



# Transparentné šifrovanie disku

**Príručka administrátora**

(AN363612)

*Júl 2014*

# Obsah

<b>1 Charakteristika</b>	<b>3</b>
<b>2 Systémové požiadavky</b>	<b>3</b>
<b>3 Inicializácia Tokenu</b>	<b>3</b>
<b>4 Príklad: Šifrovaný disk aplikácie TrueCrypt</b>	<b>4</b>
<b>5 Dokumentácia</b>	<b>5</b>

Táto príručka popisuje nastavenie a prevádzku systému transparentného šifrovania obsahu disku (*on-the-fly encryption, OTFE*) administrátorom. Tu uvedený postup je platný pre nastavenie aplikácie *TrueCrypt* [4]. Obdobné nastavenie je možné použiť pre podobné aplikácie, napríklad *FreeOTFE* [5].

## 1 Charakteristika

- Hardvérový bezpečnostný modul **GNT USB Token** [1] od spoločnosti **SoftIdea** je možné použiť ako úložisko kľúčových súborov (*keyfiles*) v aplikáciách pre transparentné šifrovanie disku, napríklad *TrueCrypt*.
- Kľúčové súbory sú uložené v chránenej pamäti Tokenu a prístup k nim je podmienený znalosťou hesla užívateľa Tokenu (*UPW*)

## 2 Systémové požiadavky

- Operačný systém: Microsoft Windows XP, Vista, 7, 8.
- GNT USB Token
- Nástroj administrátora *Ginit* [2]
- Rozhranie SIPKCS [3]

## 3 Inicializácia Tokenu

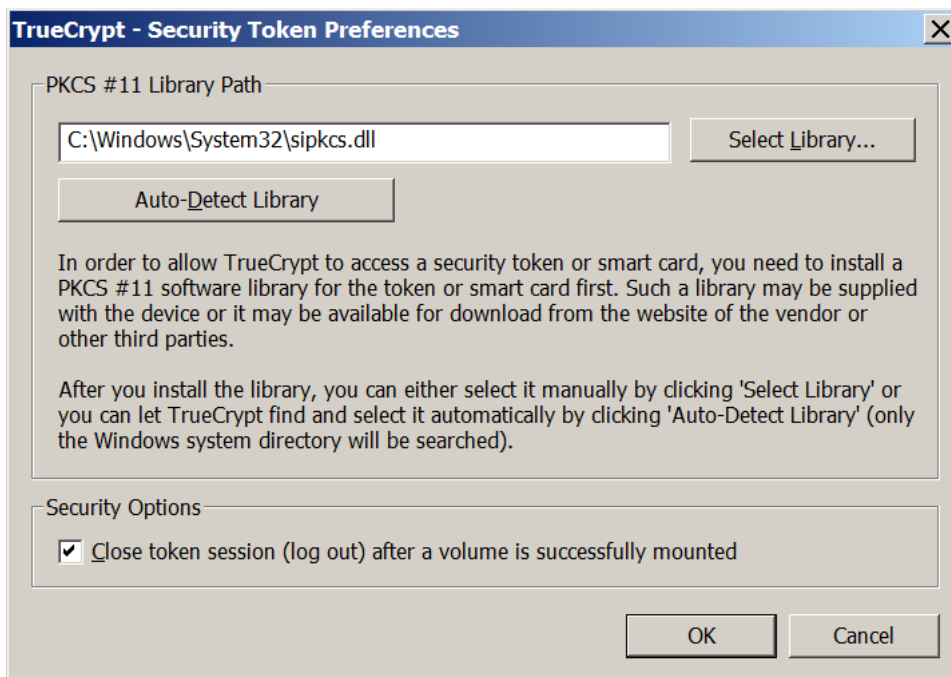
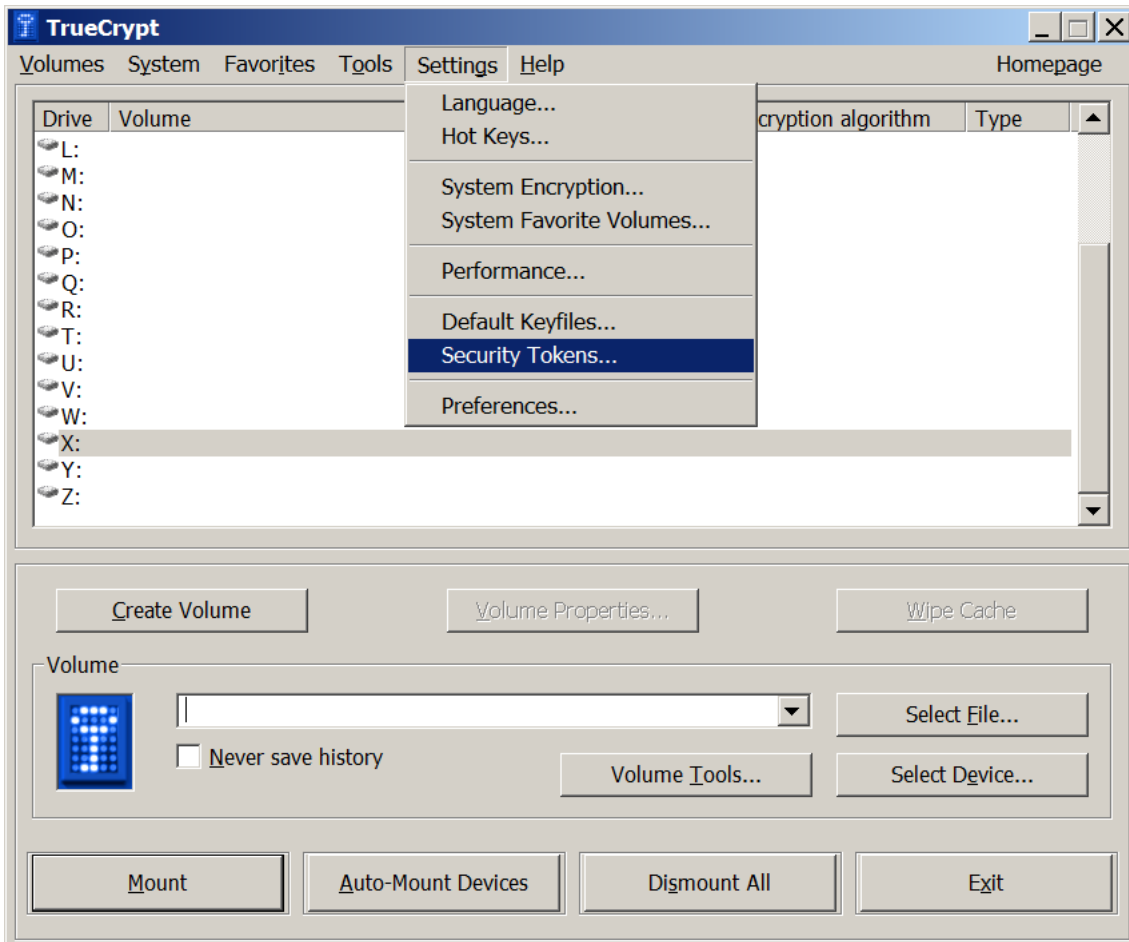
Pomocou nástroja *Ginit* inicializujte token užívateľa pre rozhranie SIPKCS. V poli PIN1 nastavte heslo UPW.

The screenshot shows the Ginit 3.0 application window. The interface is divided into several sections:

- Issue:** Radio buttons for 'Custom' and 'PKCS#11'. Buttons for 'Issue' and 'Unissue' are at the bottom.
- Info:** Fields for 'Token ID' (0x00001237), 'Firmware version' (32.128), 'Production state' (issued), and 'Current wrong logins' (0). A 'Get token info' button is present.
- Configuration:**
  - PINs:** Input fields for PIN1, PIN2, and APW, with a 'Set' button and a 'Show PINs' checkbox.
  - Max. number of wrong logins allowed:** Input field set to 0.
  - User memory:** Fields for 'RSA slots' (17), 'MEM1 size' (9155 Bytes), 'MEM2 size' (16909 Bytes), 'MEM3 size' (16 Bytes), and 'Total of available' (35328 Bytes).
  - RSA slots' attributes:** A 'Slot index' dropdown (set to 1) and checkboxes for 'exportable', 'importable', 'exportable during generation only', 'generatable', and 'erasable'. A sub-section 'Allowed operations' has checkboxes for 'enc/decryption', 'signature gen./verification', and 'wrapping/unwrapping'.
  - MEM area access rights:** A 'MEM index' dropdown (set to 1) and checkboxes for 'Read' and 'Write' for PIN2 and PIN1, with 'free' checkboxes.
- Buttons at the bottom: 'Load configuration', 'Save configuration', and 'Clear configuration'.

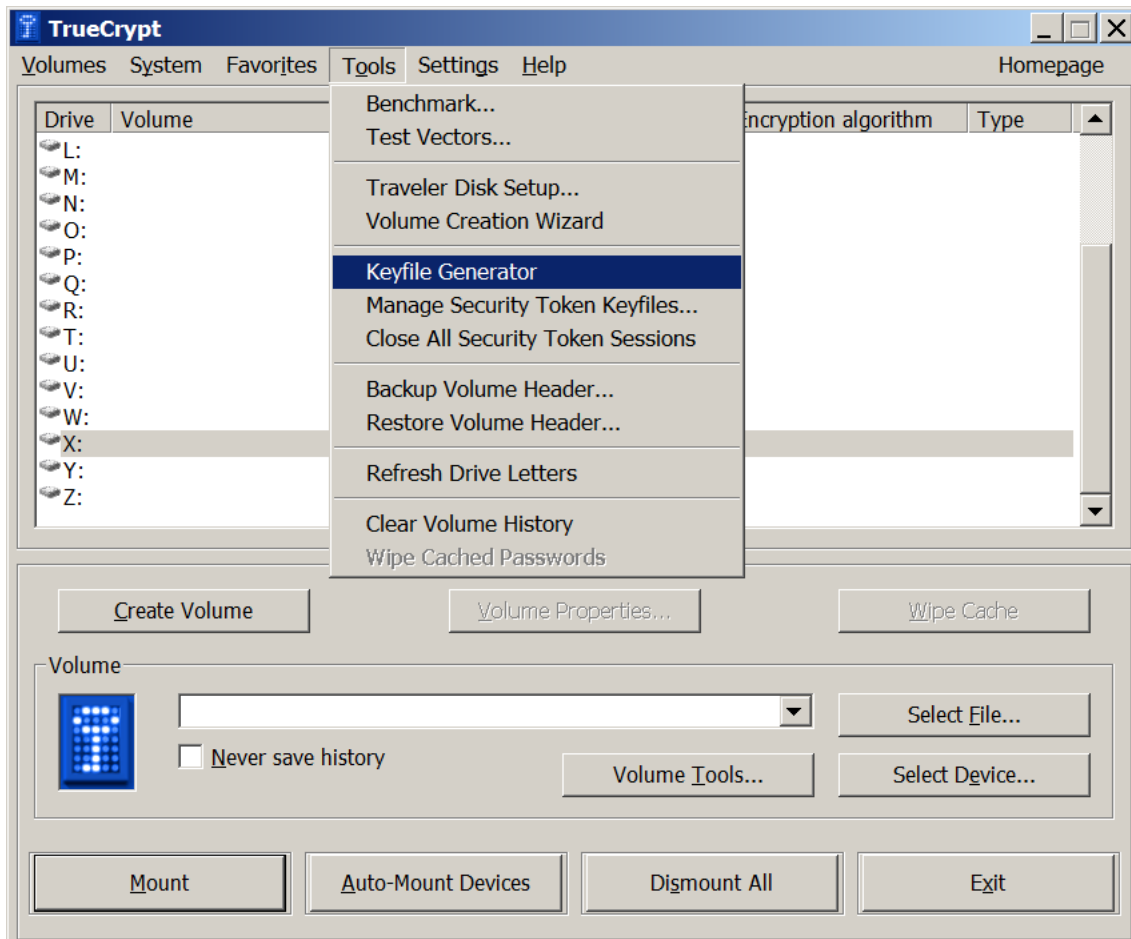
## 4 Príklad: Šifrovanie disku aplikáciou TrueCrypt

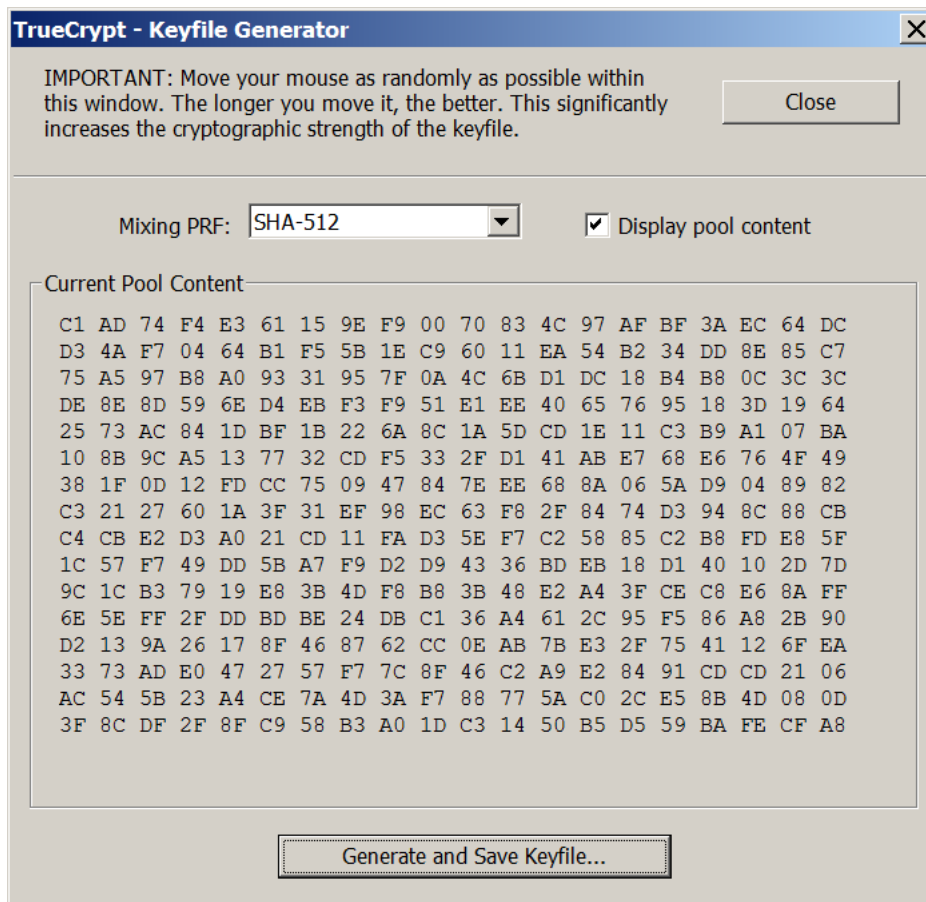
### 4.1 Zvoľte rozhranie SIPKCS



Označte pole „Close token session...“ v časti „Security Options“.

## 4.2 Vygenerujte kľúčový súbor a uložte ho dočasne na disk



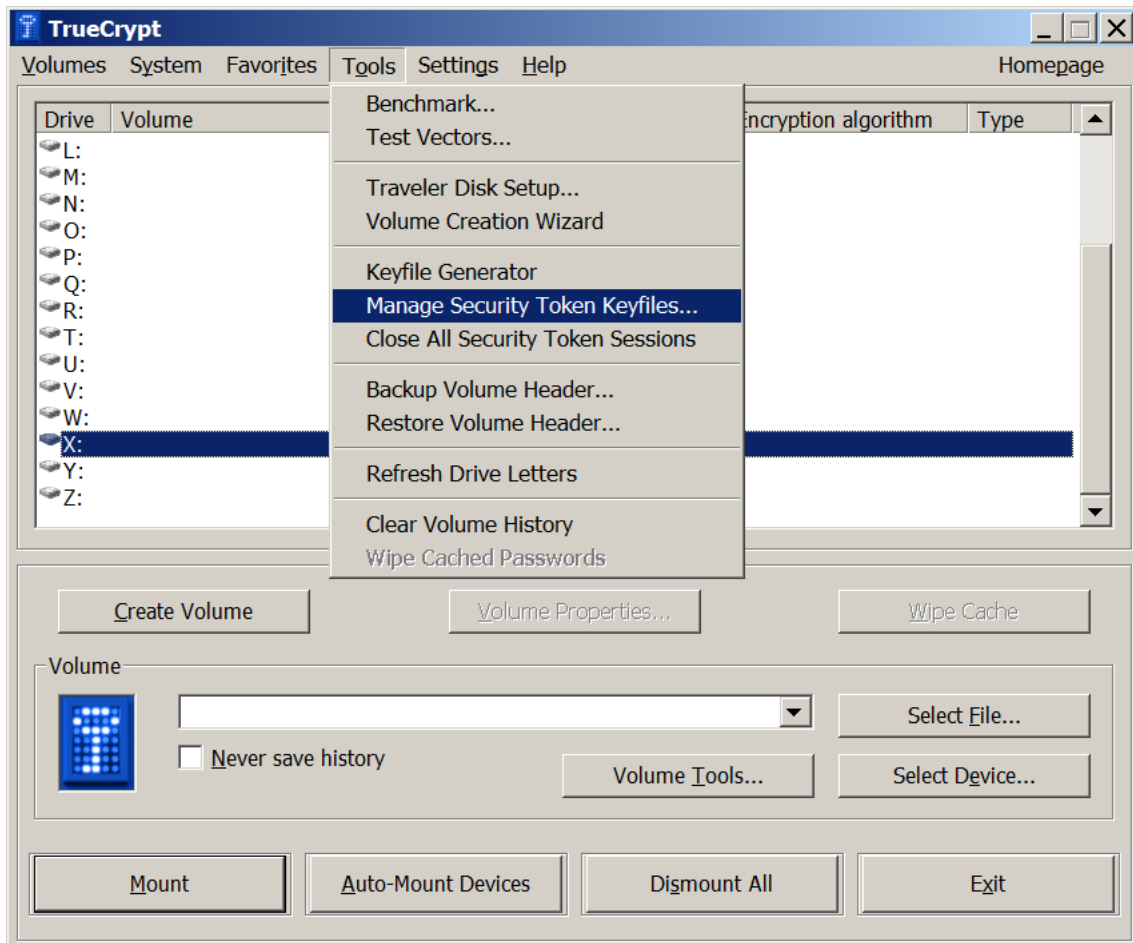


Zvoľte lokalitu pre uloženie dočasného súboru.

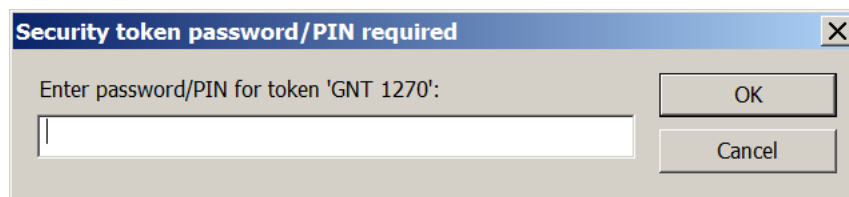


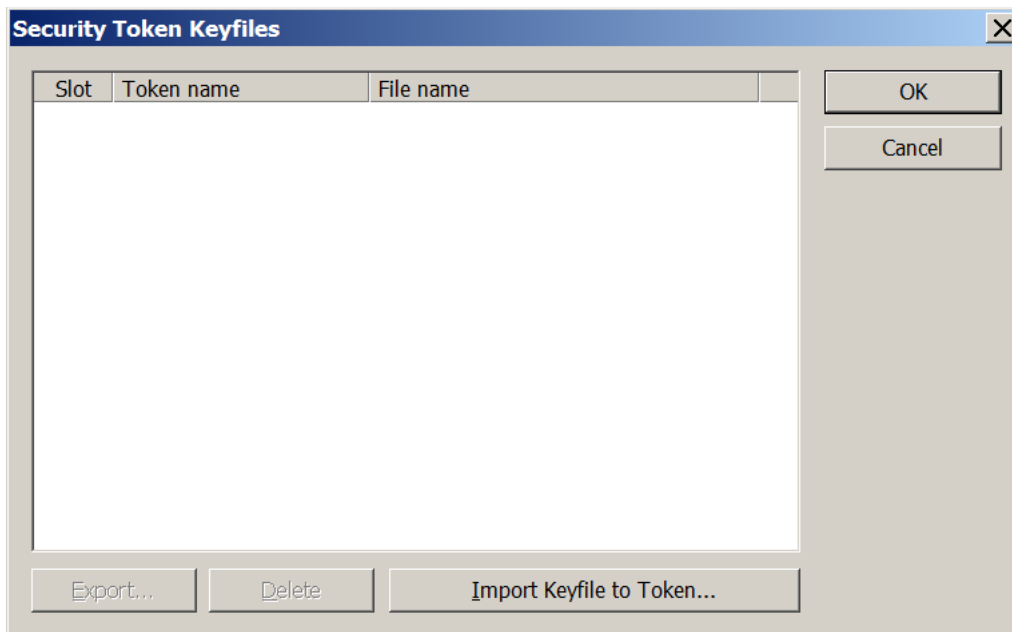
Potvrďte informáciu a zatvorte okno „Keyfile generator“.

### 4.3 Uložte kľúčový súbor na Token



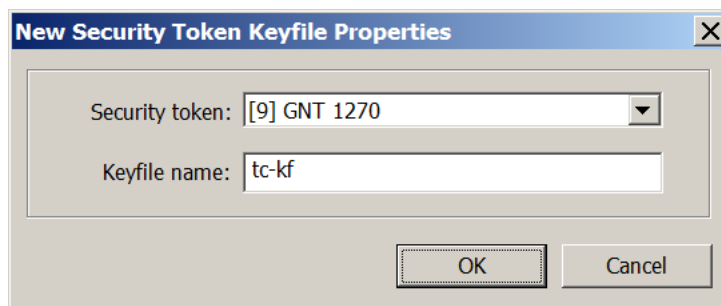
Vložte heslo UPW:





Zvoľte „Import Keyfile to Token...“.

Zvoľte dočasný súbor uložený v predchádzajúcom kroku (4.2).

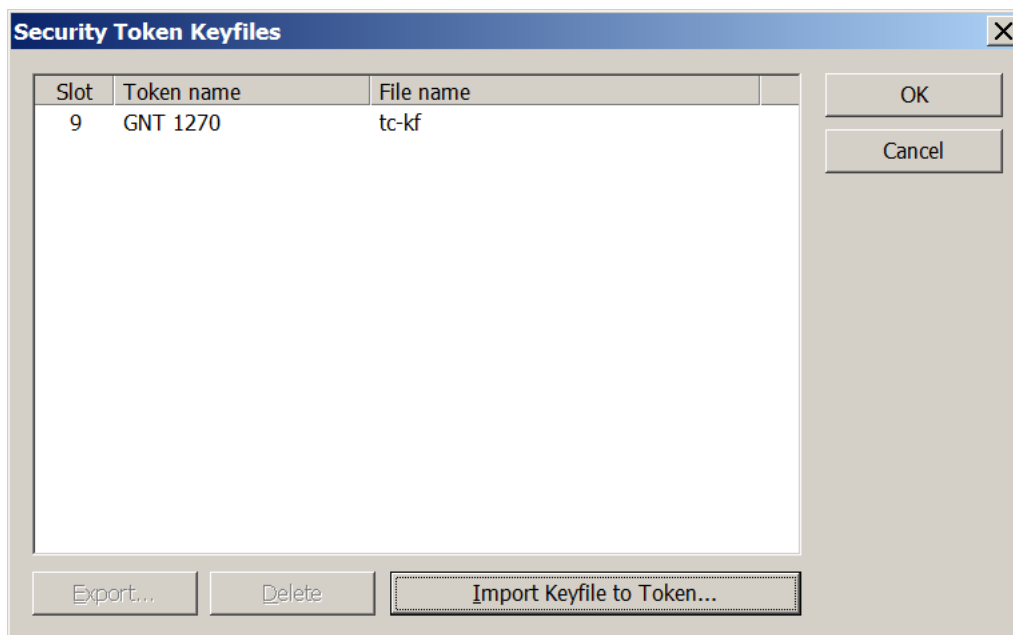


Podľa potreby upravte „Keyfile name“.

Potvrďte vlastnosti kľúčového súboru vytváraného na Tokene.



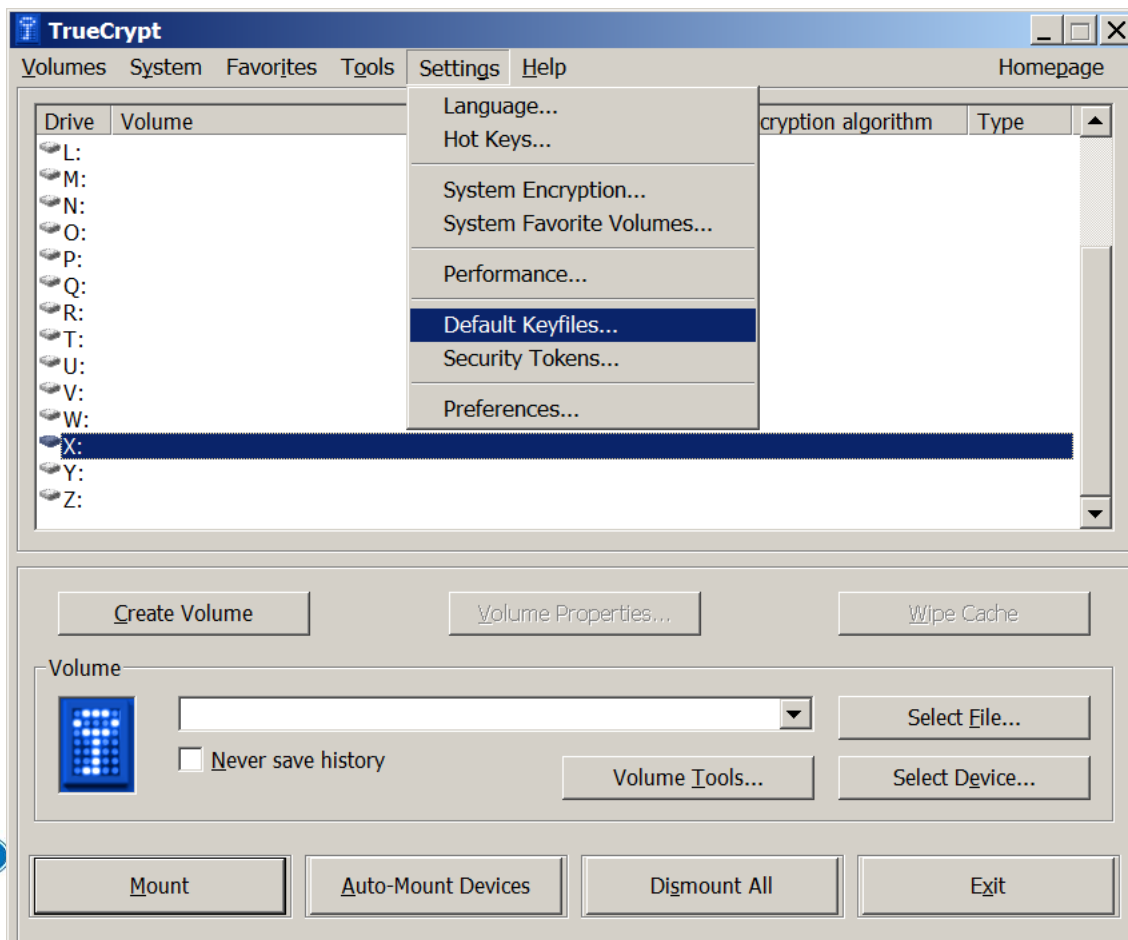
Kľúčový súbor bol úspešne uložený v chránenej pamäti Tokenu:

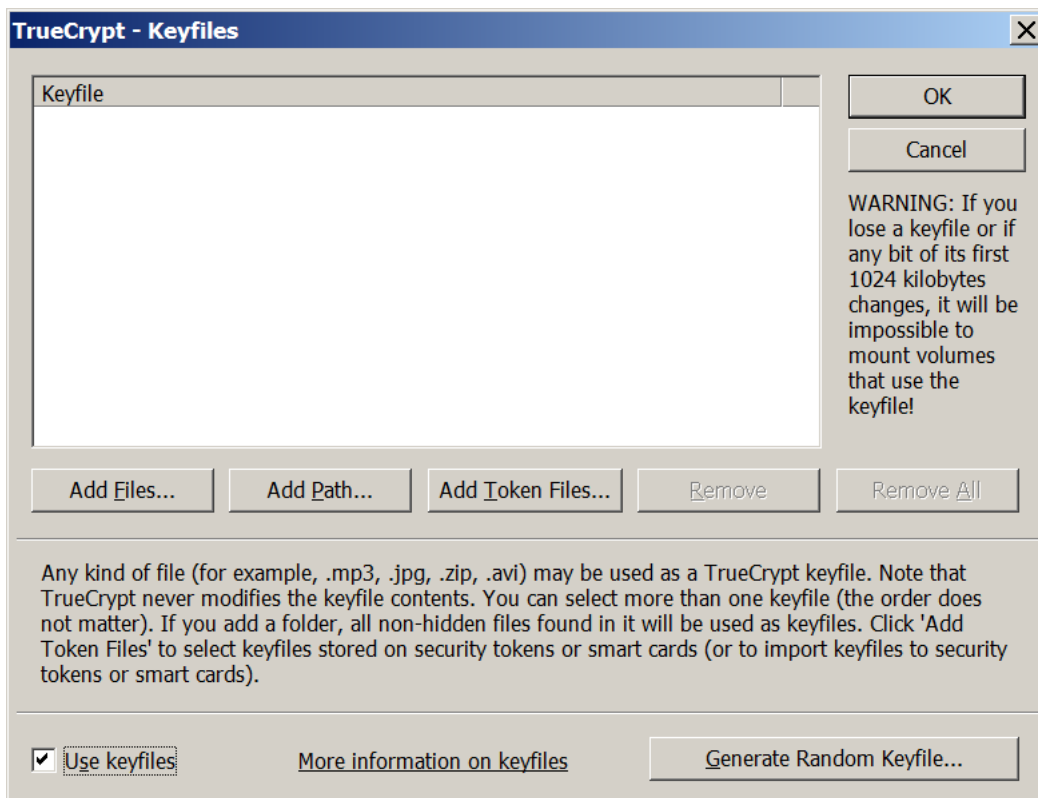


Bezpečne odstráňte dočasný súbor uložený v kroku (4.2).

Zatvorte okno „Security Token Keyfiles“.

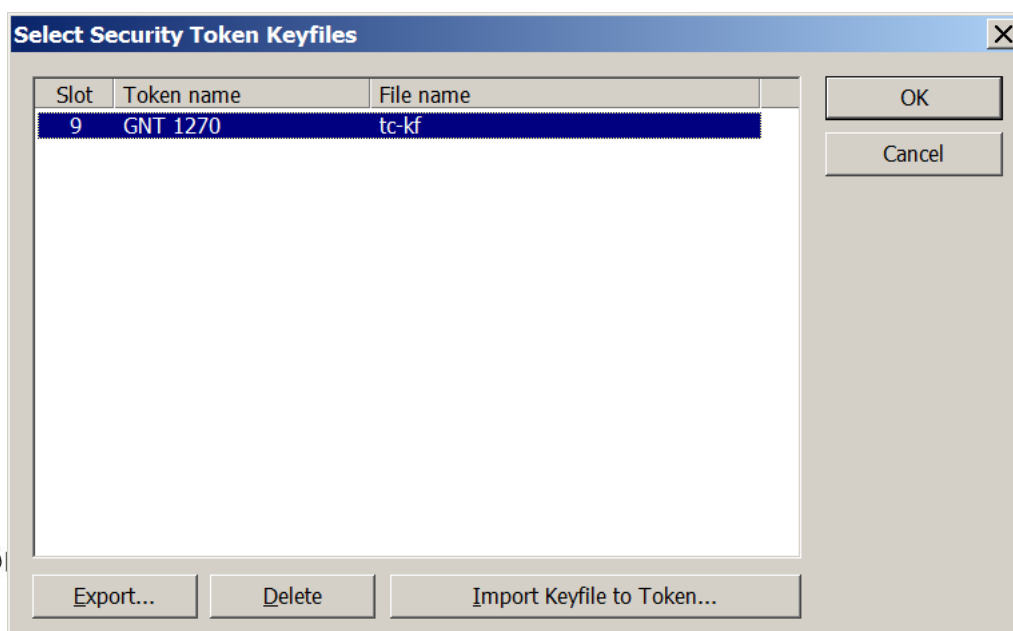
#### 4.4 Zvoľte prednastavený kľúčový súbor





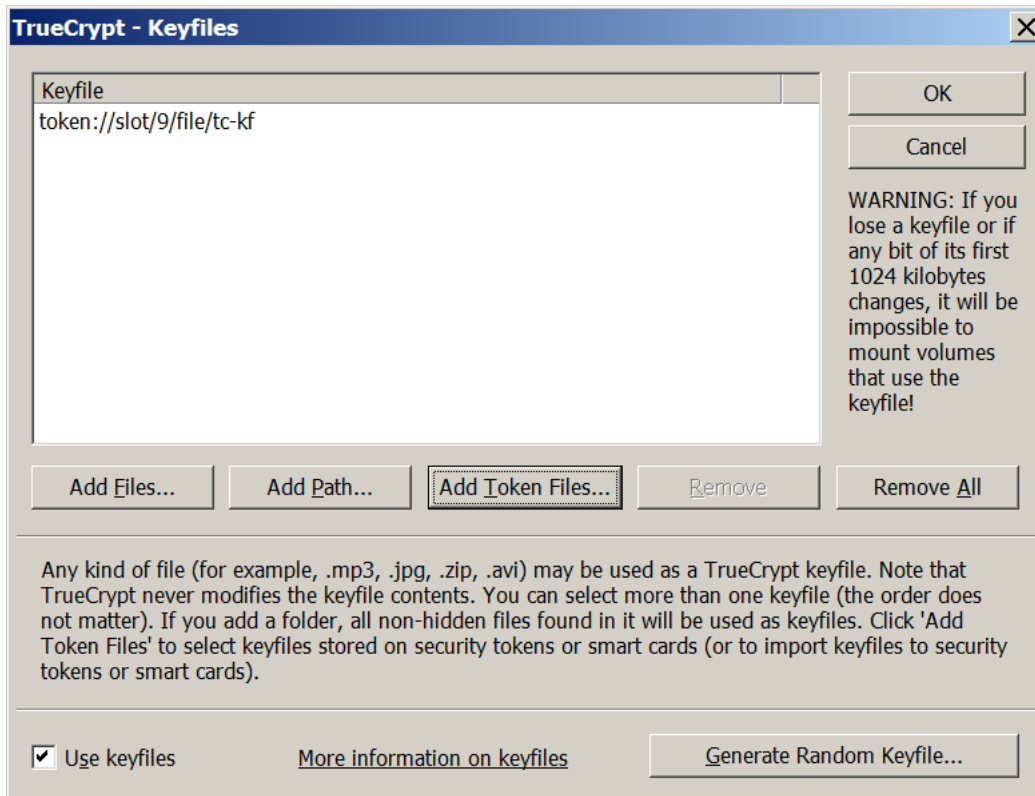
Označte pole „Use keyfiles“.

Zvoľte „Add Token Files“.



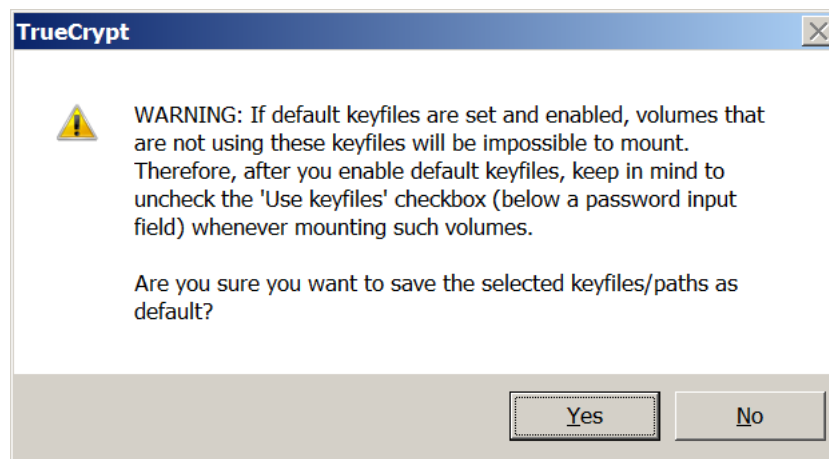
Označte kľúčový súbor a potvrdte (OK).

Prednastavený kľúčový súbor je zvolený:



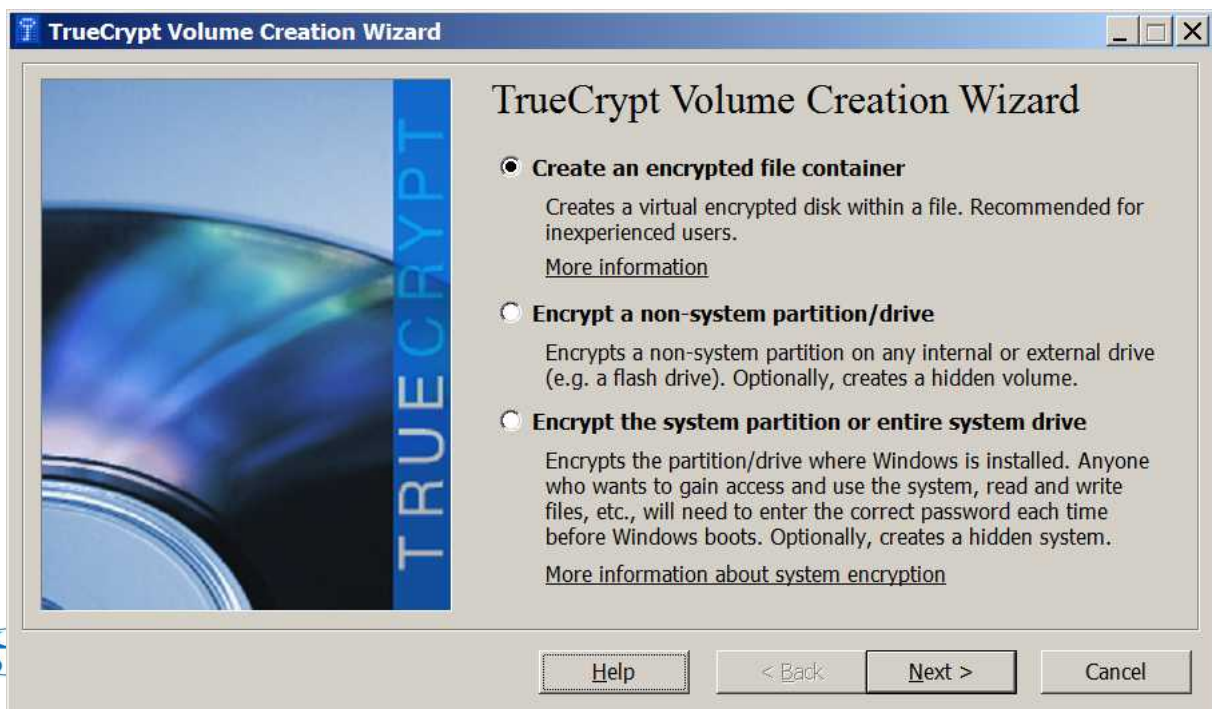
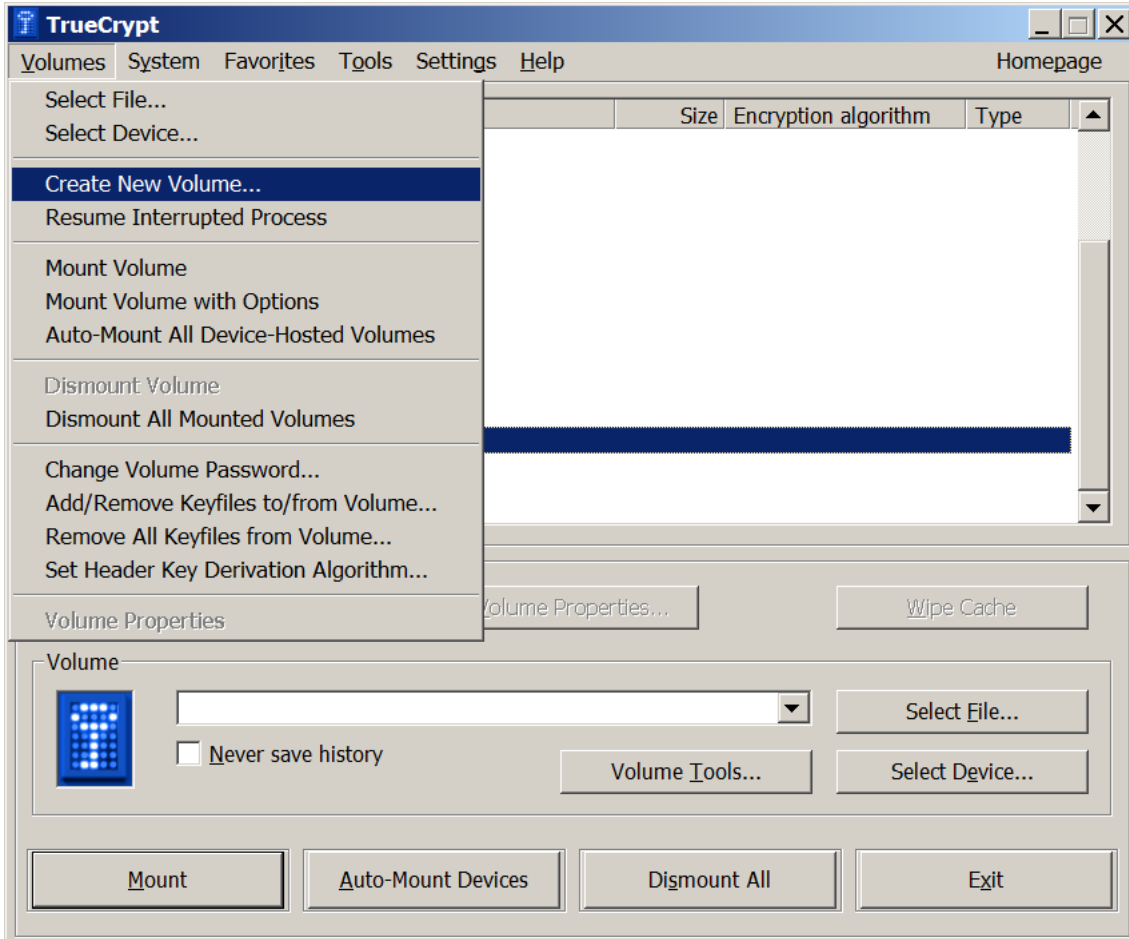
**Poznámka:** Voľba prednastaveného kľúčového súboru v aplikácii TrueCrypt zahŕňa USB slot, v ktorom je Token zasunutý. **Pre korektné použitie daného kľúčového súboru budete musieť Token vždy zasunúť do toho istého USB slotu.**

Potvrdte (OK).



Potvrďte varovanie (Yes).

## 4.5 Vytvorte novú jednotku



**Poznámka: Voľbu „Encrypt the system partition...“ nie je možné použiť v kombinácii s kľúčovým súborom uloženým na Tokene.**

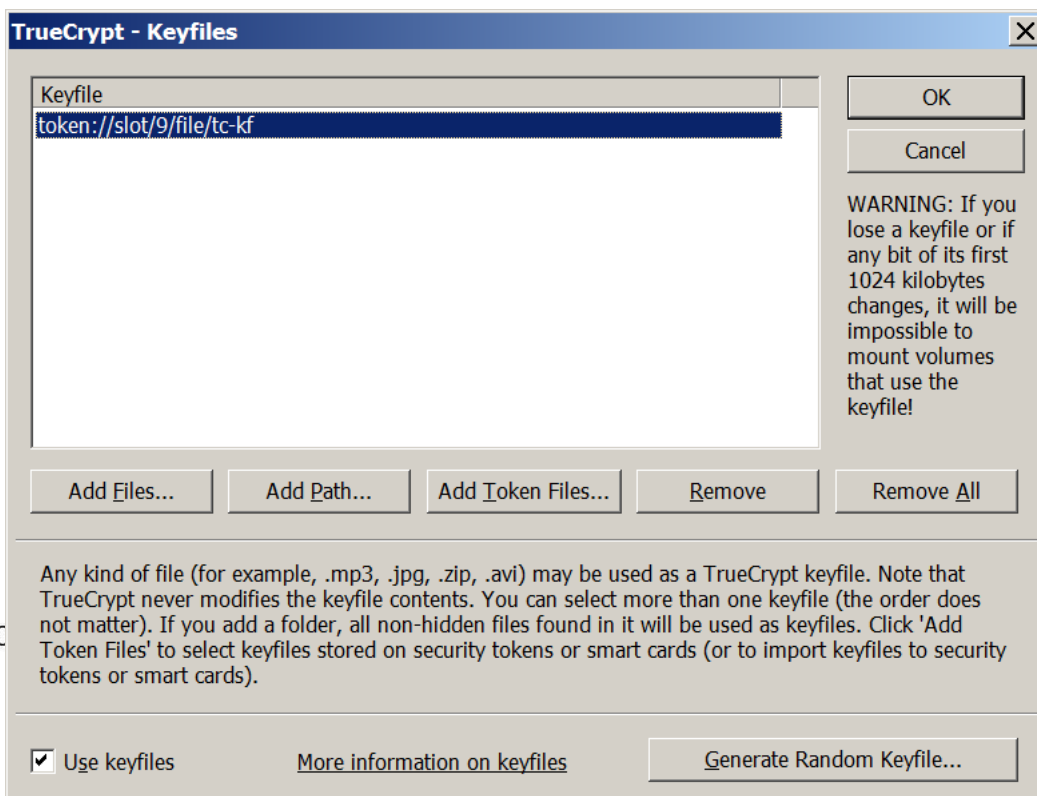
Podľa potreby zvolíte parametre novo vytváranej jednotky v nasledujúcich oknách.

V okne „Volume password“ označte voľbu „Use keyfiles“



Zvoľte tlačidlo „Keyfiles“.

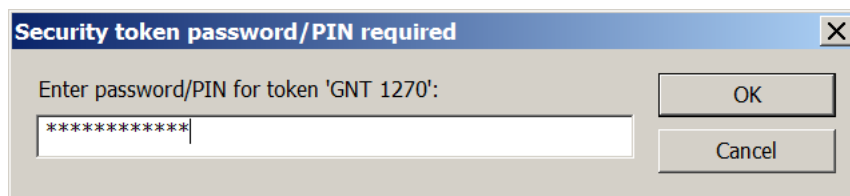
V nasledujúcom okne označte kľúčový súbor na Tokene.



Potvrďte voľbu (OK):

Zvoľte tlačidlo „Next“ v okne „Volume password“ .

Po výzve vložte UPW Tokenu:



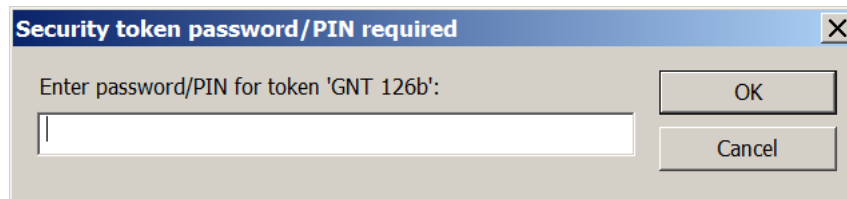
Dokončíte vytvorenie jednotky.

## 4.6 Uvedenie šifrovaného disku do prevádzky

Zvoľte umiestnenie disku:

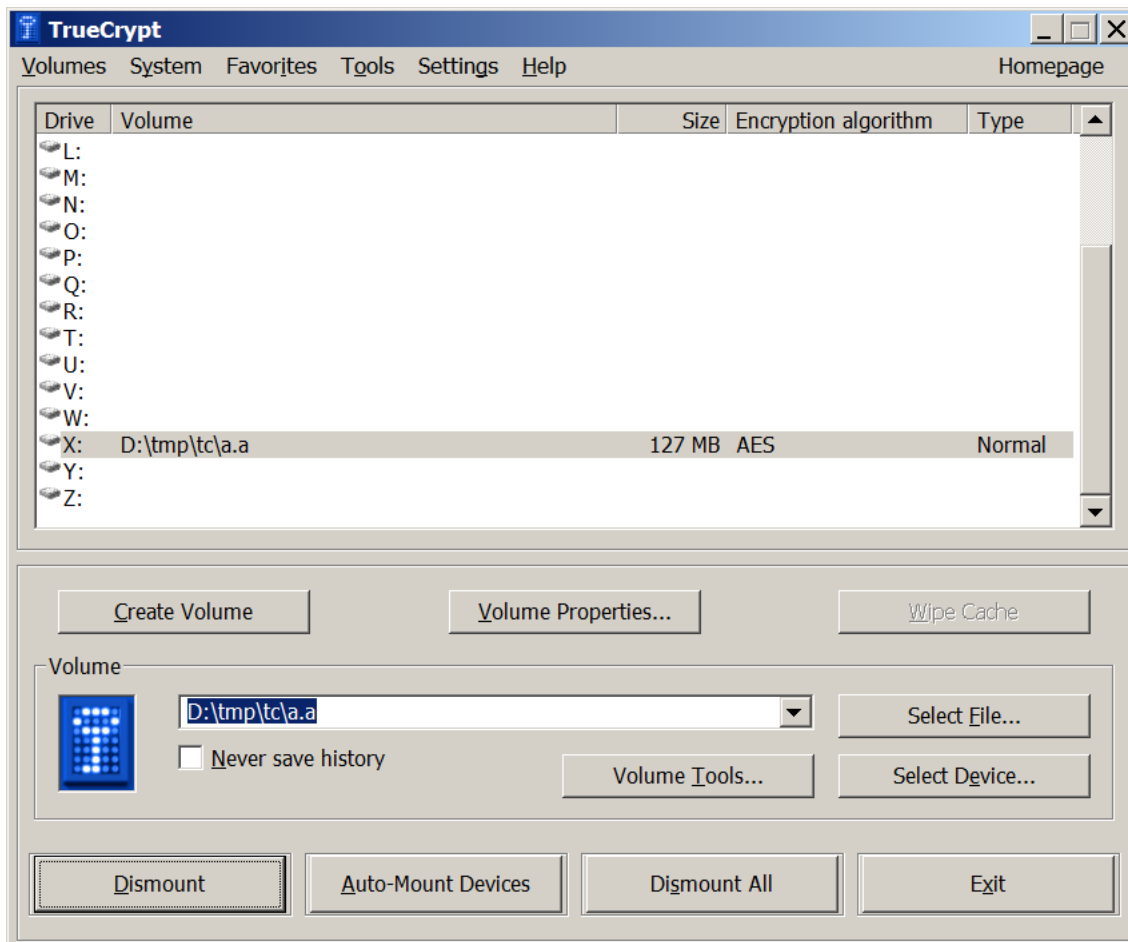


Zvoľte tlačidlo „Mount“.



Vložte heslo a potvrďte (OK).

Disk je pripravený na použitie:



V príklade na obrázku vyššie bol uvedený do prevádzky šifrovaný disk „X“. Zašifrované údaje disku „X“ sú uložené ako súbor „a.a“.

## 5 Dokumentácia

- [1] GNT USB Token - dátový list, SoftIdea, s.r.o. , Máj 2011, [http://www.softidea.sk/gnt\\_datasheet\\_sk.pdf](http://www.softidea.sk/gnt_datasheet_sk.pdf)
- [2] GINIT - užívateľský manuál, SoftIdea, s.r.o. , May 2011, [http://www.softidea.sk/ginit\\_manual\\_sk.pdf](http://www.softidea.sk/ginit_manual_sk.pdf)
- [3] SIPKCS - Aplikačné programové rozhranie PKCS#11 pre GNT USB Token, SoftIdea, s.r.o. , Máj 2011, [http://www.softidea.sk/sipkcs\\_specification\\_sk.pdf](http://www.softidea.sk/sipkcs_specification_sk.pdf)
- [4] TrueCrypt Setup 7.1a.exe, available [online] on July 2014: <https://www.grc.com/misc/truecrypt/TrueCrypt%20Setup%207.1a.exe>, Digitally signed by TrueCrypt Foundation on Tuesday, February 07, 2012 22:56:09 .
- [5] FreeOTFE, [online], July 2014, <http://sourceforge.net/projects/freetofe.mirror/>

SoftIdea s.r.o.  
Sliachska 10, 831 02 Bratislava  
tel.: +421 2 444 60 444  
fax.: +421 2 446 40 441  
<http://www.softidea.sk>  
[info@softidea.sk](mailto:info@softidea.sk)

*Tento dokument je intelektuálnym vlastníctvom spoločnosti SoftIdea s.r.o. Všetky práva vyhradené.*