SOFTIDEA

Transparentné šifrovanie disku

Príručka administrátora

(AN363612)

Júl 2014

Obsah

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

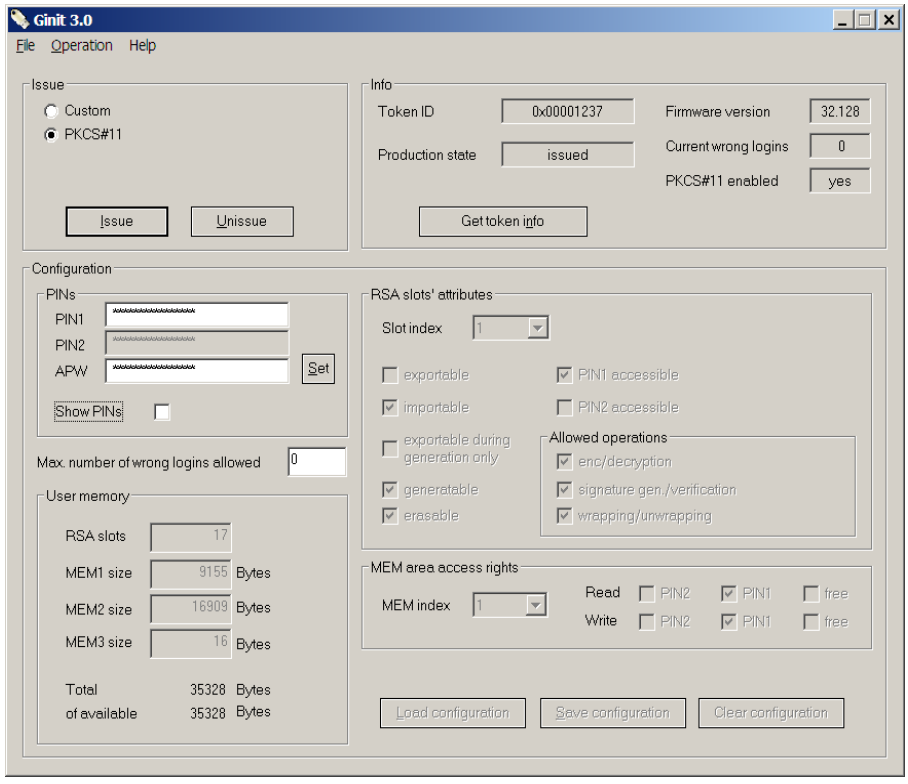
- Hardvérový bezpečnostný modul ***GNT USB Token*** [1] od spoločnosti ***SoftIdea*** je možné použiť ako úložisko kľúčových súborov (*keyfiles*) v aplikáciách pre transparentné šifrovanie disku, napríklad *TrueCrypt.*
- Kľúčové súbory sú uložené v chránenej pamäti Tokenu a prístup k nim je podmienený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

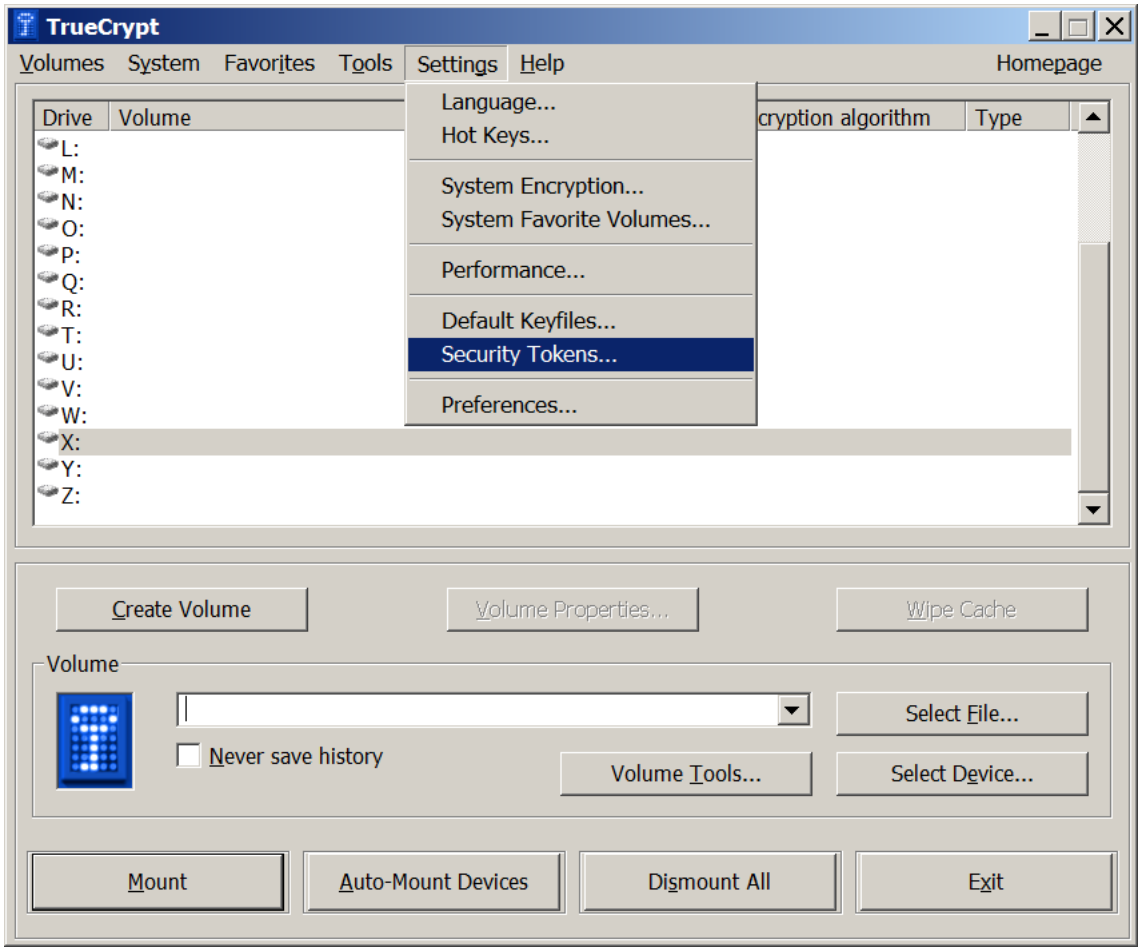
3 Inicializácia Tokenu

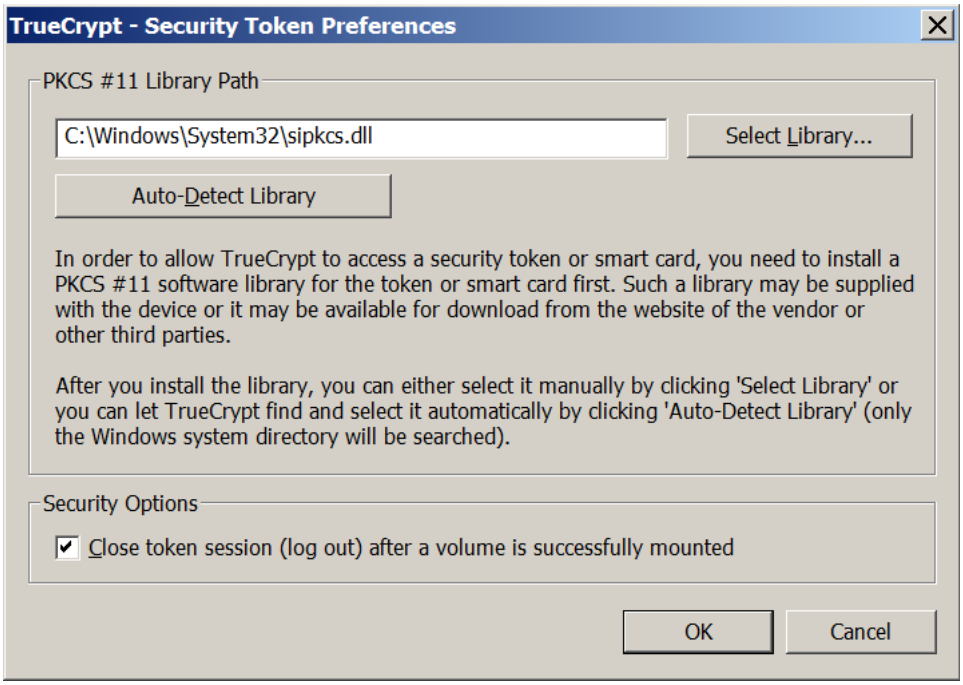
Pomocou nástroja *Ginit* inicializujte token užívateľa pre rozhranie SIPKCS. V poli PIN1 nastavte heslo UPW.



4 Príklad: Šifrovanie disku aplikáciou TrueCrypt

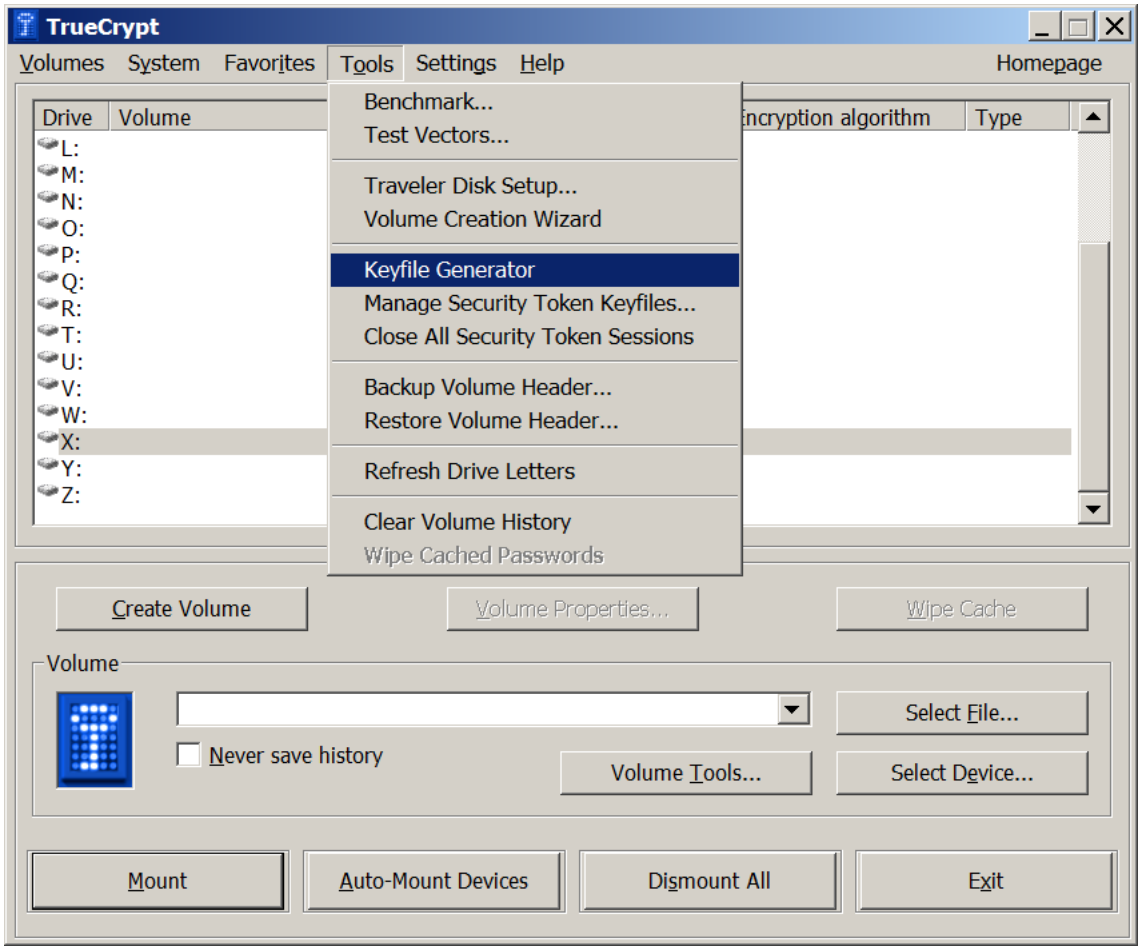
4.1 Zvoľte rozhranie SIPKCS

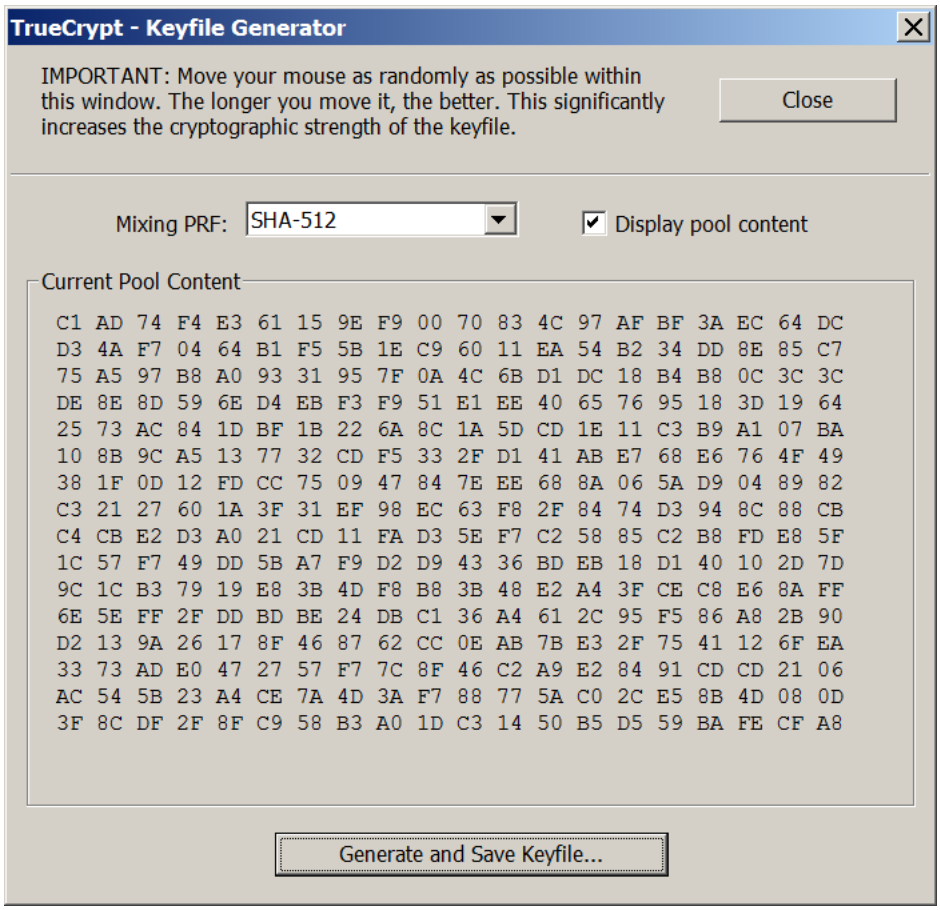




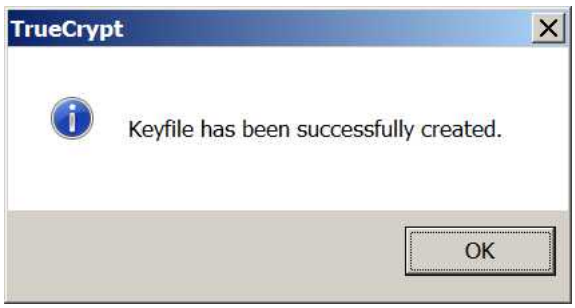
Označte pole „Close token session...“ v časti „Security Options“.

4.2 Vygenerujte kľúčový súbor a uložte ho dočasne na disk



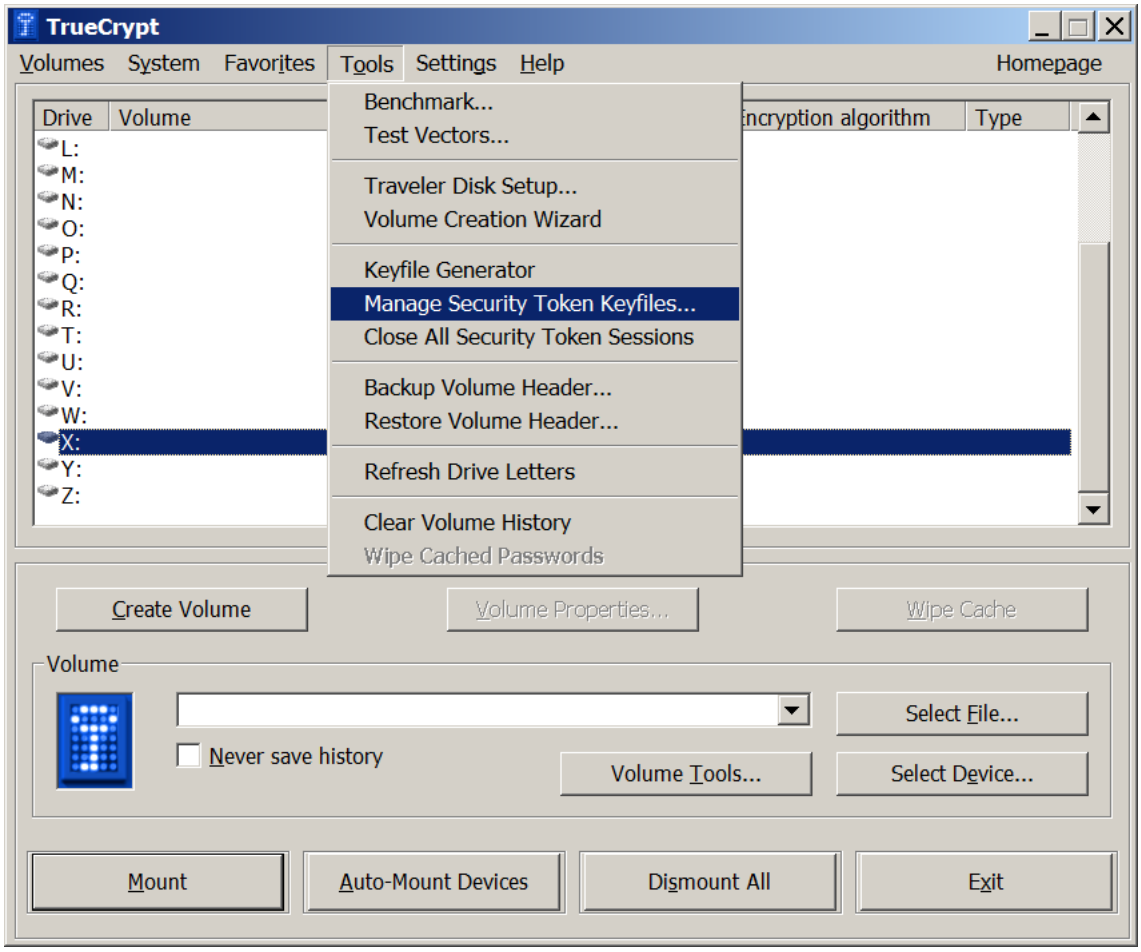


Zvoľte lokalitu pre uloženie dočasného súboru.

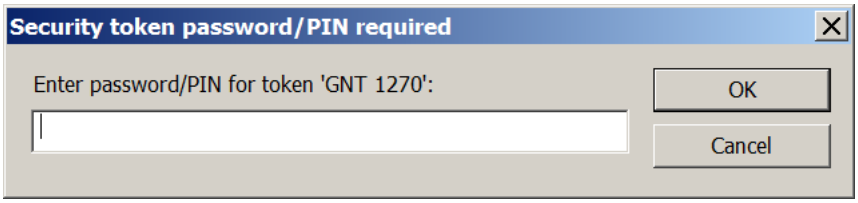


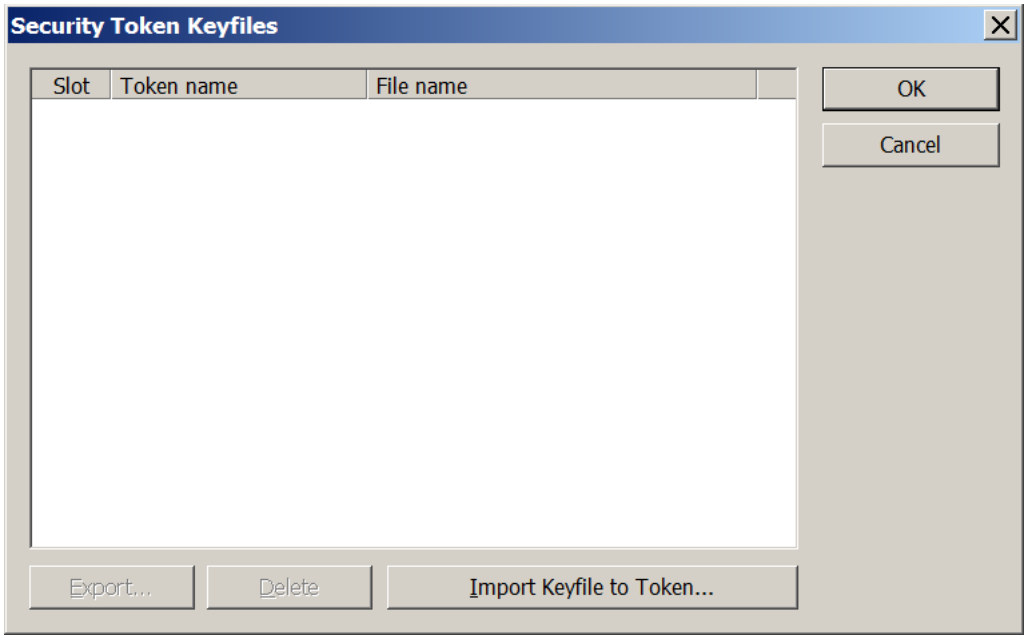
Potvrďte informáciu a zatvorte okno „Keyfile generator“.

4.3 Uložte kľúčový súbor na Token



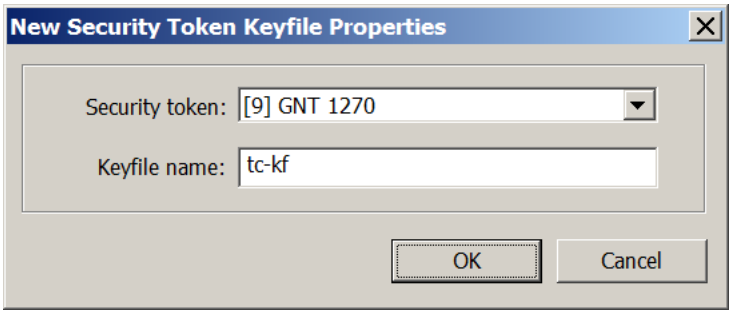
Vložte heslo UPW:





Zvoľte „Import Keyfile to Token...“.

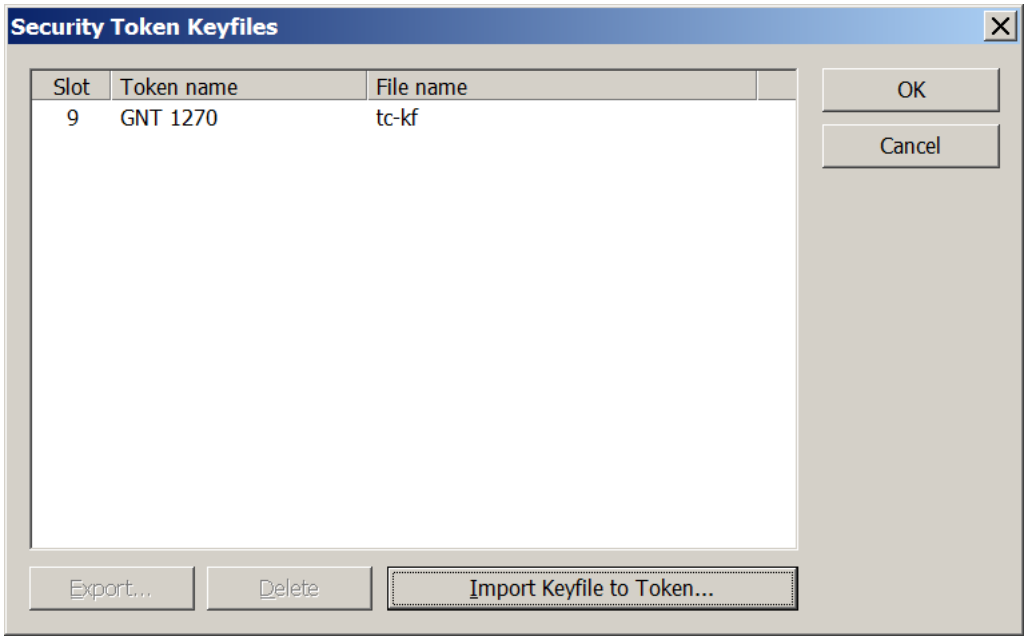
Zvoľte dočasný súbor uložený v predchádzajúcom kroku (4.2).



Podľa potreby upravte „Keyfile name“.

Potvrďte vlastnosti kľúčového súboru vytváraného na Tokene.

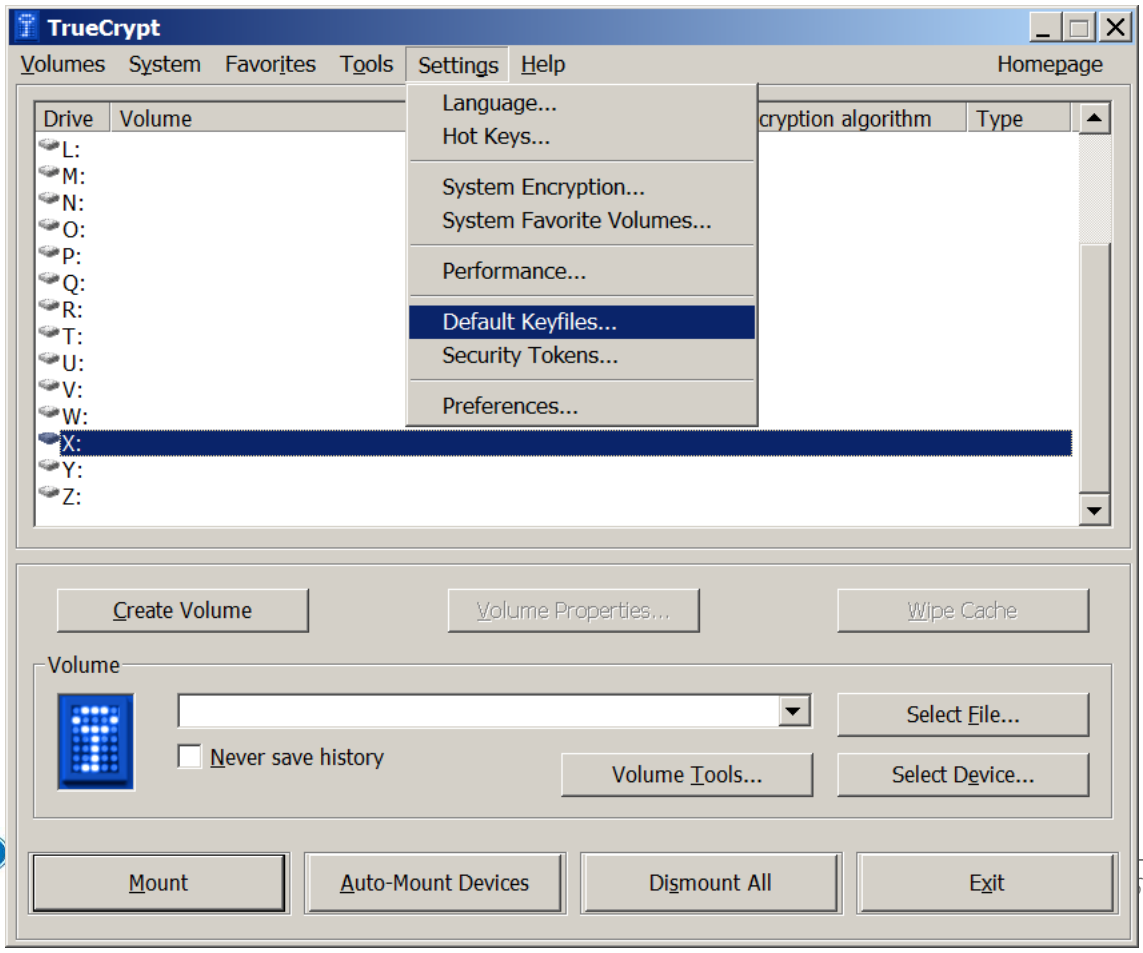
Kľúčový súbor bol úspešne uložený v chránenej pamäti Tokenu:

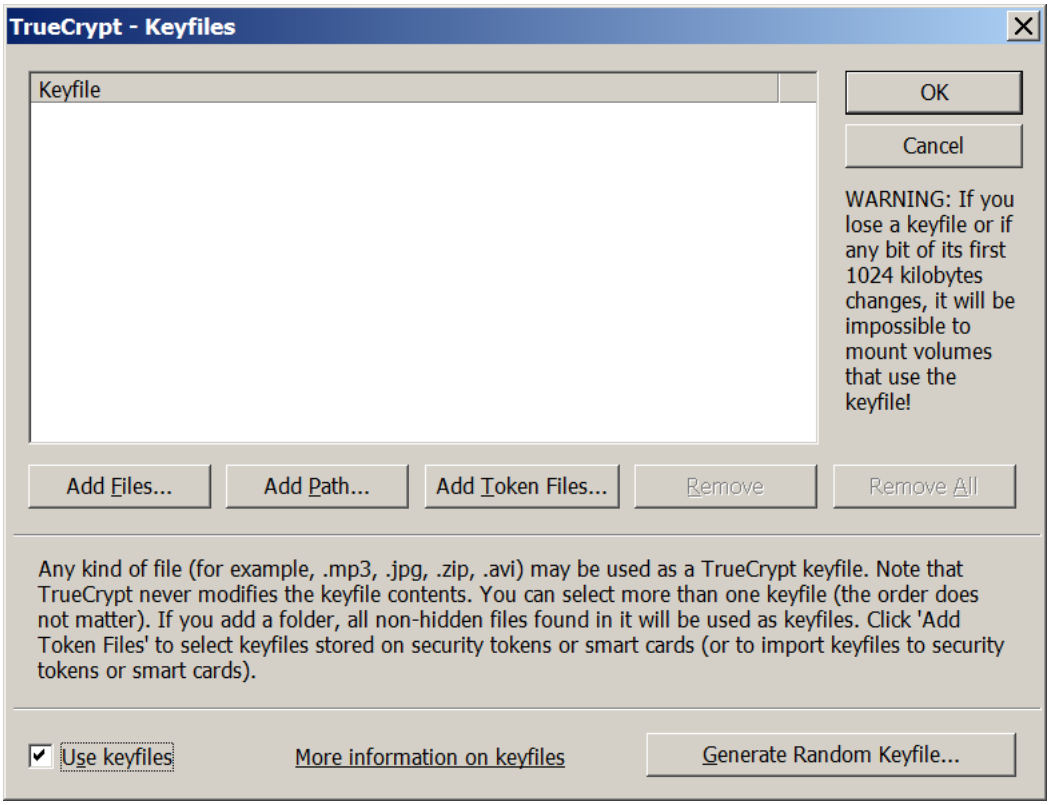


Bezpečne odstránte dočasný súbor uložený v kroku (4.2).

Zatvorte okno „Security Token Keyfiles“.

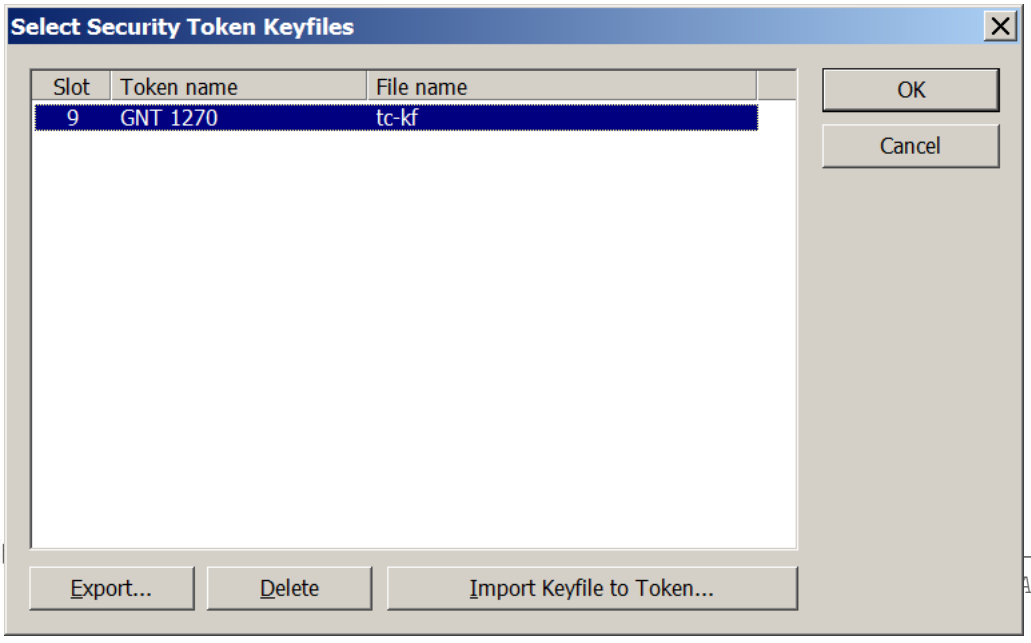
4.4 Zvoľte prednastavený kľúčový súbor





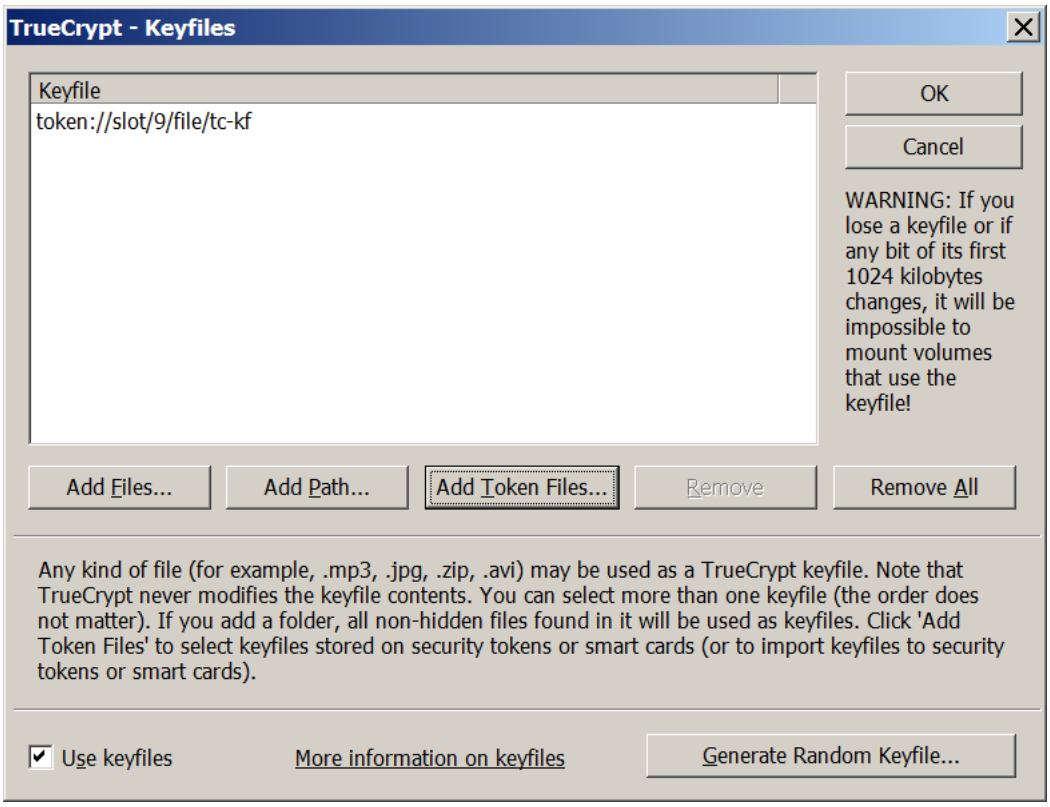
Označte pole „Use keyfiles“.

Zvoľte „Add Token Files“.



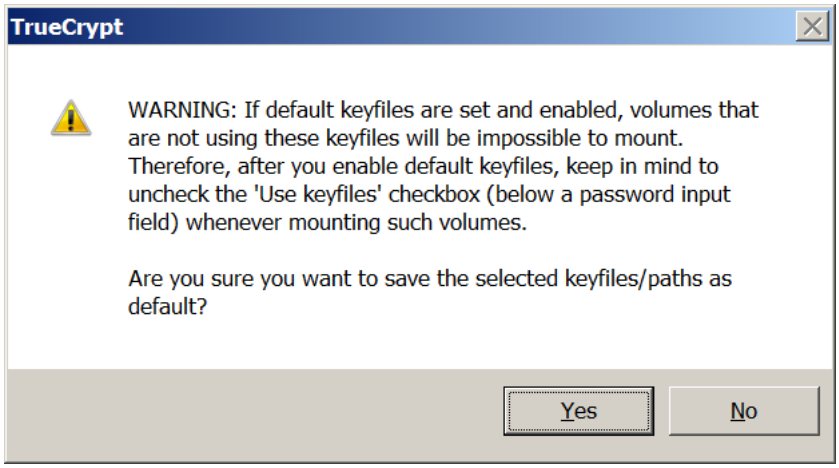
Označte kľúčový súbor a potvrďte (OK).

Prednastavený kľúčový súbor je zvolený:



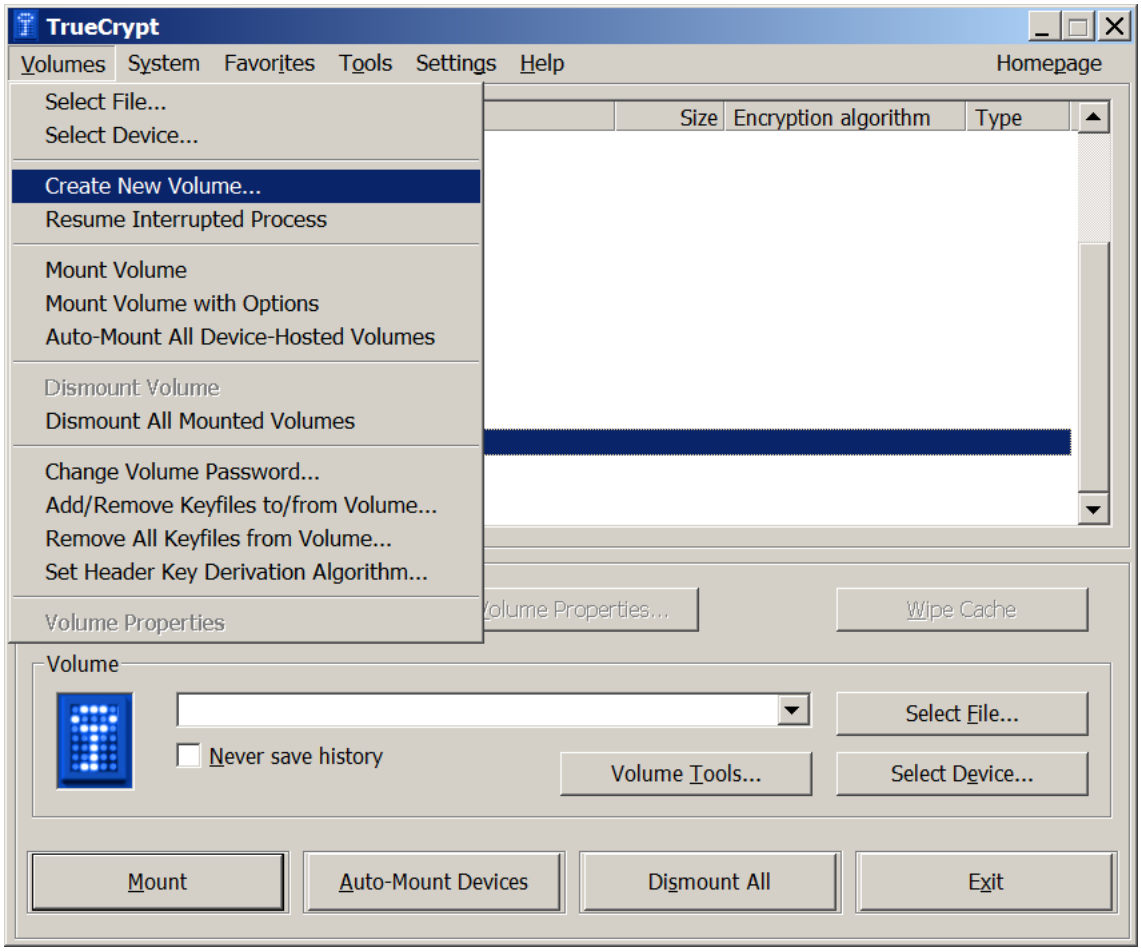
Poznámka: Voľba prednastaveného kľúčového súboru v aplikácii TrueCrypt zahŕňa USB slot, v ktorom je Token zasunutý. ***Pre korektné použitie daného kľúčového súboru budete musieť Token vždy zasunúť do toho istého USB slotu.***

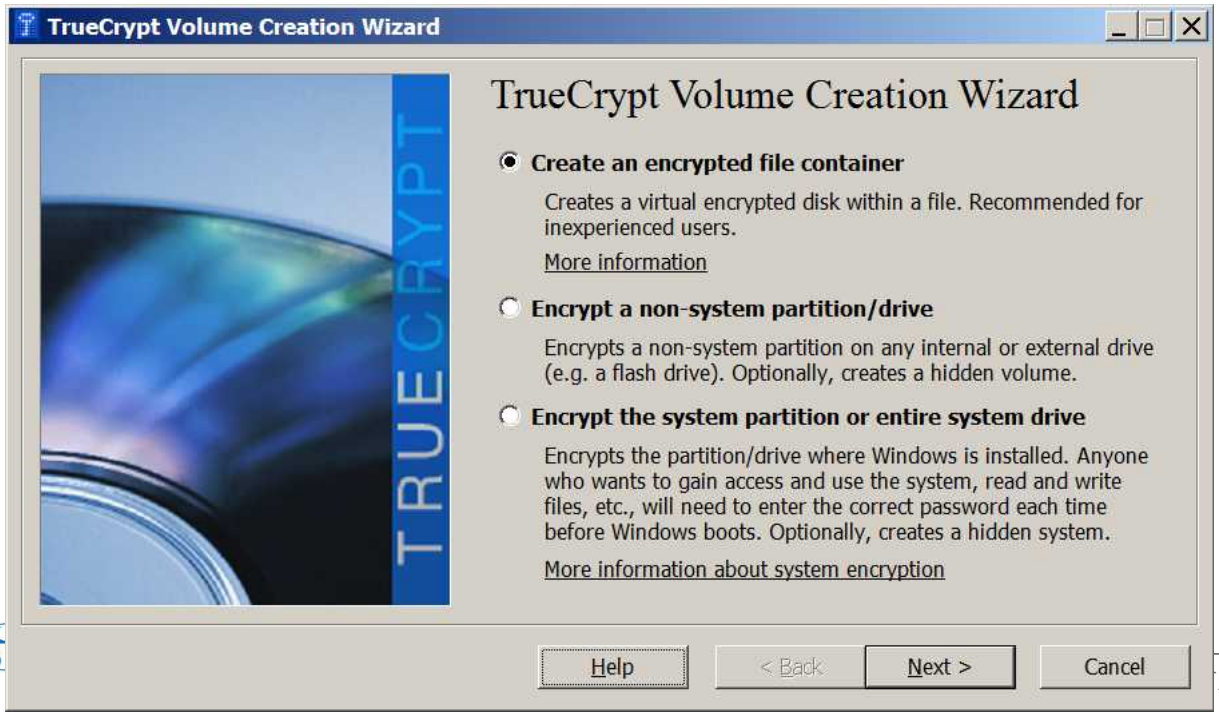
Potvrďte (OK).



Potvrďte varovanie (Yes).

4.5 Vytvorte novú jednotku

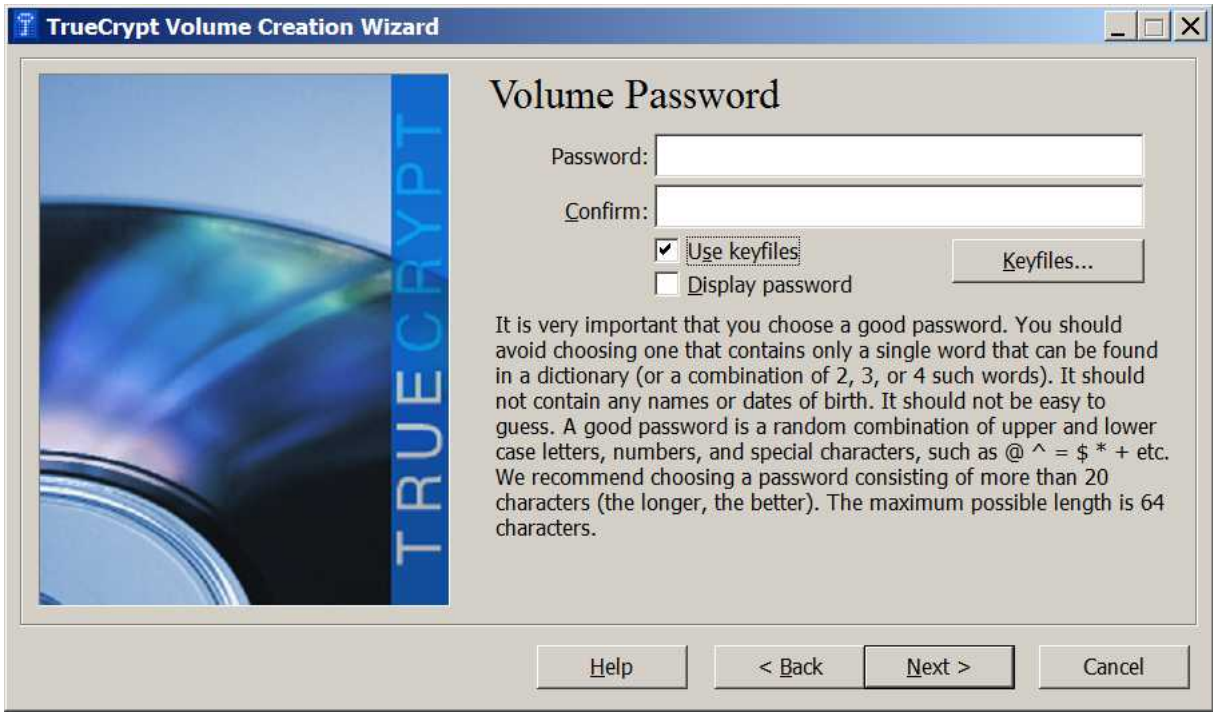




Poznámka: ***Voľbu „Encrypt the system partition...“ nieje možné použiť v kombinácii s kľúčovým súborom uloženým na Tokene****.*

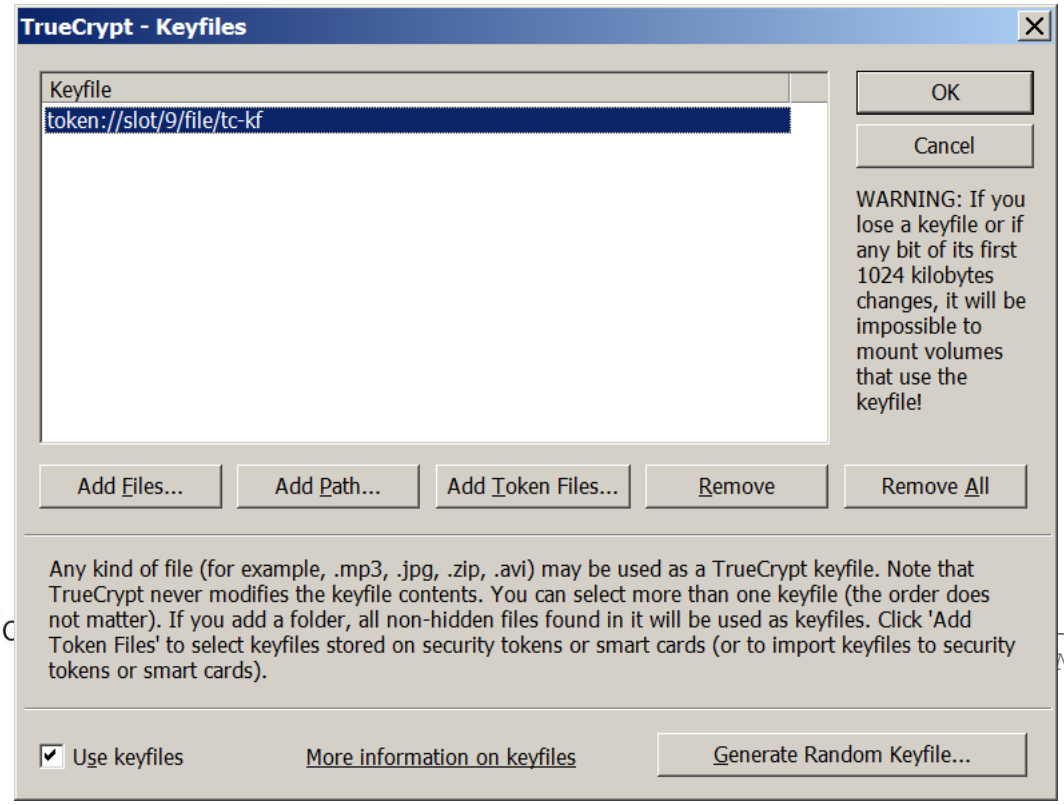
Podľa potreby zvoľte parametre novo vytváranej jednotky v nasledujúcich oknách.

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



Zvoľte tlačidlo „Keyfiles“.

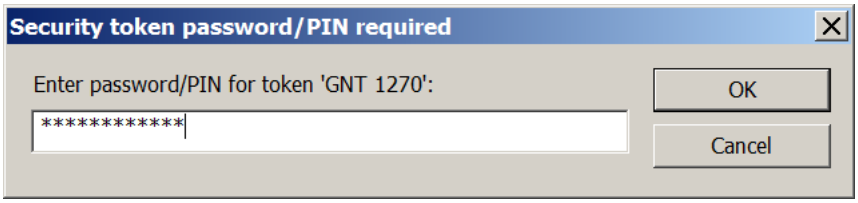
V nasledujúcom okne označte kľúčový súbor na Tokene.



Potvrďte voľbu (OK):

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

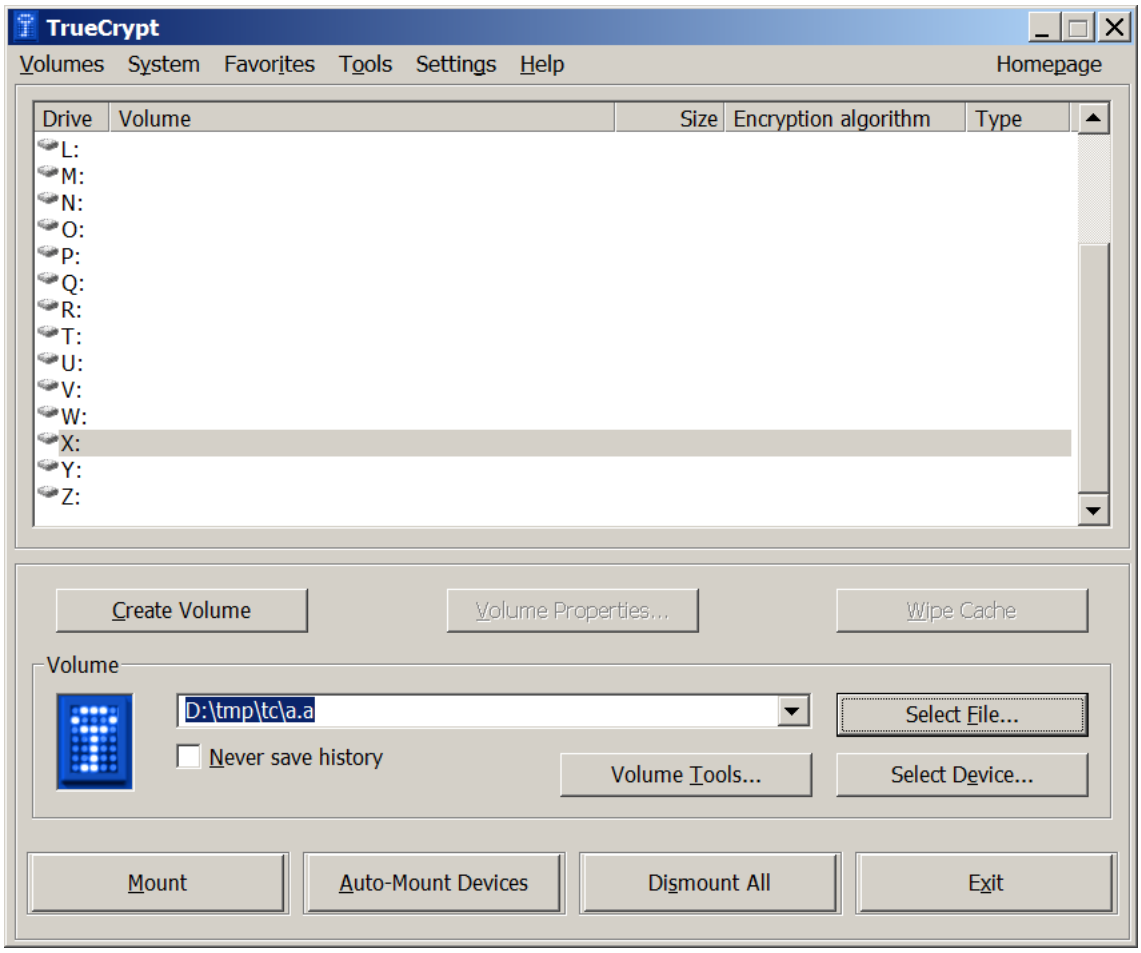
Po výzve vložte UPW Tokenu:



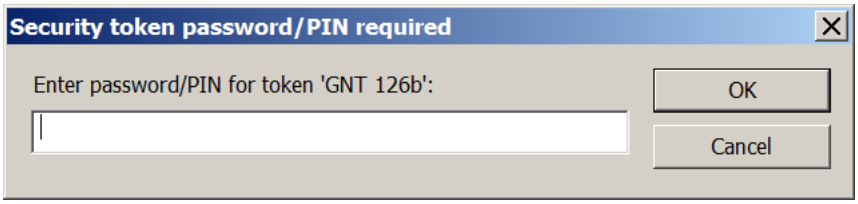
Dokončite vytvorenie jednotky.

4.6 Uvedenie šifrovaného disku do prevádzky

Zvoľte umiestnenie disku:

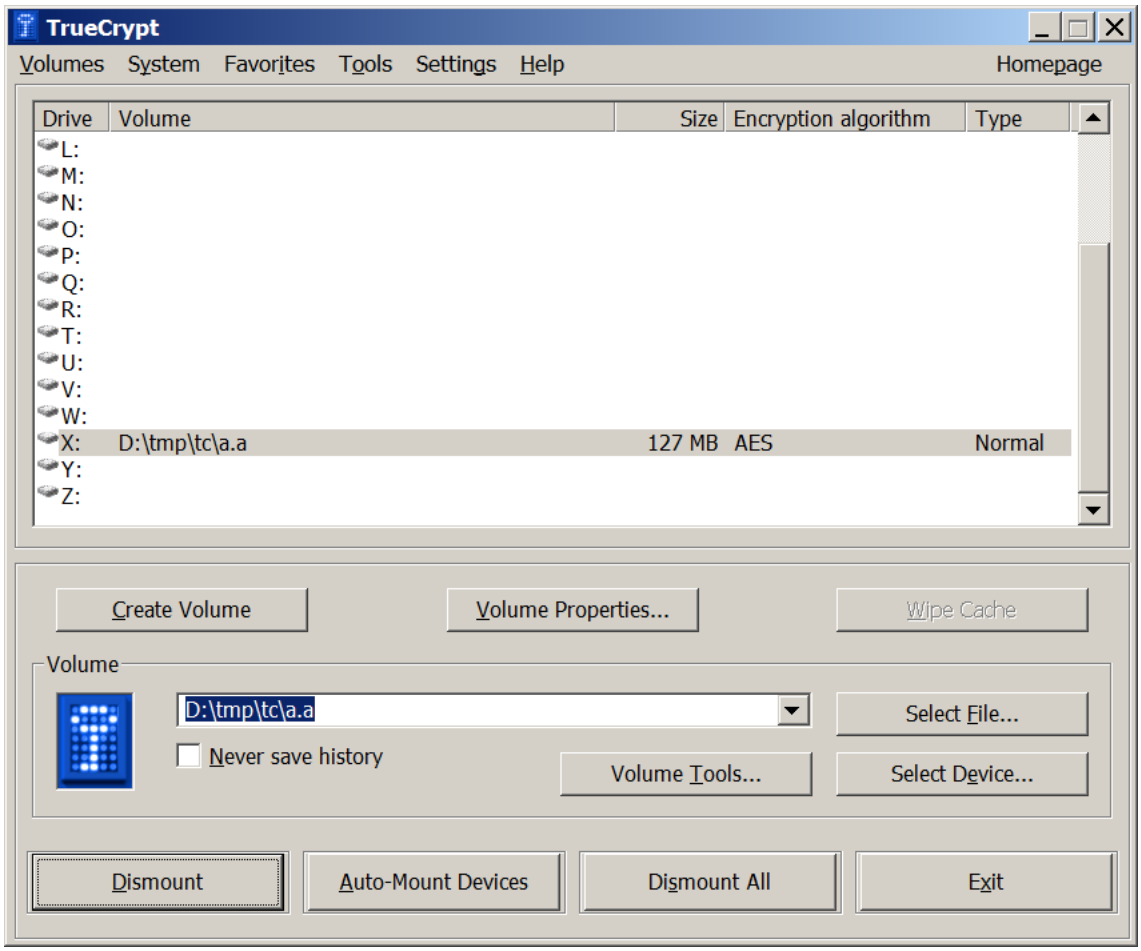


Zvoľte tlačidlo „Mount“.



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

[2] GINIT - užívateľský manuál, SoftIdea, s.r.o. , May 2011, 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

[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/freeotfe.mirror/

SoftIdea s.r.o.
Sliačska 10, 831 02 Bratislava
tel.: +421 2 444 60 444
fax.: +421 2 446 40 441
http://www.softidea.sk
info@softidea.sk