Application Notes ANCT18

TrueCrypt

ANCT18-9Oct013ks(TrueCrypt).odt

Purpose of Application: Using the CrypToken as access key to encrypted drives
Version: TrueCrypt 7.1a (Win32/64), CrypToken Kit 1.50 or higher
Last Update: 16 October 2013 by Steffen Kaetsch
Target Operating Systems: Windows 8/7/Vista (32 & 64 bit), XP
Target Processor Platforms: Intel x86
Applicable for Product: CrypToken® MX2048 JCOP, CrypToken M2048 MULTOS

Using the CrypToken with TrueCrypt for On-the-Fly Encryption of Disks and Storage Devices

TrueCrypt is an open-source solution for secure disk encryption. It creates virtual encrypted disks and mounts them as real disks, or it can encrypt existing partitions and storage devices such as hard drives or USB sticks.

The CrypToken adds professional Two-Factor-Authentication to TrueCrypt. All key files required to open the encrypted drives are stored in the small and portable USB device.

CrypToken®

- Runs on all operating systems with CCID support without separate driver
- Multiple keys and certificates can be stored in one token
- Certified smart card chip meets highest security standards according to Common Criteria
- Multi-platform support: Windows, Linux, Mac OS X
- Existing JavaCard or MULTOS applications for smart cards run without modification
- Ability to load customer-specific applications and algorithms
- Solid metal casing

Table of Contents

1. CrypToken® Installation

1.1 SafeSign Installation

To install SafeSign open the folder \SafeSign\Windows on the "CrypToken Kit" CD. There are two .exe files:

SafeSign-Identity-Client-admin.exe - Administrator Installation (for System Administrators)
SafeSign-Identity-Client-user.exe - User Installation (for normal Users)

The Administrator Installation installs an extended Token Administration Utility (TAU) which does not only allow to configure the CrypToken, it also provides administrative tasks which will be performed automatically when the Token is attached (for example, checking the validity of installed certificates). A detailed description can be found on the CrypToken CDROM at folder \Documentation\Application Notes (AET):

TAU_Guide_SafeSign-IC-Standard_v2.1.pdf - description of the Token Administration Utility
TMU_Guide_SafeSign-IC-Standard_v2.1.pdf - description of the Token Management Utility (User)

Start the SafeSign installation by double-clicking the suitable .exe file. On the Welcome screen, click "Next", then confirm the License Agreement and select the installation folder. At the next screen select the program features (see Fig. 1.1). There is no need to change anything here: If you leave the default settings, all necessary components for accessing the CrypToken on your PC will be installed automatically. The most important component is PKCS#11 which is mandatory for the CrypToken to work with TrueCrypt.

After the SafeSign installation is complete, click the "Finish" button.

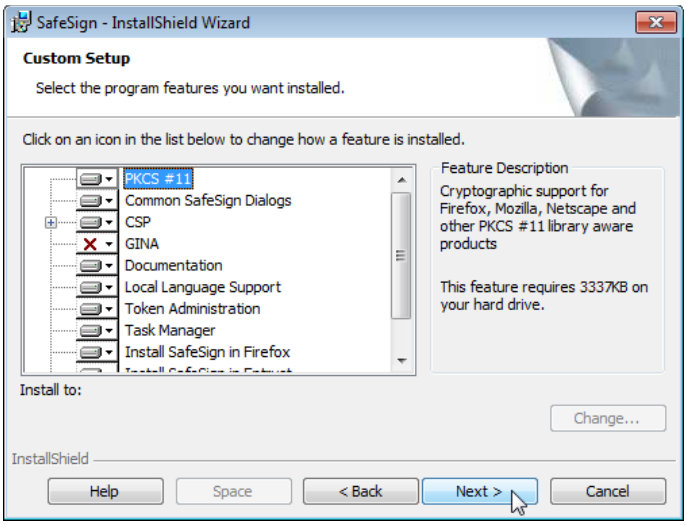


Fig. 1.1: SafeSign installation

1.2 CrypToken Driver Installation

Attach the CrypToken to a USB port. Windows will recognize the new device and open the "Found New Hardware Wizard" (see Fig. 1.2). You can click on the balloon icon in the lower right corner to get more details. If your computer is on-line, Windows will automatically obtain the driver from Windows Update.

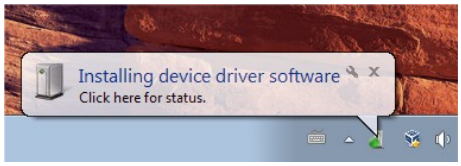


Fig. 1.2: CrypToken Driver Installation

With Windows XP, you will be asked if Windows should connect to Windows Update and search for the driver (see Fig. 1.3). Select the "Yes, this time only" radio button and click next. If you have no Internet connection, or you want to install the driver manually, put the "CrypToken Kit" CD in your CD-ROM drive and let Windows browse for drivers at the location of your CD-ROM drive (for instance E:\). You may also download the latest CrypToken drivers at www.cryptoken.com ⇨ Support ⇨ Download Area.

Fig. 1.3: CrypToken Driver Installation with Windows XP

Windows will notify you when the driver installation was finished successfully (see Fig. 1.4).

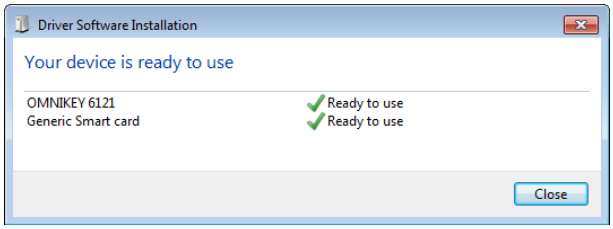


Fig. 1.4: Finishing CrypToken Driver Installation

If Windows 8/7/Vista reports that the "Generic Smart card" driver cannot be found, then you most probably did not install SafeSign yet. Please refer to chapter 1.1 for SafeSign installation.

2. Initializing the CrypToken

The CrypToken needs to be initialized prior to use it for storing keyfiles within TrueCrypt. To do so, attach the CrypToken to the USB port and start the Token Administration Tool with:

Start - Programs - SafeSign Standard - Token Administration (Administrator Installation, see 1.1)

or

Start - Programs - SafeSign Standard - Token Management (User Installation, see 1.1)

The following information will be displayed:

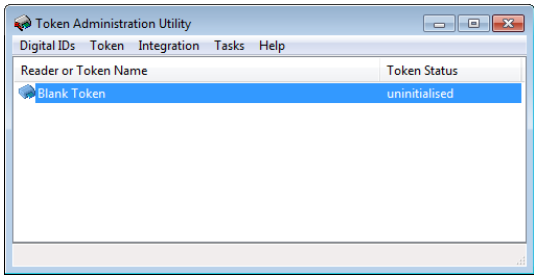


Fig. 2.1: Token Management: uninitialized CrypToken

Select the menu point "Token" and "Initialize Token". Choose a Token label, specify PIN and PUK for the attached CrypToken and confirm them. Then click "OK".

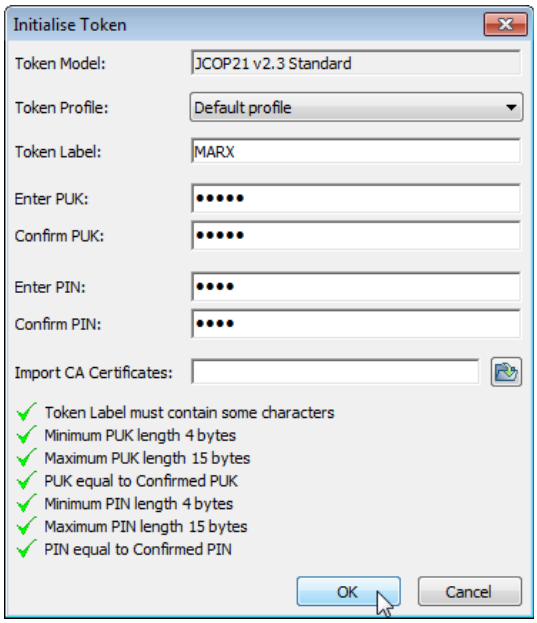


Fig. 2.2: Initializing the CrypToken

Wait until you received the message that the initialization was successful and click "OK" to finish. The CrypToken is now operable.

You can change the PIN and PUK of the CrypToken later, if required. Choose the menu point "Token" and "Change PIN" resp. "Change PUK" to do so. If you entered the wrong PIN 3 times, the CrypToken will be blocked. To unlock the PIN (the correct PUK is required for this operation) choose "Unlock PIN" from the "Token" menu. However, if the wrong PUK was entered 3 times, the CrypToken will be blocked completely!

3. Using the CrypToken with TrueCrypt

3.1 Installing the SafeSign PKCS#11 Library

Make sure that Truecrypt is properly installed on your computer and the CrypToken is plugged into the USB port.

In order to allow TrueCrypt to access the CrypToken, the SafeSign PKCS#11 library needs to be installed in TrueCrypt. Start TrueCrypt and click “Settings” → “Security Tokens”.

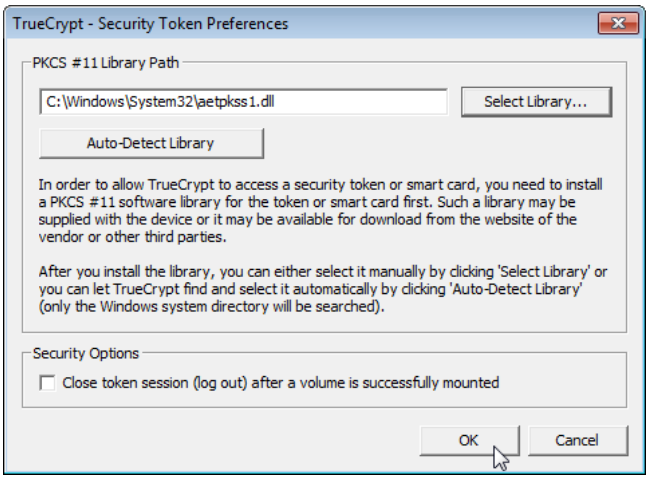


Fig. 3.1: Installing the PKCS#11 library in TrueCrypt

Click on “Select Library” and choose the SafeSign PKCS#11 library at C:\Windows\System32\aetpkss1.dll.

3.2 Creating a New TrueCrypt Volume

On the Truecrypt main screen, click the “Create Volume” button.

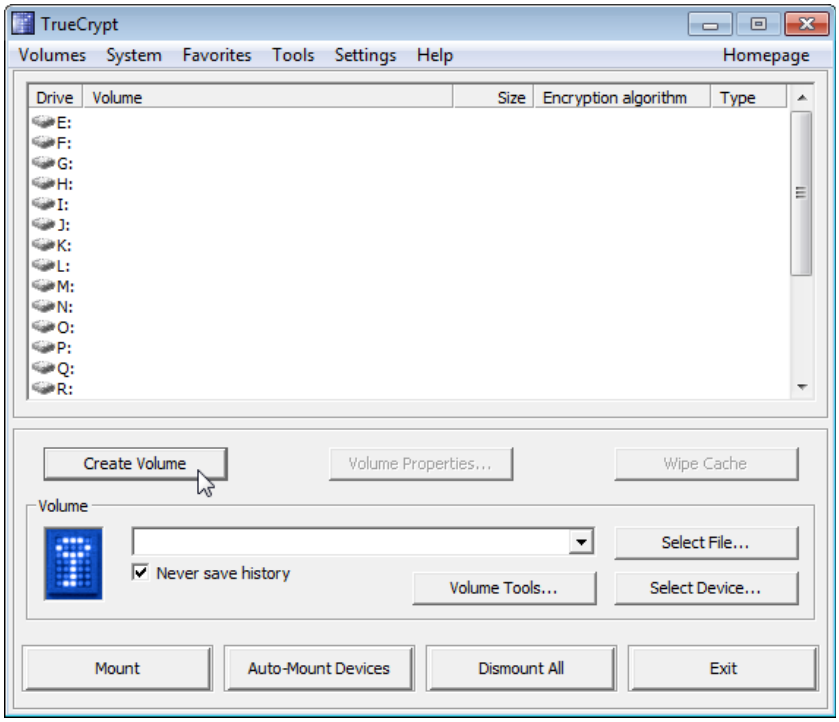


Fig. 3.2: Creating a New Volume

Now select the first or the second option. In this guide we will pick the first option (creating a virtual disk), because it will be the most common option and does not require deeper knowledge of the system.

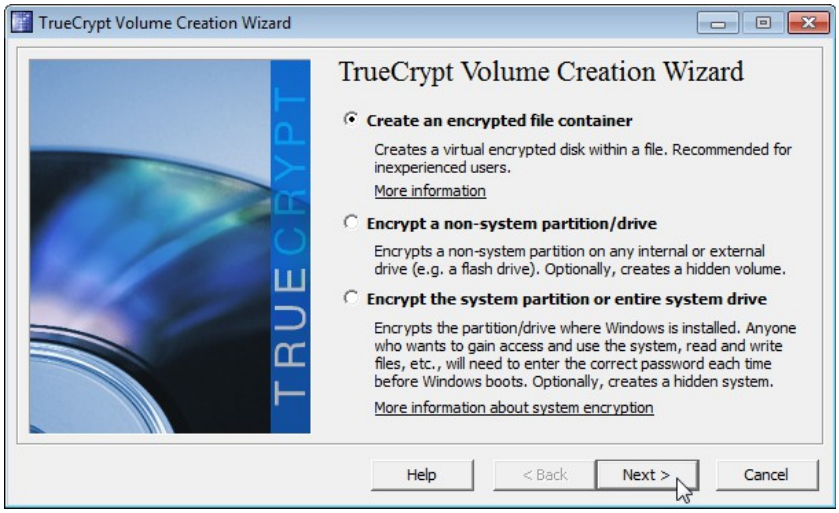


Fig. 3.3: Creating an Encrypted File Container

Select the second option only if you are familiar with partitions and hard drives available on your computer. Choosing the wrong partition may harm your system!
The third option “Encrypt the system partition or entire system drive” cannot be used in combination with the CrypToken.

In the next window, you will be asked for the volume type. Choose the first option “Standard TrueCrypt

volume".

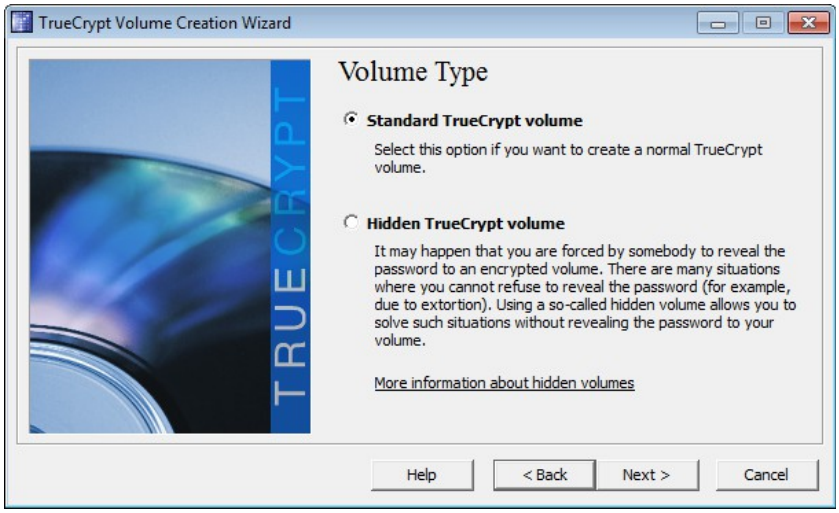


Fig. 3.4: Volume Type

If you prefer to create a hidden volume, click on the „More information about hidden volumes" button to open the TrueCrypt documentation which contains more details about it.

Click "Next" to get to the "Volume Location" screen. Click "Select File" to choose a location where you want to store your virtual encrypted disk. It can be either on your computer's internal hard drive, or on an external drive or an USB stick. Type in a name for the volume (e.g. MyDrive) and click "Save".

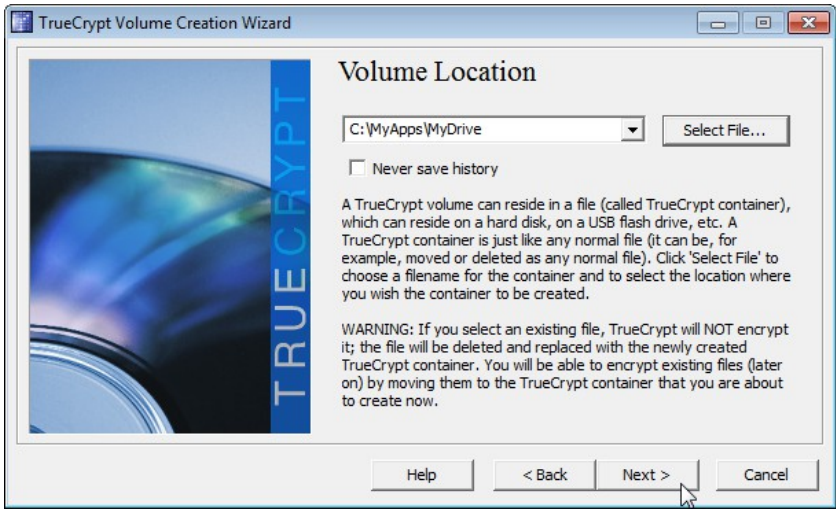


Fig. 3.5: Choosing the Volume Location

On the next screen, you can choose the encryption algorithm used for your TrueCrypt volume. We recommend to leave the default settings and click "Next".

Check the TrueCrypt documentation at www.truecrypt.org/docs to get more details on the available encryption algorithms.

Now choose the size of your encrypted volume, then click "Next"

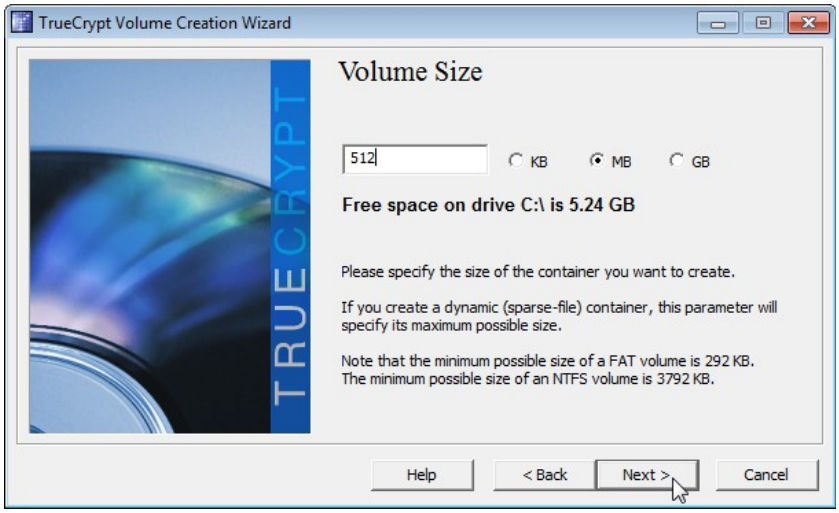


Fig. 3.6: Volume Size

3.3 Storing a Key on the CrypToken

On the next screen you can specify a volume password and/or a keyfile required to open the encrypted volume. You can use both options together, but in this case you have to type in the volume password, and the CrypToken PIN every time when you want to open the encrypted drive. To use the CrypToken as key to your encrypted drive, you have to check the option “Use keyfile”.

Fig. 3.7: Select Volume Password and/or key file

Click on “Keyfiles”. A new Window will come up – click on “Add Token Files”. Now you will be asked for the CrypToken PIN (see chapter *2*).

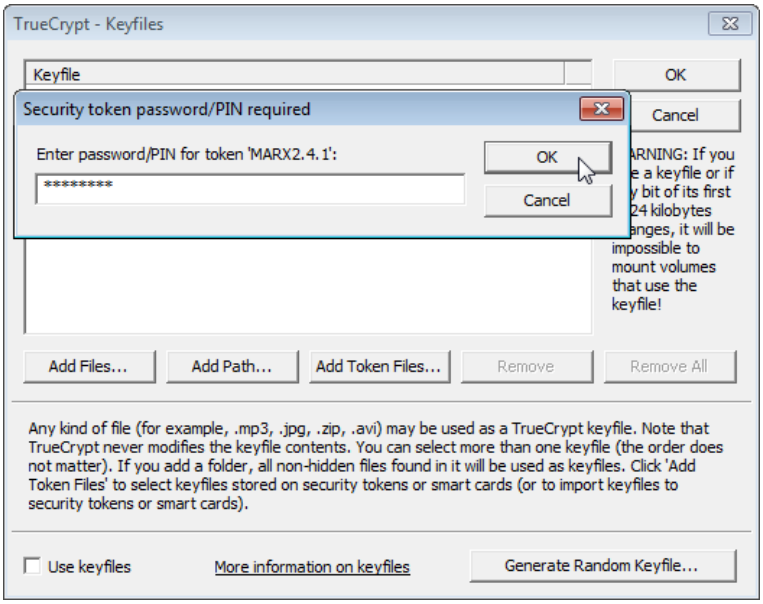


Fig. 3.8: Open the CrypToken

Click on “Import Key File to Token”. Now you can select a file which will act as keyfile to open the encrypted volume. This can be any kind of file (for example, a .txt file with some text or passphrase). Or use the “Generate Random Keyfile” option.

⚠ Please be aware that the internal memory of the CrypToken is limited (overall memory size about 72KB, depending on the model)! Therefore larger files, such as MP3 music, pictures or videos will not work (an error will occur when trying to import them to the CrypToken).

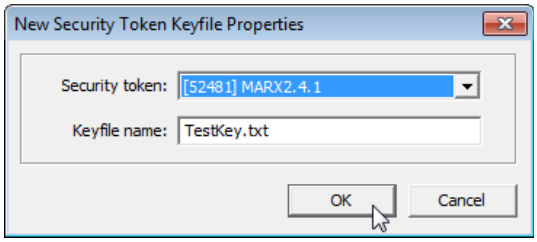


Fig. 3.9: Adding a Keyfile to the CrypToken

After you have imported the keyfile to the CrypToken successfully, it will be shown in the keyfile list:

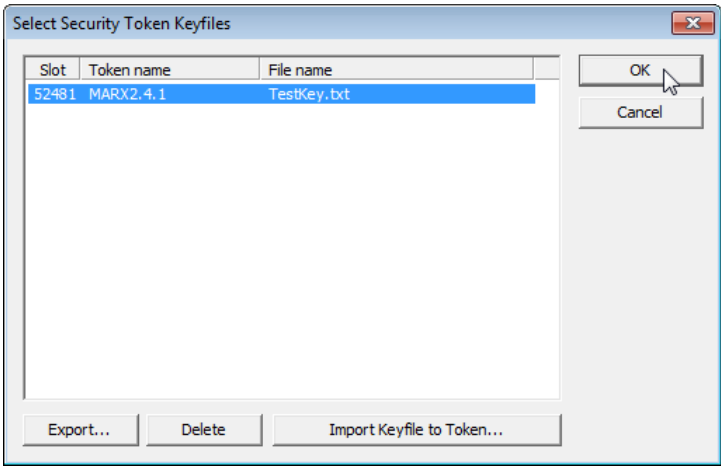


Fig. 3.10: Keyfiles stored in the CrypToken

Select this keyfile and click “OK”. Confirm the question if you want to use this keyfile as default with “Yes”.

At the next step, TrueCrypt will format the volume you have created before. Move the mouse to generate random numbers which will be used for encryption. Them click on “Format”.

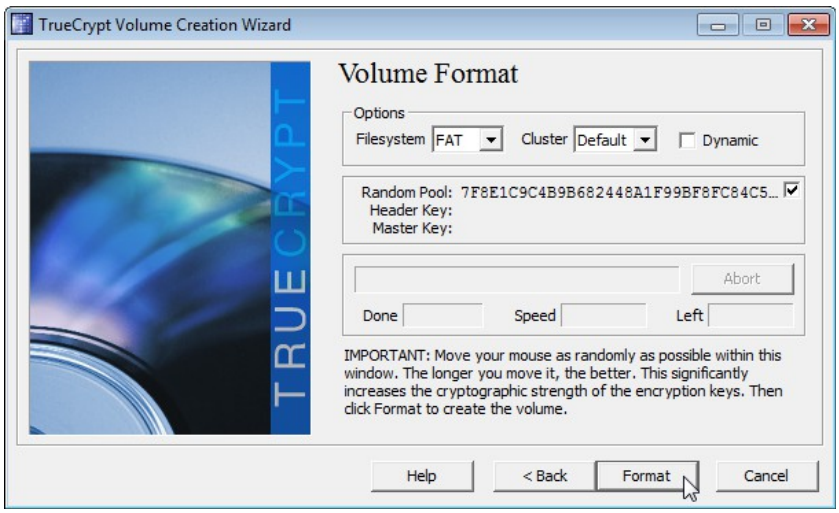
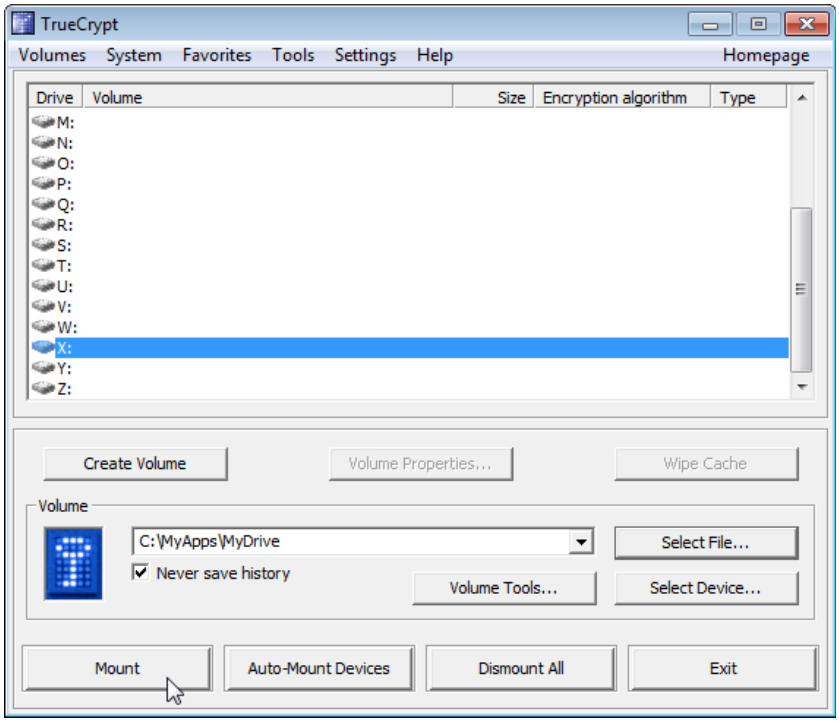


Fig. 3.11: Formatting the encrypted Volume

After formatting is finished, you will get a message that the volume was created. Click the “Exit” button to go back to the main screen.

3.4 Mounting the Encrypted Volume



In the upper part of the main screen, select the drive letter where your encrypted volume has to be mounted to. Then click on “Select File” and choose the volume you have created before (see chapter *3.2*).

If you check the “Never save history” option, TrueCrypt will not remember the location (path) to your volume file and you have to select the path manually each time you mount the volume.

Now click on “Mount”. TrueCrypt will ask you again for your CrypToken PIN, then it will mount the encrypted Volume to the drive letter you specified before.

In case the CrypToken is not present on the computer, TrueCrypt will show an error message that the keyfile was not found.

After you have finished working with your encrypted drive, click on “Dismount” or “Dismount All” to dismount the encrypted volume.

TrueCrypt will not dismount the volume automatically when the CrypToken is removed.

MARX cryptotech authentication done right™

Application Notes ANCT18

TrueCrypt

CrypToken Data Sheet

	CrypToken M2048	CrypToken MX2048
Supported Standards	PKSC#11, Microsoft CSP	PKSC#11, Microsoft CSP, Minidriver
Operation System	MULTOS	JCOP
Smart Card Chip	Infineon SLE66CX	SmartMX/JCOP41
Smart Card Chip Certifications	EAL 5+, EMV, ISO 7816	EAL 4+, EMV, ISO 7816, JavaCard 2.4.1, Global Platform
Controller Chip	Atmel/Omnikey	Atmel/Omnikey
Controller Chip Certifications	WHQL, USB CCID, PC/SC, HBCI, EMV2000	WHQL, USB CCID, PC/SC, HBCI, EMV2000
Memory (total)	64 KByte	80 KByte
Ability to Load Customer Specific Applications	yes	yes
Tamper-Proof Hardware	yes	yes
Secure Against External Interception	yes	yes
Operating Systems Supported	Windows, Linux, Mac OS X	Windows, Linux, Mac OS X
Data Retention Time	minimum 10 years	minimum 10 years
Write Cycles	>500.000	>500.000
Default Middleware Configuration	SafeSign	SafeSign
Available w/o Middleware	Yes	Yes
Electrical Certificates	FCC, CE, RWTÜV	FCC, CE, RWTÜV
Dimensions	15 x 8 x 36 mm	15 x 8 x 36 mm
Weight	9.5g	9.5g
Temperature	0°C to +60°C / 32°F to 140°F	0°C to +60°C / 32°F to 140°F
Humidity	0% to 95% relative humidity	0% to 95% relative humidity

CrypToken Certifications

CrypToken Developer's Kit

www.cryptoken.com/cryptoken-kit

MARX Data Security GmbH
Vohburger Strasse 68
85104 Wackerstein, Germany
Phone: +49 (0) 8403 / 9295-14
Fax: +49 (0) 8403 / 9295-29
contact-de@cryptotech.com

MARX CryptoTech LP
3355 Annandale Lane, Suite 2
Suwanee, GA 30024 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 770 904 3893
contact@cryptotech.com

www.cryptoken.com