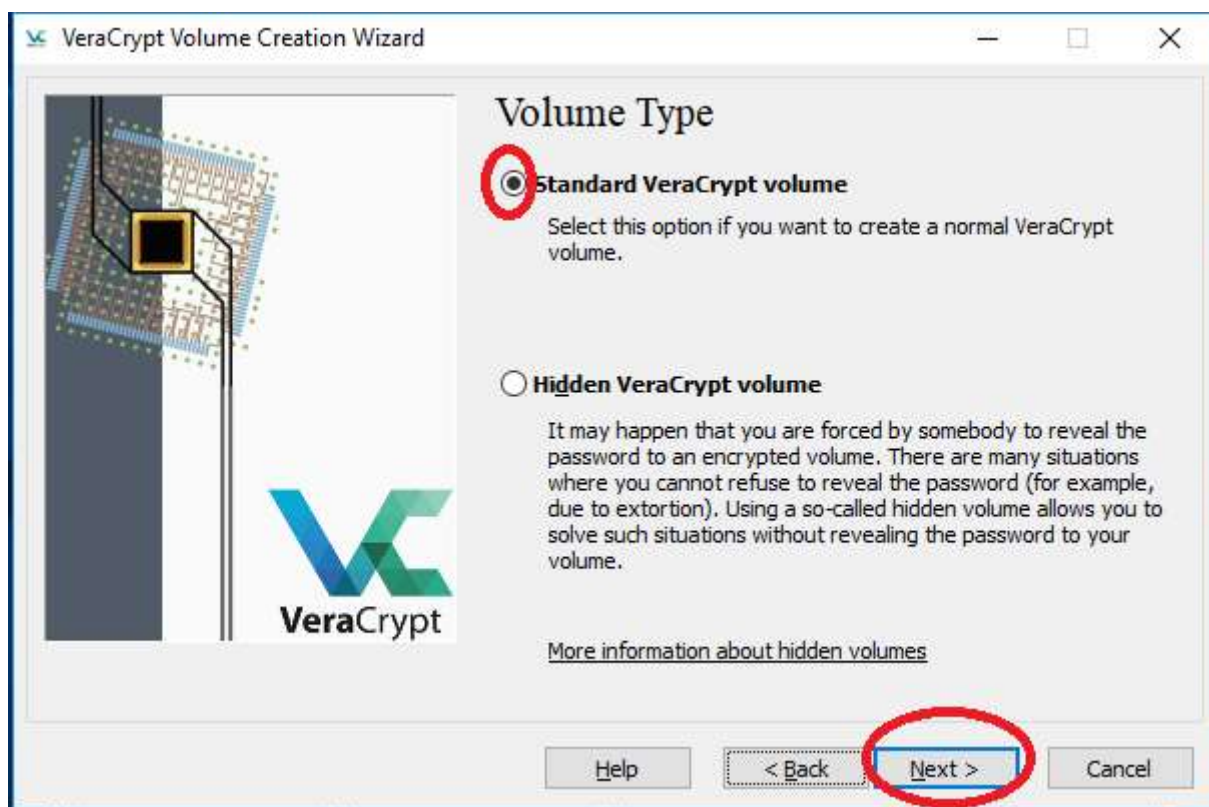
Pro vytvoření nového šifrovaného úložiště stiskněte tlačítko „Create Volume“.



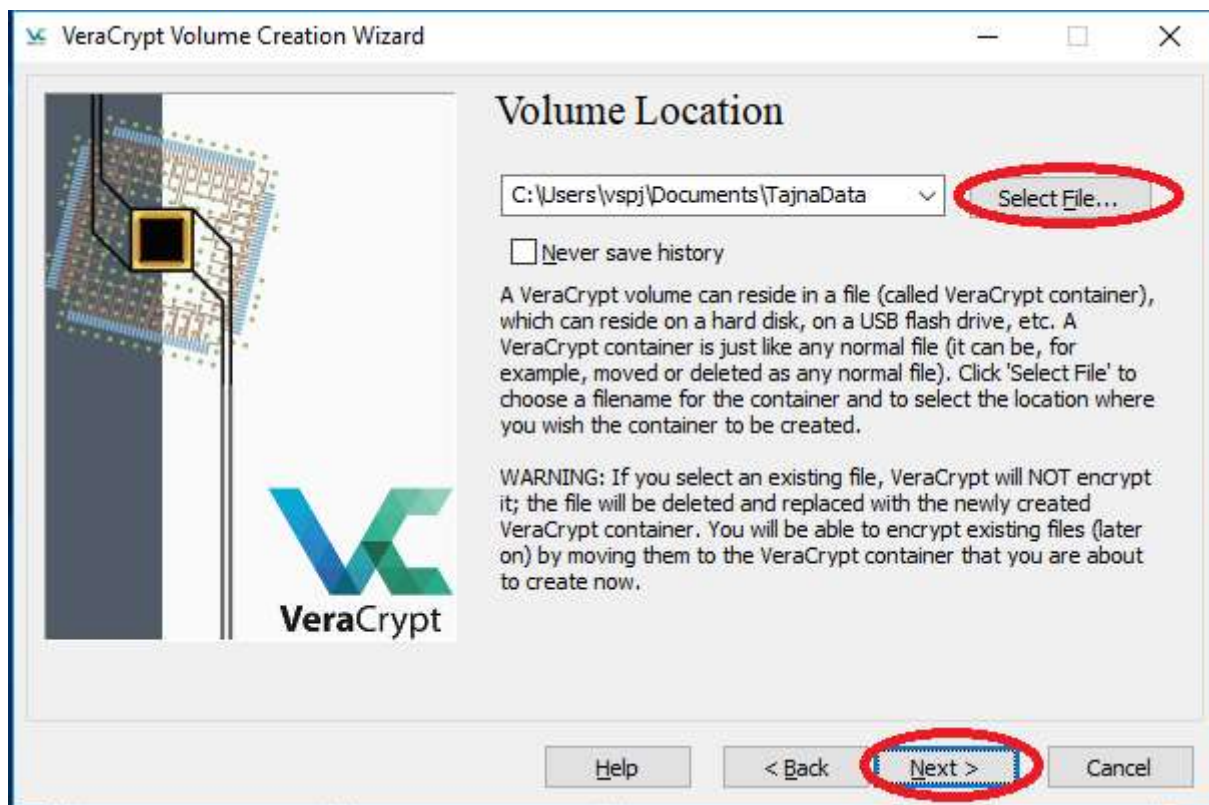
Zvolte možnost „Create an encrypted file container“ a pokračujte tlačítkem „Next >“.



Ponechte výchozí typ „Standard VeraCrypt volume“ a pokračujte tlačítkem „Next >“.



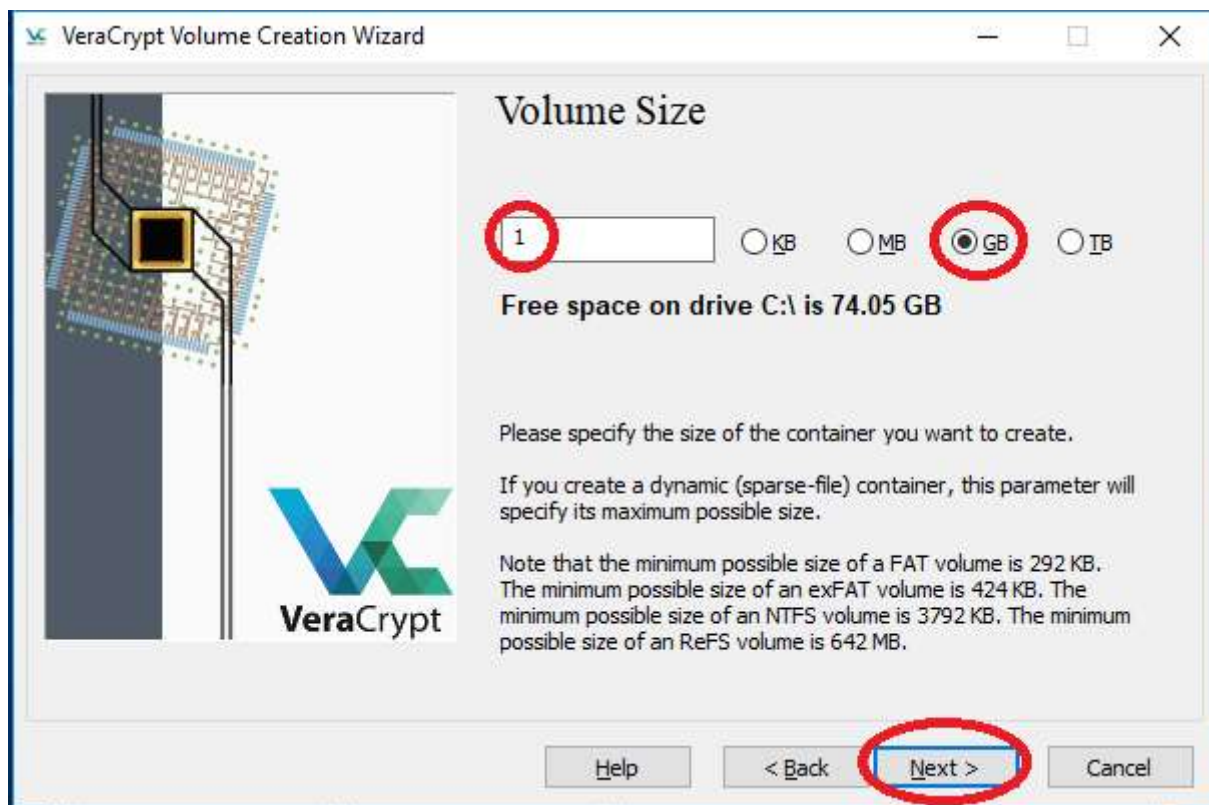
Nyní zvolte umístění a název šifrovaného souboru. Zvolte takové umístění, kde budete soubor snadno k nalezení, ale nebudou k němu mít přístup neoprávněné osoby. Poté pokračujte tlačítkem „Next >“.



Ponechte výchozí nastavení šifrovacího algoritmu a pokračujte tlačítkem „Next >“.



V závislosti na předpokládaném objemu ukládaných dat nastavte maximální kapacitu šifrovaného úložiště. V tomto návodu byla zvolena kapacita 1GB.

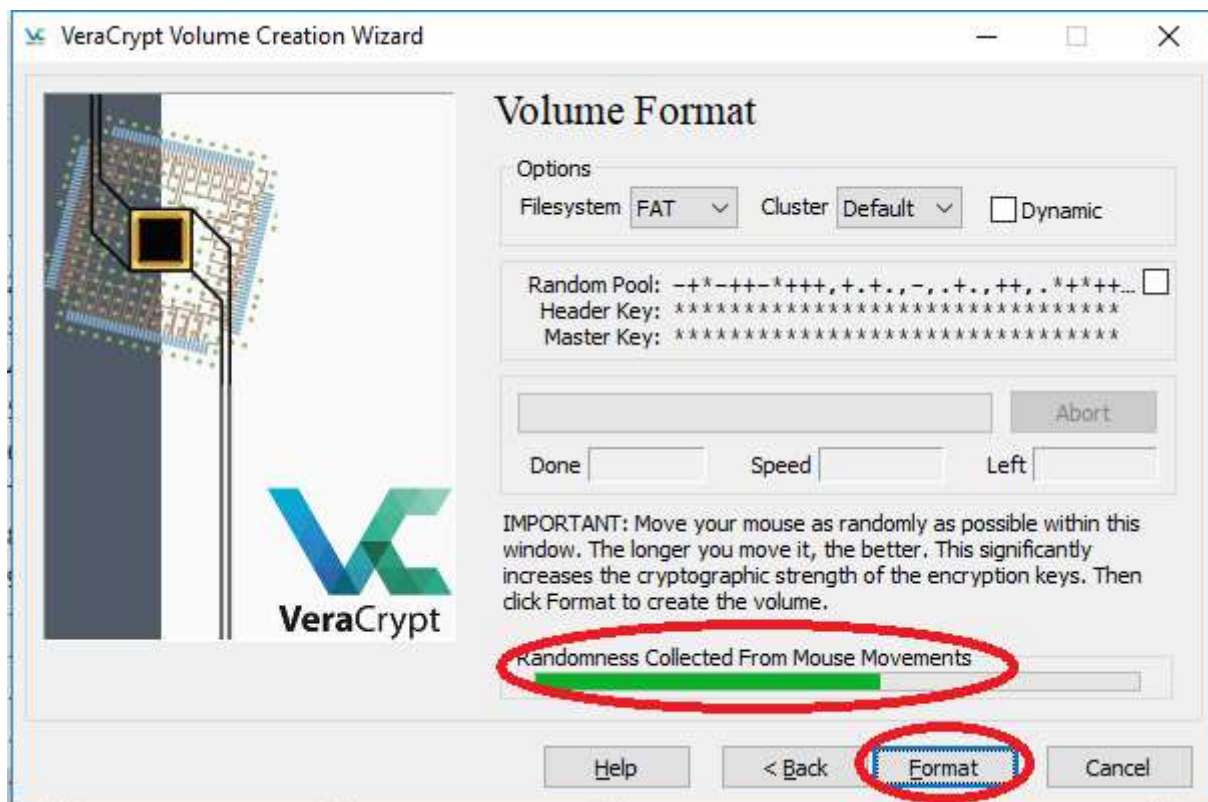


Nyní zadejte heslo, kterým budou data chráněna. Heslo by mělo být dostatečně silné, aby nebylo snadné jej prolomit, ale současně i zapamatovatelné, neboť jej budete muset psát po každém restartu počítače, když budete chtít s úložištěm pracovat.

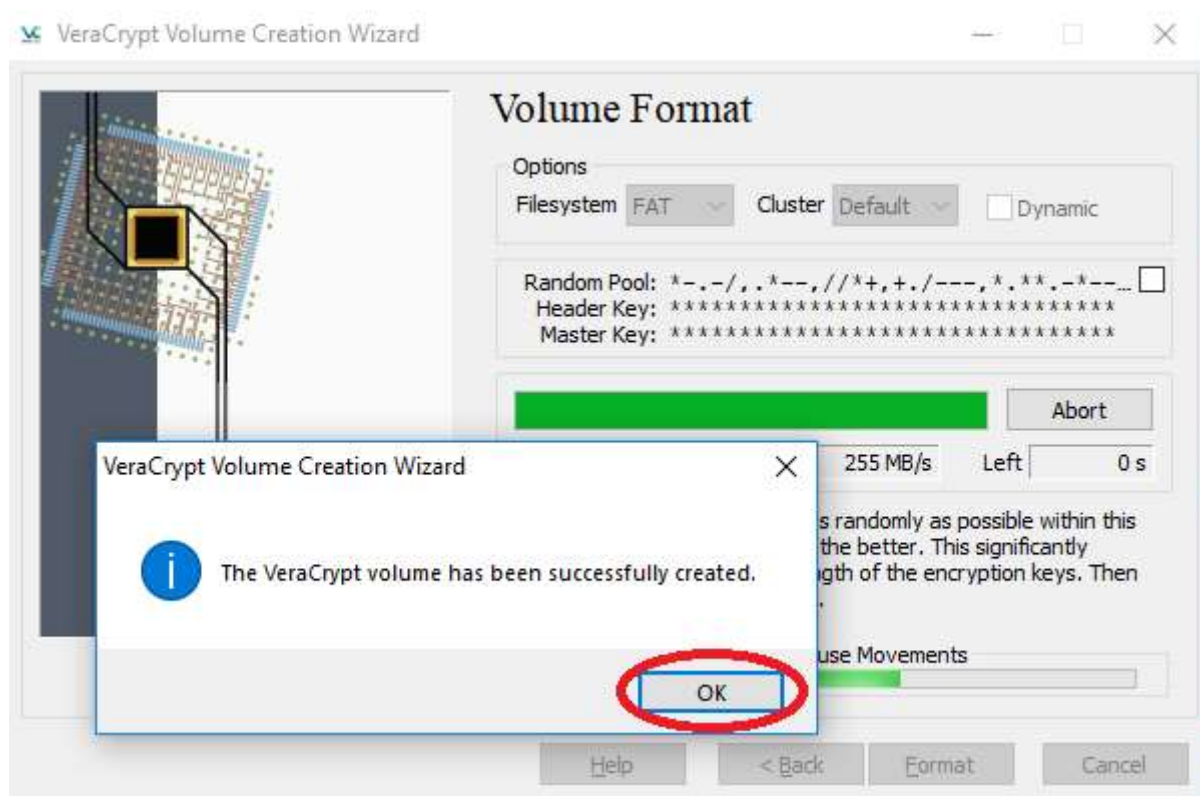
Za minimální délku hesla lze považovat 8 znaků složených z velkých a malých písmen, číslic a speciálních symbolů (jako: = , : & @ a podobně). Heslo by nemělo být založeno na jménech či slovech neboť takové heslo je snadno prolomitelné slovníkovým útokem. Doporučená délka hesla je 20 znaků a maximální 64 znaků. **POZOR!** V případě zapomenutí hesla není možné již data z šifrovaného úložiště otevřít.



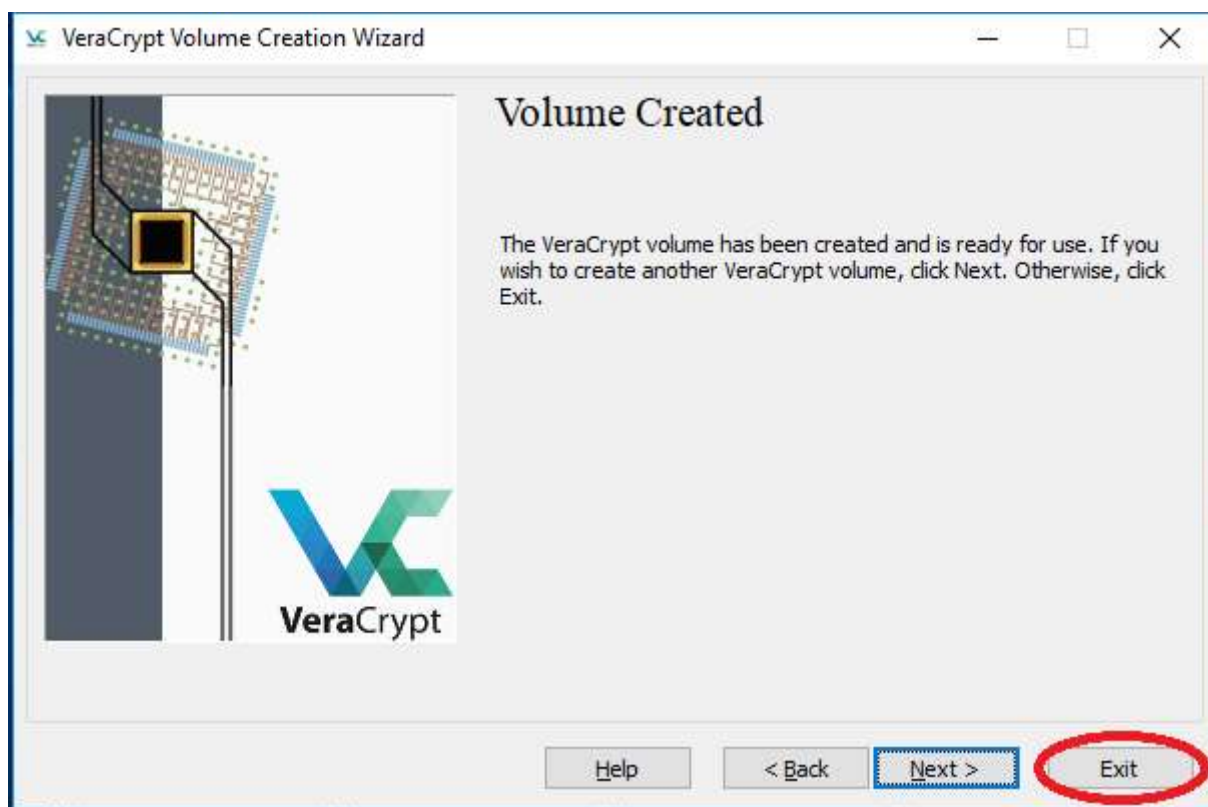
Nyní je nutno, pohybovat myší po formuláři, než indikátor délky náhodných hodnot změni barvu na zelenou. Poté pokračujte tlačítkem „Format“.



Dokončení formátování šifrovaného úložiště potvrďte tlačítkem „OK“.



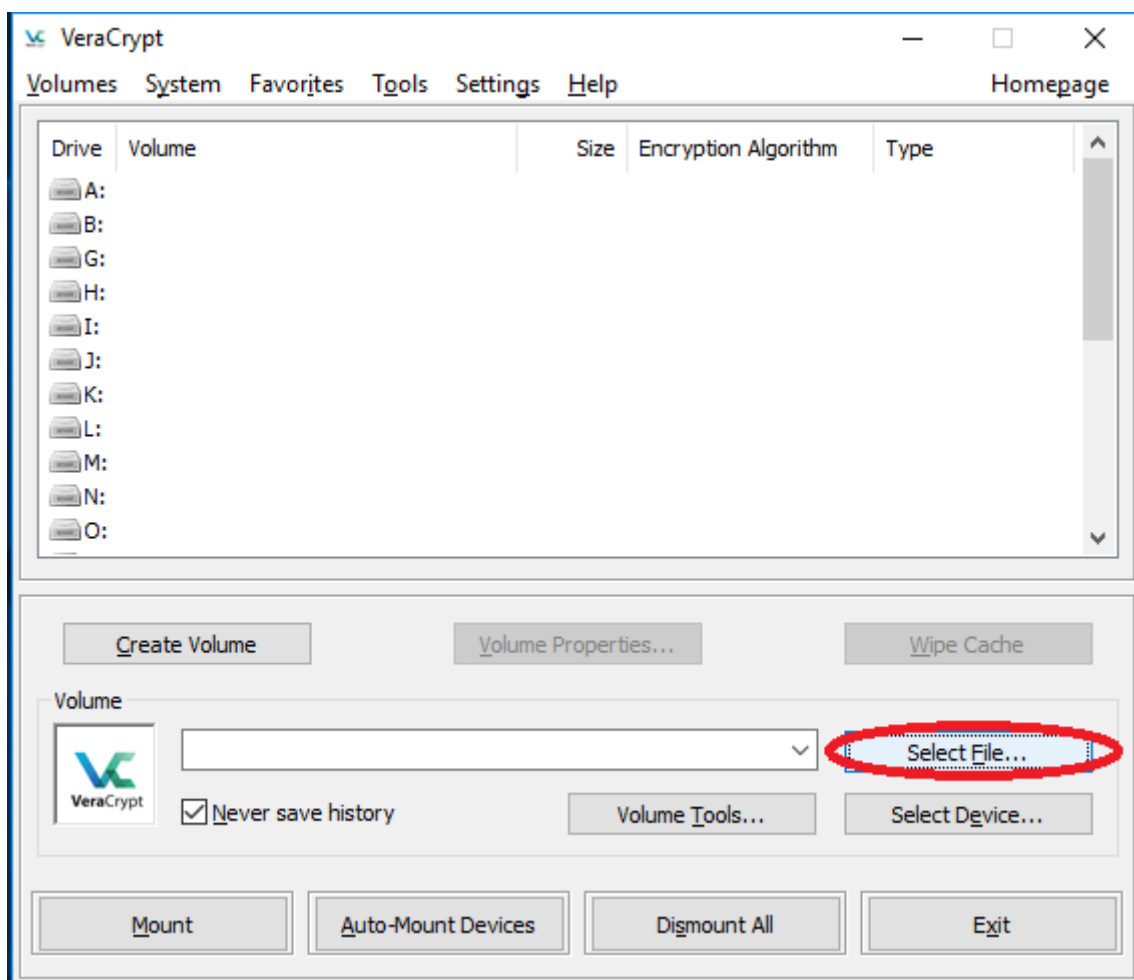
Nyní je šifrované úložiště vytvořeno a průvodce můžeme ukončit tlačítkem „Exit“.



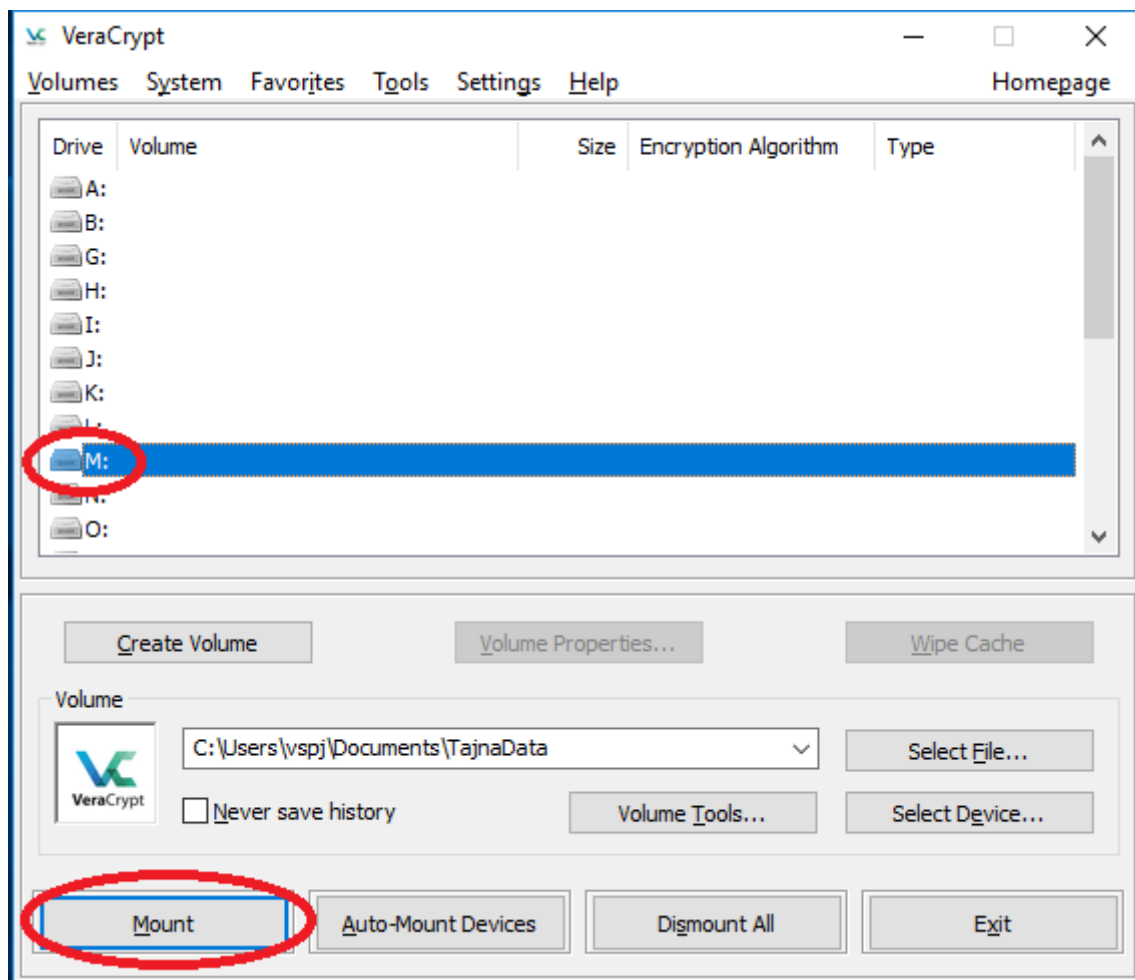
Otevření šifrovaného úložiště

Aby bylo možné do šifrovaného úložiště ukládat data nebo je číst, je potřeba toto úložiště tzv. „přimontovat“ na nějakou volnou diskovou jednotku.

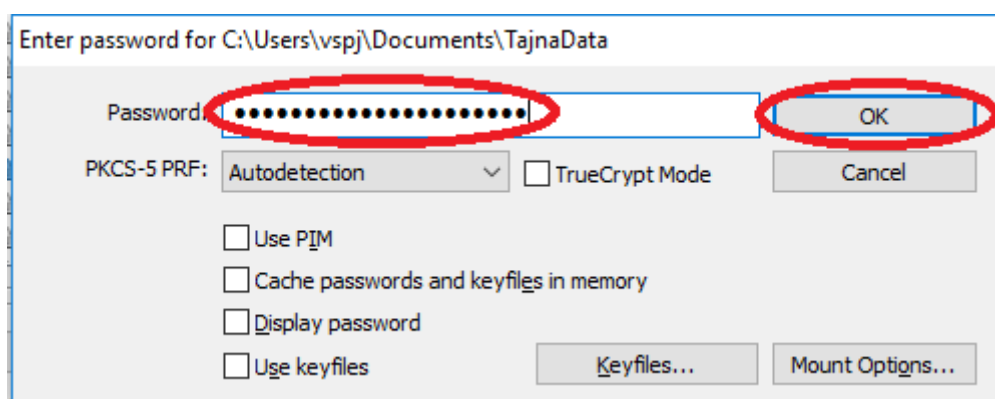
Přes tlačítko „Select file“ vyberte soubor šifrovaného úložiště.



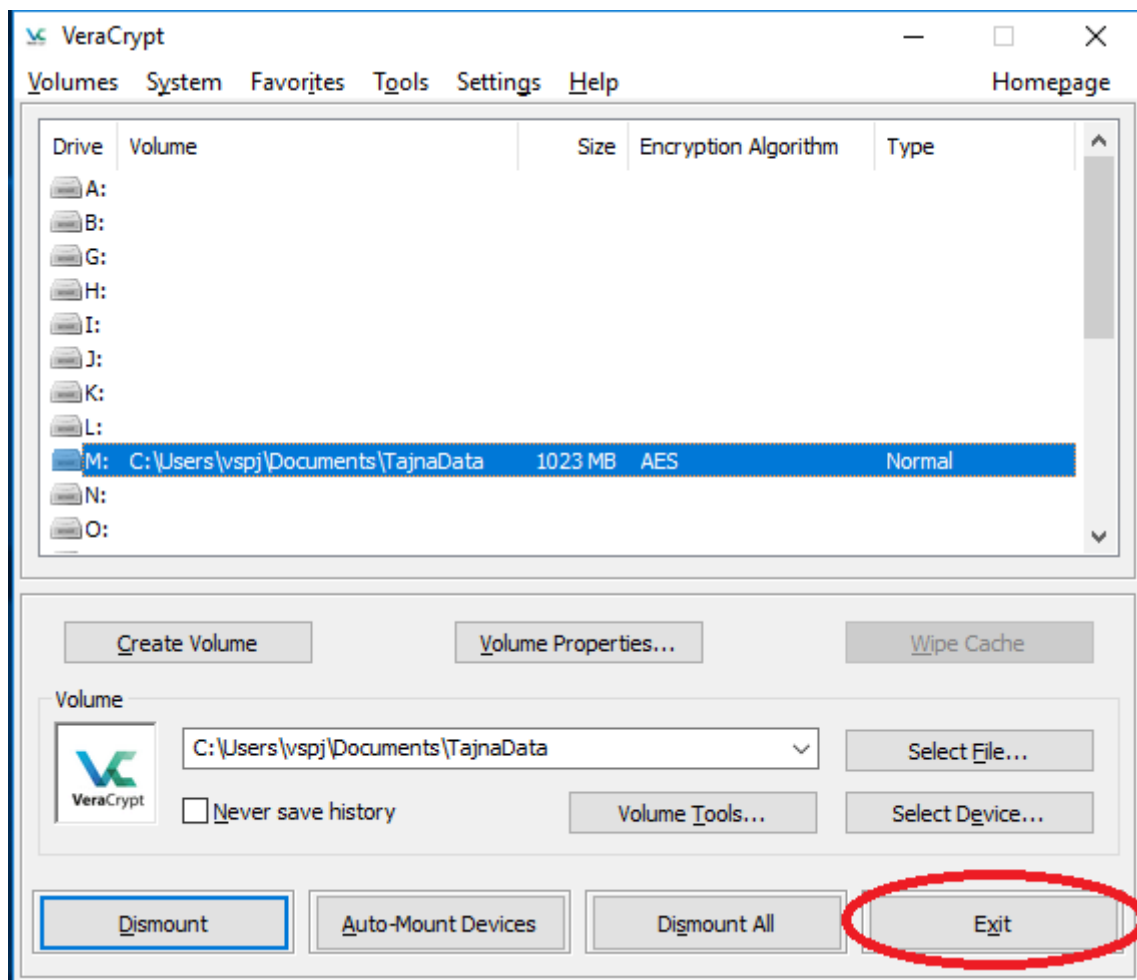
Nyní označte nějaké písmeno volné diskové jednotky, kterou chcete pro ukládání používat. V návodu bylo zvoleno písmeno „M:“. Pokračujte tlačítkem „Mount“.



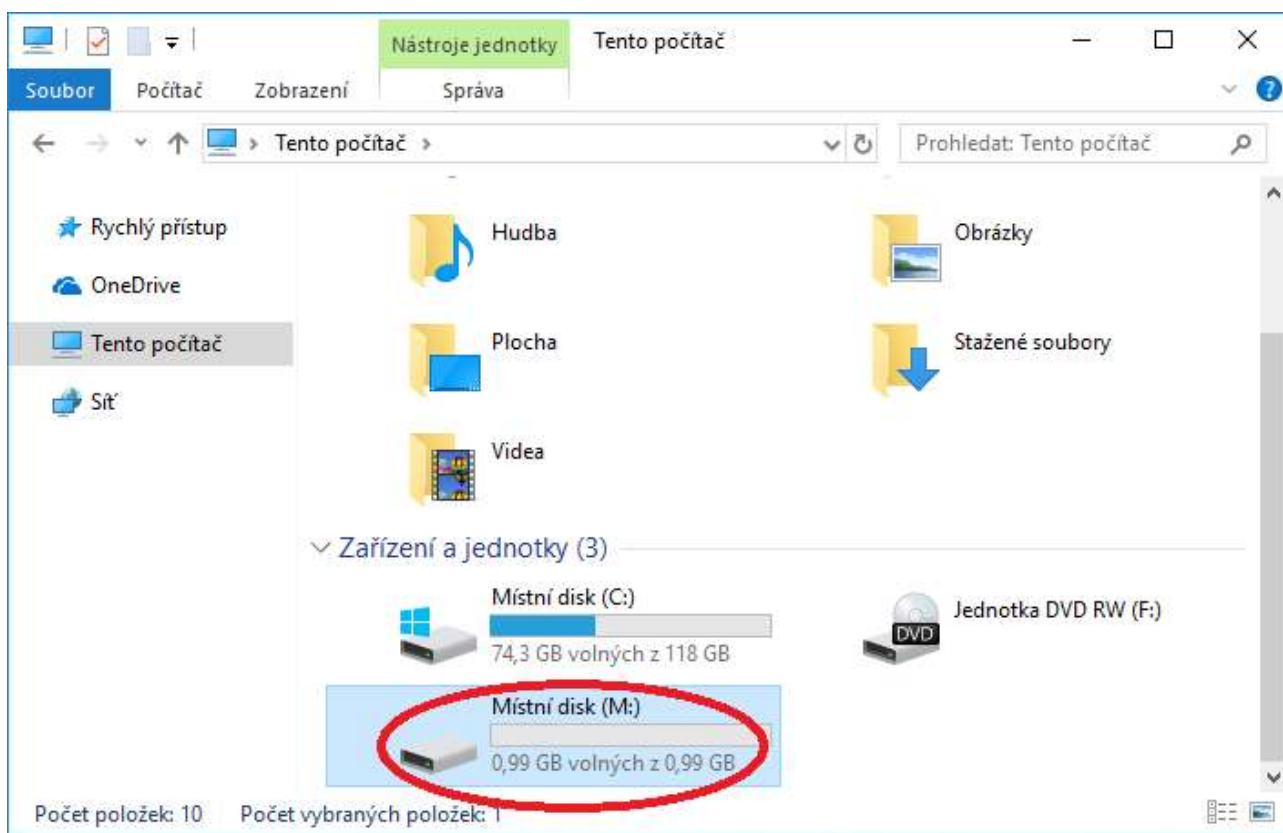
Nyní zadejte heslo, kterým jste úložiště zašifrovali v době jeho vytváření a stiskněte tlačítko „OK“. Pro urychlení, v případě, že zadáte chybné heslo, můžete namísto „Autodetection“ zvolit správný formát šifrování. V tomto návodu je to „HMAC-SHA-512“.



Pokud se rozšifrování úložiště podařilo, vidíte pod zvoleným písmenem disku onen „namontovaný“ soubor. Můžete aplikaci ukončit tlačítkem „Exit“.



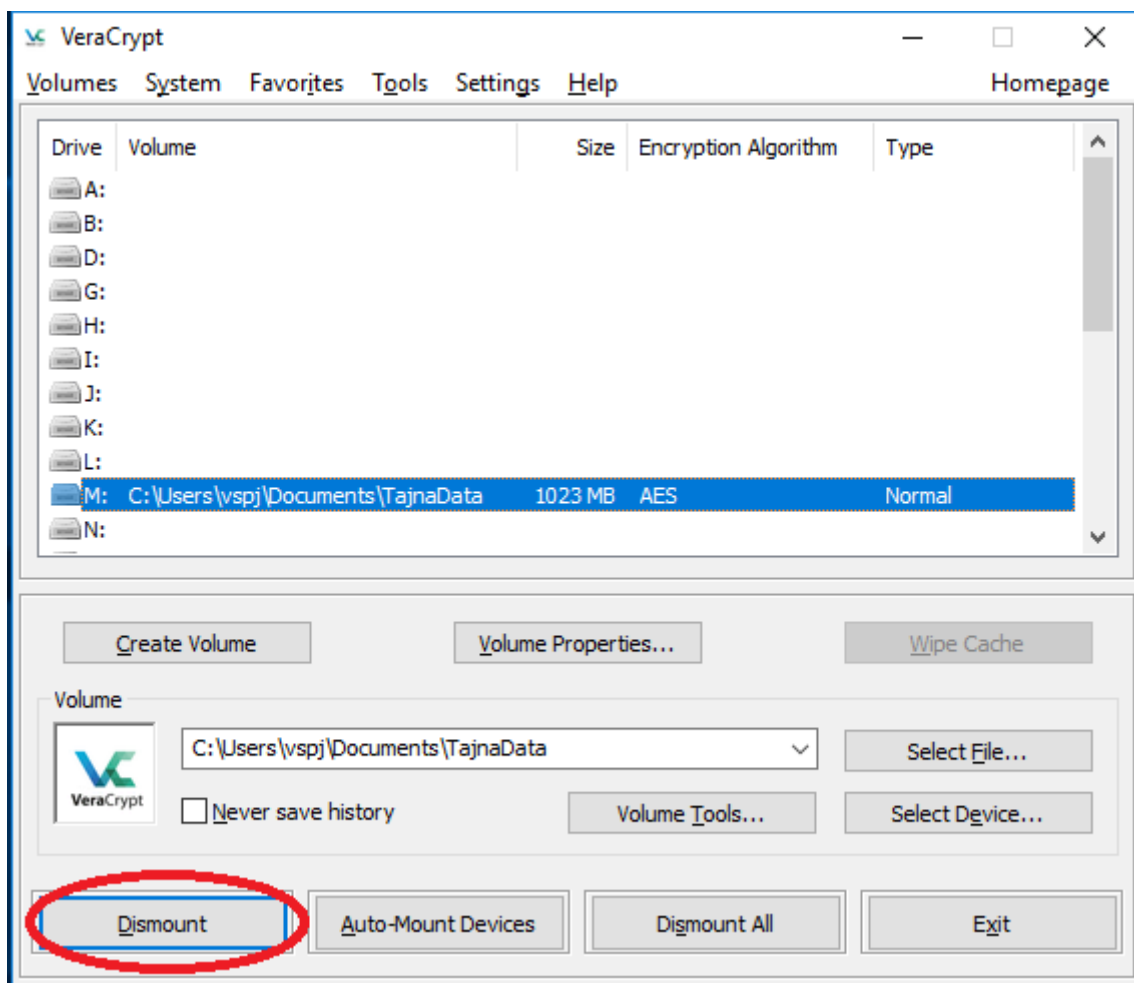
V závislosti na zvoleném písmenku je nyní v části „Tento počítač“ vidět nový disk s tímto písmenkem. V tomto návodu je to „M:“. S tímto diskem je možno nyní pracovat jako s každým jiným diskem. Lze na něj utajované soubory ukládat či je z něj kopírovat nebo rovnou otevírat.



Odpojení šifrovaného úložiště

Jestliže je práce s úložištěm dokončena nebo pokud chcete soubor s úložištěm přesunout třeba na flešku nebo vypálit na CD, je potřeba toto úložiště nejprve „odmontovat“.

Otevřete program VeraCrypt, označte písmeno s připojeným úložištěm a stiskněte na tlačítko „Dismount“.



Varianta 3: VeraCrypt – šifrování disků

Program VeraCrypt umožňuje také šifrování celých disků, obdobně jako BitLocker. Na rozdíl od programu BitLocker není vytvořen žádný obnovovací klíč, takže v případě zapomenutí hesla již není možné se k datům dostat. Také po vložení zašifrovaného disku jej nejsou Windows schopny otevřít a vybízejí k jeho naformátování. **POZOR!** Disk nesmíte naformátovat, jinak ztratíte všechna data, která na něm jsou.

K otevření takto šifrovaného disku je nutno spustit VeraCrypt a disk „namontovat“.

Šifrovaný disk musí být formátován na souborový systém NTFS.

Stažení a instalace

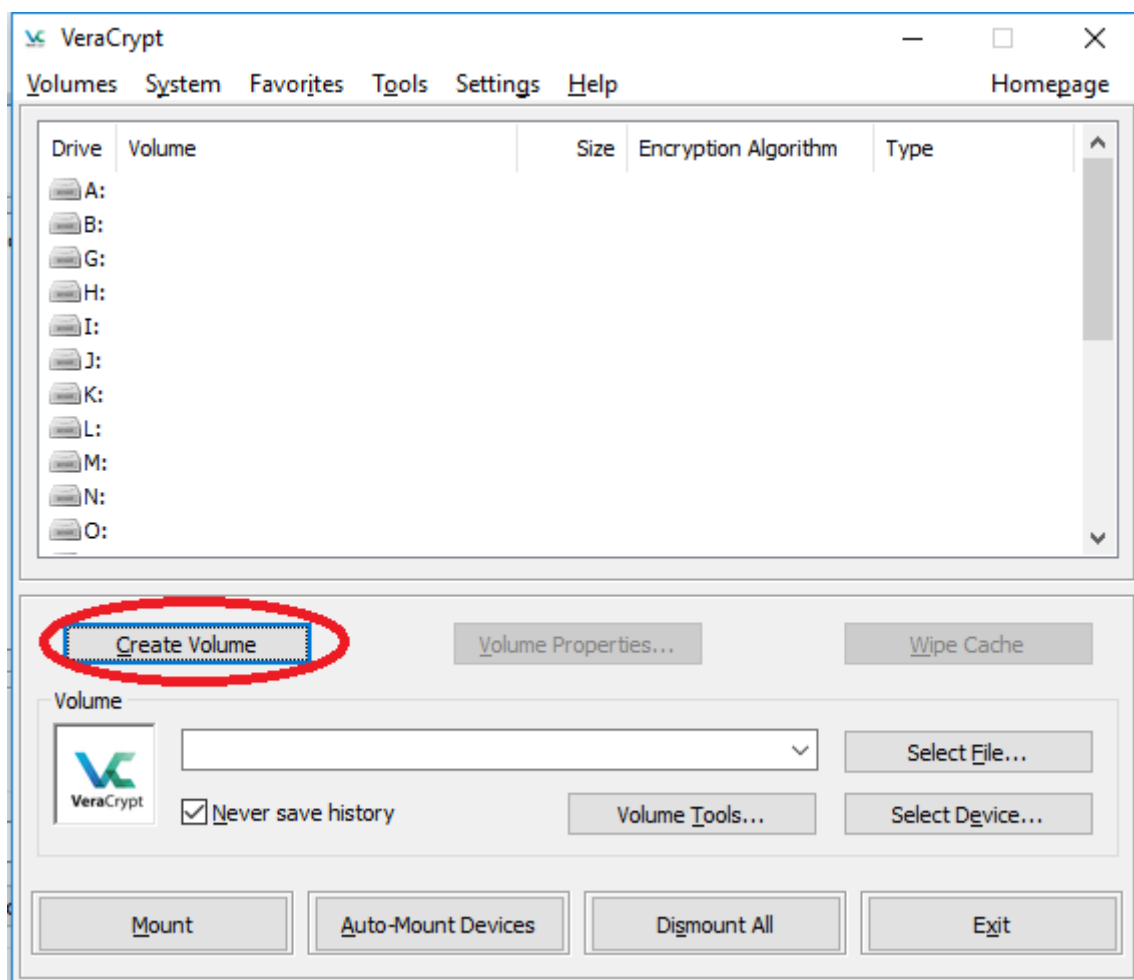
Tyto úkony jsou popsány v oddílech Stažení programu VeraCrypt a Instalace programu VeraCrypt.

Zašifrování disku

Spustíte program VeraCrypt přes ikonu na ploše.



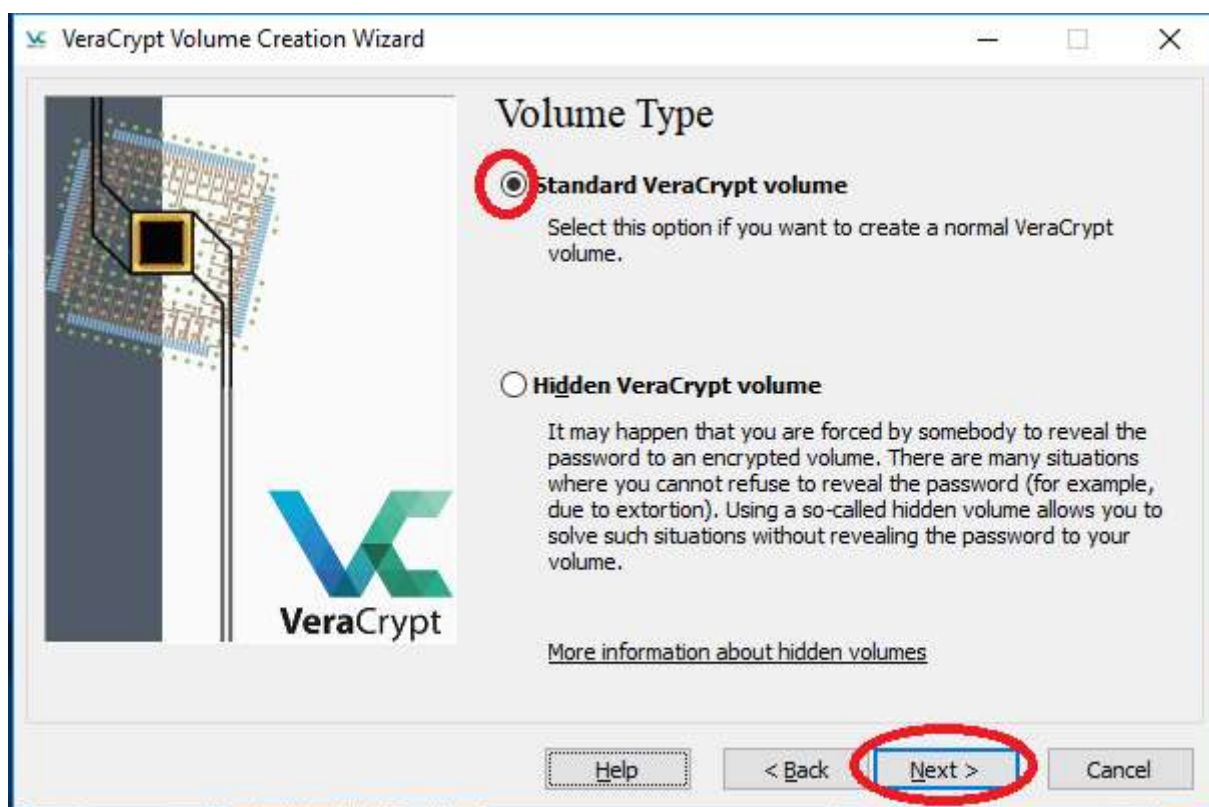
Stiskněte tlačítko „Create volume“.



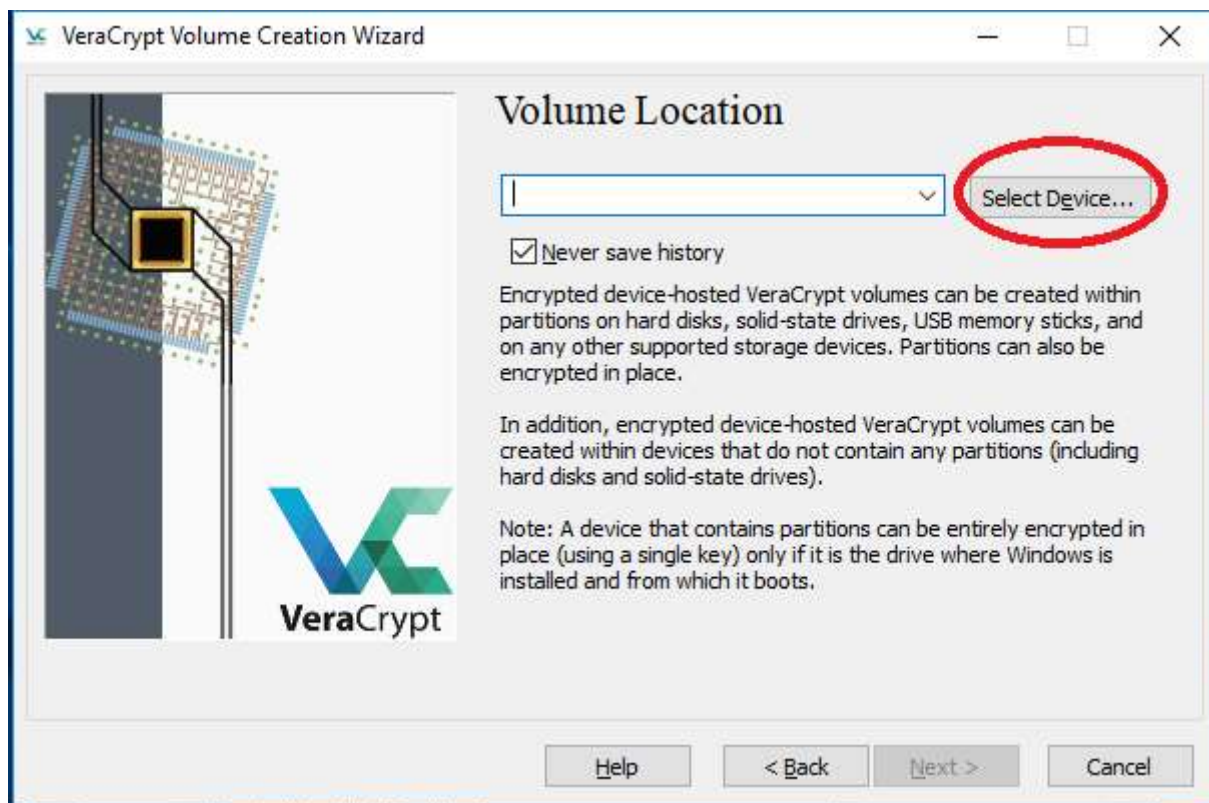
Vyberte šifrování nesystémového oddílu a stiskněte „Next >“. Následně potvrďte přepnutí do privilegovaného „admin“ režimu.



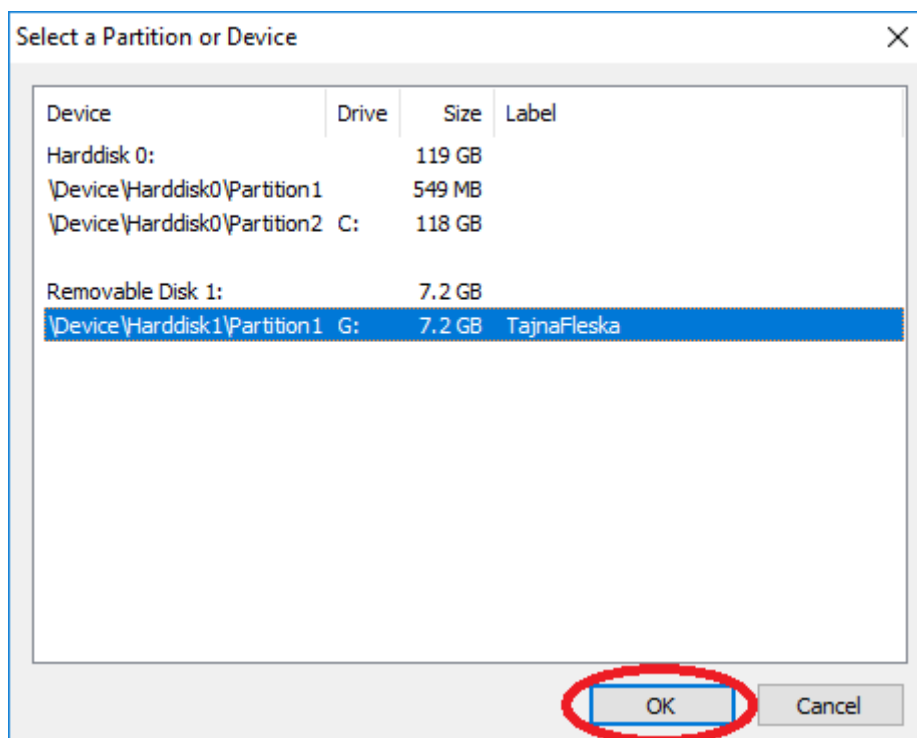
Ponechte standardní oddíl a pokračujte tlačítkem „Next >“.



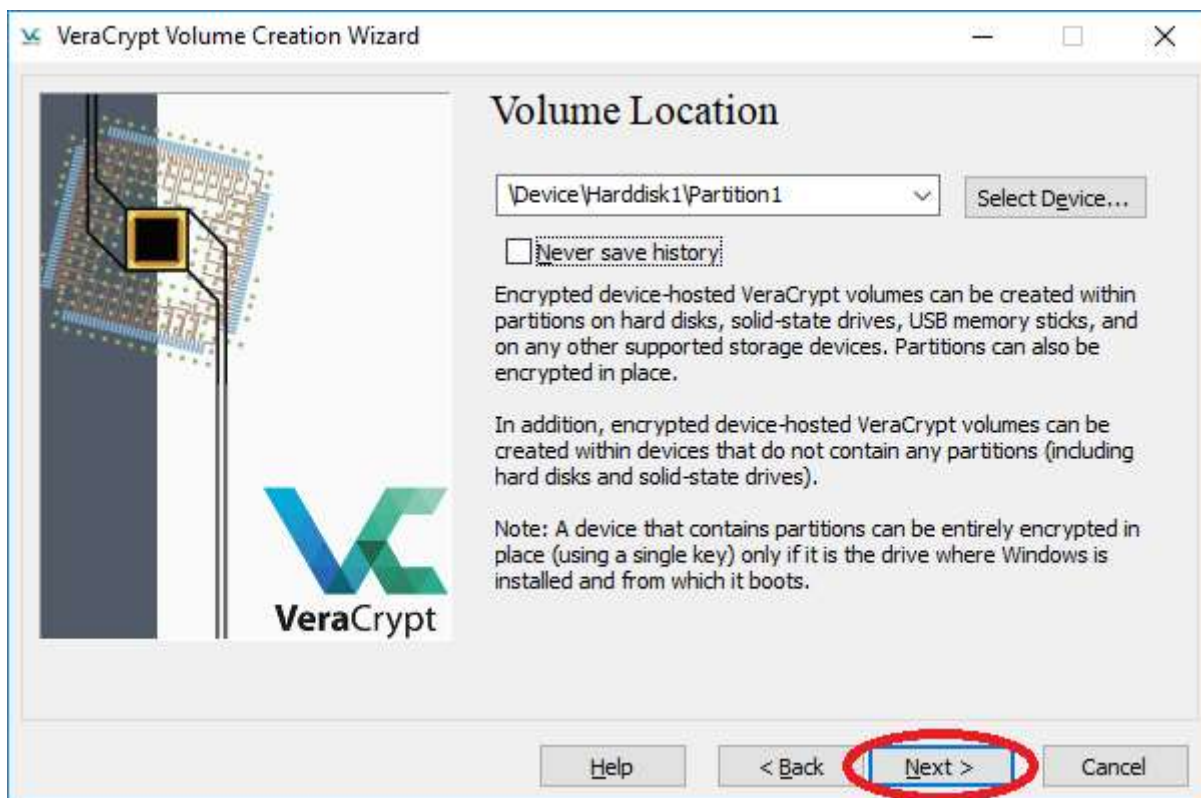
Stiskněte „Select Device“ pro výběr oddílu k zašifrování.



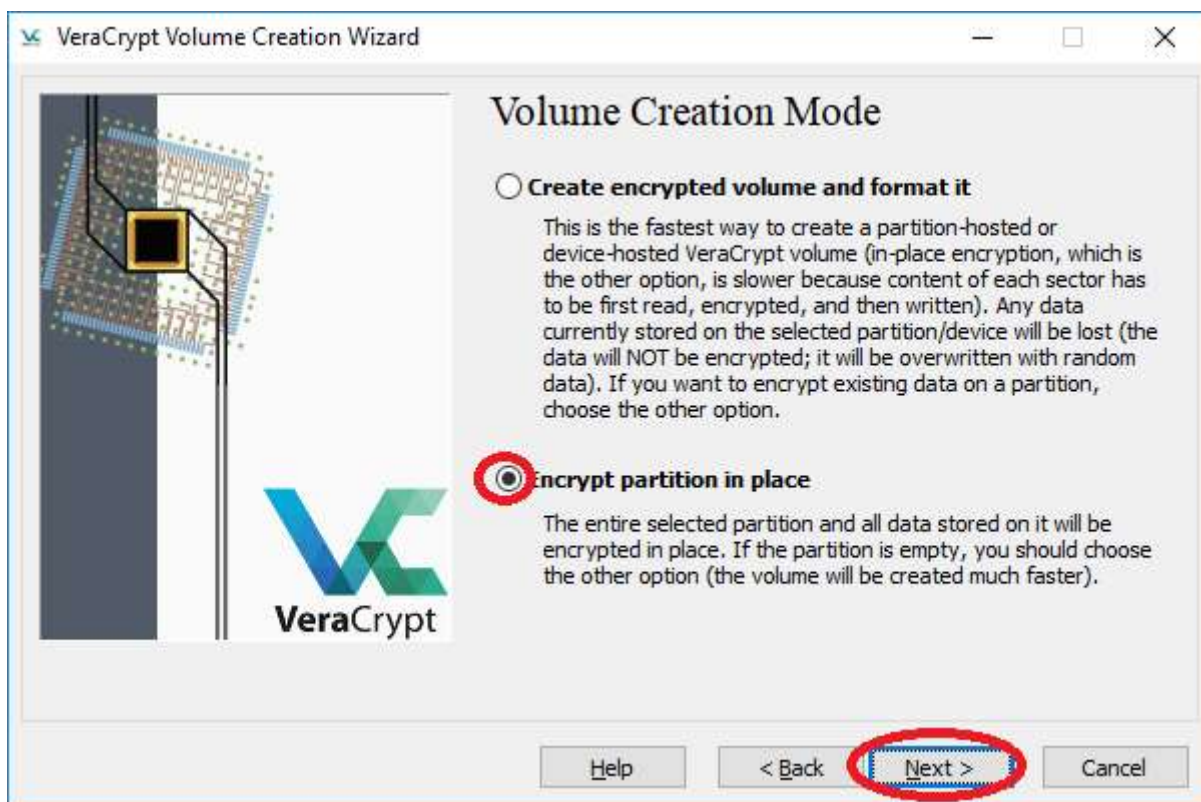
Nyní na základě písmenka disku vyberte, který oddíl chcete šifrovat. V tomto návodu je to písmeno „G“.



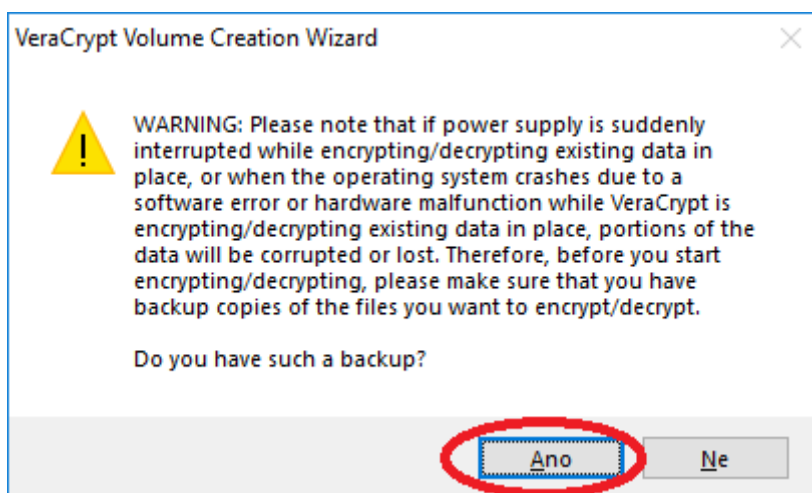
Pokračujte tlačítkem „Next >“.



Ponechte šifrování stávajícího oddílu a stiskněte „Next >“.



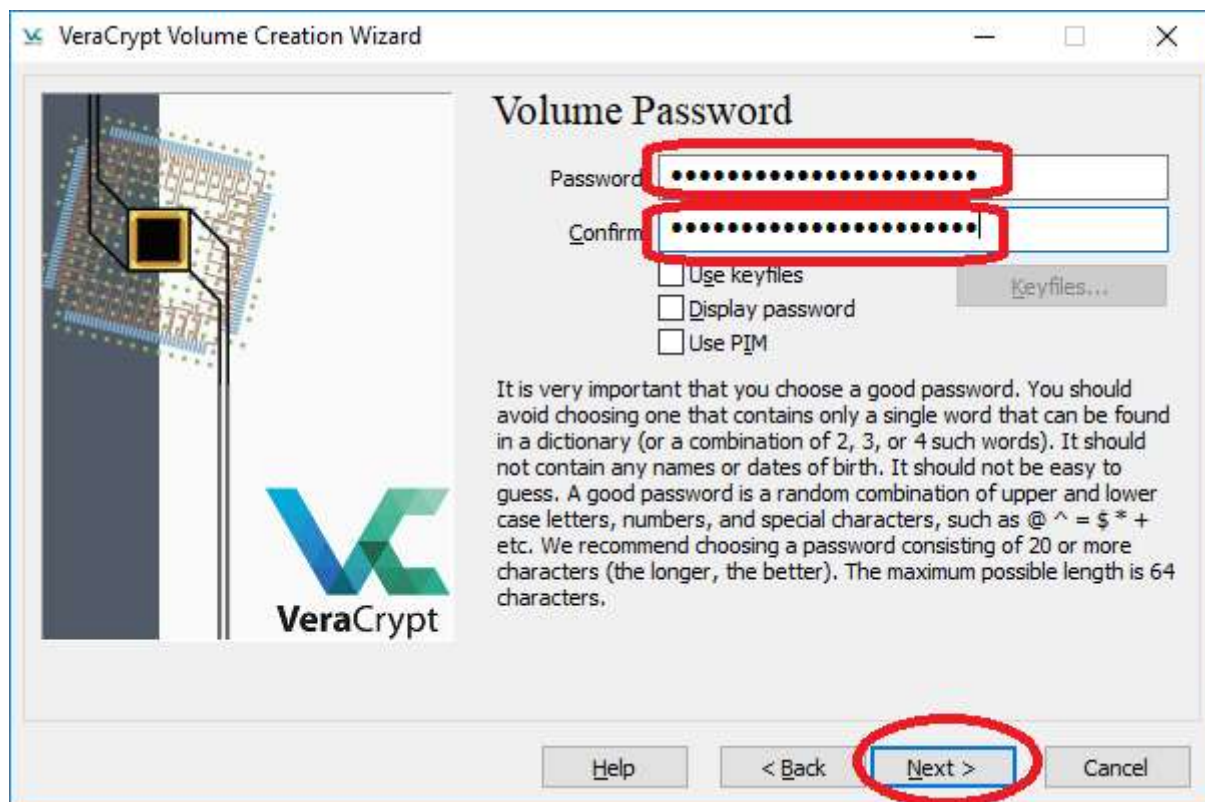
Potvrďte upozornění na to, že v průběhu šifrování nesmíte zařízení odpojit.



Ponechte výchozí nastavení šifrování a stiskněte „Next >“.



Nyní zadejte silné avšak zapamatovatelné heslo. To by se mělo skládat z velkých a malých písmen, číslic a speciálních znaků (jako: @ = . +). **POZOR!** V případě zapomenutí hesla nebude možné data obnovit.



VeraCrypt Volume Creation Wizard

Volume Password

Password: [Redacted]

Confirm: [Redacted]

☐ Use keyfiles Keyfiles...

☐ Display password

☐ Use PIM

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

Help < Back **Next >** Cancel

VeraCrypt Volume Creation Wizard

Collecting Random Data

Current pool content (partial)

```

** .+ /, /x +, /- x/ -x /x .x ** /, -/ .x ..
/x -. /x -- +- .. +- -- +, -+ ,/ /- /+ /+ **
-, ., x- +, ,, , x/ x/ -, +, +, x- +x
x /x +/ x+ x* /+ -/ .. +, -x ,+ x+
/, -/ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+
./ ,x +, ++ .+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+ ,+
x. ++ /x +/ -, ., - - - /- ,+ x* x- .. .+ +x
.. +. +/ /+ . / +/ x+ x* x/ -x x* /+ .. .+ ..

```

☐ Display pool content

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Next to continue.

Randomness Collected From Mouse Movements

Help < Back Next > Cancel

VeraCrypt Volume Creation Wizard

Wipe Mode

Wipe mode: None (fastest)

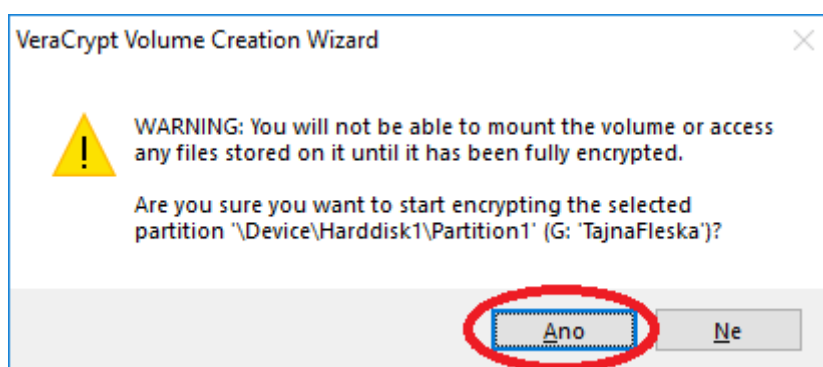
On some types of storage media, when data is overwritten with other data, it may be possible to recover the overwritten data using techniques such as magnetic force microscopy. This also applies to data that are overwritten with their encrypted form (which happens when VeraCrypt initially encrypts an unencrypted partition or drive). According to some studies and governmental publications, recovery of overwritten data can be prevented (or made very difficult) by overwriting the data with pseudorandom and certain non-random data a certain number of times. Therefore, if you believe that an adversary might be able to use such techniques to recover the data you intend to encrypt, you may want to select one of the wipe modes (existing data will NOT be lost). Note that wiping will NOT be performed after the partition/disk is encrypted. When the partition/disk is fully encrypted, no unencrypted data is written to it. Any data being written to it is first encrypted on the fly in memory and only then is the (encrypted) data written to the disk.

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

Šifrování zahájíte tlačítkem „Encrypt“.



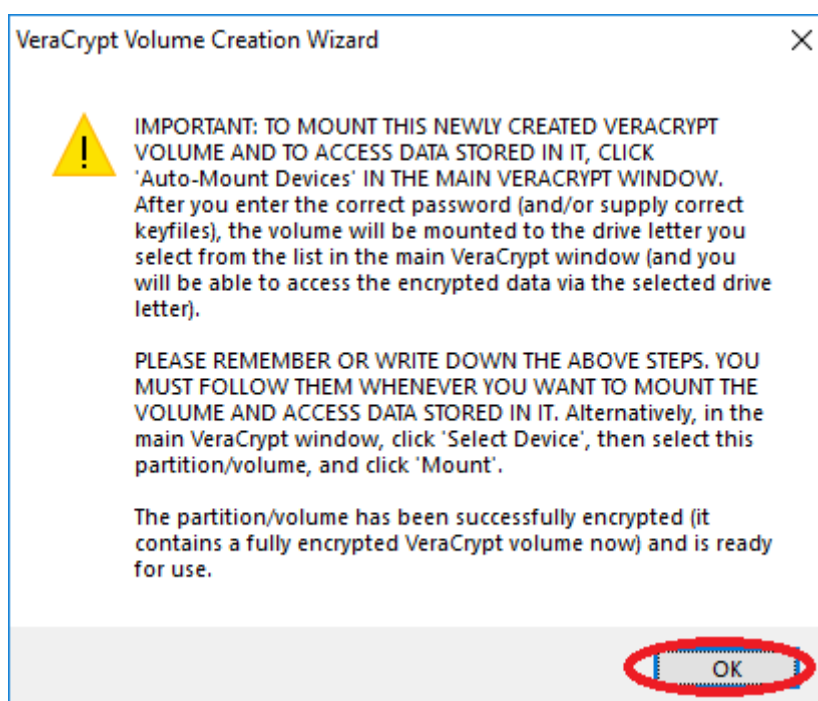
Odsouhlaste upozornění, že data nebudou dostupná, dokud šifrování nedoběhne.



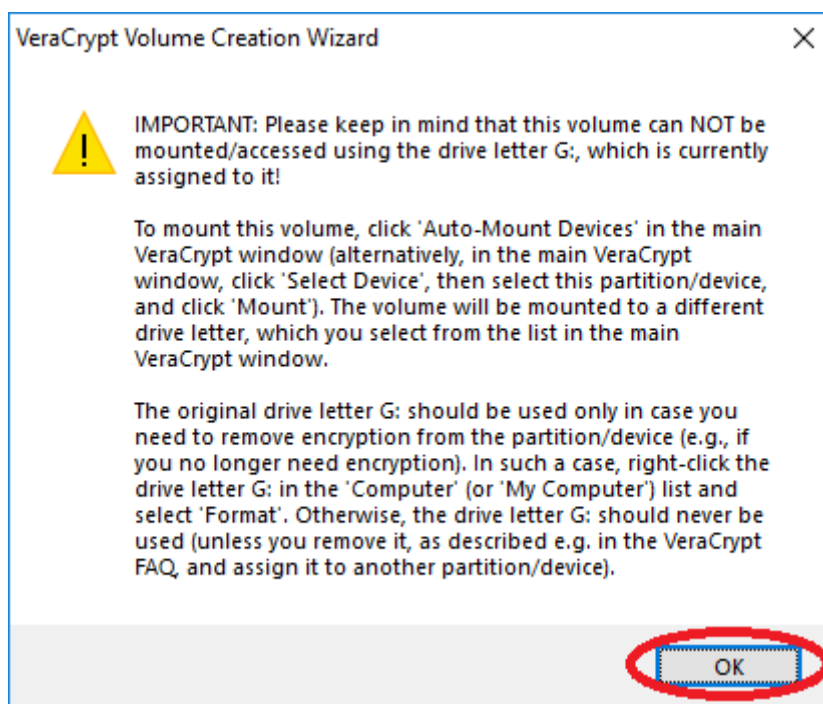
Nyní bude probíhat šifrování oddílu. To může trvat i několik hodin, v závislosti na kapacitě a rychlosti záznamového média.



Po dokončení potvrďte upozornění na nutnost „namontování“ disku.



Potvrďte upozornění, že Windows nebudou moci otevřít takto šifrovaný disk.



Po skončení šifrování stiskněte tlačítko „Finish“.



Otevření zašifrovaného disku

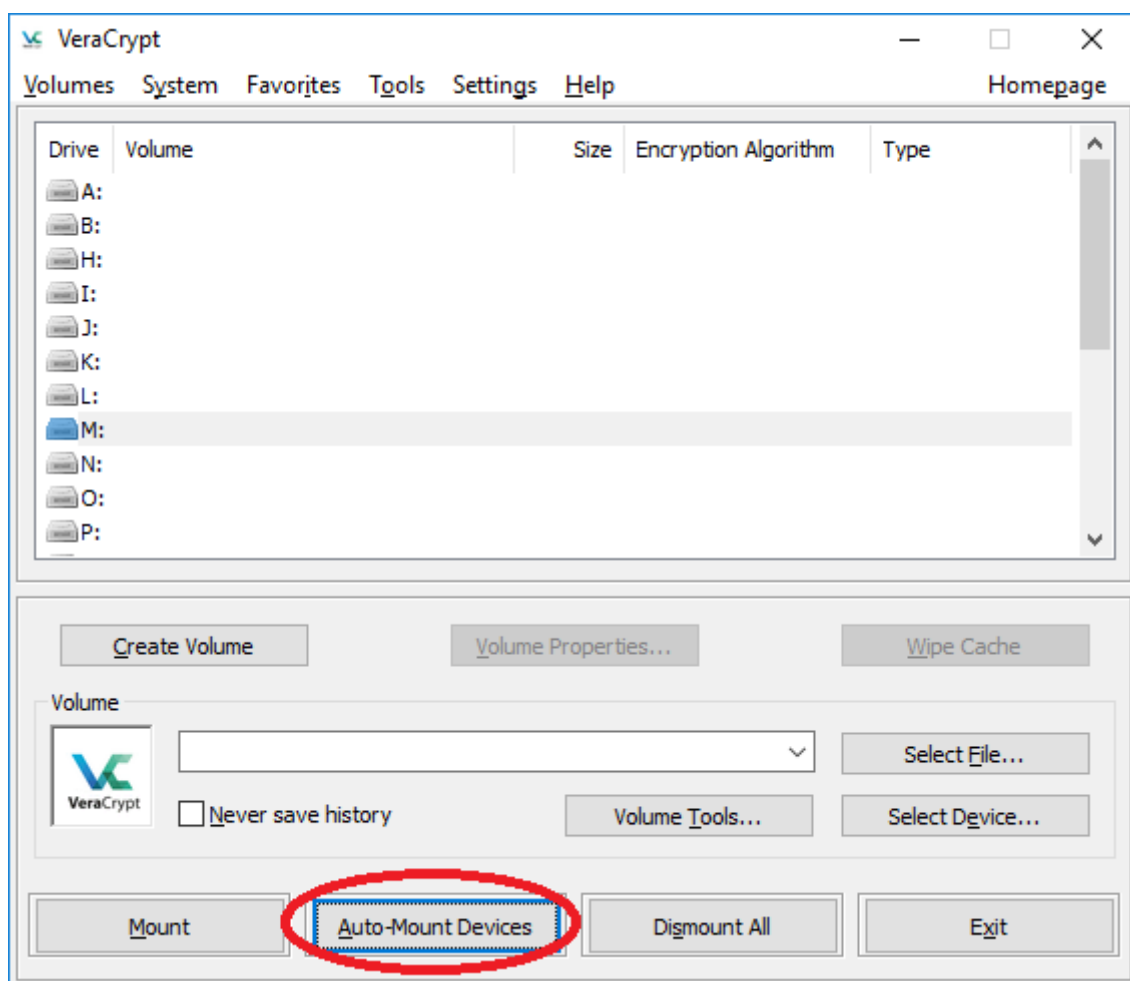
Operační systém Windows nerozpozná, že je disk zašifrován, považuje jej za nečitelný a vyzývá k jeho naformátování.

POZOR! Formátováním disku smažete všechna data, co se na něm nacházejí.

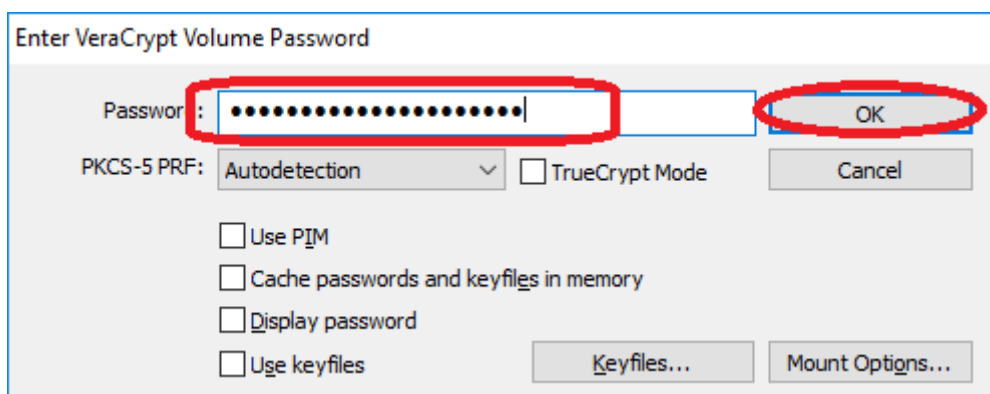
Připojte zašifrovaný disk k počítači a spusťte program VeraCrypt.



Stiskem tlačítka „Auto-Mount Devices“ se program pokusí vyhledat a rozšifrovat všechny připojené zašifrované disky.



Zadejte heslo, které bylo použito pro zašifrování a dejte „OK“.



Pokud se povedlo pomocí zadaného hesla disk rozšifrovat, „namountuje“ se pod nějaké volné písmenko disku. V tomto návodu je to „M:“. Poté je možné disk normálně využívat.

