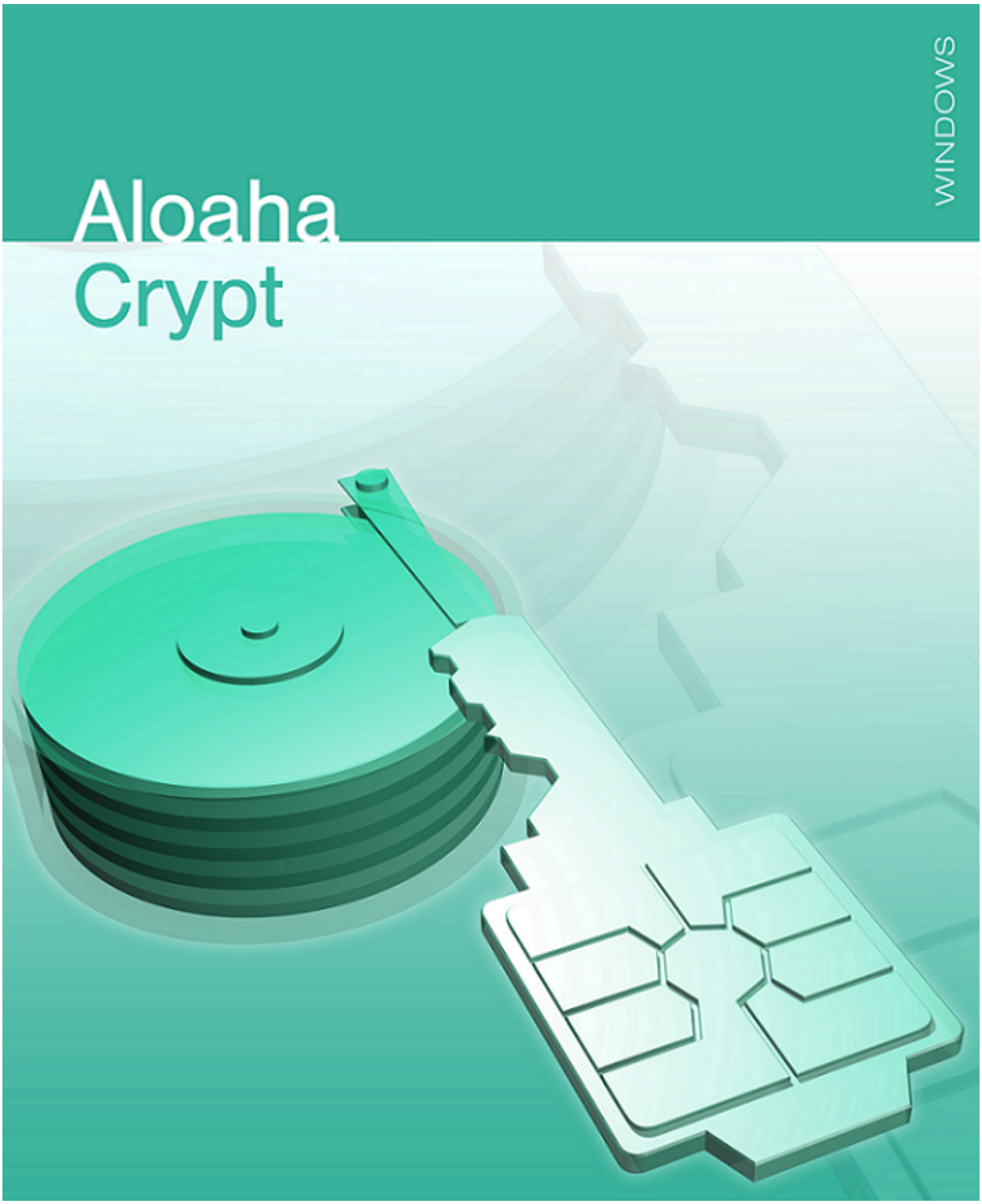



# Aloaha Crypt DE

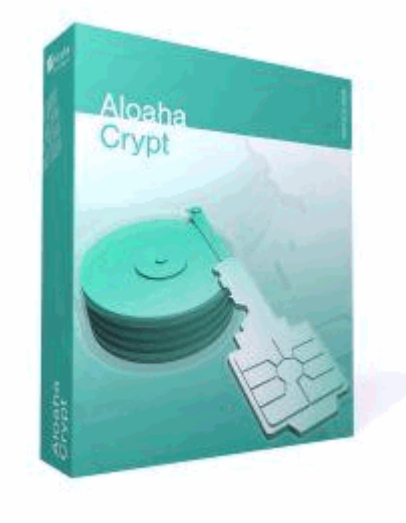
# Aloaha Crypt DE



Printed: Januar 2010

# Inhalt

# 1. Einleitung




## Aloaha Crypt

Chipkartenunterstützte Diskettenverschlüsselungssoftware für Windows 7/Vista/XP

### Haupteigenschaften:

- Erstellt eine virtuell verschlüsseltes Laufwerk innerhalb einer Datei und mountet es als ein echtes Laufwerk
- Transparente, automatische in Echtzeit (während der Übertragung) durchgeführte Verschlüsselung
- Parallelisierung und Parallelverarbeitung erlaubt Daten so schnell wie möglich zu lesen / schreiben, sofern das Laufwerk nicht verschlüsselt wurde
- Provides plausible deniability, in case an adversary forces you to reveal the smart card PIN
- Verborgener Datenträger (steganography) mit zweiter Chipkarte
- Verschlüsselungs Algorythmen: AES-256, Serpent und Twofish. Modus der Operation: XTS.

Um Aloha Crypt zu installieren laden Sie sich aus den Internet folgende Datei herunter:
**`http://www.aloaha.com/download/AloahaCryptSetup.zip`**

Überzeugen Sie sich, ob Sie entweder den Aloaha Cardconnector oder den Credential Provider installiert haben.

Aloaha Crypt ist ein Softwaresystem, um schnell verschlüsselte Datenträger (Datenspeicher) zu erstellen und unterstützen. Verschlüsselung während der Übertragung bedeutet, dass Daten automatisch ver- oder direkt entschlüsselt werden, bevor sie geladen oder ohne Benutzereingreifen gespeichert werden. Keine der auf einem verschlüsselten Datenträger gespeicherten Daten können (entschlüsselt) gelesen werden, ohne die richtige PIN zu verwenden. Das komplette Dateisystem wird (z.B, Dateinamen, Ordnernamen, Inhalt jeder Datei, freier Speicher, Metadaten, usw.) verschlüsselt.

Dateien können von und auf einen gemounteten Aloaha Crypt Datenträger (z.B. durch Drag 'n' Drop) kopiert werden, wie sie auf jede normale Diskette kopiert werden. Dateien werden automatisch entschlüsselt (im Speicher/RAM), während sie gelesen oder von einem verschlüsseltenten Aloaha Crypt verzeichnis kopiert werden. Ähnlich werden Dateien, die geschrieben oder zum Aloaha Crypt Verzeichnis kopiert werden, im RAM automatisch verschlüsselt (direkt, bevor sie zur Diskette geschrieben werden). Dies bedeutet nicht, dass die ganze Datei, die verschlüsselt/entschlüsselt werden soll, im RAM gespeichert werden muss, bevor sie verschlüsselt/entschlüsselt werden kann. Es gibt keine Zusatzspeicher (RAM) Voraussetzungen für Aloaha Crypt. Für eine Illustration der Durchführung lesen Sie sich den folgenden Absatz durch.

Angenommen es existiert eine in einem Aloaha Crypt Verzeichnis gespeicherte *.avi Videodatei (die Videodatei komplett verschlüsselt). Der Anwender gibt die PIN ein und mounted den Aloaha

Crypt Datenträger. Wenn der Anwender auf das Ikon der Videodatei klickt, startet das Betriebssystem die Anwendung, die mit der Dateiart - i.d.R. ein Mediaplayer - verbunden ist. Der Mediaplayer beginnt damit einen Teil der verschlüsselten Videodatei vom Aloaha Crypt Datenträger in den RAM (Speicher) zu laden, um sie zu abzuspielen. Während der Teil geladen wird, entschlüsselt Aloaha Crypt ihn (im RAM) automatisch. Der entschlüsselte Teil des Videos wird vom Mediaplayer abgespielt. Während dieser Teil abgespielt wird, beginnt der Mediaplayer den nächsten Teil der Videodatei vom verschlüsselten Aloaha Cryt Datenträger zum RAM zu laden und den Prozess zu wiederholen. Dieser Prozess wird Verschlüsselung / Entschlüsselung während der Übertragung genannt. Dies gilt für alle Dateiarten.
Beachten Sie, dass Aloaha Crypt nie irgendwelche entschlüsselten Daten auf eine Diskette speichert - nur provisorisch im RAM (Speicher). Selbst wenn das Volumen gemounted ist, bleiben die im Datenträger gespeicherten Daten verschlüsselt. Wenn Sie Windows erneut starten oder Ihren Computer ausschalten, wird der Datenträger dismounted und die darin gespeicherten (verschlüsselten) Daten unzugänglich sein. Selbst wenn die Stromversorgung plötzlich unterbrochen wird (ohne vorheriges herunterfahren des Systems), sind die im Datenträger gespeicherten Daten unzugänglich. Um sie wieder zugänglich zu machen, müssen Sie den Datenträger erneut mounten.

# 2. Anwendung

Enter topic text here.

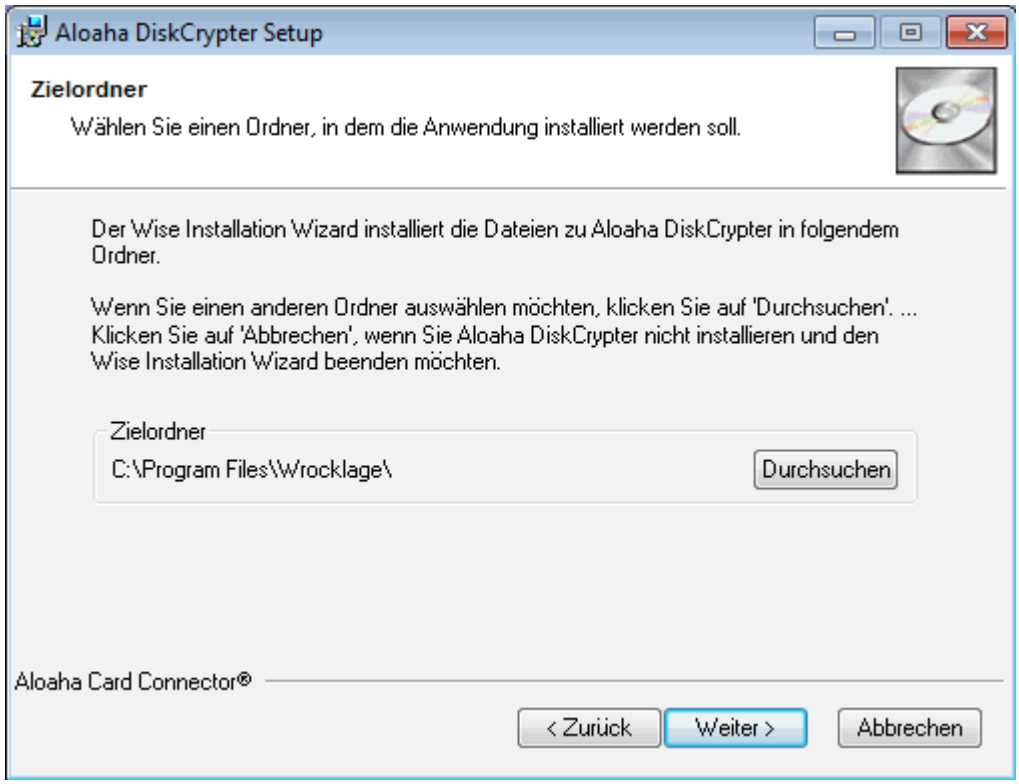
# 3. Installation

Aloaha Crypt können Sie sich direkt aus dem Internet unter http://www.aloaha.com/download/AloahaCryptSetup.zip. herunterladen.

Die Datei speichern Sie direkt auf Ihrer Festplatte. Sobald der Download beendet ist, entpacken Sie die Archivdatei und doppelklicken auf "credentialprovider.exe"

Anschließend beginnt die Installation.


Klicken Sie auf Weiter. Im nächsten Dialog wählen Sie bitte das Installationsverzeichnis. Standardmässig ist das auf c:\programme\wrocklage voreingestellt.

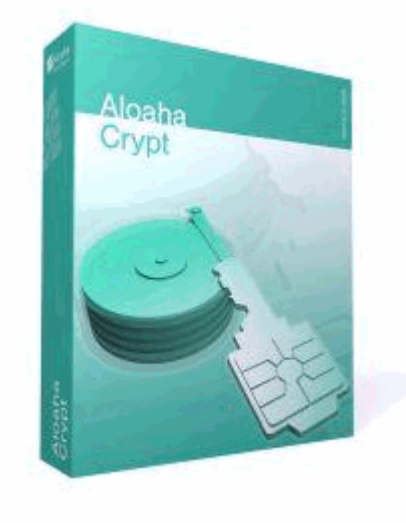



An dieser Stelle der Installation können Sie wählen ob Sie noch einmal einen Schritt zurück gehen möchten oder ob die Installation beginnen soll. Klicken Sie dazu auf Back oder Next.


Nach der erfolgreichen Installation schließen Sie den Installationsvorgang mit "Fertigstellen" ab.

Jetzt können Sie Aloaha Crypt verwenden. In Ihrem Startmenü unter **Start>Alle Programme>Aloaha** finden Sie eine Verknüpfung zum Starten des Programmes.

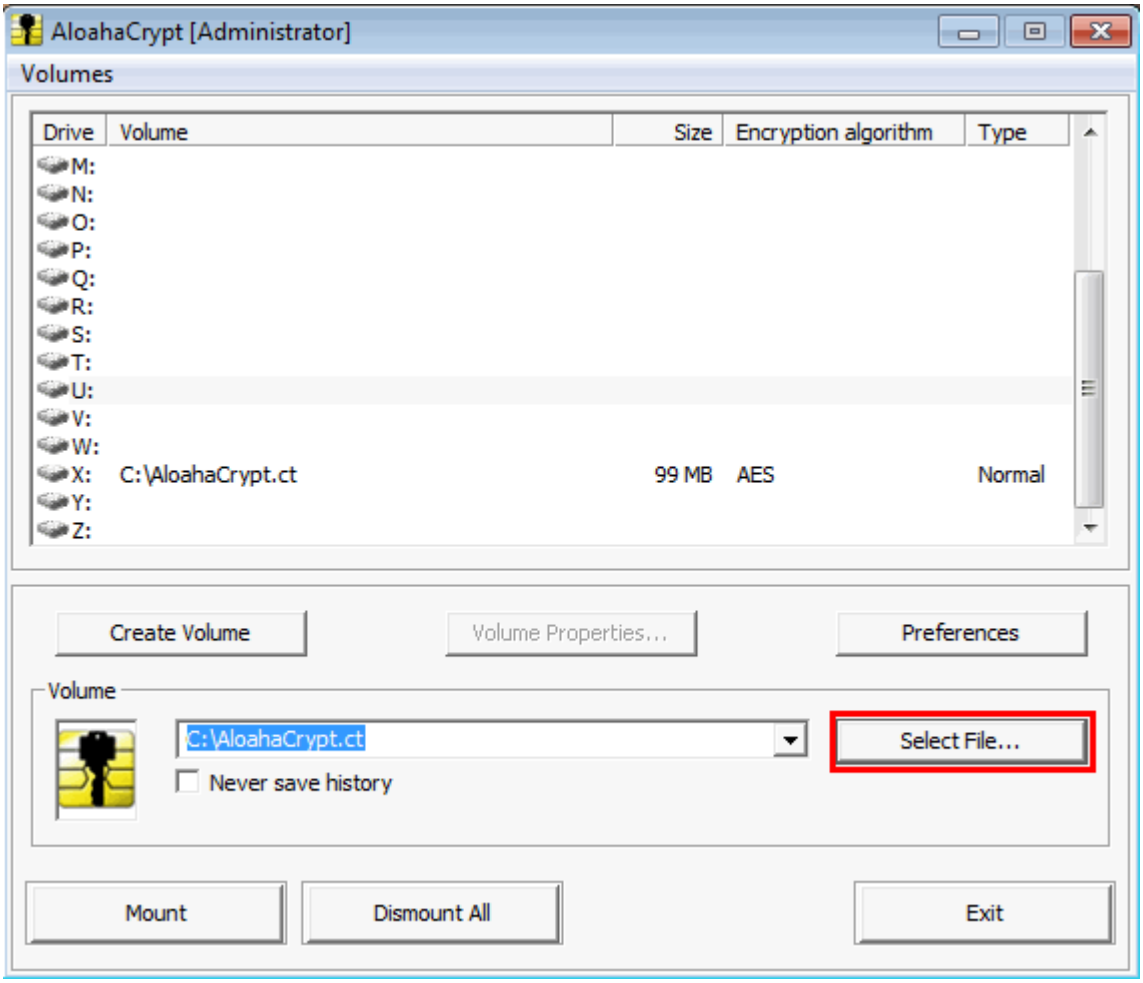
# 4. Konfiguration



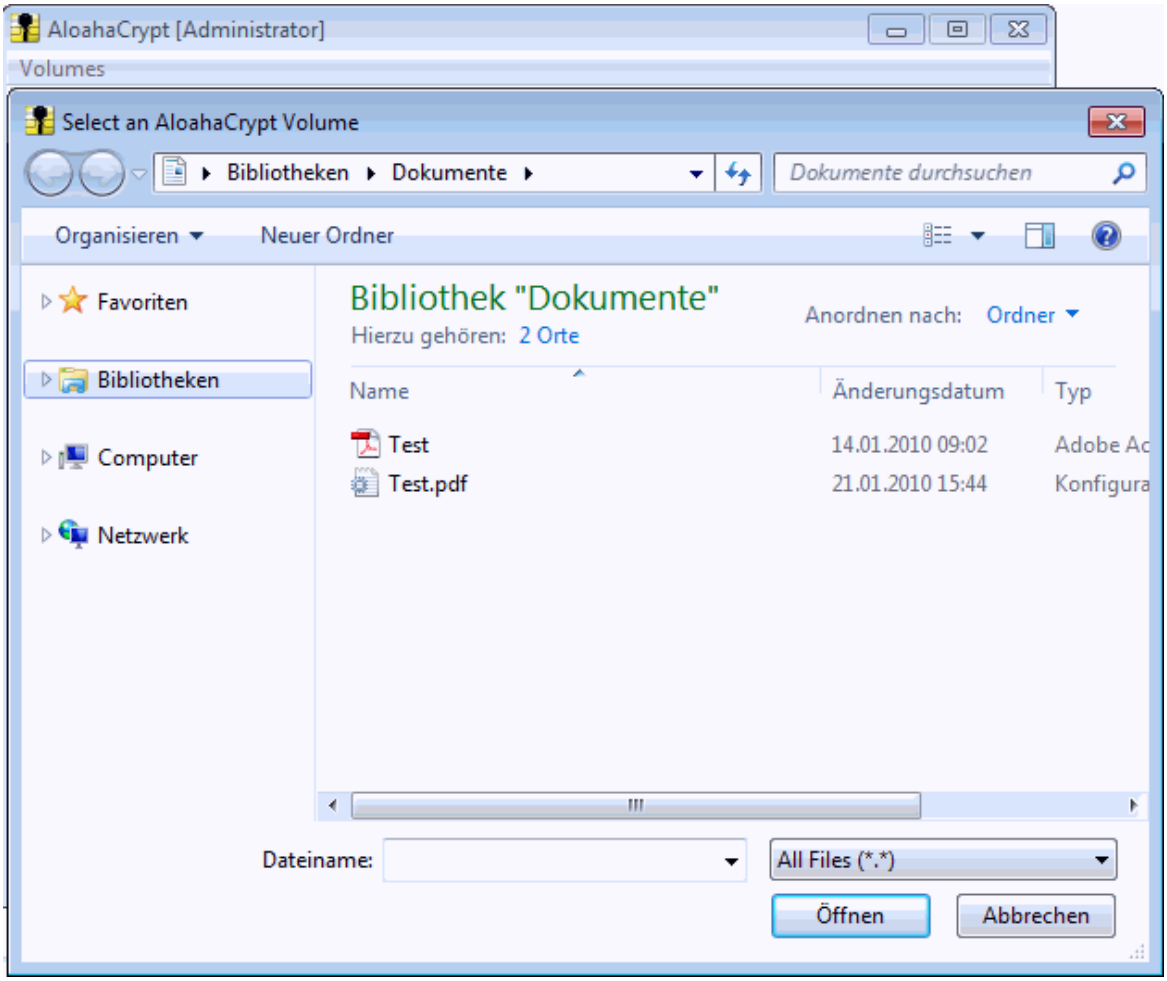

Datei auswählen
Gerät auswählen
Datenträger mounten
Datenträger mit Optionen mounten
Datenträger entfernen
Alle Datenträger entfernen
Erstelle neuen Datenträger
Datenträger-Eigenschaften

## 4.1 Datei auswählen

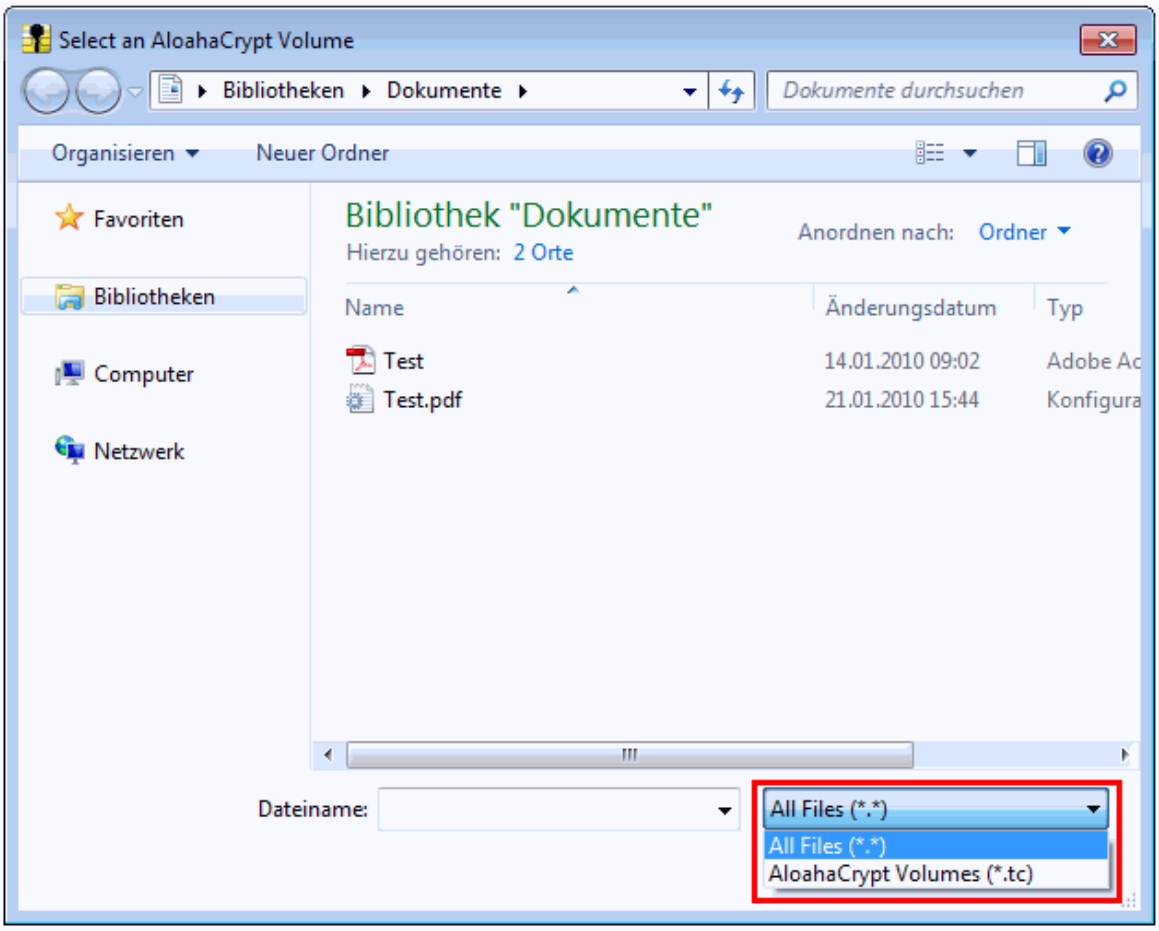
Wenn Sie Dateien verschlüsseln möchten, klicken Sie auf "Select File ...".



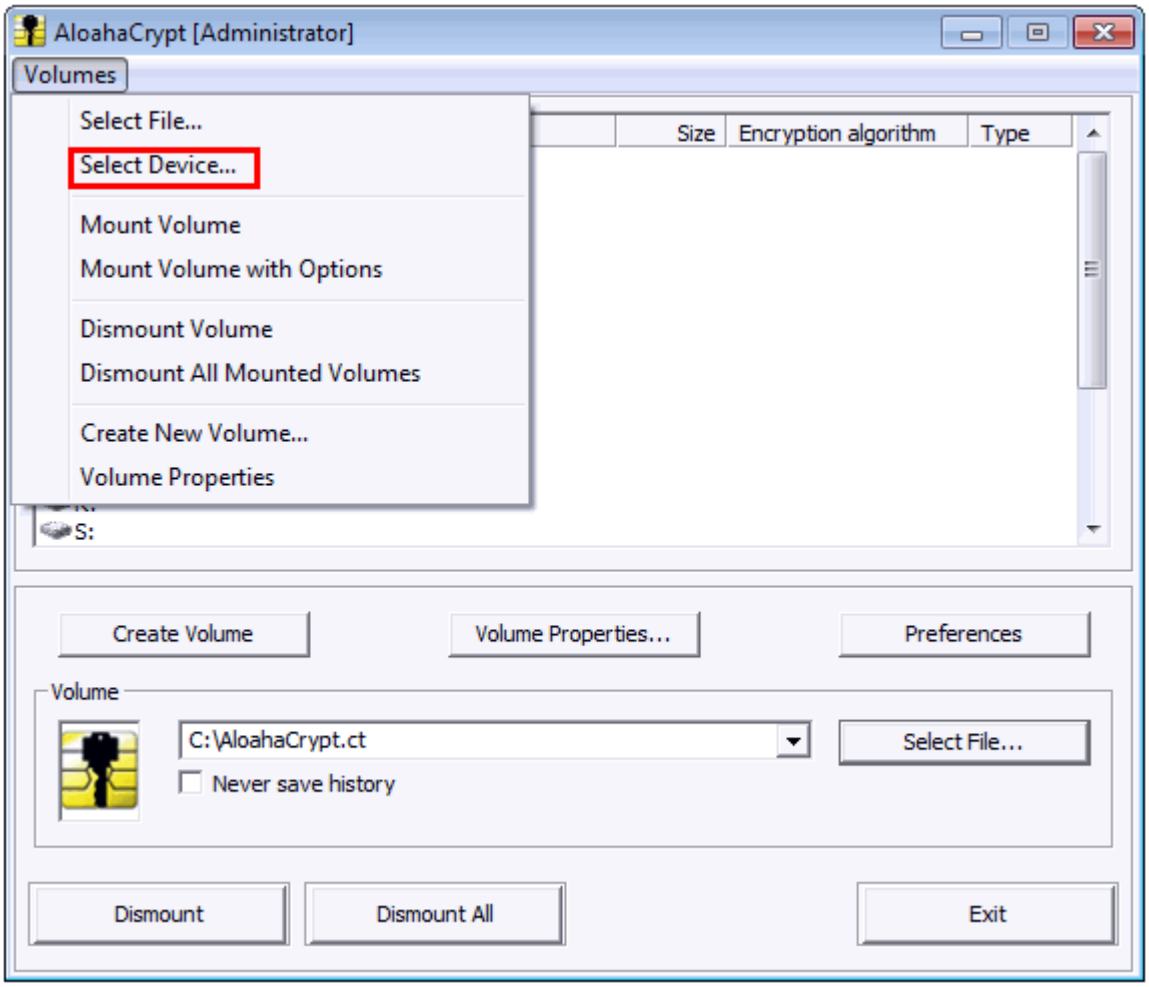
Ein neues Fenster, welches wie der Windows Explorer aussieht, öffnet sich. Hier können Sie die entsprechenden Dateien auswählen.

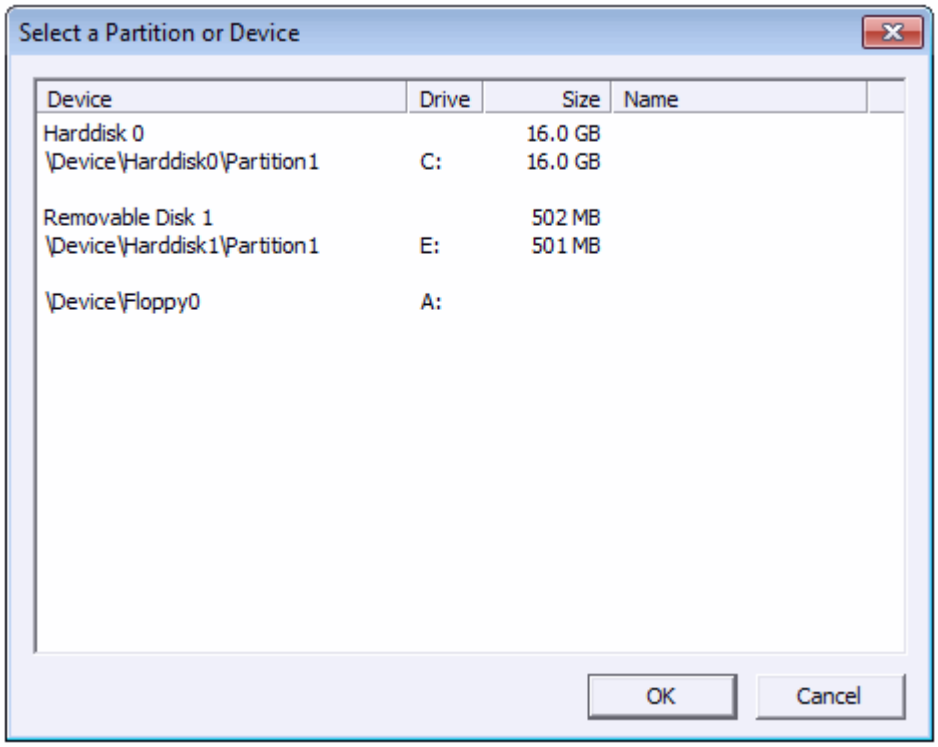


Sollten Sie nur die "AloahaCrypt Volumes" verwenden wollen, beutzen Sie den Filter, andernfalls wählen Sie "All Files".



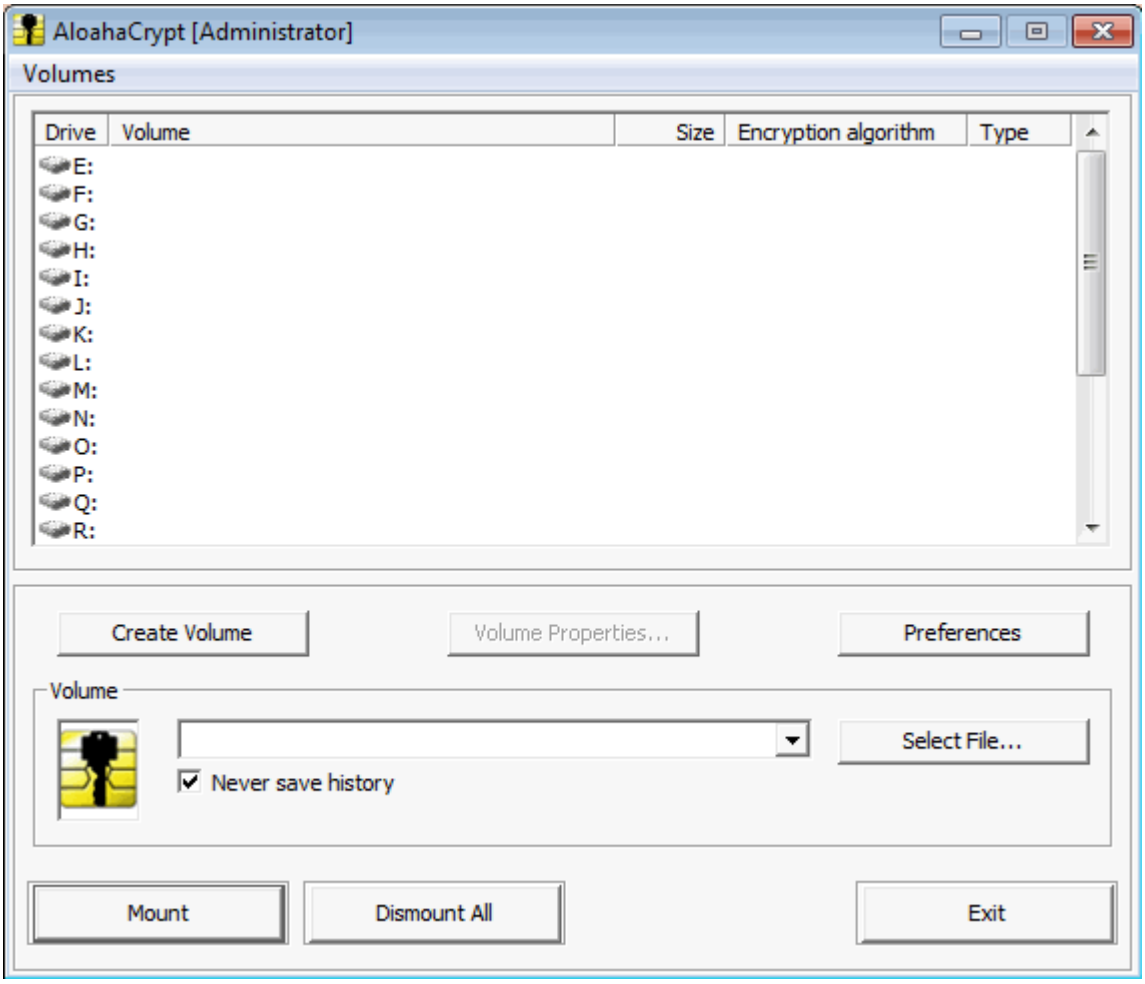
## 4.2 Laufwerk auswählen



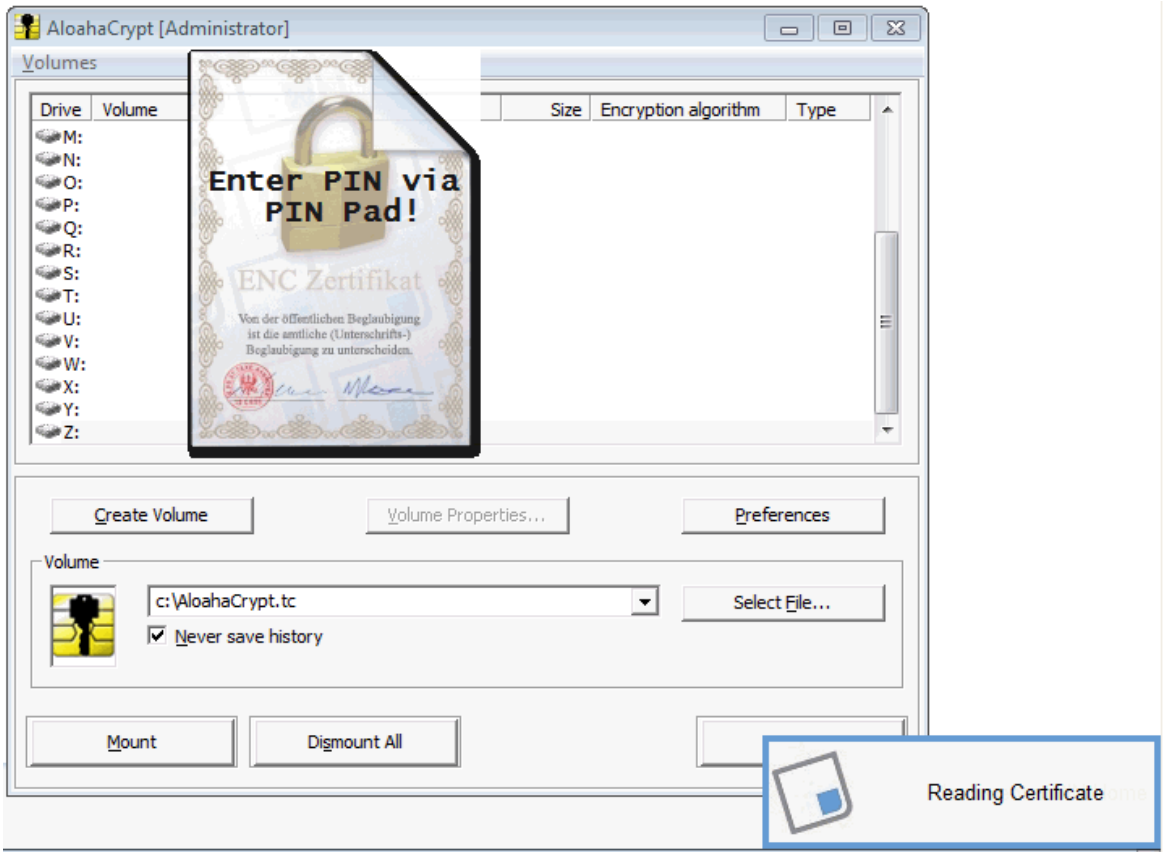



## 4.3 Datenträger mounten

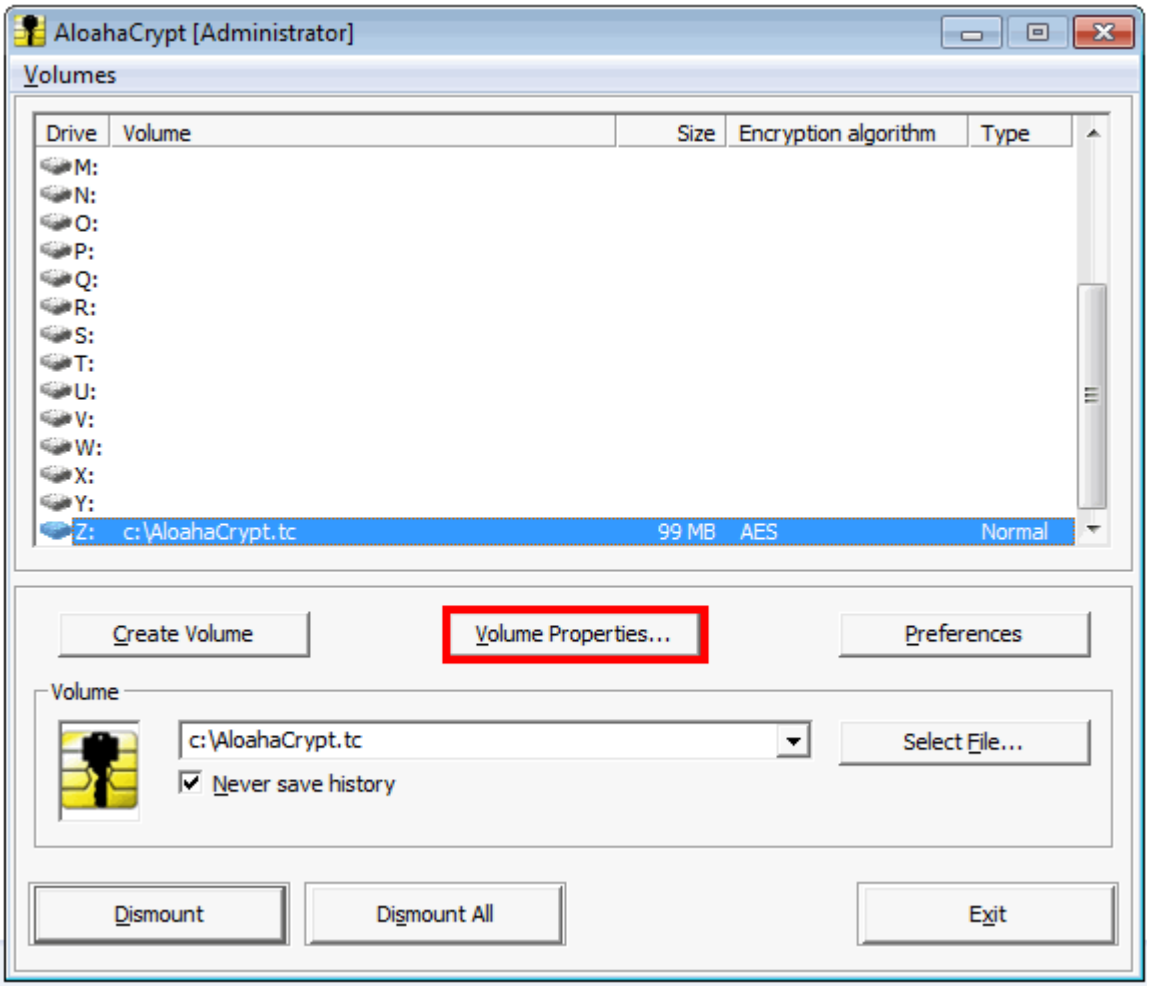
Bestimmen Sie den Pfad des Datenträger-Verzeichnisses und klicken Sie auf den Button "Mount".



Sie werden aufgefordert, Ihre PIN einzugeben. Anschließend wird das 64 Byte Passwort per SmartCard verschlüsselt und das Laufwerk gemountet.



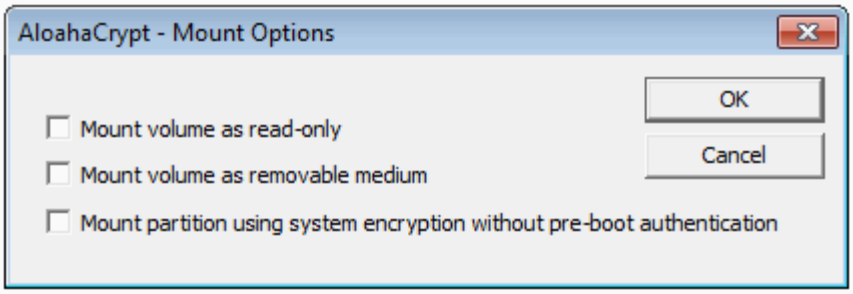
Der Datenträger wurde als Laufwerk z: gemountet



## 4.4 Datenträger mit Optionen mounten

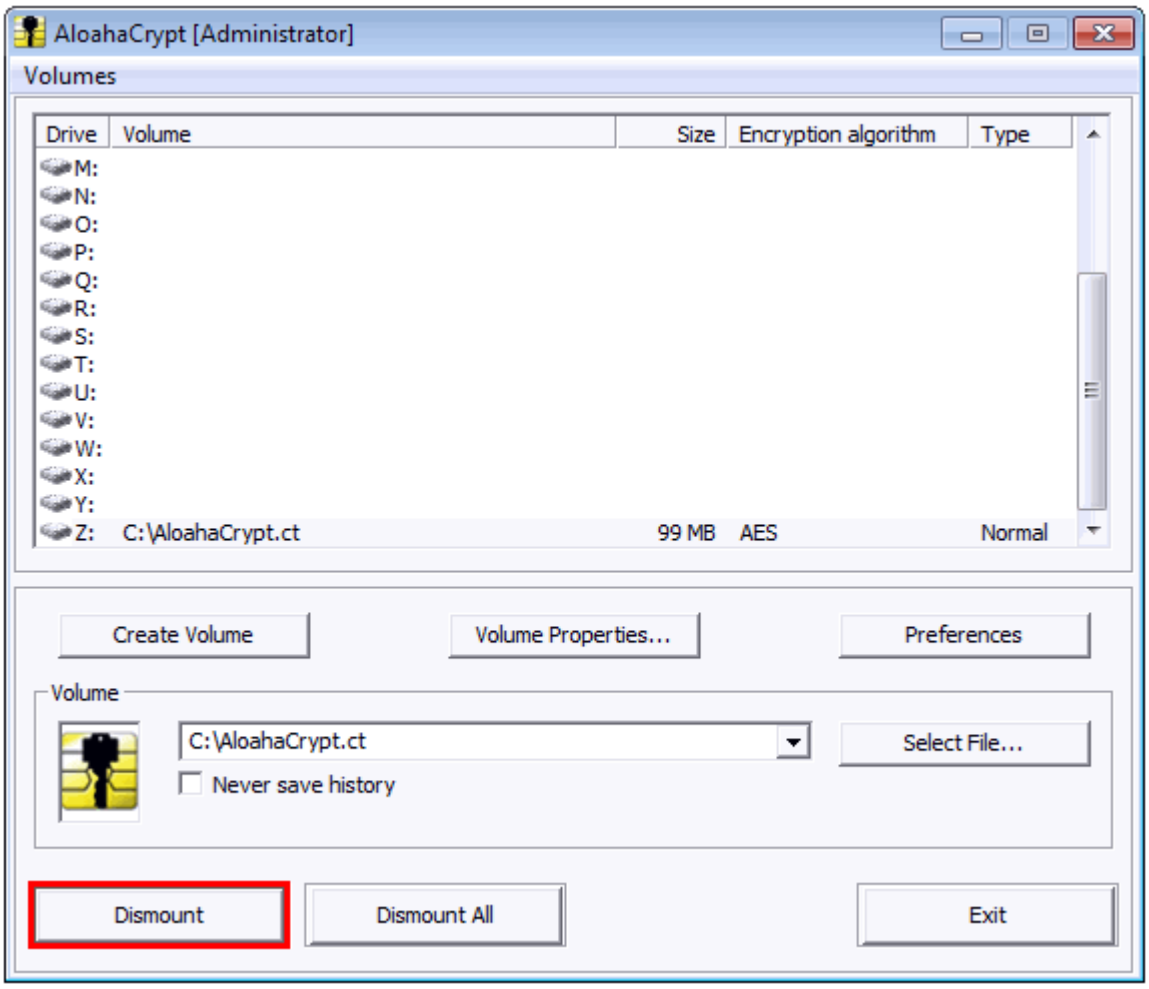
Sie haben drei Möglichkeiten, einen Datenträger zu mounten.

- Datenträger schreibgeschützt mounten (nur Lesemodus)
  Ein schreibgeschützter Datenträger wird erstellt. Dokumente können nur gelesen werden.
- Datenträger als Wechseldatenträger mounten
  Ein Datenträger, welcher entfernt werden kann, wird erstellt z.B. USB-Stick
- Einen Teilbereich (Partition), der die systemseitige Verschlüsselung ohne pre-boot authentication nutzt erstellen.
  Eine Partition, welche die systemseitige Verschlüsselung nutzt wird gemountet.

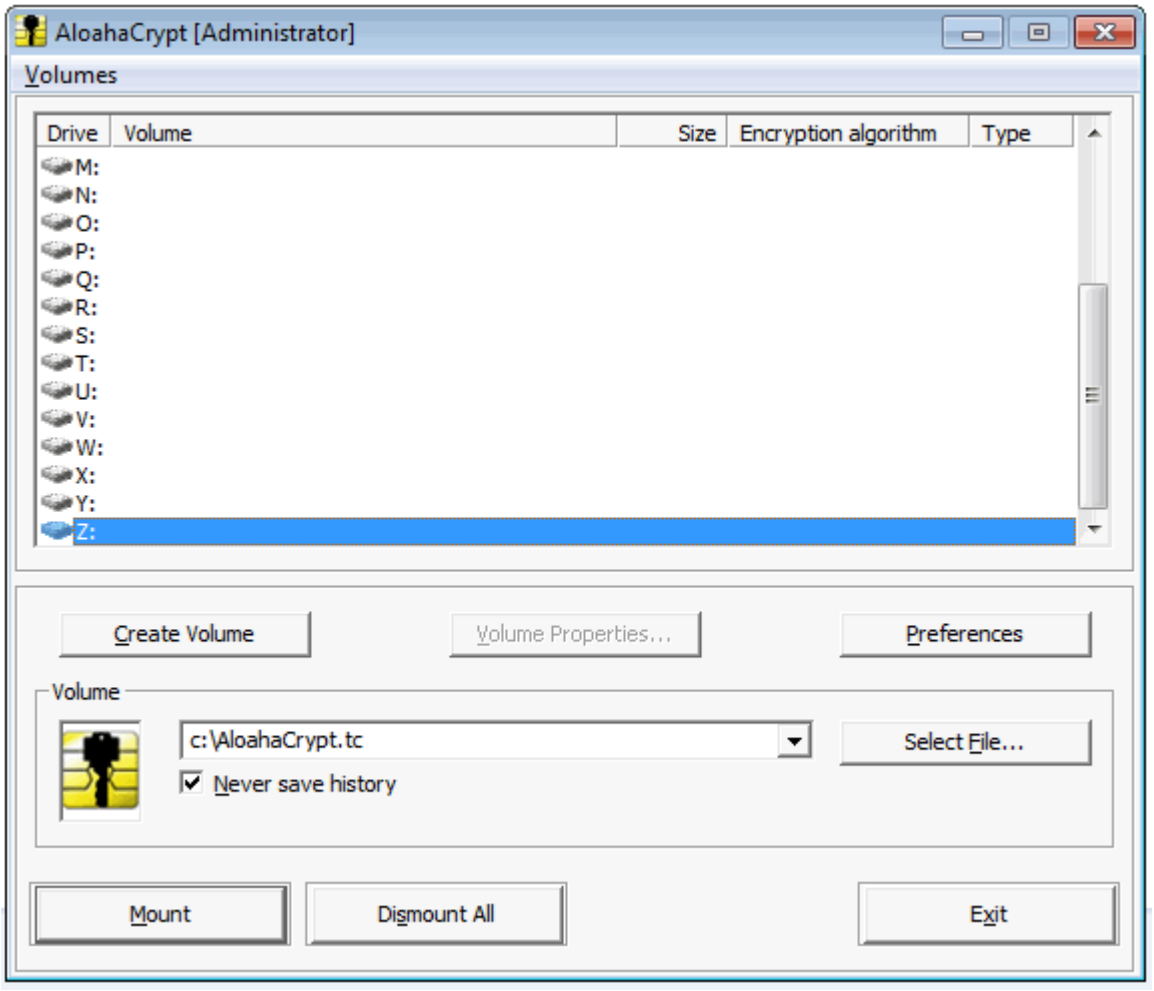



## 4.5 Datenträger entfernen

Sie sehen hier ein gemountetes Laufwerk.

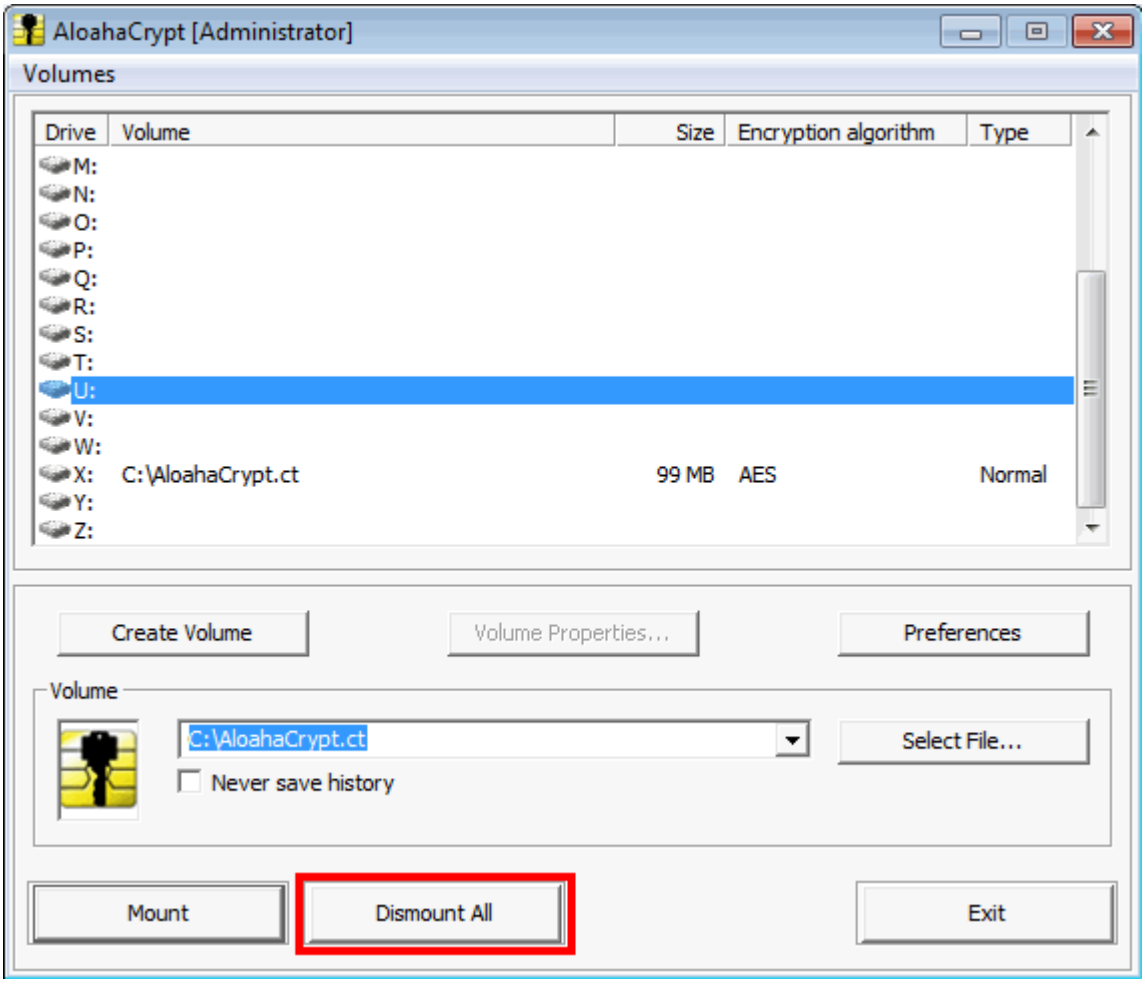


Wenn Sie nun auf "Dismount" klicken, verschwindet das Laufwerk, wie im folgenden Bild dargestellt.



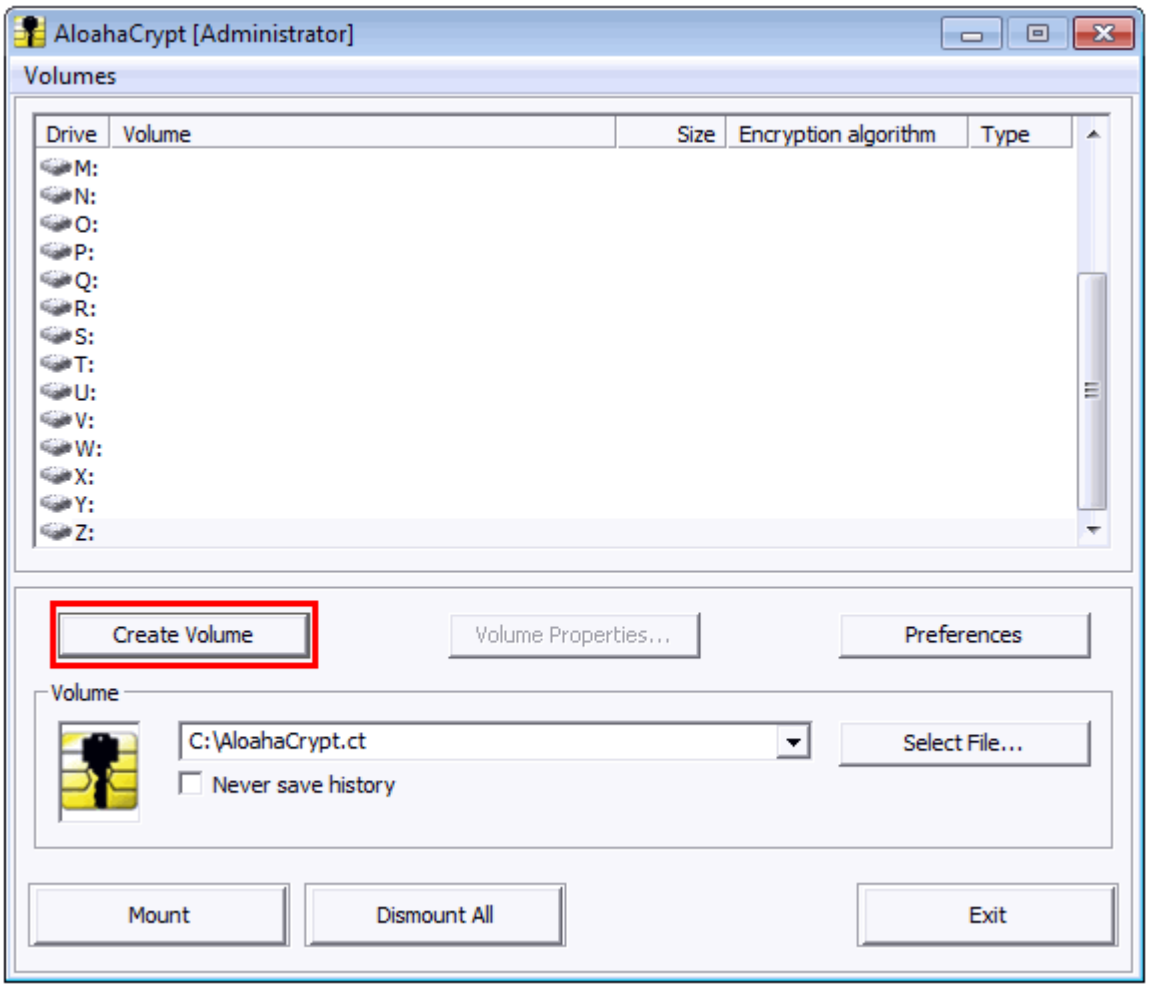
## 4.6 Alle Datenträger entfernen

Wenn Sie mehr als ein gemountetes Laufwerk haben, können Sie diese auch alle auf einmal dismounten.
Klicken Sie auf "Dismount All" und alle gemounteten Laufwerke verschwinden.

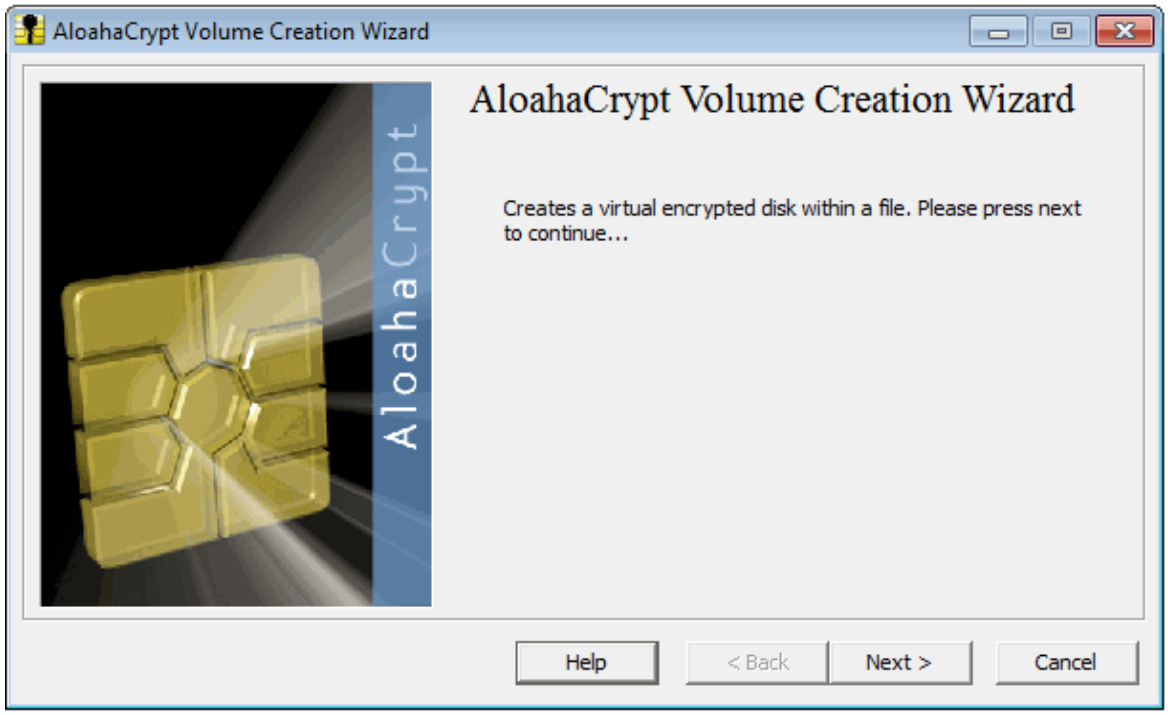


## 4.7 Erstelle neuen Datenträger

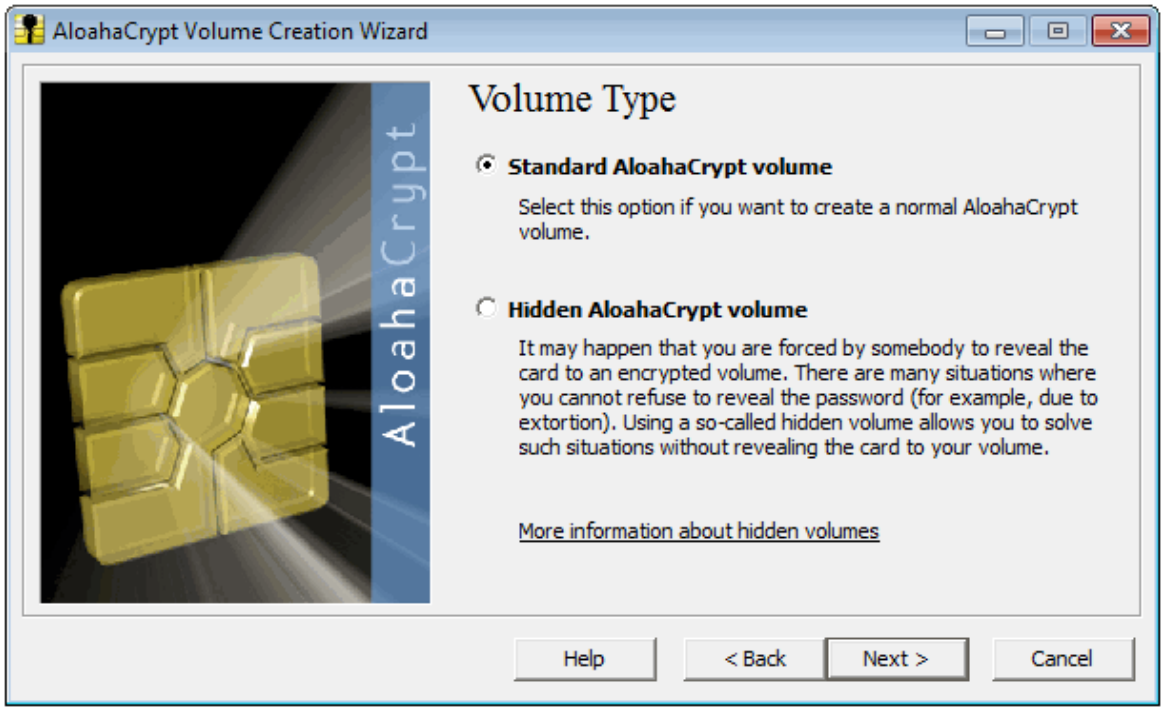
Klicken Sie auf "Erstelle Datenträger"



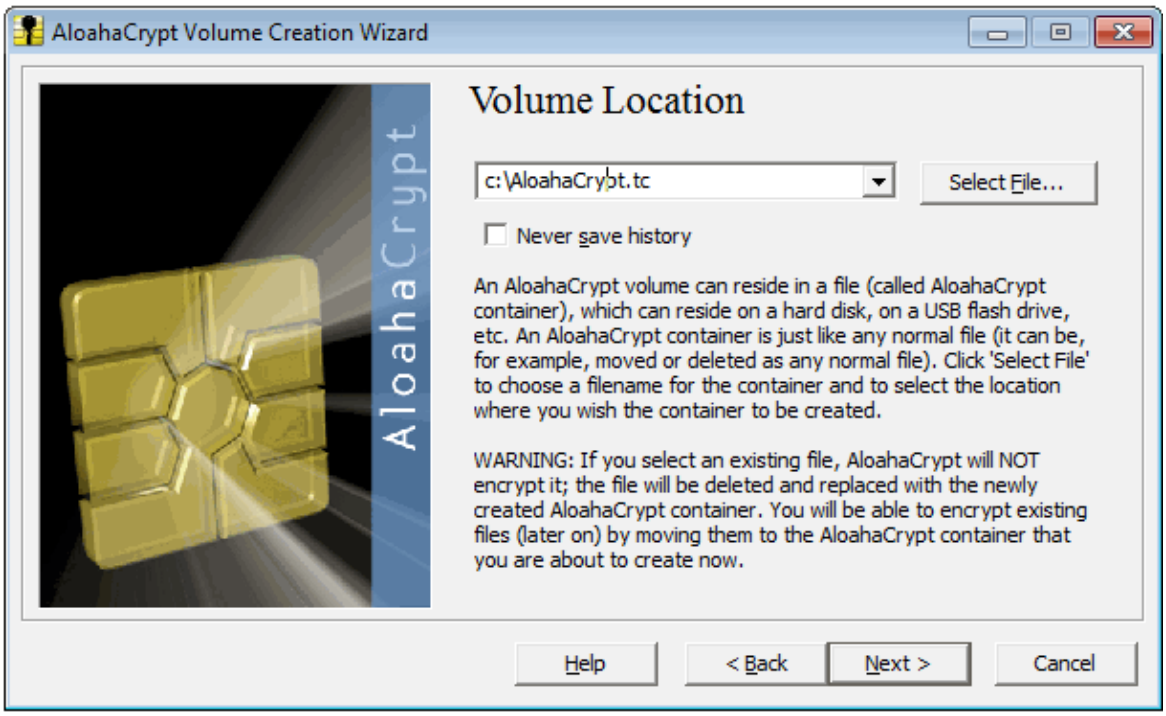
Wählen Sie "Erstelle einen schreibgeschützten Datenträger"




Wählen Sie "Standard AloahaCrypt Datenträger". Wenn Sie die zweite Option wählen, können Sie einen versteckten Datenträger erstellen.

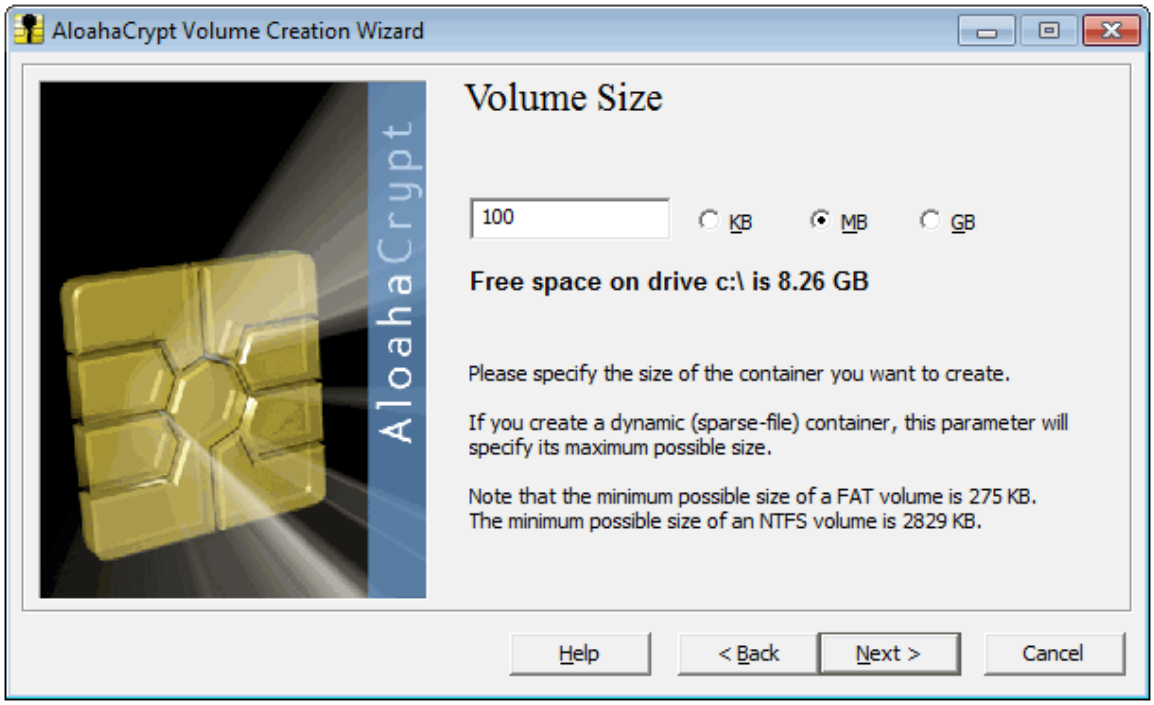


Legen Sie den Pfad des Datenträgers fest.




Wählen Sie Verschlüsselungs- und Hash-Algorythmus.

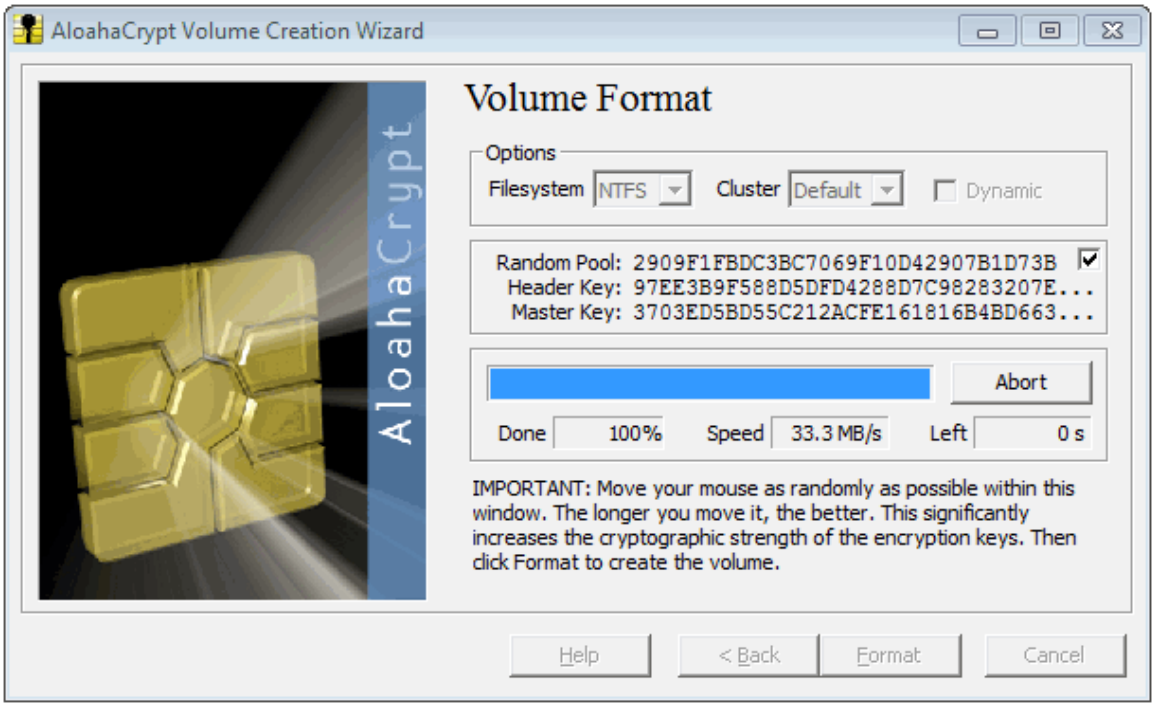
Legen Sie die Datenträgergröße fest



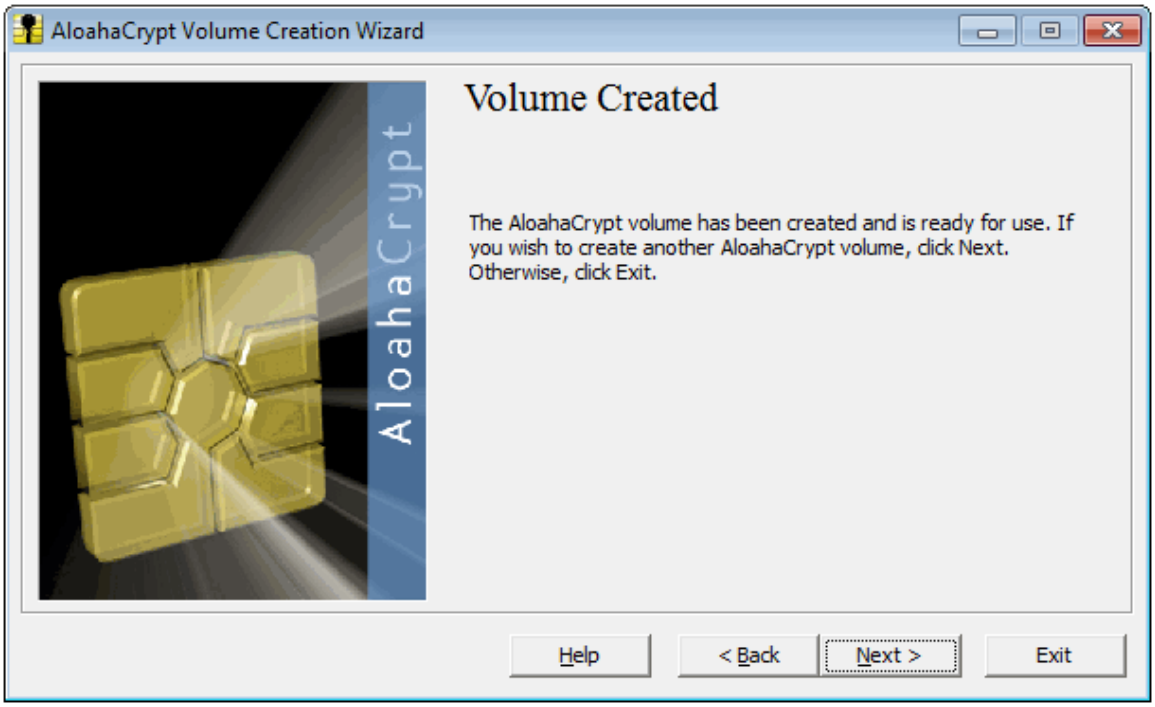

Sollten sich ihre SmartCart nicht im Kartenleser befinden, aktivieren Sie sie diese jetzt und klicken auf "Next".

Aloaha Crypt erstellt ein zufälliges 64-Byte-Verschlüsselungskennwort und verschlüsselt es mit dem Public Key der zuerst eingesteckten
Smartcard. Etwas später wird das Kennwort wieder entschlüsselt und Sie werden nach Ihrer Karten-PIN gefragt.


Der Datenträger kann nun formatiert werden.

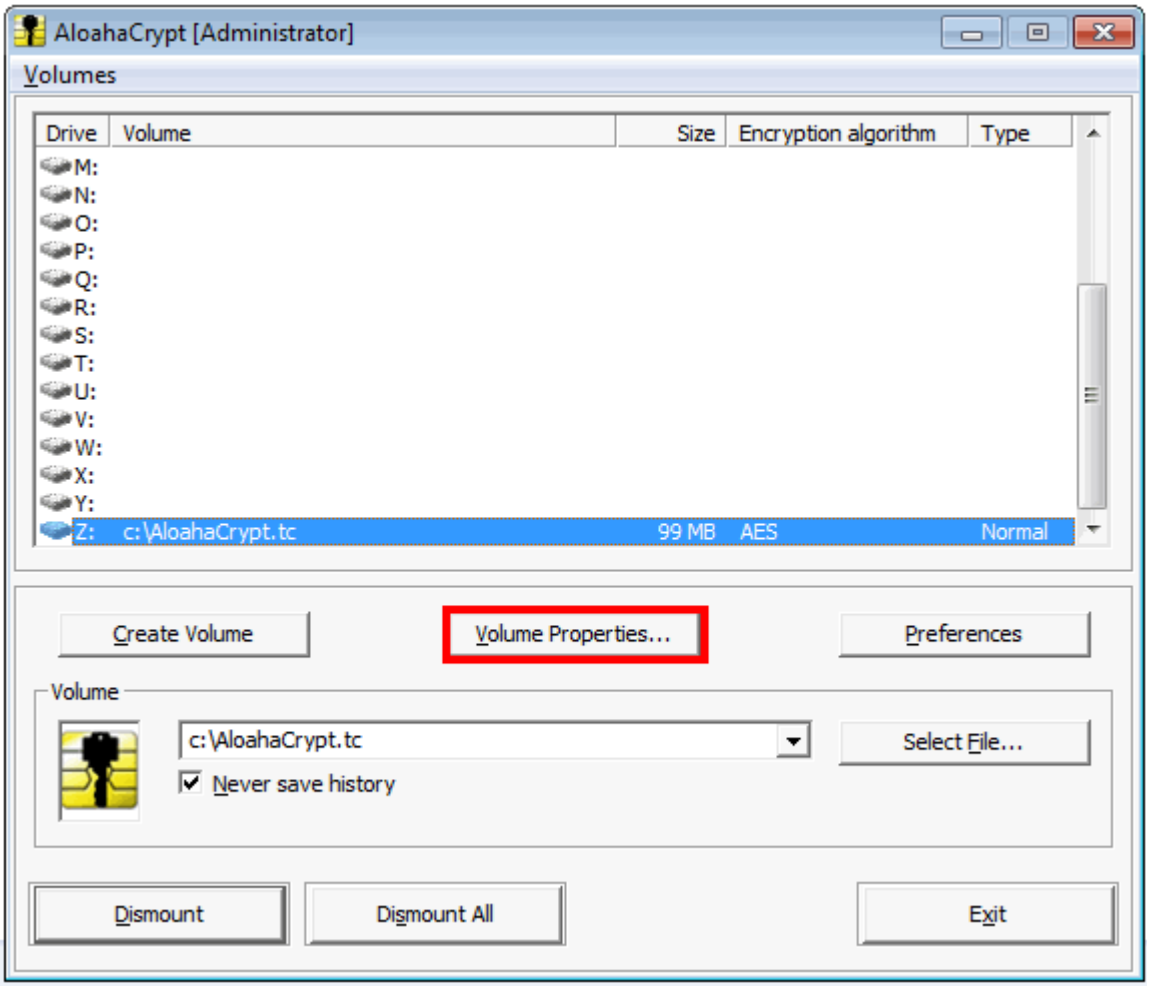


Sobald das Laufwerk erstellt ist, klicken Sie auf den Button "Exit". Wenn Sie auf "Next" klicken, können Sie einen weiteren Datenträger anlegen.

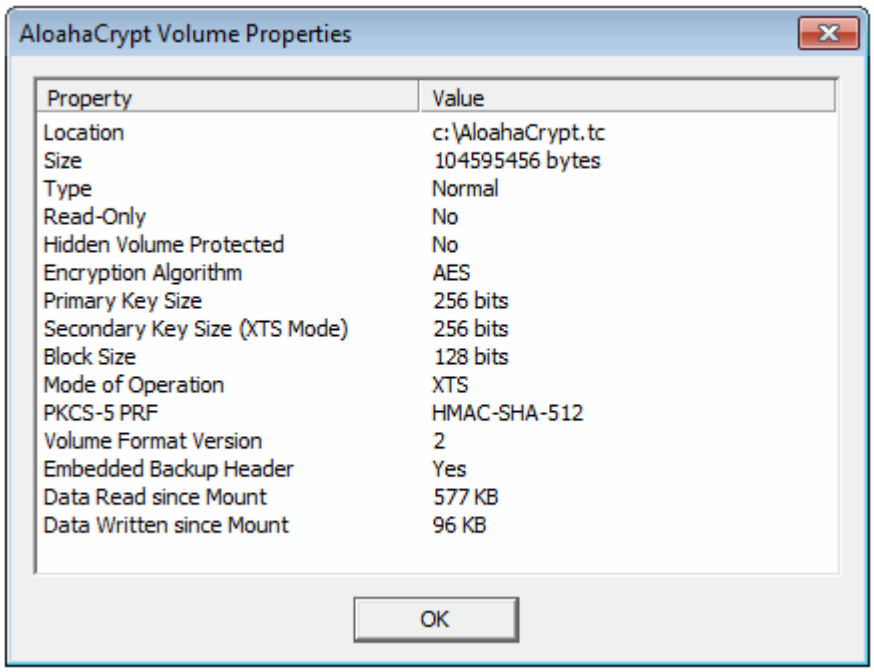


## 4.8 Datenträger-Eigenschaften

Wenn Sie den Button "Volume Properties" auswählen, erhalten Sie Informationen zu dem angelegten Datenträger.



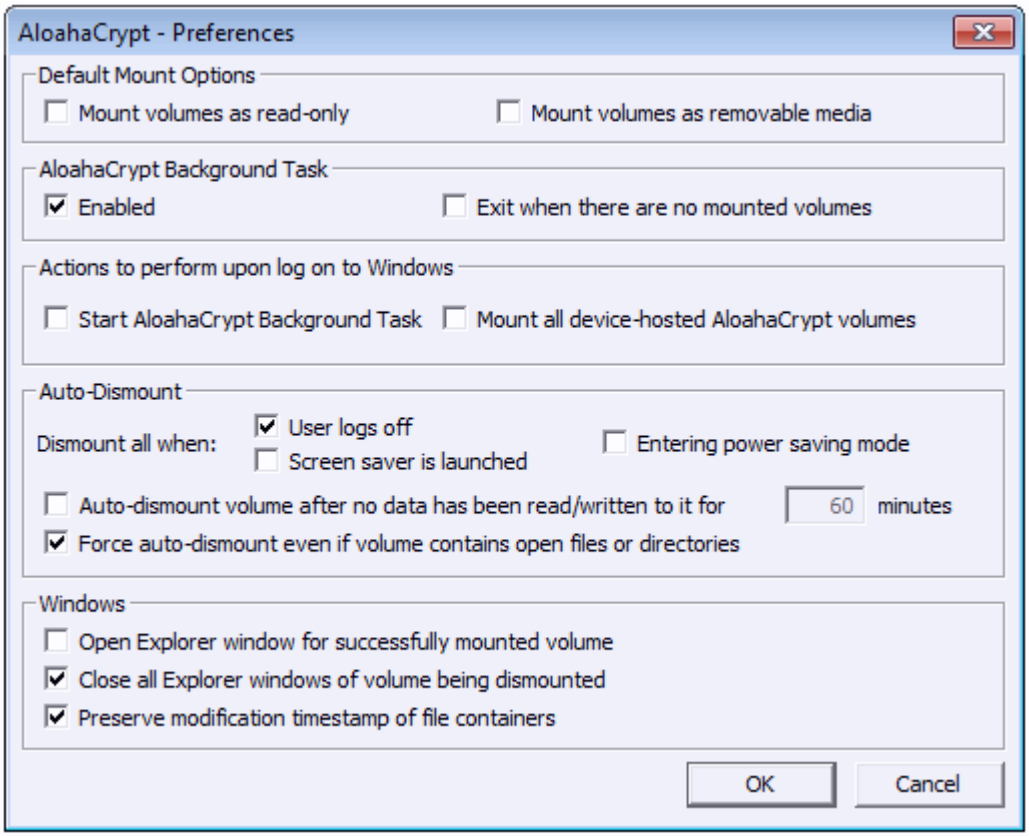
Sie können nun alle Eigenschaften zu dem installierten Datenträger sehen.



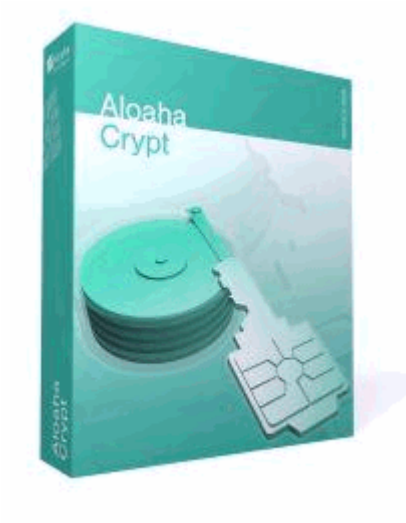

Wählen Sie "Preferences", können weitere Einstellungen wie

- Default Mount Options
- AloahaCrypt Background Task
- Actions to perform upon log on to Windows
- Auto-Dismount
- Windows

vorgenommen werden. Bestätigen Sie anschließend die vorgenommenen Änderungen mit OK.



# 5. Help




Parallelisierung

Parallelverarbeitung
Verborgenes Betriebssystem
**Plausible Deniability ???**
Verborgener Datenträger
Erstellung verborgener Betriebssysteme
**Plausible Deniability and Data Leak Protection ???**
Existenz von zwei Aloaha Crypt Partitionen auf einem Laufwerk
Sicherheitsmaßnahmen und -bedingungen verborgener Betriebssysteme
Aloaha Crypt ohne Administrator Rechte
Verschlüsselungsschema
Portabler Modus
Physische Sicherheit
**Malware ???**
Sichere Datensicherung
Systemfremde Datenträger
System Partitionen
**Header Key Derivation, Salt, and Iteration Count ???**
Unterstützte Betriebssysteme
Kommandozeilennutzung
Teilnahme über das Netzwerk
Entfernen der Verschlüsselung

## 5.1 Info

**Parallelisierung**
Wenn Ihr Computer einen Mehrkernprozessor/CPU (oder mehrere Prozessoren/CPUs) besitzt, verwendet Aloaha Crypt alle Prozessoren parallel für die Ver- und Entschlüsselung. Wenn z.B. Aloaha Crypt eine große Menge an Daten entschlüsseln soll, werden daraus zunächst mehrere kleinere Datenpakete erstellt. Die Anzahl der Datenpakete ist der Anzahl der Kerne / CPUs gleich. Dann werden alle Datenpakete parallel entschlüsselt. Dieselbe Methode wird für die Verschlüsselung verwendet.

Besitzt Ihr Computer z.B. einen QuadCoreProzessor, dann sind Ver- und Entschlüsselung viermal schneller als auf einem SingleCoreProzessor mit gleichwertigen Spezifizierungen.

Die Geschwindigkeitszunahme der Ver- / Entschlüsselung ist der Anzahl von Kernen und/oder Prozessoren proportional.

When your computer has a multi-core processor/CPU (or multiple processors/CPUs), header key derivation is parallelized too. As a result, mounting of a volume is several times faster on a multi-

core processor (or multi-processor computer) than on a single-core processor (or a single-processor computer) with equivalent specifications.

### Parallelverarbeitung

When encrypting or decrypting data, Aloaha Crypt uses so-called pipelining (asynchronous processing). While an application is loading a portion of a file from a Aloaha Crypt-encrypted volume/drive, Aloaha Crypt is automatically decrypting it (in RAM). Thanks to pipelining, the application does not have wait for any portion of the file to be decrypted and it can start loading other portions of the file right away.The same applies to encryption when writing data to an encrypted volume/drive.

Pipelining allows data to be read from and written to an encrypted drive as fast as if the drive was not encrypted (the same applies to file-hosted and partition-hosted Aloaha Crypt volumes).

### Verborgenes Betriebssystem

It may happen that you are forced by somebody to decrypt the operating system. There are many situations where you cannot refuse to do so (for example, due to extortion). Aloaha Crypt allows you to create a hidden operating system whose existence will be impossible to prove (provided that certain guidelines are followed). Thus, you will not have to decrypt or reveal the password for the hidden operating system. For more information, see the section Hidden Operating System in the chapter Plausible Deniability.

### Plausible Deniability ???

In case an adversary forces you to reveal your password, Aloaha Crypt provides and supports two kinds of plausible deniability:

1. Hidden volumes (see the section Hidden Volume) and hidden operating systems (see the section Hidden Operating System).

2. Until decrypted, a Aloaha Crypt partition/device appears to consist of nothing more than random data (it does not contain any kind of "signature"). Therefore, it is impossible to prove that a partition or a device is a Aloaha Crypt volume or that it has been encrypted (provided that the security requirements and precautions listed in the chapter Security Requirements and Precautions are followed). A possible plausible explanation for the existence of a partition/device containing solely random data is that you have wiped (securely erased) the content of the partition/device using one of the tools that erase data by overwriting it with random data (in fact, Aloaha Crypt can be used to securely erase a partition/device too, by creating an empty encrypted partition/device-hosted volume within it). However, you need to prevent data leaks (see the section Data Leaks) and also note that, for system encryption, the first drive track contains the (unencrypted) Aloaha Crypt Boot Loader, which can be easily identified as such (for more information, see the chapter System Encryption). When using system encryption, plausible deniability can be achieved by creating a hidden operating system (see the section Hidden Operating System).

Although file-hosted Aloaha Crypt volumes (containers) do not contain any kind of "signature" either (until decrypted, they appear to consist solely of random data), they cannot provide this kind of plausible deniability, because there is practically no plausible explanation for the existence of a file containing solely random data. However, plausible deniability can still be achieved with a file-hosted Aloaha Crypt volume (container) by creating a hidden volume within it (see above).

#### Notes

- When formatting a hard disk partition as a Aloaha Crypt volume, the partition table (including the partition type) is never modified (no Aloaha Crypt "signature" or "ID" is written to the partition table).
- There are methods to find files or devices containing random data (such as Aloaha Crypt volumes). Note, however, that this does not affect plausible deniability in any way. The adversary still cannot prove that the partition/device is a Aloaha Crypt volume or that the file, partition, or device, contains a hidden Aloaha Crypt volume (provided that you follow the security requirements and precautions listed in the chapter Security Requirements and Precautions and subsection Security Requirements and Precautions Pertaining to Hidden Volumes).

### Verborgener Datenträger

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

The layout of a standard Aloaha Crypt volume before and after a hidden volume was created within it. BILD !!!!!!!!!!!!!!

The layout of a standard Aloaha Crypt volume before and after a hidden volume was created within it. BILD !!!!!!!!!!!!!!

The principle is that a Aloaha Crypt volume is created within another Aloaha Crypt volume (within the free space on the volume). Even when the outer volume is mounted, it is impossible to prove whether there is a hidden volume within it or not*, because free space on any Aloaha Crypt volume is always filled with random data when the volume is created** and no part of the (dismounted) hidden volume can be distinguished from random data. Note that Aloaha Crypt does not modify the file system (information about free space, etc.) within the outer volume in any way.

The password for the hidden volume must be substantially different from the password for the outer volume. To the outer volume, (before creating the hidden volume within it) you should copy some sensitive-looking files that you actually do NOT want to hide. These files will be there for anyone who would force you to hand over the password. You will reveal only the password for the outer volume, not for the hidden one. Files that really are sensitive will be stored on the hidden volume.

A hidden volume can be mounted the same way as a standard Aloaha Crypt volume: Click Select File or Select Device to select the outer/host volume (important: make sure the volume is not mounted). Then click Mount, and enter the password for the hidden volume. Whether the hidden or the outer volume will be mounted is determined by the entered password (i.e., when you enter the password for the outer volume, then the outer volume will be mounted; when you enter the password for the hidden volume, the hidden volume will be mounted).

Aloaha Crypt first attempts to decrypt the standard volume header using the entered password. If it fails, it loads the area of the volume where a hidden volume header can be stored (i.e. the bytes 65536–131071, which contain solely random data when there is no hidden volume within the volume) to RAM and attempts to decrypt it using the entered password. Note that hidden volume headers cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted (for information on how Aloaha Crypt determines that it was successfully decrypted, see the section Encryption Scheme), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset).

A hidden volume can be created within any type of Aloaha Crypt volume, i.e., within a file-hosted volume or partition/device-hosted volume (requires administrator privileges). To create a hidden Aloaha Crypt volume, click on Create Volume in the main program window and select Create a hidden Aloaha Crypt volume. The Wizard will provide help and all information necessary to successfully create a hidden Aloaha Crypt volume.

When creating a hidden volume, it may be very difficult or even impossible for an inexperienced user to set the size of the hidden volume such that the hidden volume does not overwrite data on the outer volume. Therefore, the Volume Creation Wizard automatically scans the cluster bitmap of the outer volume (before the hidden volume is created within it) and determines the maximum possible size of the hidden volume.***

If there are any problems when creating a hidden volume, refer to the chapter Troubleshooting for possible solutions.

Note that it is also possible to create and boot an operating system residing in a hidden volume.

### Verborgenes Betriebssystem 2

If your system partition or system drive is encrypted using Aloaha Crypt, you need to enter your

pre-boot authentication password in the Aloaha Crypt Boot Loader screen after you turn on or restart your computer. It may happen that you are forced by somebody to decrypt the operating system or to reveal the pre-boot authentication password. There are many situations where you cannot refuse to do so (for example, due to extortion). Aloaha Crypt allows you to create a hidden operating system whose existence will be impossible to prove (provided that certain guidelines are followed — see below). Thus, you will not have to decrypt or reveal the password for the hidden operating system.

Before you continue reading this section, make sure you have read the section Hidden Volume and that you understand what a hidden Aloaha Crypt volume is.

A hidden operating system is a system (for example, Windows Vista or Windows XP) that is installed in a hidden Aloaha Crypt volume. It is impossible to prove that a hidden Aloaha Crypt volume exists (provided that certain guidelines are followed; for more information, see the section Hidden Volume) and, therefore, it is impossible to prove that a hidden operating system exists.

However, in order to boot a system encrypted by Aloaha Crypt, an unencrypted copy of the Aloaha Crypt Boot Loader has to be stored on the system drive or on a Aloaha Crypt Rescue Disk. Hence, the mere presence of the Aloaha Crypt Boot Loader can indicate that there is a system encrypted by Aloaha Crypt on the computer. Therefore, to provide a plausible explanation for the presence of the Aloaha Crypt Boot Loader, the Aloaha Crypt helps you create a second encrypted operating system, so-called decoy operating system, during the process of creation of a hidden operating system. A decoy operating system must not contain any sensitive files. Its existence is not secret (it is not installed in a hidden volume). The password for the decoy operating system can be safely revealed to anyone forcing you to disclose your pre-boot authentication password.*

You should use the decoy operating system as frequently as you use your computer. Ideally, you should use it for all activities that do not involve sensitive data. Otherwise, plausible deniability of the hidden operating system might be adversely affected (if you revealed the password for the decoy operating system to an adversary, he could find out that the system is not used very often, which might indicate the existence of a hidden operating system on your computer). Note that you can save data to the decoy system partition anytime without any risk that the hidden volume will get damaged (because the decoy system is not installed in the outer volume — see below).

There will be two pre-boot authentication passwords — one for the hidden system and the other for the decoy system. If you want to start the hidden system, you simply enter the password for the hidden system in the Aloaha Crypt Boot Loader screen (which appears after you turn on or restart your computer). Likewise, if you want to start the decoy system (for example, when asked to do so by an adversary), you just enter the password for the decoy system in the Aloaha Crypt Boot Loader screen.

**Note:** When you enter a pre-boot authentication password, the Aloaha Crypt Boot Loader first attempts to decrypt (using the entered password) the last 512 bytes of the first logical track of the system drive (where encrypted master key data for non-hidden encrypted system partitions/drives are normally stored). If it fails and if there is a partition behind the active partition, the Aloaha Crypt Boot Loader (even if there is actually no hidden volume on the drive) automatically tries to decrypt (using the same entered password again) the area of the first partition behind the active partition where the encrypted header of a possible hidden volume might be stored (however, if the size of the active partition is less than 256 MB, then the data is read from the second partition behind the active one, because Windows 7 and later, by default, do not boot from the partition on which they are installed). Note that Aloaha Crypt never knows if there is a hidden volume in advance (the hidden volume header cannot be identified, as it appears to consist entirely of random data). If the header is successfully decrypted (for information on how Aloaha Crypt determines that it was successfully decrypted, see the section Encryption Scheme), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset). For further technical details, see the section Encryption Scheme in the chapter Technical Details.

When running, the hidden operating system appears to be installed on the same partition as the original operating system (the decoy system). However, in reality, it is installed within the partition behind it (in a hidden volume). All read/write operations are transparently redirected from the system partition to the hidden volume. Neither the operating system nor applications will know that data written to and read from the system partition is actually written to and read from the partition

behind it (from/to a hidden volume). Any such data is encrypted and decrypted on the fly as usual (with an encryption key different from the one that is used for the decoy operating system).

Note that there will also be a third password — the one for the outer volume. It is not a pre-boot authentication password, but a regular Aloaha Crypt volume password. It can be safely disclosed to anyone forcing you to reveal the password for the encrypted partition where the hidden volume (containing the hidden operating system) resides. Thus, the existence of the hidden volume (and of the hidden operating system) will remain secret. If you are not sure you understand how this is possible, or what an outer volume is, please read the section Hidden Volume. The outer volume should contain some sensitive-looking files that you actually do not want to hide.

To summarize, there will be three passwords in total. Two of them can be revealed to an attacker (for the decoy system and for the outer volume). The third password, for the hidden system, must remain secret.

Example Layout of System Drive Containing Hidden Operating System BILD !!!!!!!!!!!

Example Layout of System Drive Containing Hidden Operating System

### Erstellung verborgener Betriebssysteme

To start the process of creation of a hidden operating system, select System > Create Hidden Operating System and then follow the instructions in the wizard.

Initially, the wizard verifies that there is a suitable partition for a hidden operating system on the system drive. Note that before you can create a hidden operating system, you need to create a partition for it on the system drive. It must be the first partition behind the system partition and it must be at least 5% larger than the system partition (the system partition is the one where the currently running operating system is installed). However, if the outer volume (not to be confused with the system partition) is formatted as NTFS, the partition for the hidden operating system must be at least 110% (2.1 times) larger than the system partition (the reason is that the NTFS file system always stores internal data exactly in the middle of the volume and, therefore, the hidden volume, which is to contain a clone of the system partition, can reside only in the second half of the partition).

In the next steps, the wizard will create two Aloaha Crypt volumes (outer and hidden) within the first partition behind the system partition. The hidden volume will contain the hidden operating system. The size of the hidden volume is always the same as the size of the system partition. The reason is that the hidden volume will need to contain a clone of the content of the system partition (see below). Note that the clone will be encrypted using a different encryption key than the original. Before you start copying some sensitive-looking files to the outer volume, the wizard tells you the maximum recommended size of space that the files should occupy, so that there is enough free space on the outer volume for the hidden volume.

Remark: After you copy some sensitive-looking files to the outer volume, the cluster bitmap of the volume will be scanned in order to determine the size of uninterrupted area of free space whose end is aligned with the end of the outer volume. This area will accommodate the hidden volume, so it limits its maximum possible size. The maximum possible size of the hidden volume will be determined and it will be verified that it is greater than the size of the system partition (which is required, because the entire content of the system partition will need to be copied to the hidden volume — see below). This ensures that no data stored on the outer volume will be overwritten by data written to the area of the hidden volume (e.g. when the system is being copied to it). The size of the hidden volume is always the same as the size of the system partition.

Then, Aloaha Crypt will create the hidden operating system by copying the content of the system partition to the hidden volume. Data being copied will be encrypted on the fly with an encryption key different from the one that will be used for the decoy operating system. The process of copying the system is performed in the pre-boot environment (before Windows starts) and it may take a long time to complete; several hours or even several days (depending on the size of the system partition and on the performance of the computer). You will be able to interrupt the process, shut down your computer, start the operating system and then resume the process. However, if you interrupt it, the entire process of copying the system will have to start from the beginning (because the content of the system partition must not change during cloning). The hidden operating system

will initially be a clone of the operating system under which you started the wizard.

Windows creates (typically, without your knowledge or consent) various log files, temporary files, etc., on the system partition. It also saves the content of RAM to hibernation and paging files located on the system partition. Therefore, if an adversary analyzed files stored on the partition where the original system (of which the hidden system is a clone) resides, he might find out, for example, that you used the Aloaha Crypt wizard in the hidden-system-creation mode (which might indicate the existence of a hidden operating system on your computer). To prevent such issues, Aloaha Crypt will securely erase the entire content of the partition where the original system resides after the hidden system has been created. Afterwards, in order to achieve plausible deniability, Aloaha Crypt will prompt you to install a new system on the partition and encrypt it using Aloaha Crypt. Thus, you will create the decoy system and the whole process of creation of the hidden operating system will be completed.

**Note:** Aloaha Crypt will erase the content of the partition where the original system resides by filling it with random data entirely. If you revealed the password for the decoy system to an adversary and he asked you why the free space of the (decoy) system partition contains random data, you could answer, for example: "The partition previously contained a system encrypted by Aloaha Crypt, but I forgot the pre-boot authentication password (or the system was damaged and stopped booting), so I had to reinstall Windows and encrypt the partition again."

### Plausible Deniability and Data Leak Protection ???

For security reasons, when a hidden operating system is running, Aloaha Crypt ensures that all local unencrypted filesystems and non-hidden Aloaha Crypt volumes are read-only (i.e. no files can be written to such filesystems or Aloaha Crypt volumes).† Data is allowed to be written to any filesystem that resides within a hidden Aloaha Crypt volume (provided that the hidden volume is not located in a container stored on an unencrypted filesystem or on any other read-only filesystem).

There are three main reasons why such countermeasures have been implemented:

1. It enables the creation of a secure platform for mounting of hidden Aloaha Crypt volumes. Note that we officially recommend that hidden volumes are mounted only when a hidden operating system is running. For more information, see the subsection Security Requirements and Precautions Pertaining to Hidden Volumes.
2. In some cases, it is possible to determine that, at a certain time, a particular filesystem was not mounted under (or that a particular file on the filesystem was not saved or accessed from within) a particular instance of an operating system (e.g. by analyzing and comparing filesystem journals, file timestamps, application logs, error logs, etc). This might indicate that a hidden operating system is installed on the computer. The countermeasures prevent these issues.
3. It prevents data corruption and allows safe hibernation. When Windows resumes from hibernation, it assumes that all mounted filesystems are in the same state as when the system entered hibernation. Aloaha Crypt ensures this by write-protecting any filesystem accessible both from within the decoy and hidden systems. Without such protection, the filesystem could become corrupted when mounted by one system while the other system is hibernated.

If you need to securely transfer files from the decoy system to the hidden system, follow these steps:

1. Start the decoy system.
2. Save the files to an unencrypted volume or to an outer/normal Aloaha Crypt volume.
3. Start the hidden system
4. If you saved the files to a Aloaha Crypt volume, mount it (it will be automatically mounted as read-only).
5. Copy the files to the hidden system partition or to another hidden volume.

### Existenz von zwei Aloaha Crypt Partitionen auf einem Laufwerk

An adversary might ask why you created two Aloaha Crypt-encrypted partitions on a single drive (a system partition and a non-system partition) rather than encrypting the entire disk with a single encryption key. There are many possible reasons to do that. However, if you do not know any (other than creating the hidden operating system), you can provide, for example, one of the following explanations:

- If there are more than two partitions on a system drive and you want to encrypt only two of them (the system partition and the one behind it) and to leave the other partitions unencrypted (for example, to achieve the best possible performance when reading and writing data, which is not sensitive, to such unencrypted partitions), the only way to do that is to encrypt both partitions separately (note that, with a single encryption key, Aloaha Crypt could encrypt the entire system drive and all partitions on it, but it cannot encrypt only two of them — only one or all of the partitions can be encrypted with a single key). As a result, there will be two adjacent Aloaha Crypt partitions on the system drive (the first will be a system partition, the second will be a non-system one), each encrypted with a different key (which is also the case when you create a hidden operating system, and therefore it can be explained this way).

If you do not know any good reason why there should be more than one partition on a system drive at all:

It is generally recommended to separate non-system files (documents) from system files. One of the easiest and most reliable ways to do that is to create two partitions on the system drive; one for the operating system and the other for documents (non-system files). The reasons why this practice is recommended include:

- If the filesystem on one of the partitions is damaged, files on the partition may get corrupted or lost, whereas files on the other partition are not affected.
- It is easier to reinstall the system without losing your documents (reinstallation of an operating system involves formatting the system partition, after which all files stored on it are lost). If the system is damaged, full reinstallation is often the only option.

- A cascade encryption algorithm (e.g. AES-Twofish-Serpent) can be up to four times slower than a non-cascade one (e.g. AES). However, a cascade encryption algorithm may be more secure than a non-cascade one (for example, the probability that three distinct encryption algorithms will be broken, e.g. due to advances in cryptanalysis, is significantly lower than the probability that only one of them will be broken). Therefore, if you encrypt the outer volume with a cascade encryption algorithm and the decoy system with a non-cascade encryption algorithm, you can answer that you wanted the best performance (and adequate security) for the system partition, and the highest possible security (but worse performance) for the non-system partition (i.e. the outer volume), where you store the most sensitive data, which you do not need to access very often (unlike the operating system, which you use very often, and therefore you need it to have the best possible performance). On the system partition, you store data that is less sensitive (but which you need to access very often) than data you store on the non-system partition (i.e. on the outer volume).

- Provided that you encrypt the outer volume with a cascade encryption algorithm (e.g. AES-Twofish-Serpent) and the decoy system with a non-cascade encryption algorithm (e.g. AES), you can also answer that you wanted to prevent the problems about which Aloaha Crypt warns when the user attempts to choose a cascade encryption algorithm for system encryption (see below for a list of the problems). Therefore, to prevent those problems, you decided to encrypt the system partition with a non-cascade encryption algorithm. However, you still wanted to use a cascade encryption algorithm (because it is more secure than a non-cascade encryption algorithm) for the most sensitive data, so you decided to create a second partition, which those problems do not affect (because it is non-system) and to encrypt it with a cascade encryption algorithm. On the system partition, you store data that is less sensitive than data you store on the non-system partition (i.e. on the outer volume).

**Note:** When the user attempts to encrypt the system partition with a cascade encryption algorithm, Aloaha Crypt warns him or her that it can cause the following problems (and implicitly recommends to choose a non-cascade encryption algorithm instead):

- For cascade encryption algorithms, the Aloaha Crypt Boot Loader is larger than normal and, therefore, there is not enough space in the first drive track for a backup of the Aloaha Crypt Boot Loader. Hence, whenever it gets damaged (which often happens, for example, during inappropriately designed anti-piracy activation procedures of certain programs), the user must use the Aloaha Crypt Rescue Disk to repair the Aloaha Crypt Boot Loader or to boot.
- On some computers, resuming from hibernation takes longer.

- In contrast to a password for a non-system Aloaha Crypt volume, a pre-boot authentication password needs to be typed each time the computer is turned on or restarted. Therefore, if the pre-boot authentication password is long (which is required for security purposes), it may be very tiresome to type it so frequently. Hence, you can answer that it was more convenient for you to use a short (and therefore weaker) password for the system partition (i.e. the decoy system) and that it is more convenient for you to store the most sensitive data (which you do not need to access as often) in the non-system Aloaha Crypt partition (i.e. in the outer volume) for which you chose a very long password.

As the password for the system partition is not very strong (because it is short), you do not intentionally store sensitive data on the system partition. However, you still prefer the system partition to be encrypted, because potentially sensitive or mildly sensitive data is stored on it as a result of your everyday use of the computer (for example, passwords to online forums you visit, which can be automatically remembered by your browser, browsing history, applications you run, etc.)

- When an attacker gets hold of your computer when a Aloaha Crypt volume is mounted (for example, when you use a laptop outside), he can, in most cases, read any data stored on the volume (data is decrypted on the fly as he reads it). Therefore, it may be wise to limit the time the volume is mounted to a minimum. Obviously, this may be impossible or difficult if the sensitive data is stored on an encrypted system partition or on an entirely encrypted system drive (because you would also have to limit the time you work with the computer to a minimum). Hence, you can answer that you created a separate partition (encrypted with a different key than your system partition) for your most sensitive data and that you mount it only when necessary and dismount it as soon as possible (so as to limit the time the volume is mounted to a minimum). On the system partition, you store data that is less sensitive (but which you need to access often) than data you store on the non-system partition (i.e. on the outer volume).

### Sicherheitsmaßnahmen und -bedingungen verborgener Betriebssysteme

As a hidden operating system resides in a hidden Aloaha Crypt volume, a user of a hidden operating system must follow all of the security requirements and precautions that apply to normal hidden Aloaha Crypt volumes. These requirements and precautions, as well as additional requirements and precautions pertaining specifically to hidden operating systems, are listed in the subsection Security Requirements and Precautions Pertaining to Hidden Volumes.

**WARNING:** If you do not protect the hidden volume (for information on how to do so, refer to the section Protection of Hidden Volumes Against Damage), do not write to the outer volume (note that the decoy operating system is not installed in the outer volume). Otherwise, you may overwrite and damage the hidden volume (and the hidden operating system within it)!

If all the instructions in the wizard have been followed and if the security requirements and precautions listed in the subsection Security Requirements and Precautions Pertaining to Hidden Volumes are followed, it will be impossible to prove that the hidden volume and hidden operating system exist, even when the outer volume is mounted or when the decoy operating system is decrypted or started.

- It is not practical (and therefore is not supported) to install operating systems in two Aloaha Crypt volumes that are embedded within a single partition, because using the outer operating system would often require data to be written to the area of the hidden operating system (and if such write operations were prevented using the hidden volume protection feature, it would inherently cause system crashes, i.e. 'Blue Screen' errors).

† This does not apply to filesystems on CD/DVD-like media and on custom, atypical, or non-standard devices/media.

### Nutzung von Aloaha Crypt ohne Administrator Rechte

In Windows, a user who does not have administrator privileges can use Aloaha Crypt, but only after a system administrator installs Aloaha Crypt on the system. The reason for that is that Aloaha Crypt needs a device driver to provide transparent on-the-fly encryption/decryption, and users

without administrator privileges cannot install/start device drivers in Windows.

After a system administrator installs Aloaha Crypt on the system, users without administrator privileges will be able to run Aloaha Crypt, mount/dismount any type of Aloaha Crypt volume, load/save data from/to it, and create file-hosted Aloaha Crypt volumes on the system. However, users without administrator privileges cannot encrypt/format partitions, cannot create NTFS volumes, cannot install/uninstall Aloaha Crypt, cannot change passwords/keyfiles for Aloaha Crypt partitions/devices, cannot backup/restore headers of Aloaha Crypt partitions/devices, and they cannot run Aloaha Crypt in portable mode.

**Note:** As regards personal privacy, in most cases, it is not safe to work with sensitive data under systems where you do not have administrator privileges, because the administrator can easily capture and copy the sensitive data, including the passwords and keys.

### Verschlüsselungsschema

When mounting a Aloaha Crypt volume (assume there are no cached passwords/keyfiles) or when performing pre-boot authentication, the following steps are performed:

1. The first 512 bytes of the volume (i.e., the standard volume header) are read into RAM, out of which the first 64 bytes are the salt (see Aloaha Crypt Volume Format Specification). For system encryption (see the chapter System Encryption), the last 512 bytes of the first logical drive track are read into RAM (the Aloaha Crypt Boot Loader is stored in the first track of the system drive and/or on the Aloaha Crypt Rescue Disk).
2. Bytes 65536–66047 of the volume are read into RAM (see the section Aloaha Crypt Volume Format Specification). For system encryption, bytes 65536–66047 of the first partition located behind the active partition* are read into RAM (see the section Hidden Operating System). If there is a hidden volume within this volume (or within the partition behind the active partition), we have read its header at this point; otherwise, we have just read random data (whether or not there is a hidden volume within it has to be determined by attempting to decrypt this data; for more information see the section Hidden Volume).
3. Now Aloaha Crypt attempts to decrypt the standard volume header read in (1). All data used and generated in the course of the process of decryption are kept in RAM (Aloaha Crypt never saves them to disk). The following parameters are unknown** and have to be determined through the process of trial and error (i.e., by testing all possible combinations of the following):

3.1. PRF used by the header key derivation function (as specified in PKCS #5 v2.0; see the section Header Key Derivation, Salt, and Iteration Count), which can be one of the following:

HMAC-SHA-512, HMAC-RIPEMD-160, HMAC-Whirlpool.

A password entered by the user (to which one or more keyfiles may have been applied – see the section Keyfiles) and the salt read in (1) are passed to the header key derivation function, which produces a sequence of values (see the section Header Key Derivation, Salt, and Iteration Count) from which the header encryption key and secondary header key (XTS mode) are formed. (These keys are used to decrypt the volume header.)

3.2. Encryption algorithm: AES-256, Serpent, Twofish, AES-Serpent, AES-Twofish-Serpent, etc.

3.3. Mode of operation: XTS, LRW (deprecated/legacy), CBC (deprecated/legacy)

3.4. Key size(s)

4. Decryption is considered successful if the first 4 bytes of the decrypted data contain the ASCII string "TRUE", and if the CRC-32 checksum of the last 256 bytes of the decrypted data (volume header) matches the value located at byte #8 of the decrypted data (this value is unknown to an adversary because it is encrypted – see the section Header Key Derivation, Salt, and Iteration Count). If these conditions are not met, the process continues from (3) again, but this time, instead of the data read in (1), the data read in (2) are used (i.e., possible hidden volume header). If the conditions are not met again, mounting is terminated (wrong password, corrupted volume, or not a Aloaha Crypt volume).

5. Now we know (or assume with very high probability) that we have the correct password, the

correct encryption algorithm, mode, key size, and the correct header key derivation algorithm. If we successfully decrypted the data read in (2), we also know that we are mounting a hidden volume and its size is retrieved from data read in (2) decrypted in (3).

6. The encryption routine is reinitialized with the primary master key*** and the secondary key (XTS mode), which are retrieved from the decrypted volume header (see the section Aloaha Crypt Volume Format Specification). These keys can be used to decrypt any sector of the volume, except the volume header area (or the key data area, for system encryption), which has been encrypted using the header keys. The volume is mounted.

* If the size of the active partition is less than 256 MB, then the data is read from the second partition behind the active one (Windows 7 and later, by default, do not boot from the partition on which they are installed).
** These parameters are kept secret not in order to increase the complexity of an attack, but primarily to make Aloaha Crypt volumes unidentifiable (indistinguishable from random data), which would be difficult to achieve if these parameters were stored unencrypted within the volume header. Also note that if a non-cascaded encryption algorithm is used for system encryption, the algorithm is known (it can be determined by analyzing the contents of the unencrypted Aloaha Crypt Boot Loader stored in the first logical drive track or on the Aloaha Crypt Rescue Disk).
*** The master keys were generated during the volume creation and cannot be changed later. Volume password change is accomplished by re-encrypting the volume header using a new header key (derived from a new password).

### Portabler Modus

Aloaha Crypt can run in so-called portable mode, which means that it does not have to be installed on the operating system under which it is run. However, there are two things to keep in mind:

- You need administrator privileges in order to able to run Aloaha Crypt in portable mode (for reasons, see the chapter Using Aloaha Crypt Without Administrator Privileges).

Also note that, as regards personal privacy, in most cases, it is not safe to work with sensitive data under systems where you do not have administrator privileges, because the administrator can easily capture and copy the sensitive data, including the passwords and keys.

- After examining the registry file, it may be possible to tell that Aloaha Crypt was run (and that a Aloaha Crypt volume was mounted) on a Windows system even if it had been run in portable mode.

If you need to solve these problems, we recommend using BartPE for this purpose. For further information on BartPE, see the question "Is it possible to use Aloaha Crypt without leaving any 'traces' on Windows?" in the section Frequently Asked Questions.

There are two ways to run Aloaha Crypt in portable mode:

- After you extract files from the Aloaha Crypt self-extracting package, you can directly run Aloaha Crypt.exe.

**Note:** To extract files from the Aloaha Crypt self-extracting package, run it, and then select Extract (instead of Install) on the second page of the Aloaha Crypt Setup wizard.

- You can use the Traveler Disk Setup facility to prepare a special traveler disk and launch Aloaha Crypt from there.

The second option has several advantages, which are described in the following sections in this chapter.

Note: When running in portable mode, the Aloaha Crypt driver is unloaded when it is no longer needed (e.g., when all instances of the main application and/or of the Volume Creation Wizard are

closed and no Aloaha Crypt volumes are mounted). However, if you force dismount on a Aloaha Crypt volume when Aloaha Crypt runs in portable mode, or mount a writable NTFS-formatted volume on Windows Vista or later, the Aloaha Crypt driver will not be unloaded when you exit Aloaha Crypt (it will be unloaded only when you shut down or restart the system). This prevents various problems caused by a bug in Windows (for instance, it would be impossible to start Aloaha Crypt again as long as there are applications using the dismounted volume).

**Tools -> Traveler Disk Setup**

You can use this facility to prepare a special traveler disk and launch Aloaha Crypt from there. Note that Aloaha Crypt 'traveler disk' is not a Aloaha Crypt volume but an unencrypted volume. A 'traveler disk' contains Aloaha Crypt executable files and optionally the 'autorun.inf' script (see the section AutoRun Configuration below). After you select Tools -> Traveler Disk Setup, the Traveler Disk Setup dialog box should appear. Some of the parameters that can be set within the dialog deserve further explanation:

***Include Aloaha Crypt Volume Creation Wizard***

Check this option, if you need to create new Aloaha Crypt volumes using Aloaha Crypt run from the traveler disk you will create. Unchecking this option saves space on the traveler disk.

***AutoRun Configuration (autorun.inf)***

In this section, you can configure the 'traveler disk' to automatically start Aloaha Crypt or mount a specified Aloaha Crypt volume when the 'traveler disk' is inserted. This is accomplished by creating a special script file called 'autorun.inf' on the traveler disk. This file is automatically executed by the operating system each time the 'traveler disk' is inserted.

Note, however, that this feature only works for removable storage devices such as CD/DVD (Windows XP SP2, Windows Vista, or a later version of Windows is required for this feature to work on USB memory sticks) and only when it is enabled in the operating system. Depending on the operating system configuration, these auto-run and auto-mount features may work only when the traveler disk files are created on a non-writable CD/DVD-like medium (which is not a bug in Aloaha Crypt but a limitation of Windows).

Also note that the 'autorun.inf' file must be in the root directory (i.e., for example G:\, X:\, or Y:\ etc.) of an **unencrypted** disk in order for this feature to work.

**Physische Sicherheit**

If an attacker can physically access the computer hardware and you use it after the attacker has physically accessed it, then Aloaha Crypt may become unable to secure data on the computer.* This is because the attacker may modify the hardware or attach a malicious hardware component to it (such as a hardware keystroke logger) that will capture the password or encryption key (e.g. when you mount a Aloaha Crypt volume) or otherwise compromise the security of the computer. Therefore, you must not use Aloaha Crypt on a computer that an attacker has physically accessed. Furthermore, you must ensure that Aloaha Crypt (including its device driver) is not running when the attacker physically accesses the computer. Additional information pertaining to hardware attacks where the attacker has direct physical access is contained in the section Unencrypted Data in RAM.

Furthermore, even if the attacker cannot physically access the computer hardware directly, he or she may be able to breach the physical security of the computer by remotely intercepting and analyzing emanations from the computer hardware (including the monitor and cables). For example, intercepted emanations from the cable connecting the keyboard with the computer can reveal passwords you type. It is beyond the scope of this document to list all of the kinds of such attacks (sometimes called TEMPEST attacks) and all known ways to prevent them (such as shielding or radio jamming). It is your responsibility to prevent such attacks. If you do not, Aloaha Crypt may become unable to secure data on the computer.

**Malware ???**

The term 'malware' refers collectively to all types of malicious software, such as computer viruses, Trojan horses, spyware, or generally any piece of software (including Aloaha Crypt or an operating

system component) that has been altered, prepared, or can be controlled, by an attacker. Some kinds of malware are designed e.g. to log keystrokes, including typed passwords (such captured passwords are then either sent to the attacker over the Internet or saved to an unencrypted local drive from which the attacker might be able to read it later, when he or she gains physical access to the computer). If you use Aloaha Crypt on a computer infected with any kind of malware, Aloaha Crypt may become unable to secure data on the computer.* Therefore, you must not use Aloaha Crypt on such a computer.

It is important to note that Aloaha Crypt is encryption software, not anti-malware software. It is your responsibility to prevent malware from running on the computer. If you do not, Aloaha Crypt may become unable to secure data on the computer.

There are many rules that you should follow to help prevent malware from running on your computer. Among the most important rules are the following: Keep your operating system, Internet browser, and other critical software, up-to-date. In Windows XP or later, turn on DEP for all programs.** Do not open suspicious email attachments, especially executable files, even if they appear to have been sent by your relatives or friends (their computers may be infected with malware sending malicious emails from their computers/accounts without their knowledge). Do not follow suspicious links contained in emails or on websites (even if the email/website appears to be harmless or trustworthy). Do not visit any suspicious websites. Do not download or install any suspicious software. Consider using good, trustworthy, anti-malware software.

### How to Back Up SecurelySichere Datensicherung

Due to hardware or software errors/malfunctions, files stored on a Aloaha Crypt volume may become corrupted. Therefore, we strongly recommend that you backup all your important files regularly (this, of course, applies to any important data, not just to encrypted data stored on Aloaha Crypt volumes).

### Systemfremde Datenträger

To back up a non-system Aloaha Crypt volume securely, it is recommended to follow these steps:

1. Create a new Aloaha Crypt volume using the Aloaha Crypt Volume Creation Wizard (do not enable the Quick Format option or the Dynamic option). It will be your backup volume so its size should match (or be greater than) the size of your main volume.

If the main volume is a hidden Aloaha Crypt volume, the backup volume must be a hidden Aloaha Crypt volume too. Before you create the hidden backup volume, you must create a new host (outer) volume for it without enabling the Quick Format option. In addition, especially if the backup volume is file-hosted, the hidden backup volume should occupy only a very small portion of the container and the outer volume should be almost completely filled with files (otherwise, the plausible deniability of the hidden volume might be adversely affected).

2. Mount the newly created backup volume.

3. Mount the main volume.

4. Copy all files from the mounted main volume directly to the mounted backup volume.

**IMPORTANT: If you store the backup volume in any location that an adversary can repeatedly access (for example, on a device kept in a bank's safe deposit box), you should repeat all of the above steps (including the step 1) each time you want to back up the volume (see below).**

If you follow the above steps, you will help prevent adversaries from finding out:

- Which sectors of the volumes are changing (because you always follow step 1). This is particularly important, for example, if you store the backup volume on a device kept in a bank's safe deposit box (or in any other location that an adversary can repeatedly access) and the volume contains a hidden volume (for more information, see the subsection Security Requirements and Precautions Pertaining to Hidden Volumes in the chapter Plausible Deniability).

- That one of the volumes is a backup of the other.

### System Partitionen

**Note:** In addition to backing up files, we recommend that you also back up your Aloaha Crypt Rescue Disk (select System > Create Rescue Disk).

To back up an encrypted system partition securely and safely, it is recommended to follow these steps:

1. If you have multiple operating systems installed on your computer, boot the one that does not require pre-boot authentication.

If you do not have multiple operating systems installed on your computer, you can boot a WinPE or BartPE CD/DVD (i.e. 'live' Windows entirely stored on and booted from a CD/DVD; for more information, search the Aloaha Crypt FAQ for the keyword 'BartPE').

If none of the above is possible, connect your system drive as a secondary drive to another computer and then boot the operating system installed on the computer.

**Note:** For security reasons, if the operating system that you want to back up resides in a hidden Aloaha Crypt volume (see the section Hidden Operating System), then the operating system that you boot in this step must be either another hidden operating system or a "live-CD" operating system (see above). For more information, see the subsection Security Requirements and Precautions Pertaining to Hidden Volumes in the chapter Plausible Deniability.

2. Create a new non-system Aloaha Crypt volume using the Aloaha Crypt Volume Creation Wizard (do not enable the Quick Format option or the Dynamic option). It will be your backup volume so its size should match (or be greater than) the size of the system partition that you want to back up.

If the operating system that you want to back up resides in a hidden Aloaha Crypt volume (see the section Hidden Operating System), the backup volume must be a hidden Aloaha Crypt volume too. Before you create the hidden backup volume, you must create a new host (outer) volume for it without enabling the Quick Format option. In addition, especially if the backup volume is file-hosted, the hidden backup volume should occupy only a very small portion of the container and the outer volume should be almost completely filled with files (otherwise, the plausible deniability of the hidden volume might be adversely affected).

3. Mount the newly created backup volume.

4. Mount the system partition that you want to back up by following these steps:

4.1. Click Select Device and then select the system partition that you want to back up (in case of a hidden operating system, select the partition containing the hidden volume in which the operating system is installed).

4.2. Click OK.

4.3. Select System > Mount Without Pre-Boot Authentication.

4.4. Enter your pre-boot authentication password and click OK.

5. Mount the backup volume and then copy all files from the system partition (mounted as a regular Aloaha Crypt volume since the previous step) directly to the mounted backup volume.

**IMPORTANT: If you store the backup volume in any location that an adversary can repeatedly access (for example, on a device kept in a bank's safe deposit box), you should repeat all of the above steps (including the step 2) each time you want to back up the volume (see below).**

If you follow the above steps, you will help prevent adversaries from finding out:

- Which sectors of the volumes are changing (because you always follow step 2). This is particularly important, for example, if you store the backup volume on a device kept in a bank's safe deposit box (or in any other location that an adversary can repeatedly access) and the volume contains a hidden volume (for more information, see the subsection Security Requirements and Precautions Pertaining to Hidden Volumes in the chapter Plausible Deniability).

- That one of the volumes is a backup of the other.

### Generelle Hinweise

If you store the backup volume in any location where an adversary can make a copy of the volume, consider encrypting the volume with a cascade of ciphers. Otherwise, if the volume is encrypted only with a single encryption algorithm and the algorithm is later broken (for example, due to advances in cryptanalysis), the attacker might be able to decrypt his copies of the volume. The probability that three distinct encryption algorithms will be broken is significantly lower than the probability that only one of them will be broken (each of the ciphers in a cascade uses its own key).

### Header Key Derivation, Salt, and Iteration Count ???

Header key is used to encrypt and decrypt the encrypted area of the Aloaha Crypt volume header (for system encryption, of the keydata area), which contains the master key and other data (see the sections Encryption Scheme and Aloaha Crypt Volume Format Specification). In volumes created by Aloaha Crypt 5.0 or later (and for system encryption), the area is encrypted in XTS mode (see the section Modes of Operation). The method that Aloaha Crypt uses to generate the header key and the secondary header key (XTS mode) is PBKDF2, specified in PKCS #5 v2.0; see [7] (the document specifying PBKDF2 is also available courtesy of RSA Laboratories at: http://www.Aloaha Crypt.org/docs/pkcs5v2-0.pdf).

512-bit salt is used, which means there are 2512 keys for each password. This decreases vulnerability to 'off-line' dictionary attacks (pre-computing all the keys for a dictionary of passwords is very difficult when a salt is used) [7]. The salt consists of random values generated by the Aloaha Crypt random number generator during the volume creation process. The header key derivation function is based on HMAC-SHA-512, HMAC-RIPEMD-160, or HMAC-Whirlpool (see [8, 9, 20, 22]) – the user selects which. The length of the derived key does not depend on the size of the output of the underlying hash function. For example, a header key for the AES-256 cipher is always 256 bits long even if HMAC-RIPEMD-160 is used (in XTS mode, an additional 256-bit secondary header key is used; hence, two 256-bit keys are used for AES-256 in total). For more information, refer to [7]. 1000 iterations (or 2000 iterations when HMAC-RIPEMD-160 is used as the underlying hash function) of the key derivation function have to be performed to derive a header key, which increases the time necessary to perform an exhaustive search for passwords (i. e., brute force attack) [7].

Header keys used by ciphers in a cascade are mutually independent, even though they are derived from a single password (to which keyfiles may have been applied). For example, for the AES-Twofish-Serpent cascade, the header key derivation function is instructed to derive a 768-bit encryption key from a given password (and, for XTS mode, in addition, a 768-bit secondary header key from the given password). The generated 768-bit header key is then split into three 256-bit keys (for XTS mode, the secondary header key is split into three 256-bit keys too, so the cascade actually uses six 256-bit keys in total), out of which the first key is used by Serpent, the second key is used by Twofish, and the third by AES (in addition, for XTS mode, the first secondary key is used by Serpent, the second secondary key is used by Twofish, and the third secondary key by AES). Hence, even when an adversary has one of the keys, he cannot use it to derive the other keys, as there is no feasible method to determine the password from which the key was derived (except for brute force attack mounted on a weak password).

### Unterstützte Betriebssysteme

Aloaha Crypt currently supports the following operating systems:

- Windows 7
- Windows 7 x64 (64-bit) Edition

- Windows Vista
- Windows Vista x64 (64-bit) Edition
- Windows XP
- Windows XP x64 (64-bit) Edition
- Windows Server 2008
- Windows Server 2008 x64 (64-bit)
- Windows Server 2003
- Windows Server 2003 x64 (64-bit)
- Windows 2000 SP4

- Mac OS X 10.6 Snow Leopard (32-bit)
- Mac OS X 10.5 Leopard
- Mac OS X 10.4 Tiger

- Linux (kernel 2.4, 2.6 or compatible)

**Note:** The following operating systems (among others) are not supported: Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64, Windows 95/98/ME/NT.

### Kommandozeilennutzung

Note that this section applies to the Windows version of Aloaha Crypt. For information on command line usage applying to the **Linux and Mac OS X versions**, please run: Aloaha Crypt –h

/help or /?

Display command line help.

/volume or /v

File and path name of a Aloaha Crypt volume to mount (do not use when dismounting). To mount a partition/device-hosted volume, use, for example, /v \Device\Harddisk1\Partition3 (to determine the path to a partition/device, run Aloaha Crypt and click Select Device). You can also mount a partition or dynamic volume using its volume name (for example, /v \\?\Volume{5cceb196-48bf-46ab-ad00-70965512253a}\). To determine the volume name use e.g. mountvol.exe. Also note that device paths are case-sensitive.

/letter or /l

Driver letter to mount the volume as. When /l is omitted and when /a is used, the first free drive letter is used.

/explore or /e

Open an Explorer window after a volume has been mounted.

/beep or /b

Beep after a volume has been successfully mounted or dismounted.

/auto or /a

If no parameter is specified, automatically mount the volume. If devices is specified as the parameter (e.g., /a devices), auto-mount all currently accessible device/partition-hosted Aloaha Crypt volumes. If favorites is specified as the parameter, auto-mount favorite volumes. Note that /auto is implicit if /quit and /volume are specified.

/dismount or /d

Dismount volume specified by drive letter (e.g., /d x). When no drive letter is specified, dismounts all currently mounted Aloaha Crypt volumes.

/force or /f

Forces dismount (if the volume to be dismounted contains files being used by the system or an application) and forces mounting in shared mode (i.e., without exclusive access).

/keyfile or /k

Specifies a keyfile or a keyfile search path. For multiple keyfiles, specify e.g.:
/k c:\keyfile1.dat /k d:\KeyfileFolder /k c:\kf2
To specify a keyfile stored on a security token or smart card, use the following syntax: token://slot/SLOT_NUMBER/file/FILE_NAME

/tokenlib

Use the specified PKCS #11 library for security tokens and smart cards.

/cache or /c

y or no parameter: enable password cache; n: disable password cache (e.g., /c n). Note that turning the password cache off will not clear it (use /w to clear the password cache).

/history or /h

y or no parameter: enables saving history of mounted volumes; n: disables saving history of mounted volumes (e.g., /h n).

/wipecache or /w

Wipes any passwords cached in the driver memory.

/password or /p

The volume password. If the password contains spaces, it must be enclosed in quotation marks (e.g., /p "My Password"). Use /p "" to specify an empty password. Warning: This method of entering a volume password may be insecure, for example, when an unencrypted command prompt history log is being saved to unencrypted disk.

/quit or /q

Automatically perform requested actions and exit (main Aloaha Crypt window will not be displayed). If preferences is specified as the parameter (e.g.,
/q preferences), then program settings are loaded/saved and they override settings specified on the command line.
/q background launches the Aloaha Crypt Background Task (tray icon) unless it is disabled in the Preferences.

/silent or /s

If /q is specified, suppresses interaction with the user (prompts, error messages, warnings, etc.). If /q is not specified, this option has no effect.

/mountoption or /m

ro or readonly: Mount volume as read-only.

rm or removable: Mount volume as removable medium.

ts or timestamp: Do not preserve container modification timestamp

sm or system: Without pre-boot authentication, mount a partition that is within the key scope of system encryption (for example, a partition located on the encrypted system drive of another operating system that is not running). Useful e.g. for backup or repair operations.
**Note:** If you supply a password as a parameter of /p, make sure that the password has been typed

using the standard US keyboard layout (in contrast, the GUI ensures this automatically).

bk or headerbak: Mount volume using embedded backup header.
**Note:** All volumes created by Aloaha Crypt 6.0 or later contain an embedded backup header (located at the end of the volume).

recovery: Do not verify any checksums stored in the volume header. This option should be used only when the volume header is damaged and the volume cannot be mounted even with the mount option headerbak.

Example: /m ro. To specify multiple mount options, use e.g.: /m rm /m ts

***Aloaha Crypt Format.exe (Aloaha Crypt Volume Creation Wizard):***

/noisocheck or /n

Do not verify that Aloaha Crypt Rescue Disks are correctly burned. This can be useful e.g. in corporate environments where it may be more convenient to maintain a central repository of ISO images rather than a repository of CDs or DVDs. **WARNING**: Never attempt to use this option to facilitate the reuse of a previously created Aloaha Crypt Rescue Disk. Note that every time you encrypt a system partition/drive, you must create a new Aloaha Crypt Rescue Disk even if you use the same password. A previously created Aloaha Crypt Rescue Disk cannot be reused because it was created for a different master key.

**Syntax**
Aloaha Crypt.exe [/a [devices|favorites]] [/b] [/c [y|n]] [/d [drive letter]] [/e] [/f] [/h [y|n]] [/k keyfile or search path] [/l drive letter] [/m {rm|ro|sm|ts}] [/p password] [/q [background|preferences]] [/s] [/v volume] [/w]

"Aloaha Crypt Format.exe" [/n]

Note that the order in which options are specified does not matter.

**Examples**
Mount the volume d:\ myvolume as the first free drive letter, using the password prompt (the main program window will not be displayed):

Aloaha Crypt /q /v d:\myvolume

Dismount a volume mounted as the drive letter X (the main program window will not be displayed):

Aloaha Crypt /q /dx

Mount a volume called myvolume.tc using the password MyPassword, as the drive letter X. Aloaha Crypt will open an explorer window and beep; mounting will be automatic:

Aloaha Crypt /v myvolume.tc /lx /a /p MyPassword /e /b

### Teilnahme über das Netzwerk

If there is a need to access a single Aloaha Crypt volume simultaneously from multiple operating systems, there are two options:

1. A Aloaha Crypt volume is mounted only on a single computer (for example, on a server) and only the content of the mounted Aloaha Crypt volume (i.e., the file system within the Aloaha Crypt volume) is shared over a network. Users on other computers or systems will not mount the volume (it is already mounted on the server).

Advantages: All users can write data to the Aloaha Crypt volume. The shared volume may be both

file-hosted and partition/device-hosted.

Disadvantage: Data sent over the network will not be encrypted. However, it is still possible to encrypt them using e.g. SSL, TLS, VPN, or other technologies.

Remarks: Note that, when you restart the system, the network share will be automatically restored only if the volume is a system favorite volume or an encrypted system partition/drive (to configure a volume as a system favorite volume, mount it and select Volumes > 'Save Currently Mounted Volumes as System Favorites').

2. A dismounted Aloaha Crypt file container is stored on a single computer (for example, on a server). This encrypted file is shared over a network. Users on other computers or systems will locally mount the shared file. Thus, the volume will be mounted simultaneously under multiple operating systems.

Advantage: Data sent over the network will be encrypted (however, it is still recommended to encrypt them using e.g. SSL, TLS, VPN, or other appropriate technologies to make traffic analysis more difficult and to preserve the integrity of the data).

Disadvantages: The shared volume may be only file-hosted (not partition/device-hosted). The volume must be mounted in read-only mode under each of the systems (see the section Mount Options for information on how to mount a volume in read-only mode). Note that this requirement applies to unencrypted volumes too. One of the reasons is, for example, the fact that data read from a conventional file system under one OS while the file system is being modified by another OS might be inconsistent (which could result in data corruption).

### Entfernen der Verschlüsselung

Please note that Aloaha Crypt can in-place decrypt only system partitions and system drives (select System > Permanently Decrypt System Partition/Drive). If you need to remove encryption (e.g., if you no longer need encryption) from a non-system volume, please follow these steps:

1. Mount your Aloaha Crypt volume.
2. Move all files from the Aloaha Crypt volume to any location outside the Aloaha Crypt volume (note that the files will be decrypted on the fly).
3. Dismount the Aloaha Crypt volume.
4. If the Aloaha Crypt volume is file-hosted, delete it (the container) just like you delete any other file.

If the volume is partition-hosted (applies also to USB flash drives), in addition to the steps 1-3, do the following:

1. Right-click the 'Computer' (or 'My Computer') icon on your desktop, or in the Start Menu, and select Manage. The 'Computer Management' window should appear.
2. In the Computer Management window, from the list on the left, select 'Disk Management' (within the Storage sub-tree).
3. Right-click the partition you want to decrypt and select 'Change Drive Letter and Paths'.
4. The 'Change Drive Letter and Paths' window should appear. If no drive letter is displayed in the window, click Add. Otherwise, click Cancel.

   If you clicked Add, then in the 'Add Drive Letter or Path' (which should have appeared), select a drive letter you want to assign to the partition and click OK.
5. In the Computer Management window, right-click the partition you want to decrypt again and select Format. The Format window should appear.
6. In the Format window, click OK. After the partition is formatted, it will no longer be required to mount it with Aloaha Crypt to be able to save or load files to/from the partition.

If the volume is device-hosted (i.e., there are no partitions on the device, and the device is entirely encrypted), in addition to the steps 1-3, do the following:

1. Right-click the 'Computer' (or 'My Computer') icon on your desktop, or in the Start Menu, and select Manage. The 'Computer Management' window should appear.
2. In the Computer Management window, from the list on the left, select 'Disk Management' (within the Storage sub-tree).
3. Right-click the area representing the storage space of the encrypted device and select 'New Partition' or 'New Simple Volume'.

4. **WARNING**: Before you continue, make sure you have selected the correct device, as all files stored on it will be lost. The 'New Partition Wizard' or 'New Simple Volume Wizard' window should appear now; follow its instructions to create a new partition on the device. After the partition is created, it will no longer be required to mount the device with Aloaha Crypt to be able to save or load files to/from the device.

### Verschlüsselungsschema

When mounting a Aloaha Crypt volume (assume there are no cached passwords/keyfiles) or when performing pre-boot authentication, the following steps are performed:

1. The first 512 bytes of the volume (i.e., the standard volume header) are read into RAM, out of which the first 64 bytes are the salt (see Aloaha Crypt Volume Format Specification). For system encryption (see the chapter System Encryption), the last 512 bytes of the first logical drive track are read into RAM (the Aloaha Crypt Boot Loader is stored in the first track of the system drive and/or on the Aloaha Crypt Rescue Disk).
2. Bytes 65536–66047 of the volume are read into RAM (see the section Aloaha Crypt Volume Format Specification). For system encryption, bytes 65536–66047 of the first partition located behind the active partition* are read into RAM (see the section Hidden Operating System). If there is a hidden volume within this volume (or within the partition behind the active partition), we have read its header at this point; otherwise, we have just read random data (whether or not there is a hidden volume within it has to be determined by attempting to decrypt this data; for more information see the section Hidden Volume).
3. Now Aloaha Crypt attempts to decrypt the standard volume header read in (1). All data used and generated in the course of the process of decryption are kept in RAM (Aloaha Crypt never saves them to disk). The following parameters are unknown** and have to be determined through the process of trial and error (i.e., by testing all possible combinations of the following):

3.1. PRF used by the header key derivation function (as specified in PKCS #5 v2.0; see the section Header Key Derivation, Salt, and Iteration Count), which can be one of the following:

HMAC-SHA-512, HMAC-RIPEMD-160, HMAC-Whirlpool.

A password entered by the user (to which one or more keyfiles may have been applied – see the section Keyfiles) and the salt read in (1) are passed to the header key derivation function, which produces a sequence of values (see the section Header Key Derivation, Salt, and Iteration Count) from which the header encryption key and secondary header key (XTS mode) are formed. (These keys are used to decrypt the volume header.)

3.2. Encryption algorithm: AES-256, Serpent, Twofish, AES-Serpent, AES-Twofish-Serpent, etc.

3.3. Mode of operation: XTS, LRW (deprecated/legacy), CBC (deprecated/legacy)

3.4. Key size(s)

4. Decryption is considered successful if the first 4 bytes of the decrypted data contain the ASCII string "TRUE", and if the CRC-32 checksum of the last 256 bytes of the decrypted data (volume header) matches the value located at byte #8 of the decrypted data (this value is unknown to an adversary because it is encrypted – see the section Header Key Derivation, Salt, and Iteration Count). If these conditions are not met, the process continues from (3) again, but this time, instead of the data read in (1), the data read in (2) are used (i.e., possible hidden volume header). If the conditions are not met again, mounting is terminated (wrong password, corrupted volume, or not a Aloaha Crypt volume).

5. Now we know (or assume with very high probability) that we have the correct password, the correct encryption algorithm, mode, key size, and the correct header key derivation algorithm. If we successfully decrypted the data read in (2), we also know that we are mounting a hidden volume and its size is retrieved from data read in (2) decrypted in (3).

6. The encryption routine is reinitialized with the primary master key*** and the secondary key (XTS mode), which are retrieved from the decrypted volume header (see the section Aloaha Crypt Volume Format Specification). These keys can be used to decrypt any sector of the volume, except the volume header area (or the key data area, for system encryption), which has been

encrypted using the header keys. The volume is mounted.

See also the section Modes of Operation and the section Header Key Derivation, Salt, and Iteration Count.

* If the size of the active partition is less than 256 MB, then the data is read from the second partition behind the active one (Windows 7 and later, by default, do not boot from the partition on which they are installed).
** These parameters are kept secret not in order to increase the complexity of an attack, but primarily to make Aloaha Crypt volumes unidentifiable (indistinguishable from random data), which would be difficult to achieve if these parameters were stored unencrypted within the volume header. Also note that if a non-cascaded encryption algorithm is used for system encryption, the algorithm is known (it can be determined by analyzing the contents of the unencrypted Aloaha Crypt Boot Loader stored in the first logical drive track or on the Aloaha Crypt Rescue Disk).
*** The master keys were generated during the volume creation and cannot be changed later. Volume password change is accomplished by re-encrypting the volume header using a new header key (derived from a new password).

# 6. FAQ

**Can Aloaha Crypt encrypt a partition/drive where Windows is installed?**
Yes, see the chapter System Encryption in the Aloaha Crypt User Guide.

**I forgot my PIN – is there any way to recover the files from my Aloaha Crypt volume?**
Aloaha Crypt does not contain any mechanism or facility that would allow partial or complete recovery of your encrypted data without knowing the correct PIN or the key used to encrypt the data. The only way to recover your files is to try to "crack" the PIN or the key, but it could take thousands or millions of years depending on the length and quality of the PIN/keyfiles, on software/hardware efficiency, and other factors.

**Can I directly play a video (.avi, .mpg, etc.) stored on a Aloaha Crypt volume?**
Yes, Aloaha Crypt-encrypted volumes are like normal disks. You enter the correct PIN (and/or keyfile) and mount (open) the Aloaha Crypt volume. When you double click the icon of the video file, the operating system launches the application associated with the file type – typically a media player. The media player then begins loading a small initial portion of the video file from the Aloaha Crypt-encrypted volume to RAM (memory) in order to play it. While the portion is being loaded, Aloaha Crypt is automatically decrypting it (in RAM). The decrypted portion of the video (stored in RAM) is then played by the media player. While this portion is being played, the media player begins loading next small portion of the video file from the Aloaha Crypt-encrypted volume to RAM (memory) and the process repeats.

The same goes for video recording: Before a chunk of a video file is written to a Aloaha Crypt volume, Aloaha Crypt encrypts it in RAM and then writes it to the disk. This process is called on-the-fly encryption/decryption and it works for all file types, not only for video files.

**Does Aloaha Crypt also encrypt file names and folder names?**
Yes. The entire file system within a Aloaha Crypt volume is encrypted (including file names, folder names, and contents of every file). This applies to both types of Aloaha Crypt volumes – i.e., to file containers (virtual Aloaha Crypt disks) and to Aloaha Crypt-encrypted partitions/devices.

**How can I use Aloaha Crypt on a USB flash drive?**
You have two options:

- Encrypt the entire USB flash drive. However, you will not be able run Aloaha Crypt from the USB flash drive.
  Note: Windows does not support multiple partitions on USB flash drives.

- Create a Aloaha Crypt file container on the USB flash drive (for information on how to do so, see the chapter Beginner's Tutorial, in the Aloaha Crypt User Guide). If you leave enough space on the USB flash drive (choose an appropriate size for the Aloaha Crypt container), you will also be able to store Aloaha Crypt on the USB flash drive (along with the container – not in the

container) and you will be able to run Aloaha Crypt from the USB flash drive (see also the chapter Portable Mode in the Aloaha Crypt User Guide).

**Does Aloaha Crypt use parallelization?**
Yes. Increase in encryption/decryption speed is directly proportional to the number of cores/ processors your computer has. For more information, please see the chapter Parallelization in the documentation.

**Can data be read from and written to an encrypted volume/drive as fast as if the drive was not encrypted?**
Yes, since Aloaha Crypt uses pipelining and parallelization. For more information, please see the chapters Pipelining and Parallelization in the documentation.

**Is it possible to boot Windows installed in a hidden Aloaha Crypt volume?**
Yes, it is. For more information, please see the section Hidden Operating System in the documentation.

**Will I be able to mount my Aloaha Crypt volume (container) on any computer?**
Yes, virtual Aloaha Crypt volumes (in contrast to Aloaha Crypt-encrypted physical system partitions/drives) are independent of the operating system. You will be able to mount your Aloaha Crypt volume on any computer on which you can run Aloaha Crypt (see also the question 'Can I use Aloaha Crypt on Windows if I do not have administrator privileges?').

**Can I unplug or turn off a hot-plug device (for example, a USB flash drive or USB hard drive) when there is a mounted Aloaha Crypt volume on it?**
Before you unplug or turn off the device, you should always dismount the Aloaha Crypt volume in Aloaha Crypt first, and then perform the 'Eject' operation if available (right-click the device in the 'Computer' or 'My Computer' list), or use the 'Safely Remove Hardware' function (built in Windows, accessible via the taskbar notification area). Otherwise, data loss may occur.

**What is a hidden operating system?**
See the section Hidden Operating System in the documentation.

**What is plausible deniability?**
See the chapter Plausible Deniability in the documentation.

**Will I be able to mount my Aloaha Crypt partition/container after I reinstall or upgrade the operating system?**
Yes, Aloaha Crypt volumes are independent of the operating system. However, you need to make sure your operating system installer does not format the partition where your Aloaha Crypt volume resides.

Note: If the system partition/drive is encrypted and you want to reinstall or upgrade Windows, you need to decrypt it first (select System > Permanently Decrypt System Partition/Drive). However, a running operating system can be updated (security patches, service packs, etc.) without any problems even when the system partition/drive is encrypted.

**I use pre-boot authentication. Can I prevent a person (adversary) that is watching me start my computer from knowing that I use Aloaha Crypt?**
Yes. To do so, boot the encrypted system, start Aloaha Crypt, select Settings > System Encryption, enable the option 'Do not show any texts in the pre-boot authentication screen' and click OK. Then, when you start the computer, no texts will be displayed by the Aloaha Crypt boot loader (not even when you enter the wrong PIN). The computer will appear to be "frozen" while you can type your PIN. It is, however, important to note that if the adversary can analyze the content of the hard drive, he can still find out that it contains the Aloaha Crypt boot loader.

**I use pre-boot authentication. Can I configure the Aloaha Crypt Boot Loader to display only a fake error message?**
Yes. To do so, boot the encrypted system, start Aloaha Crypt, select Settings > System Encryption, enable the option 'Do not show any texts in the pre-boot authentication screen' and enter the fake error message in the corresponding field (for example, the "Missing operating system" message, which is normally displayed by the Windows boot loader if it finds no Windows boot partition). It is,

however, important to note that if the adversary can analyze the content of the hard drive, he can still find out that it contains the Aloaha Crypt boot loader.

### Can I configure Aloaha Crypt to mount automatically whenever Windows starts selected non-system Aloaha Crypt volumes that use the same PIN as my system partition/drive (i.e. my pre-boot authentication PIN)?

Yes. Mount the volume(s) and then select 'Volumes' > 'Save Currently Mounted Volumes as System Favorites'. For more information, see the chapter 'Main Program Window', section 'Program Menu', subsection 'Volumes -> Save Currently Mounted Volumes as System Favorites' in the documentation.

### Can I configure Aloaha Crypt to mount certain volumes automatically whenever I log on to Windows?

Yes. To do so, follow these steps:

1. Mount the volume(s) and then select 'Volumes' > 'Save Currently Mounted Volumes as Favorites'.
2. Select 'Settings' > 'Preferences'. In the 'Preferences' window in the section 'Actions to perform upon log on to Windows', enable the option 'Mount favorite volumes'.
3. In the 'Preferences' window, click 'OK'.

Alternatively, if the volumes are partition/device-hosted and if you do not need to mount them to particular drive letters every time, you can skip step 1 and in the 'Preferences' window in the section 'Actions to perform upon log on to Windows' enable the option 'Mount all devices-hosted Aloaha Crypt volumes' (instead of 'Mount favorite volumes').

Note: Aloaha Crypt will not prompt you for a PIN if you have enabled caching of the pre-boot authentication PIN (Settings > 'System Encryption') and the volumes use the same PIN as the system partition/drive.

### Can my pre-boot authentication PIN be cached so that I can use it mount non-system volumes during the session?

Yes. Select Settings > 'System Encryption' and enable the following option: 'Cache pre-boot authentication PIN in driver memory'.

### How do I mount a hidden volume?

A hidden volume can be mounted the same way as a standard Aloaha Crypt volume: Click Select File or Select Device to select the outer/host volume (important: make sure the volume is not mounted). Then click Mount, and enter the PIN for the hidden volume. Whether the hidden or the outer volume will be mounted is determined by the entered PIN (i.e., when you enter the PIN for the outer volume, then the outer volume will be mounted; when you enter the PIN for the hidden volume, the hidden volume will be mounted).

Note: Aloaha Crypt first attempts to decrypt the standard volume header using the entered PIN. If it fails, it loads the area of the volume where a hidden volume header can be stored (i.e. the bytes 65536–131071, which contain solely random data when there is no hidden volume within the volume) to RAM and attempts to decrypt it using the entered PIN. Note that hidden volume headers cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted (for information on how Aloaha Crypt determines that it was successfully decrypted, see the section Encryption Scheme in the documentation), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset).

Further information may be found in the section Hidden Volume in the documentation.

### Can I save data to the decoy system partition without risking damage to the hidden system partition?

Yes. You can write data to the decoy system partition anytime without any risk that the hidden volume will get damaged (because the decoy system is not installed within the same partition as the hidden system). For more information, see the section Hidden Operating System in the documentation.

**Can I use Aloaha Crypt on Windows if I do not have administrator privileges?**
See the chapter 'Using Aloaha Crypt Without Administrator Privileges' in the documentation.

**Does Aloaha Crypt save my PIN to a disk?**
No.

**Is some hash of my PIN stored somewhere?**
No.

**How does Aloaha Crypt verify that the correct PIN was entered?**
See the section Encryption Scheme (chapter Technical Details) in the documentation.

**Can I encrypt a partition/drive without losing the data currently stored on it?**
Yes, but the following conditions must be met:

- If you want to encrypt an entire system drive (which may contain multiple partitions) or a system partition (in other words, if you want to encrypt a drive or partition where Windows is installed), you can do so provided that you use Aloaha Crypt 5.0 or later and that you use Windows XP or a later version of Windows (such as Windows 7) (select 'System' > 'Encrypt System Partition/ Drive' and then follow the instructions in the wizard).

- If you want to encrypt a non-system partition in place, you can do so provided that it contains an NTFS filesystem, that you use Aloaha Crypt 6.1 or later, and that you use Windows Vista or a later version of Windows (for example, Windows 7) (click 'Create Volume' > 'Encrypt a non-system partition' > 'Standard volume' > 'Select Device' > 'Encrypt partition in place' and then follow the instructions in the wizard).

**Can I run Aloaha Crypt if I don't install it?**
Yes, see the chapter Portable Mode in the Aloaha Crypt User Guide.

**Some encryption programs use TPM to prevent attacks. Will Aloaha Crypt use it too?**
No. Those programs use TPM to protect against attacks that require the attacker to have administrator privileges or physical access to the computer (and the attacker needs you to use the computer after such an access). However, if any of these conditions is met, it is actually impossible to secure the computer (see below) and, therefore, you must stop using it (instead of relying on TPM).

If the attacker has administrator privileges, he can, for example, reset the TPM, capture the content of RAM (containing master keys) or content of files stored on mounted Aloaha Crypt volumes (decrypted on the fly), which can then be sent to the attacker over the Internet or saved to an unencrypted local drive (from which the attacker might be able to read it later, when he gains physical access to the computer).

If the attacker can physically access the computer hardware (and you use it after such an access), he can, for example, attach a malicious component to it (such as a hardware keystroke logger) that will capture the PIN, the content of RAM (containing master keys) or content of files stored on mounted Aloaha Crypt volumes (decrypted on the fly), which can then be sent to the attacker over the Internet or saved to an unencrypted local drive (from which the attacker might be able to read it later, when he gains physical access to the computer again).

The only thing that TPM is almost guaranteed to provide is a false sense of security (even the name itself, "Trusted Platform Module", is misleading and creates a false sense of security). As for real security, TPM is actually redundant (and implementing redundant features is usually a way to create so-called bloatware). Features like this are sometimes referred to as security theater [6].

For more information, please see the sections Physical Security and Malware in the documentation .

**Why does Windows Vista (and later versions of Windows) ask me for permission to run Aloaha Crypt every time I run it in portable mode?**
When you run Aloaha Crypt in portable mode, Aloaha Crypt needs to load and start the Aloaha Crypt device driver. Aloaha Crypt needs a device driver to provide transparent on-the-fly

encryption/decryption, and users without administrator privileges cannot start device drivers in Windows. Therefore, Windows Vista and later versions of Windows ask you for permission to run Aloaha Crypt with administrator privileges.

Note that if you install Aloaha Crypt on the system (as opposed to running Aloaha Crypt in portable mode), you will not be asked for permission every time you run Aloaha Crypt.

**Do I have to dismount Aloaha Crypt volumes before shutting down or restarting Windows?**
No. Aloaha Crypt automatically dismounts all mounted Aloaha Crypt volumes on system shutdown/ restart.

**Which type of Aloaha Crypt volume is better – partition or file container?**
File containers are normal files so you can work with them as with any normal files (file containers can be, for example, moved, renamed, and deleted the same way as normal files). Partitions/ drives may be better as regards performance. Note that reading and writing to/from a file container may take significantly longer when the container is heavily fragmented. To solve this problem, defragment the file system in which the container is stored (when the Aloaha Crypt volume is dismounted).

**What's the recommended way to back up a Aloaha Crypt volume?**
See the chapter How to Back Up Securely in the documentation.

**What will happen if I format a Aloaha Crypt partition?**
See the question 'Is it possible to change the file system of an encrypted volume?'

**Is it possible to change the file system of an encrypted volume?**

Yes, when mounted, Aloaha Crypt volumes can be formatted as FAT12, FAT16, FAT32, NTFS, or any other file system. Aloaha Crypt volumes behave as standard disk devices so you can right-click the device icon (for example in the 'Computer' or 'My Computer' list) and select 'Format'. The actual volume contents will be lost. However, the whole volume will remain encrypted. If you format a Aloaha Crypt-encrypted partition when the Aloaha Crypt volume that the partition hosts is not mounted, then the volume will be destroyed, and the partition will not be encrypted anymore (it will be empty).

**Is it possible to mount a Aloaha Crypt container that is stored on a CD or DVD?**
Yes. However, if you need to mount a Aloaha Crypt volume that is stored on a read-only medium (such as a CD or DVD) under Windows 2000, the file system within the Aloaha Crypt volume must be FAT (Windows 2000 cannot mount an NTFS file system on read-only media).

**Is it possible to change the PIN for a hidden volume?**
Yes, the PIN change dialog works both for standard and hidden volumes. Just enter the PIN for the hidden volume in the 'Current PIN' field of the 'Volume PIN Change' dialog.

Remark: Aloaha Crypt first attempts to decrypt the standard volume header and if it fails, it attempts to decrypt the area within the volume where the hidden volume header may be stored (if there is a hidden volume within). In case it is successful, the PIN change applies to the hidden volume. (Both attempts use the PIN entered in the 'Current PIN' field.)

**When I use HMAC-RIPEMD-160, is the size of the header encryption key only 160 bits?**
No, Aloaha Crypt never uses an output of a hash function (nor of a HMAC algorithm) directly as an encryption key. See the section Header Key Derivation, Salt, and Iteration Count in the documentation for more information.

**Can I change the header key derivation algorithm (for example, from HMAC-RIPEMD-160 to HMAC-SHA-512) without losing data stored on the volume?**
Yes. To do so, select Volumes -> Set Header Key Derivation Algorithm.

**How do I burn a Aloaha Crypt container larger than 2 GB onto a DVD?**
The DVD burning software you use should allow you to select the format of the DVD. If it does, select the UDF format (ISO format does not support files larger than 2 GB).

### Can I use tools like chkdsk, Disk Defragmenter, etc. on the contents of a mounted Aloaha Crypt volume?

Yes, Aloaha Crypt volumes behave like real physical disk devices, so it is possible to use any filesystem checking/repairing/defragmenting tools on the contents of a mounted Aloaha Crypt volume.

### Is it possible to use Aloaha Crypt without leaving any 'traces' on unencrypted Windows?

Yes. This can be achieved by running Aloaha Crypt in portable mode under BartPE. BartPE stands for "Bart's Preinstalled Environment", which is essentially the Windows operating system prepared in a way that it can be entirely stored on and booted from a CD/DVD (registry, temporary files, etc., are stored in RAM – hard drive is not used at all and does not even have to be present). The freeware Bart's PE Builder can transform a Windows XP installation CD into BartPE. As of Aloaha Crypt 3.1, you do not need any Aloaha Crypt plug-in for BartPE. Just boot BartPE, download the Aloaha Crypt self-extracting package to the RAM disk (which BartPE creates), run it, extract its content to the RAM disk, and then run the file 'AloahaCrypt.exe' from the RAM disk.

Note: You may also want to consider creating a hidden operating system (for more information, see the section Hidden Operating System in the documentation).

### Does Aloaha Crypt support the 64-bit editions of Windows 7/Vista?

Yes. Note: The 64-bit Aloaha Crypt driver is digitally signed with the digital certificate of the Aloaha Crypt Foundation, which was issued by the certification authority GlobalSign.

### Does Aloaha Crypt run on Mac OS X?

Yes.

### Does Aloaha Crypt run on Linux?

Yes.

### Can I mount my Aloaha Crypt volume under Windows, Mac OS X, and Linux?

Yes, Aloaha Crypt volumes are fully cross-platform.

### Is there a list of all operating systems that Aloaha Crypt supports?

Yes, see the chapter Supported Operating Systems in the Aloaha Crypt User Guide.

### Is it possible to install an application to a Aloaha Crypt volume and run it from there?

Yes.

### What will happen when a part of a Aloaha Crypt volume becomes corrupted?

In encrypted data, one corrupted bit usually corrupts the whole ciphertext block in which it occurred. The ciphertext block size used by Aloaha Crypt is 16 bytes (i.e., 128 bits). The mode of operation used by Aloaha Crypt ensures that if data corruption occurs within a block, the remaining blocks are not affected. See also the question 'What do I do when the encrypted filesystem on my Aloaha Crypt volume is corrupted?

### What do I do when the encrypted filesystem on my Aloaha Crypt volume is corrupted?

File system within a Aloaha Crypt volume may become corrupted in the same way as any normal unencrypted file system. When that happens, you can use filesystem repair tools supplied with your operating system to fix it. In Windows, it is the 'chkdsk' tool. Aloaha Crypt provides an easy way to use this tool on a Aloaha Crypt volume: Right-click the mounted volume in the main Aloaha Crypt window (in the drive list) and from the context menu select 'Repair Filesystem'.

### We use Aloaha Crypt in a corporate/enterprise environment. Is there a way for an administrator to reset a volume PIN or pre-boot authentication PIN when a user forgets it (or loses a keyfile)?

Yes. Note that there is no "back door" implemented in Aloaha Crypt. However, there is a way to "reset" volume PIN/keyfiles and pre-boot authentication PIN. After you create a volume, back up its header to a file (select Tools -> Backup Volume Header) before you allow a non-admin user to use the volume. Note that the volume header (which is encrypted with a header key derived from a PIN/keyfile) contains the master key with which the volume is encrypted. Then ask the user to choose a PIN, and set it for him/her (Volumes -> Change Volume PIN); or generate a user keyfile for him/her. Then you can allow the user to use the volume and to change the PIN/keyfiles without

your assistance/permission. In case he/she forgets his/her PIN or loses his/her keyfile, you can "reset" the volume PIN/keyfiles to your original admin PIN/keyfiles by restoring the volume header from the backup file (Tools -> Restore Volume Header).

Similarly, you can reset a pre-boot authentication PIN. To create a backup of the master key data (that will be stored on a Aloaha Crypt Rescue Disk and encrypted with your administrator PIN), select 'System' > 'Create Rescue Disk'. To set a user pre-boot authentication PIN, select 'System' > 'Change PIN'. To restore your administrator PIN, boot the Aloaha Crypt Rescue Disk, select 'Repair Options' > 'Restore key data' and enter your administrator PIN.
Note: It is not required to burn each Aloaha Crypt Rescue Disk ISO image to a CD/DVD. You can maintain a central repository of ISO images for all workstations (rather than a repository of CDs/DVDs). For more information see the section Command Line Usage (option /noisocheck).

**We share a volume over a network. Is there a way to have the network share automatically restored when the system is restarted?**
Please see the chapter 'Sharing over Network' in the Aloaha Crypt User Guide.

**It is possible to access a single Aloaha Crypt volume simultaneously from multiple operating systems (for example, a volume shared over a network)?**
Please see the chapter 'Sharing over Network' in the Aloaha Crypt User Guide.

**Can a user access his or her Aloaha Crypt volume via a network?**
Please see the chapter 'Sharing over Network' in the Aloaha Crypt User Guide.

**I encrypted a non-system partition, but its original drive letter is still visible in the 'My Computer' list. When I double click this drive letter, Windows asks if I want to format the drive. Is there a way to hide or free this drive letter?**
Yes, to free the drive letter follow these steps:

1. Right-click the 'Computer' (or 'My Computer') icon on your desktop or in the Start Menu and select Manage. The 'Computer Management' window should appear.
2. From the list on the left, select 'Disk Management' (within the Storage sub-tree).
3. Right-click the encrypted partition/device and select Change Drive Letter and Paths.
4. Click Remove.
5. If Windows prompts you to confirm the action, click Yes.

**When I plug in my encrypted USB flash drive, Windows asks me if I want to format it. Is there a way to prevent that?**
Yes, but you will need to remove the drive letter assigned to the device. For information on how to do so, see the question 'I encrypted a non-system partition, but its original drive letter is still visible in the 'My Computer' list.'

**How do I remove or undo encryption if I do not need it anymore? How do I permanently decrypt a volume?**
Please see the chapter 'How to Remove Encryption' in the Aloaha Crypt User Guide.

**What will change when I enable the option 'Mount volumes as removable media'?**
You can enable this option, for example, to prevent Windows from automatically creating the 'Recycled' and/or the 'System Volume Information' folders on Aloaha Crypt volumes (in Windows, these folders are used by the Recycle Bin and System Restore facilities). However, there are some disadvantages. For example, when you enable this option under Windows Vista or earlier, the 'Computer' (or 'My Computer') list will not show free space on the volume (note that this is a Windows limitation, not a bug in Aloaha Crypt).

**Is the online documentation available for download as a single file?**
Yes, the documentation is contained in the file Aloaha Crypt User Guide.pdf that is included in all official Aloaha Crypt distribution packages. Note that you do not have to install Aloaha Crypt to obtain the PDF documentation. Just run the self-extracting installation package and then select Extract (instead of Install) on the second page of the Aloaha Crypt Setup wizard. Also note that when you do install Aloaha Crypt, the PDF documentation is automatically copied to the folder to which Aloaha Crypt is installed, and is accessible via the Aloaha Crypt user interface (by pressing F1 or choosing Help > User's Guide).

**Do I have to "wipe" free space and/or files on a Aloaha Crypt volume?**
Remark: to "wipe" = to securely erase; to overwrite sensitive data in order to render them unrecoverable.

If you believe that an adversary will be able to decrypt the volume (for example that he will make you reveal the PIN), then the answer is yes. Otherwise, it is not necessary, because the volume is entirely encrypted.

**How does Aloaha Crypt know which encryption algorithm my Aloaha Crypt volume has been encrypted with?**
Please see the section Encryption Scheme (chapter Technical Details) in the documentation.

# Index

## - A -



## - D -



## - E -



## - F -



## - H -



## - I -



## - K -



## - L -