DriveCrypt v3.03 User Manual

By Wilfried Hafner
Version 1.01

Secure Hard Disk Encryption
For Windows 95/98/ME /NT4/2000/XP

http://www.securstar.de
info@drivecrypt.com

Contents

Disclaimer:

"*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*"

-- Article 12 Universal Declaration of Human Rights --

This program employs disk volume scrambling methods to prevent unauthorised access of stored data, which may be interpreted by some as being 'encryption', and therefore the use of this program may be restricted or forbidden in some countries.

It is not intended to storage illegal data, and such use is not the purpose of the programmers or SecurStar GmbH, in providing this utility software.

The program writers and SecurStar GmbH can not be held responsible for any loss of data, due to any incompatibility of the program, running on any particular hardware, and/or software configuration.

By using the program, the person installing it, acknowledges their ***own*** responsibility to back up their important data, and is here advised to do so, before the installation of this software.

It is a condition of use, that data loss owing to any bug, error or failure of this program is not the responsibility of SecurStar GmbH. If in doubt, backup your data before installation of this software, and if possible satisfy yourself of its current operation on a system which does not contain irreplaceable data.

SecurStar GmbH cannot be responsible, or render any assistance, in the event of loss of passphrase needed to access encrypted data.

Introduction

DriveCrypt is a program that provides a virtually encrypted disk on all MS Windows operating systems. Basically, a container is created on the hard disk which is subsequently mounted by the DriveCrypt software. This software creates a new logical drive letter through which the disk is accessed. The important thing is that any data written to the new logical drive is encrypted with the algorithm of your choice.

DriveCrypt is the fastest and in its functionalities the most flexible "real time" disk cryptographic program available on the market today. Special attention has been given to render all cryptographic parts as invisible and transparent as possible.

Some of the Main Features of DriveCrypt:

1) MILITARY STRENGTH disk encryption (1344 Bit). It uses the best and most proven cryptographic algorithms such as: AES, Blowfish, TEA 16, Tea 32, DES, and Triple DES.

2) Very fast, "on the fly" encryption. The data on the disks are encrypted at any time, and they are only decoded in the RAM by the system processor.

3) Encrypts partitions as well as virtual container files

4) Possibility to hide a file-system in a WAV file. This is known as steganography.

5) Special functionalities that prevent passwords from being sniffed by programs such as Skin98 or Back Orifice.

6) Impossible to prove that a large file held on a drive is a DriveCrypt virtual disk container without knowing the pass-phrase. The DriveCrypt container files do not need a standard file extension and contain no file headers that indicate the files are anything but random data.

7) It is by far harder to mount a Dictionary or Brute Force attack against DriveCrypt compared to any of the competitors'.

8) All volumes are easily mounted/dismounted through hotkeys.

9) A keyfile allows second users to access encrypted volumes without needing the master password. These 2nd user keyfiles can be revoked at any time.

10) Allows to wipe the free space on a disk. This ensures that deleted files will never be undeleted by special disk tools.

11) The Windows console can be locked with hotkeys or a screensaver. This allows you to leave your computer on, without having to fear that others use it in the meantime.
(Only by entering the correct unlock password, the computer will run normally again).

12) Encrypted volumes can be re-sized at any time in an easy way.

13) Supports external hardware devices, such as FingerPrint- and SmartCard reader, as well as USB token.

14) Supports containers created with other leading cryptographic products.

15) Supports any kind of hard disk and removable media such as Floppy-, Zip-, Jazz, Sygate-, CD-Rom-, DVD- drives etc…..

16) Allows to manage up to ***16 Terabyte*** of encrypted data.

17) Operates on the Windows platforms : (Win 95/98/ME/NT/2000/XP)

1. Installing DriveCrypt

1.1 About this Manual :

This part of the documentation provides step-by-step guides to using the major features of DriveCrypt.

Where there is more than one way to do something, the guide will give you each of the possible options and the appropriate actions for each.

This document does not include an introduction into the way encryption works.

1.2 System Requirements

DriveCrypt has very meagre system requirements in order to run:

A PC capable of running Windows 95 /98 /ME /NT /2000 /XP
At least 1Mb of free disk space for the DriveCrypt installation.
Space to create the DriveCrypt volume files. (This could be either space on a FAT16/32 or NTFS drive, a blank partition, or a large WAV file in the case of steganography)

1.3 Installing DriveCrypt

To install DriveCrypt, run the *DC-Install.exe* file and follow the instructions.

> ***Note:*** In order to be able to install the software, you need to accept the license terms and to enter a valid serial number.

If you want to personalise your installation after accepting the license terms, you can change the installation folder in which DriveCrypt will be installed. Furthermore, you may choose a different name for the DriveCrypt program file.

Once the installation is complete and your system has restarted, you can use the DriveCrypt program to create and access encrypted volumes.

In case you would like to read encrypted containers with computers that do not have DriveCrypt installed, you can install the program in traveller mode by ticking off the appropriate box.

If you want to make sure that <u>ONLY ADMINISTRATORS</u> can create encrypted disks, and make sure that the users access these using the given keyfiles, please select the correspondent boxes during the installation process.

1.4 Removing DriveCrypt

Load the DriveCrypt application and in the main menuchoose:

<u>F</u>ile -> <u>U</u>ninstall DriveCrypt.

After confirming your intention to remove the program, DriveCrypt will be uninstalled.

2. Using DriveCrypt :

To begin using DriveCrypt, you must first of all create a so-called encrypted volume. An encrypted volume is an encrypted container in which you can store all your precious data. This volume may be a file or a physical (raw) partition on your hard drive

2.1 Creating an Encrypted Volume:

To create an encrypted volume, click the “Create Disk” icon on the mainscreen of DriveCrypt.

Alternatively, select “***Create Container***” from the file menu on the DriveCrypt main screen, or by right-clicking the DriveCrypt icon in the task bar.

Choose: ***I want to create a normal DriveCrypt (DCV) container***, and press ***NEXT***

Note : If you want your new volume to be hidden/created in a music file, (16 bit .wav) please see section : ***Hide a Volume within a Music File***

2.1.a

In the next dialog, you will be able to specify the filename for your new container, as well as its location. Furthermore, you can set the volume size and the disk formatting type.

Note: The size of the disk depends on the container formatting system.
Choose the most appropriate formatting type, according to the following table.

Formatting Type	Operating System	Volume size
FAT 16	Windows 95/98/ME NT/2000/XP	256 kb up to 2GB
FAT 32	Windows 98/ME/2000/XP	512 MB up to 4GB (64GB if container is stored on NTFS disk)
NTFS	Windows NT /2000 /XP	5 MB up to 4GB (64GB if container is stored on NTFS disk)

IMPORTANT: NTFS formatted volumes cannot be set to read-only as this is imposed by Windows. Furthermore, this implies that you cannot use NTFS volumes on read-only storage media such as CD-ROM's or you will not be able to mount/use those volumes.
If you want to use encrypted volumes on CD's, please use FAT or FAT32 volumes.

Quick Create: Tick off this option if you do not want DriveCrypt to wipe off the entire space to be used by the container before allowing you to use it. This speeds up the formatting operation, but may not be as secure, because old files on the disk can potentially be recovered, and an expert may be able to tell how many sectors you have used (but not what is in them) in your new DriveCrypt volume, because the space used by the new container file is not overwritten on the disk.

There is no advantage to Quick Create if your container is to be stored on an NTFS disk, as the NTFS file system insists on writing to some of the skipped disk space anyway.

Press ***NEXT*** to continue.

2.1.b
Choose a Password: In the password dialog, enter the password you would like to use in order to access your volume. The password is case sensitive and cannot be shorter than eight or longer than 39 characters.

Examples of good passwords include words combining upper and lowercase letters, as well as punctuation and numbers. You can use sentences as a password.

Example:
"With DriveCrypt, my data is secure !"

Note: To increase security, you can enter up to four passwords on each line (This is to encourage people to use more secure passwords. Each password must be placed correctly, and they join together to form a compound single password)…

IMPORTANT: This passphrase will be required to access the encrypted volume in future, so make sure you remember it, and the positions in which you entered it!

Once you have selected a password, and typed it twice for verification, press "***NEXT***".

2.1.c
Random Data Collection: For higher security, DriveCrypt creates every volume differently, even if they have the same size and password. In order to do this, DriveCrypt needs to collect random data.

Please move the mouse around the screen and click several times on the ”Pick/Random” button until both the ***mouse entropy*** and the **pick random bar** have been filled completely. Once done, press ***Next***.

2.1.d
Set Encryption Options:
Please specify which encryption algorithm you want to use for your volume.

The default setting is **AES 256**, alternatively you can select between :
Triple AES, Blowfish, Triple Blowfish, Tea 16, Tea 32, IDEA, DES, Triple DES, Square and Misty 1.

Once you have picked the cipher of your choice, the "**Next**" button will be enabled and you can proceed to the final step.

2.1.e
By clicking “***CREATE IT“***, your encrypted volume will be created and mounted.

2.2 Creating an Encrypted Partition

DriveCrypt allows you to transform a physical (RAW) partition into a secured, encrypted partition.

WARNING: Working with partitions can be dangerous and can cause data loss. If you are not familiar with handling partitions, it is recommended not to encrypt partitions. SecurStar GmbH does not take any responsibility for loss of data.

> **Note:** In order to prevent people from accidentally deleting their partitions, you need to enable the DriveCrypt partition management manually through the options menu. Click on ***Options*** and tick off the box “***Partition access enabled***” followed by: “***Update ALL***”. Now on the DriveCrypt main screen, all the available partitions should be visible.

To encrypt the available partitions, you can right-click them with your mouse, and select: “***Reformat Partition as DriveCrypt***” in the appearing dialog.

Select between Fat16 /32 /NTFS as your preferred formatting system.Subsequently, ***press “next” to continue…..***

Follow the steps in chapter **2.1.b** to finish the creation process.

2.3 Hide a Volume within a Music File :

DriveCrypt allows you to hide information in a sound (.wav) file.
This technique is called steganography and uses the unused space of a music file.

To create an encrypted volume into any 16 bit WAV music file, click on the Volume Wizard icon

Alternatively, select "***Create Container***" from the file menu on the DriveCrypt main screen, or by right-clicking the DriveCrypt icon in the task bar.

At this point, you should select "***I wish to hide my new disk in existing sound files***" and press "***next***"

In the next dialog, please specify how many bits of your audio file you would like to use for the volume creation. The difference between 4 and 8 bits is that 4 bits keep a better audio quality while the 8 bits variant allows the generation of a bigger volume size.

Furthermore, you need to specify the name of the file in which you would like to hide your data as well as the volume formatting system.
Subsequently, please press ***"next"*** to continue…..

In order to finish the creation process, follow the steps of chapter **2.1.b.**

Note: DriveCrypt works with 16 bit stereo .wav files. Suitable files can be created with programs such as 'WinDac' or 'Cool Edit' (you can download these programs directly from the download section of http://www.drivecrypt.com. For a better performance, please do not use wav files with pure silence at the beginning of the music file.

2.4 Mounting an Encrypted Volume

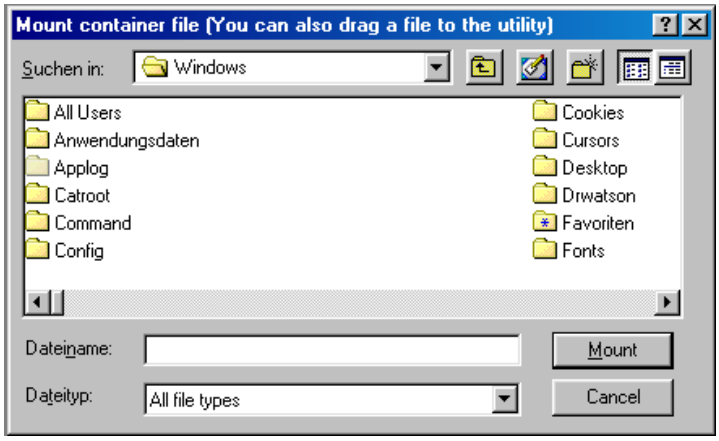
You can mount a volume in several ways :

On the **main screen**, select the "***mount volume***" icon

Alternatively, select "***Mount Container***" from the **File** menu on the DriveCrypt main screen, or by right-clicking the DriveCrypt icon in the task bar.

In the appearing dialog box :
Enter the path and name of the encrypted volume and press ***Mount***

-OR-
Browse to the volume and double-click it.



You can also mount a volume in one of the following ways :

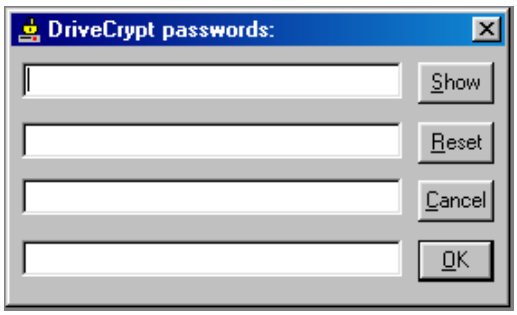
Drag the encrypted volume file from an Explorer window and drop it onto the DriveCrypt main screen.

-OR-
If you have associated the .DCV extension with DriveCrypt (see How To… Associate extensions), simply double-click the volume within Explorer.

-OR-
If you have the "Volume History" enabled, mount the last successfully mounted volume by clicking "**Files**" on the DriveCrypt main screen, and select between the last 8 successfully mounted volumes. (For more details on how to enable the "Volume History", please go to the chapter: ***Enable Mounted Volume History***).

-OR-
Press the ***Mount Hotkey***. This will mount the last successfully mounted volume. (For more details about the setup of hotkeys, please go to the chapter: ***setup Hotkey***).

Enter Volume Passwords…



Enter the passphrase you picked when you created the encrypted volume. Furthermore, enter it in the same lines that you first entered it.

Confirm with ***OK*** or ***Enter***

The mounted volume will, subsequently, appear in the first free slot on the main screen, and if you open Explorer in "My Computer" you should be able to see the drive there along with your usual hard disk drives.

NOTE : See the instructions for setting volume preferences to alter the way the volume is presented.

2.5 Mounting an Encrypted Partition

There are several ways to mount a partition with DriveCrypt :

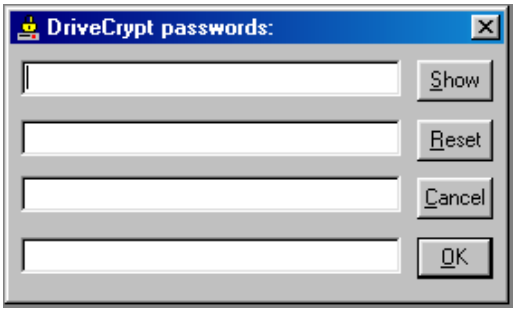
Click the password icon on the DriveCrypt main screen

-OR-
Click "***enter a Disk Password***" in the *Password option* of the main screen.

-OR-
Right-click the DriveCrypt logo in the task bar and select :
"***Enter Passwords***"

-OR-
Right-click the partition you want to mount in the "partition box" on the main screen. Then select "***Mount this Partition***"

On the appearing password screen, enter the passphrase for the partition and confirm with ***OK***.



DriveCrypt will now scan all the partitions on your system and try to mount them with the given password.

Note: If you do not want DriveCrypt to mount all partitions with the passphrase you entered, please tick off the "**No searching for DriveCrypt partition after entering passwords**" box, in the ***Option*** window.

The mounted volume will subsequently appear in the first free slot on the main screen as well as the Windows explorer "root" window (generally known in the English version of Windows as "My Computer")

NOTE: To alter the way the volume is presented, please see the instructions for setting volume preferences

2.6 Accessing an Encrypted Volume

Run DriveCrypt and follow the instructions for mounting a volume.

The volume can now be accessed in a number of ways:

> From the main screen, click on the mounted volume icon (see main screen description for further details).
>
> -OR-
> From Explorer / File Manager, in the same way that any drive is accessed.
>
> -OR-
> From any file dialog box, e.g. The **Start** menu **Run** command, the **File Open** dialog box in any Microsoft Office application etc.
>
> -OR-
> From an MS-DOS box, use the drive letter of the volume exactly as you would a local hard drive.

Operation of the encrypted volume is transparent to the user and application.

Encrypted volumes remain accessible until Windows is next shutdown, or the volume dismounted. Since the system level device driver component is always loaded and available, you do not need to keep the DriveCrypt utility running once the encrypted volumes have been mounted.

2.7 Dismounting Encrypted Volumes

In order to make a mounted volume/partition inaccessible again for others, you will have to dismount the volume

There are two different ways to dismount a volume/partition :

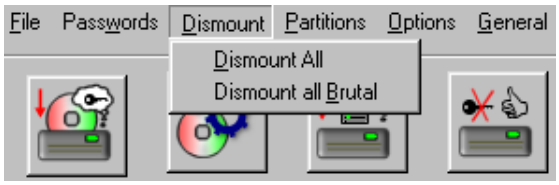
1) Normal Dismount: Allows you to dismount a partition as long as no file from that partition is in use. (This prevents you from closing a partition while you have open files that have not yet been saved).

2) Brutal Dismount: This will cause all volumes to be dismounted regardless of any open files or windows. (This is normally used in panic moments, where a very fast shutdown is requested).

Note: *On Windows NT/2000/XP, if you have installed disk utilities such as virus checkers or other programs that open pathways to your DriveCrypt drive, you may only be able to dismount your volumes brutally. This is normal !*

You can do the dismount in several ways :

From the **Dismount** menu,



Choose **Dismount All**, to dismount all the currently mounted volumes.

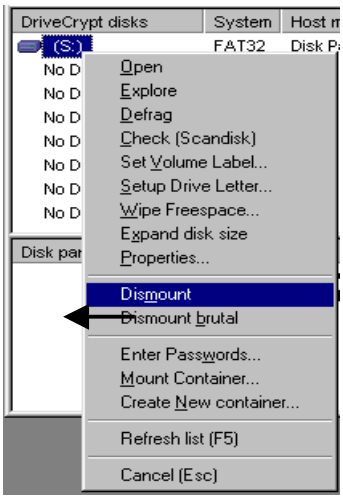
-OR-
Choose **Dismount Brutal**, to brutally dismount all the mounted volumes. DriveCrypt will wait until 2 seconds have elapsed since the last I/O operation on the volume to allow for pending writes etc.

-OR-
On the DriveCrypt main screen, to normally dismount all mounted volumes, press this icon

-OR-
On the DriveCrypt main screen, to brutally dismount all mounted volumes, press this icon

-OR-
Dismount the mounted volumes through hotkeys.
Please go to the hotkey configuration section for more details.

-OR-



If you wish to dismount a particular volume but leave the others mounted, right-click the mounted volume's icon on the DriveCrypt main screen, and click on: **Dismount /Dismount Brutal** in the appearing dialog box.

3. Disk Settings /Tools

3.1 Setting a Volume Label

DriveCrypt allows you to set/change the disk label of any disk directly fromthe main screen.

On the DriveCrypt main screen, right-click the icon of the disk/volume onto which you wish to set a label. A new dialog box will appear.

In the new dialog box select : ***Set Volume Label***

Enter the desired volume name and press ***Set***.

3.2 Assigning a Fixed Drive Letter to an Encrypted Volume

DriveCrypt allows you to assign a fixed drive letter to an encrypted volume. This letter will then be used next time the volume is mounted (if still available).

On the DriveCrypt main screen, right-click the icon of the mounted volume onto which you wish to set a fixed drive letter. This will bring up a new dialog box.

In the new dialog box select : ***Setup drive letter***

Select the desired drive letter you wish to associate to the encrypted volume,and press ***Set***.

3.3 Changing the Password of an Encrypted Volume

DriveCrypt allows you to change the volume password at any time.
On the DriveCrypt main screen, right-click the icon of the mounted volume you wish to change the password of. This will bring up a new dialog box.

In the new dialog box select : ***Properties -> New passwords***

DriveCrypt will present a password box.

Enter the ***OLD*** password and confirm it with ***OK***.
Please enter the ***NEW*** password and confirm it with ***OK***
Please ***re-enter the New password*** and confirm it with ***OK***

3.4 Defrag a Disk/ Volume

DriveCrypt allows you to defrag both disks and encrypted volumes directly on the main screen.

On the DriveCrypt main screen, right-click the icon of the disk/volume you wish to defrag. This will bring up a new dialog box.

In the new dialog box select : ***Defrag***

Note: On Windows NT and 2000, ***Defrag*** might not work if you do not have the appropriate disk tools installed. For windows 2000, you will need the commercially available version of "Diskeeper" *(*http://www.execsoft.co.uk) or equivalent to defragment DriveCrypt volumes. This is because the version that comes with Windows 2000, only allows defragmentation of those disks which are present at system boot time.

3.5 Scandisk a Disk/Volume-

DriveCrypt allows you to "scandisk" both disks and encrypted volumes directly from the main screen.

On the DriveCrypt main screen, right-click the icon of the disk/volume you wish to "scandisk". This will bring up a new diabg box.

In the new dialog box select : ***Check (Scandisk)*** → ***Start.***

3.6 Disk Properties

DriveCrypt allows you to look at and change some disk properties of a mounted, encrypted volume.

On the DriveCrypt main screen, right-click the icon of the disk/volume you wish to get the properties of. This will bring up a new dialog box.

In the new dialog box select : ***Properties***

In a new property dialog box, you will get the actual disk information. In the property dialog, you will also be able to:

- **Set encrypted Volume as Read Only**
  Tick off the entry **"Next time mount this DriveCrypt as read only"**

- **Change Volume Password:**
  Select **New passwords**

  DriveCrypt will present a password box.

  Enter the ***OLD*** password and confirm it with ***OK***.
  Please enter the ***NEW*** password and confirm it with ***OK***
  Please ***re-enter the New password*** and confirm it with ***OK***

- **Revoke DKF**
  Select the ***"Revoke DKF"*** button and confirm with ***YES***

3.7 Resize an Encrypted Volume

DriveCrypt allows you to resize an encrypted volume.

On the DriveCrypt main screen, right-click the icon of the mounted volume you wish to resize. This will bring up a new dialog box.
In the new dialog box select : ***Resize Volume***

DriveCrypt will present a password screen. This is to make sure you are the owner /authorised person to resize the volume. Please ***enter the current volume password***, and confirm it with ***OK***.

If the volume you are trying to resize is used by any program, you may want to brutally dismount it: Tick off the box "***Brutally dismount container if necessary*** ", then press "NEXT" to continue.

In the new dialog, please enter the ***New Volume Size***, and press ***NEXT*** to start the resize process.

Once the volume has been resized, you will be able to return to the main screen by pressing ***Finish.***

3.8 Wipe Disk Free Space

DriveCrypt allows to wipe a disk/volume free space.

Free space usually still holds the data that was there when the files it previously constituted were deleted.

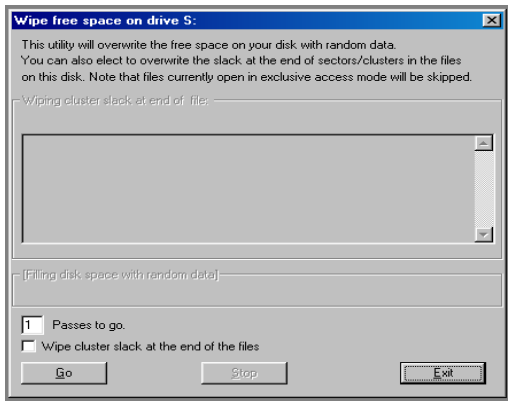
Wiping free space securely erases previously deleted files so that they cannot be restored by undelete or by a disk sector editor. This is attained by writing random data on all the free space of the disk.

It is possible to wipe the free disk space of local drives as well as mounted encrypted volume.

On the DriveCrypt main screen, right-click the icon of the disk/volume you wish to wipe the free space. This will bring up a new dialog box.

In the new dialog box select : ***Wipe Free space***

In the new wipe dialog box, set how many items you want to over-write the free space with random data, entering a number between **1 and 99** in the entry ***Passes to go***. If you wish to wipe allocated, but actually unused cluster space at the end of each file, then please also tick off the box **"Wipe cluster slack at the end of the files".**
Start the wiping process by clicking on ***GO.***



4. Setting DriveCrypt Options

4.1 Associate/Disassociate .DCV .SVL .VOL .DKF container /keyfiles files with DriveCrypt:

DriveCrypt allows you to set/cancel volume association for DriveCrypt, ScramDisk and E4M created volumes, as well as .dkf keyfiles. The file association allows you to have DriveCrypt start automatically whenever you doubleclick an encrypted volume with the extensions .dcv .svl .vol .dkf.

On the main screen click on ***Options.***

In the **Options** menu, click the **Filetypes/Startup** button.

In the appearing dialog box, tick off the file types you wish to associate/disassociate automatically.

In order to accept the new settings, please confirm with **OK** to return to the options dialog box. Confirm the changes with **Update All.**

When you subsequently click on a container /keyfile, DriveCrypt will open and request a passphrase (if it is not already cached).

4.2 Enable Mounted Volume History

In order to have a history of the last successful mounted volumes, you can enable the Mounted Volume History. This may be useful in case you want to be able to install your volumes using hotkeys or without the need of searching the volume on the system.

You can enable/disable this option by selecting the Options command on the DriveCrypt main screen.

In the appearing options dialog, tick off the box "Save File history for file options……" Confirm the changes by pressing the ***UPDATE ALL*** button.

Note: If you disable the history option, your mounted volume history will be deleted.

4.3 Setup Hotkeys: Mount/Dismount /Lockout

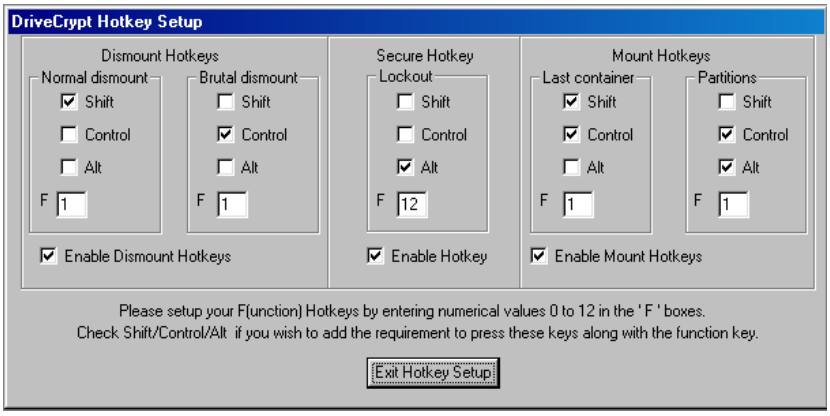
With DriveCrypt you have the possibility to use hotkeys to immediately access these commands :

- Normal Dismount all mounted volumes
- Brutal Dismount all mounted volumes
- Start Lockout Console
- Mount the last Successful Mounted volume or Partition

How to Set the Hotkeys :

On the DriveCrypt main screen, click on **Options -> Setup Hotkeys -> Secure Hotkeys**.

Enable the box of the hotkey you wish to activate, and **enter the desired Hotkey** combination.



Confirm the changes by pressing **Exit Hotkey Setup**, and in the Options dialog, press the **Update All** button.

4.4 Using the Timeout Feature

DriveCrypt allows you to set a timeout feature for the mounted volumes.
This timeout permits you to automatically (normal or brutal) dismount a mounted volume following a certain disk idle time

On the main screen press **Options.**
In the **Options** menu, choose **Setup Security**

In the appearing dialog box, tick off the **Enable Timeout Facility** box to activate this feature.

Enter the idle time in minutes that you want DriveCrypt to wait before it attempts to normally dismount all mounted volumes. This may fail if there are open Windows files on the encrypted volume(s).

Tick off the checkbox, "**Brutal dismount if still idle 15 secs after a failed closure attempt**", if you want DriveCrypt to forcibly dismount the volumes. This will take place 15 seconds after the first attempt if DriveCrypt failed on that occasion.

In order to apply the changes, please press **Exit** to return to the option menu and select **Update**.

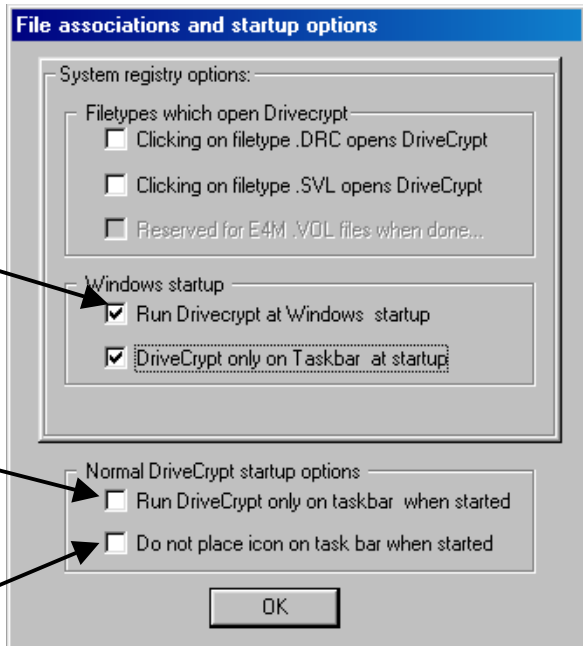
4.5 DriveCrypt Autostart and Volume Start-up options

In order to Autostart DriveCrypt automatically at windows start-up, on the main screen select: **Options-> Filetypes/Startup**

Please specify if and how to run DriveCrypt on Windows Startup by selecting the appropriated box.

Please specify if you would like to have DriveCrypt running minimised (on the windows taskbar) when started.

You can, furthermore, choose to hide the DriveCrypt icon from the task bar.



Confirm the changes by pressing **OK**,
and in the Options dialog, press the **Update All** button.

4.6 Mounting Encrypted Volume(s) or Partition(s) at Start-up

There are two different mechanisms for mounting volumes at start-up, which one you use depends on the number and type of volumes you wish to mount.

In order for either method to work, you need to have associated the file type with the DriveCrypt executable first of all. To find out how to do this, read the section entitled "How To… Associate Container and keyfiles with DriveCrypt"

Use the table below to decide which method is appropriate to you.

Encrypted Volume(s)	Method
Single, file container (.dcv) type Volume	1 - Shortcut to file name
Multiple file container (.dcv) volumes	2 - Shortcut to DKF file
Steganographic (.wav) volume(s)	2 - Shortcut to DKF file
Encrypted partition(s)	2 - Shortcut to DKF file

Method 1 - Shortcut to file name:

Open the **Start Menu** by right-clicking the **Start** button.

Browse to the **StartUp** folder (it is inside **Programs**).

Right-click a blank space in the folder.

Choose **New** and then choose **Shortcut** from the menu that pops up.

Enter the path to your container (.dcv) file in the **Command Line** box and **OK** it.

Give the shortcut a name and **OK** it.

Next time you start Windows, DriveCrypt will open and request the passphrase for your container file.

Once entered, your encrypted volume will be accessible.

Method 2 - Shortcut to SKF file:

First mount all the container files and partitions that you wish to mount at start-up.

Save an SKF file according to the instructions in the "How To… 2nd User Access - Saving a keyfile" section.

Follow **Method 1,** but enter the path to your keyfile instead of the path to a container file.

When you start Windows next time, DriveCrypt will open and request the passphrase for the keyfile.

Once entered, your encrypted volume(s) will be accessible.

4.7 Autorun Feature for Encrypted Volumes

DriveCrypt contains a feature that allows a program or associated document to be executed whenever specific containers are mounted.

Create a shortcut inside a DriveCrypt volume root directory ('f:\' for example) to something you want to have running or started (as if you have doubleclicked the shortcut) whenever the particular container is mounted.

Rename the shortcut to 'DriveCrypt'. That's it! Every time the DriveCrypt container is mounted, the application or data file pointed to by the shortcut is executed.

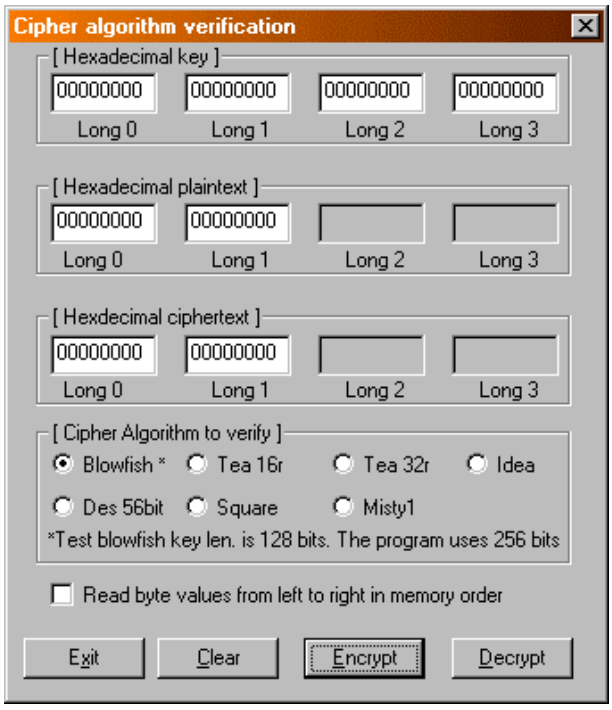
This feature is provided in response to people who complaint that applications could not be started in the Start “Startup” menu, if they were stored on DriveCrypt. Now they can, if DriveCrypt is started by the Start “Startup” menu, and the containers opened. DriveCrypt will start the applications as set up.

NOTE: It is possible to disable this feature in the **Options** dialog.

5. Verifying the Algorithms Used

Obtain a reliable set of plaintext, key and ciphertext for the algorithm you wish to verify.

On the main screen:
In the **General** menu, choose ***Verify Ciphers***. This will present the verifier utility.



In the [Hexadecimal key] section:

Enter your 'known good' key.

In the [Hexadecimal plaintext] section:

Enter your 'known good' plaintext.

In the [Cipher Algorithm to verify] section:

Choose the algorithm to be tested by clicking the radio button beside it.

Press the Encrypt button.

Tick off the values in the [Hexadecimal ciphertext] section against your 'known good' ciphertext.

N.B. The reverse may also be tested by entering “known good” ciphertext and using the **Decrypt** button to produce the plaintext for comparison

6. Working With Keyfiles (2nd User Access)

6.1 2nd User Access - Creating a Keyfile

The purpose of a keyfile is to allow others access to an encrypted volume without having to reveal the passphrase for the volume itself.

Mount all the encrypted volumes that you wish the second user to be able to access. Instructions for doing this can be found in the chapter, "**How To… Mounting an Encrypted Volume**".

On the main screen: Select the **File** menu and choose: ***Create DKF Access File***

Enter the ***keyfile name*** and the ***location*** you wish to save it in. Then press ***NEXT***

You can also impose further restrictions on the keyfile, such as the expiration date (key is valid only for X days), and/or the time during which it should be possible to use. (Example: Key may be used only during office hours, such as from 9:00h to 18:00h).

In order to have the keyfile expire after a certain amount of days, please enable the ***EXPIRE AFTER*** box, and enter the amount of days you wish the keyfile to be valid for.

To restrict the keyfile use during certain hours of the day, tick off the box:
Allow mounting of disks only between certain times.

Enter the hour and minutes, when the keyfile is to be initiated.
Enter the timeframe(in hours and minutes), during which the keyfile is to be operational.

Press ***Next*** to continue.

> **Note:** when the allowed timeframe is over,
> DriveCrypt will attempt to dismount the volumes.

Type in and confirm the ***keyfile password***, and press ***next***
in order to create the keyfile.

> **Note : The entered password is the only one the 2nd user needs to know/use to access the volumes…**

By pressing ***Finish***, you will be able to return to the DriveCrypt main screen.

The keyfile is portable, but applies only to the system it was saved on, and then only to the volumes that were mounted when it was saved.

N.B. Keyfile access to a volume can be revoked at a later date in the Volume Properties dialog box:
Right-click an encrypted volume -> Properties -> Revoke DKF.

Access via a keyfile does not allow the user to access the volume properties dialog box, the volumes must be mounted with their own passphrase(s) for this to be accessible.

6.2 2nd User Access - Mounting Encrypted Volumes

Keyfiles are mounted the same way as normal volumes are:

Point DriveCrypt to mount the keyfile the same way you normally mount a normal encrypted volume (see section Mounting an Encrypted Volume).

Enter the passphrase you have chosen when you created the keyfile volume. Furthermore, enter it in the same lines that you first entered it. Confirm with ***OK*** or ***Enter***

NOTE: Keyfiles created with an earlier version of DriveCrypt cannot be opened with DriveCrypt. You need to revoke them first (see How To… Setting Preferences for an Encrypted Volume) and then recreate them using DriveCrypt.

6.3 2nd User Access - Revoking a Keyfile

In order to revoke a keyfile, on the main screen, right-click the icon of the volume you wish to revoke the keyfile.

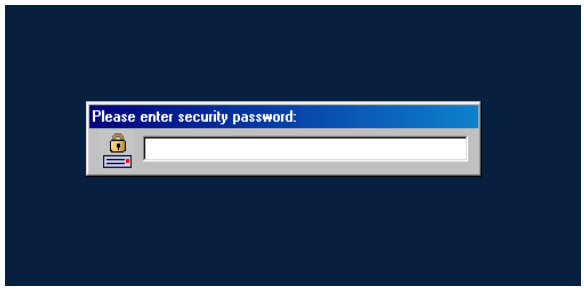
In the new appearing dialog box, select ***Properties***

In a new property dialog box, you will get the actual disk information.

Press on the **Revoke DKF** button and confirm with ***YES***

7. Lockout Local Console

The Lockout Console function allows you to block the console access to your computer, whenever you need to leave it alone for a while. The Local console hides your screen details and only allows people to work on the machine when the correct Lockout password is entered.



7.1 Setup the Local console Screen:

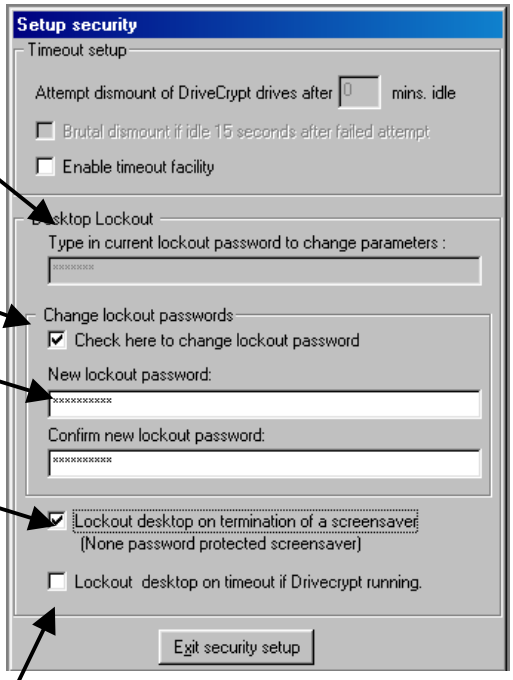
In order to enable the Lockout functionality and set a password, on the DriveCrypt main screen, select ***Options*** and ***then press on the Setup Security button*** .

Delete the entry in the password box, and enter your last lockout password. **NOTE:** For first time use, just delete the password asterisks, this will enable the other password changing boxes.

In order to be able to change the password, please tick off the appropriate box.

Enter a new password for your Lockout Screen. Confirm the new password by typing it again

If you are using a MS Screensaver, DriveCrypt is able to take it over as soon as the screen-saver has terminated and requested the user to enter the lockout password. To enable this functionality, please tick off the appropriate box. The Lockout screen can also detect the volume timeout. If you want to lock your console, on volume timeout, please tick off the apropriate box.



Once done, please press ***Exit Security Setup***, and confirm the changes on the Options Screen, by pressing ***Update All***

7.2 Use the Lockout Console Screen :

There are several different ways to use the Lockout functionality.

Starting it manually (through hotkeys or button)
Binding it to your MS Windows Screensaver
Binding it to the volume timeout

7.3 Starting the Lockout Screen Manually :

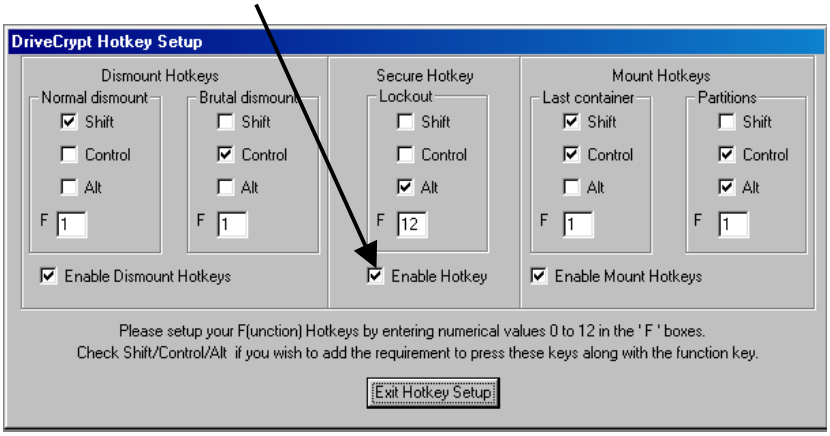
On the DriveCrypt main screen, press ***General -> Lockout Local Console***

-OR-
On the Windows task bar, ***right-click the DriveCrypt Icon*** and ***select Lockout Console***

-OR-
Press the previously defined lockout hotkey.

Note: In order to set a lockout hotkey, on the DriveCrypt main screen select: ***Options -> Setup Hotkeys -> Secure Hotkeys.)***

Enable the Secure Hotkey box, and ***enter the desired Hotkey*** combination.



Confirm the changes by pressing **Exit Hotkey Setup**, and in the Options Dialog, Press the ***Update All*** button.

Confirm the changes by pressing **Exit Hotkey Setup**, and in the Options Dialog, press the ***Update All*** button.

-OR-

Binding it to your MS Windows Screensaver

If you are using a MS Screensaver, DriveCrypt can take it over. This means that as soon as the MS Screensaver terminates (because any user activity was detected), DriveCrypt launches the Lockout screen, forcing the user to enter the Lockout Password to be able to work on the machine.

To enable this option, please see the **Setting Lockout Console** chapter.

-OR-

Binding it to the volume timeout

You can choose to start the Lockout Screen whenever a mounted volume times out.

To enable this option, please see the **Setting Lockout Console** and the **Using Timeout Features** chapters.

8. Command Line Access

DriveCrypt supports the passing of parameters via the command line for the following actions:

Mount a container file:
DriveCrypt.exe C:\crypted\mycontainer.dcv

Mount all DriveCrypt formatted partitions:
DriveCrypt.exe /MP

Dismount ALL NORMAL
DriveCrypt.exe /DN

Dismount ALL BRUTAL
DriceCrypt.exe /DB

Dismount NORMAL a container file by its name:
DriveCrypt.exe /DNF C:\crypted\mycontainer.dcv

Dismount BRUTAL a container by its file name:
DriveCrypt.exe /DBF C:\crypted\mycontainer.dcv

Dismout the DriveCrypt disk by visible logical drive letter:

Normal: {DismountNormalFile}
DriveCrypt.exe /DNF X:

Brutal:
DriveCrypt.exe /DBF X:

These last two options will also dismount individual partitions, if their logical drive letter is known.

Note: The parameters can be used with a shortcut to the DriveCrypt executable (DriveCrypt.EXE), but you must include the path to a volume in double quotes if it has spaces in it.

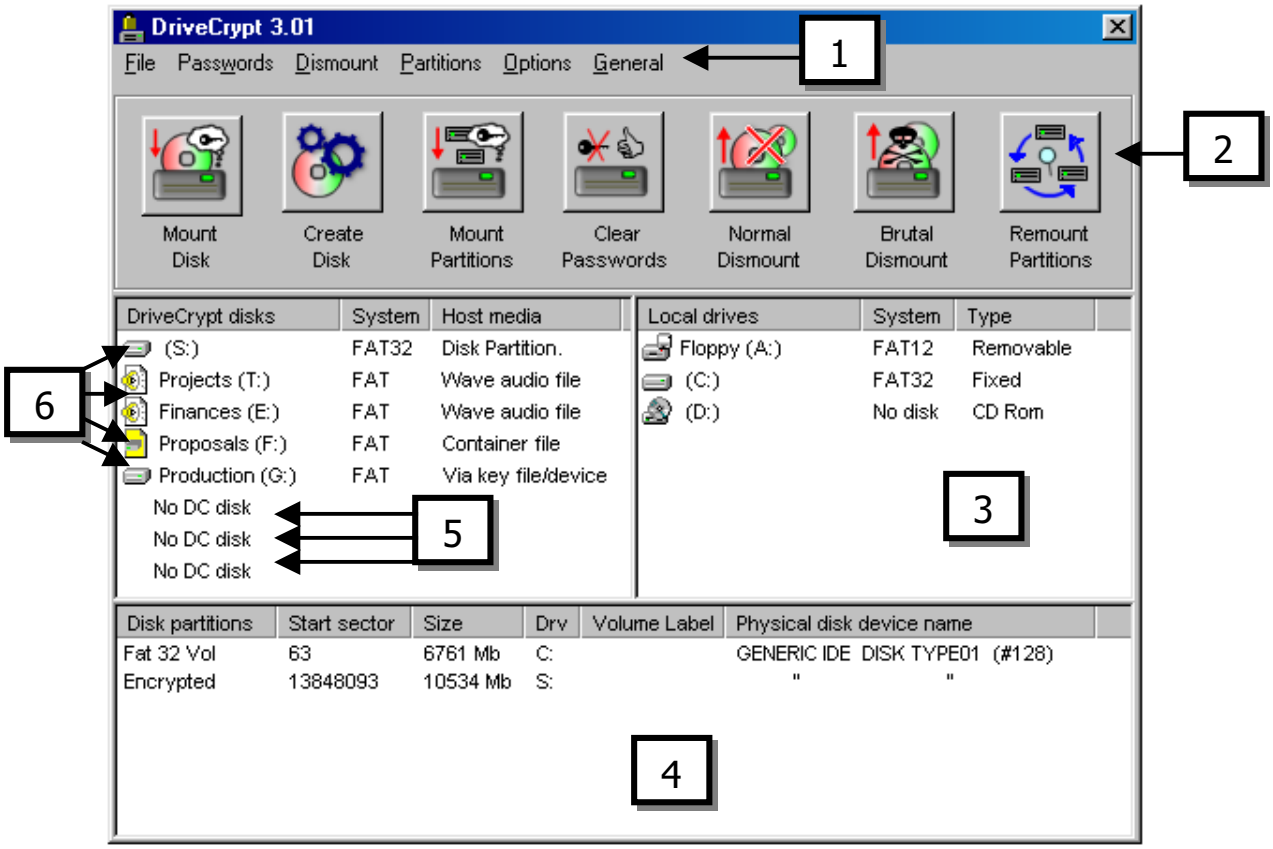
9. Screen and Menu Descriptions

This part of the documentation provides descriptions of the most frequently used screens and all the main screen menus.

The most frequently used screens are represented by a screen shot and accompanying text which explains the elements found on the screen.

All the menus on the main screen are represented by a screen shot and a description of the actions of each of its items.

9.1 The Main Screen



Key to Figure:

1 Menus.
See following pages for individual descriptions.

2 The toolbar icons can perform frequently used functions such as create/dismount encrypted volumes, clear passwords etc.

3 This area displays every normal disk available on the system.
Left-clicking an icon opens that normal disk
Right-clicking an icon opens a vertical menu dialog allowing to wipe its free space, set its volume label, defrag it etc.

4 This area displays the devices present to the system. To format a partition as a DriveCrypt partition simply right-click it. Warning! This will destroy all existing data on the partition! **Note: This area is, by default, hidden.** Show this area by enabling partition access in the options dialog box.

5 - 6 This area shows mounted volumes and available slots.
Example 6 shows five mounted volumes (a partition, two stegonographic .wav containers, a container file and a volume mounted through an external hardware device, respectively).
Example 5 shows four empty slots.

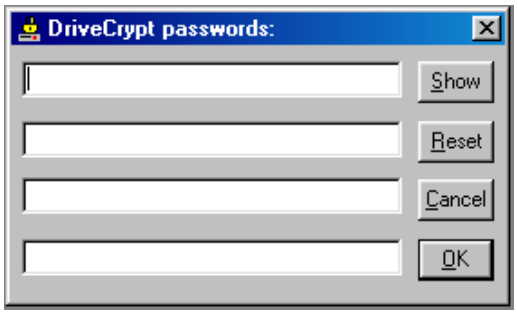
Left-clicking an empty slot brings up the password entry screen, preparing the slot for a volume to be mounted.
Left-clicking an occupied slot opens the volume.
Right-clicking an occupied slot displays the volume info dialog box.

9.2 Password and Confirm Password Screens

[Disk volume passwords]:

This section contains 4 text boxes for entering your passphrase, you may use as many of the 4 lines as you need.

Use the **Tab** and **Shift-Tab** key(s) to move between the 4 text boxes.



Toggle between displaying passwords as asterisk placeholders or plain-text.

Clears all the text boxes.

Closes the dialog box with no action taken.

Saves the passwords entered and closes the dialog box.

Note: With the exception of the title-bar text, the Confirm Passwords Screen and keyfile Password Screen are identical to the Password Screen.

9.3 The Red Low Level Message Screen (Win 95/98/Me only)

This feature is designed to avoid the possibility of keyboard messages, between Windows and the application, being copied by another programme or process.

When enabled in the "**Configure**", this feature takes over from the normal windows password entry screens.

Instead you will be presented with a red screen, rather CGA like in appearance.

The screen serves exactly the same function as the windows password screens, with keys taking the place of buttons according to the following rubric:

Key	Button
Enter	Accept
PageDown	Show
PageUp	Hide
Escape	Cancel
Home	Reset

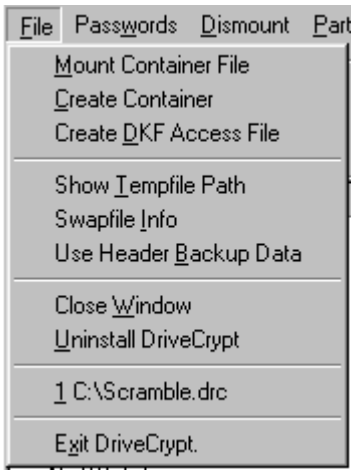
In addition to the above keys, F1 enters a | (pipe) symbol and F2 enters a # (hash).

This feature should not be used when a keyboard other then a standard QWERTY type is used (e.g. a French keyboard).

Note: The *RED Screen Mode* is currently NOT supported by Windows NT or Windows 2000.

10. Description of Menu Functions

File



Mount a container file:
Used to mount a present encrypted volume.
See 'How To.. Mount an Encrypted Volume' for full usage.

Create a container file:
Used to create a new encrypted volume.
See 'How To.. Create an Encrypted Volume' for full usage.

Create an SKF keyfile to allow others to access your DriveCrypt Volumes:
See the "How To… 2nd User Access" section.

Show 'TEMP' path:
Displays the path to the directory where temporary data is saved by applications (the value of the TEMP environment variable), and allows you to explore that directory. Data saved here is not encrypted and therefore represents a possible avenue for data theft.

Swapfile info:
Windows 'pages' out data from memory that is not needed immediately to disk, as means of providing 'Virtual Memory'. Data saved in this 'virtual memory' swapfile is not encrypted and therefore represents a possible avenue for data theft. *See also the* ***Wipe Disk Free Space*** *section for help on wiping the swap file slack.*

Use Header Backup Data
When the DriveCrypt container is created, there is 2K of critical data, which is needed to open the disk.... data for creating unique initial values ("IVs") for each sector and the cryptography key. Without these data, the disk cannot be mounted.... In case of failure of the 2K due to a sector error etc., a second 2K block exists in the header and this can be used instead. It is doubly encrypted rather than simply duplicated to prevent the possibility of identifying DriveCrypt containers. So, if the disk won't mount, and you suspect it is because the critical data has become corrupted, then go to File, select "use header backup data" and tick off the use header backup data, and then try and mount the volume again.

Normally of course, this mounts the volume, but it will have used the backup table to do it. The option lasts for the current DriveCrypt session only.

Another way to help secure disks against header trouble is to use DKF files, which contain their own separately encrypted copy of the header. The container file must remain in the same position on the disk, as the DKF file contains encrypted information on the path of the container...

Close Window:
Closes the DriveCrypt screen. The program will, however, still run minimised.

Uninstall DriveCrypt:
Completely removes the DriveCrypt programme and driver from the system.

Exit:
Exits DriveCrypt, offering you the choice of whether to clear the password cache before doing so.

NOTE : Your encrypted volumes will still be accessible until you dismount them, or you restart MS Windows.

Passwords

Enter a disk password:
Brings up a dialog box for entering your passphrase for mounting an encrypted volume.

Clear cached passwords:
Clears any passphrase held in memory by both the VxD component and the DriveCrypt interface.

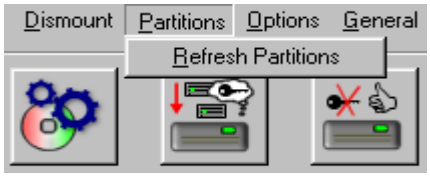
NOTE: If the "**Enter all passwords in low level RED message mode**" setting is enabled, then the "enter a Disk Password item" will use this rather than the standard windows password screens. (Not currently supported by NT or Windows 2000)

Dismount :

Dismount All:
Dismounts all mounted volumes.

Dismount all Brutal:
Brutally dismounts all the mounted volumes.
See “How To… Dismounting Encrypted Volumes” for more information.

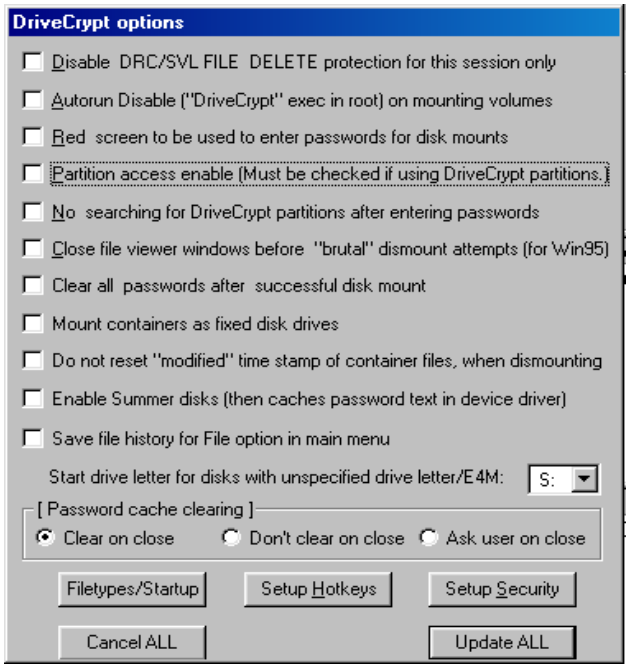
Partitions



Refresh Partitions:
Updates the device / partition window and causes DriveCrypt to attempt to mount any encrypted partitions for which it has cached the passphrase.

Options: 

Invokes the following options dialog for configuring DriveCrypt.



Disable DRC/SVL FILE DELETE protection for this session only:
DriveCrypt contains a feature preventing the accidental deletion of SVL files. If you really need to delete a container file, then simply tick off this option, delete the file, and then finally deselect this option.

Autorun Disable (“DriveCrypt” exec in root) on mounting volumes:
Turns off the autorun feature present in DriveCrypt.

Red "DOS" screen to be used to enter password for disk mounts (Win95/98/ME only) : Enables/Disables the RED low level screen which can be used when you enter a password. See the "**Screen Descriptions and Menus**" section for more details about the RED DOS Screen.

Partition access enable (Must be ticked off if using DriveCrypt Partitions):
Turn this setting on to view the physical partitions connected to the machine. (Default off)

No searching for DriveCrypt partitions after entering passwords:
Tells DriveCrypt not to perform a scan of hard disk partitions when you enter a new passphrase.

Close fileviewer windows before Brutal dismount attempts (for Win 95):
Automatically closes all Explorer windows viewing contents of encrypted volumes when drives are brutally dismounted. On windows 98/ME/NT/2000 this option is not needed, as open windows do not make the system think that files are open.

Default clear password after successful mount of container files:
Select this option to clear all the passwords from the system cache as soon as a container is successfully mounted.

Mount container as fixed disk drives:
With this option you can specify if you want an encrypted volume to be recognised and mounted as a fixed or removable disk.

Do not reset "Modified" time stamp of container files, when dismounting:
This specifies if the "Last Modified" timestamp of a container is reset to the creation date when the container was dismounted. By default the "Last Modified" time is reset to the container file's creation date, when a read/write container is dismounted, to make it appear to snoopers that the container file has never been modified since it was created. This is especially important for WAV files which would rarely be modified after creation.

Enable Summer Disks
This allows very old obsolete ScramDisk formatted disks to be opened on Windows 95/98/ME only. (Note: this caches passwords text in the device driver.)

Save file history for File option in main menu:
This enables history information of the last eight containers you mounted to be saved. When this option is enabled, you can see listed in the File menu items, the filepath of the last eight containers mounted, starting after the option is set. You can then select one of these in the file menu, to remount the particular container once more, without having to click on it, or browse for it etc.

Default start drive letter for disks with unspecified drive letter:
If you do not specify the drive letter for the mounted container to be used, the letter set here will be the letter used for that container. The next container where the drive letter is not specified will use the next letter after this, and so on. Always assuming the letters are available of course.

[Password cache clearing on closing utility window]:
Allows you to specify whether DriveCrypt clears passwords from its cache when the utility is closed.

FileType / Startup
Brings up the setting screen for the AutoStart functionality as well as the file type associations settings. For more details, see the "**AutoStart Drivecrypt"** and the **"Set Volume Association"** section.

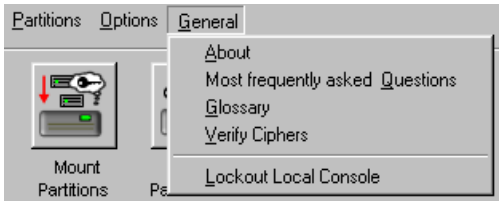
Setup Hotkeys
Brings up the setting screen for the configuration of the Hotkeys that allows you to mount/dismount volumes rapidly, and to start the Lockout console.

Setup Security
Brings up the setting screen and lets you configure:
The *timeout security settings* and the *password of the Lockout console*.

Cancel All
Discards all the changes made on the configuration screen and return to the DriveCrypt main screen.

Update All
Accept all changes and return to the DriveCrypt main screen.

General



About:
Credits and Version information.

Most Frequently asked Questions:
Questions and answers to the most frequently asked questions about DriveCrypt

Glossary:
Explanation of used technical words.

Cipher Verifier:
Invokes a utility that allows you to verify that the algorithms used by DriveCrypt produce the same ciphertext as 'known good' implementations published elsewhere.

Lockout Local Console:
Start the Local Console lockout mode.
(For more details, see section ***Lockout Local Console)***

11. Hardware Support

DriveCrypt supports different hardware deviceslike fingerprint and smartcard readers as well as USB Token. These hardware devices offer a two-factor security by requiring the user (Fingerprint) or the devices (Smart Card or Token) to be present in addition to the DriveCrypt passphrase authenticationprior to decrypting the data.

In order to use DriveCrypt together with the supported hardware devices, you need to install the appropriate hardware drivers. Some of these drivers are available for download in the download area on our homepage http://www.securstar.de/

11.1 USB Token Support

DriveCrypt has especially been designed to support the USB token from Aladdin, Rainbow, Eutron and other PKCS#11 compliant tokens. USB-token can be used on any universal serial bus (USB) equipped workstation. They provide the reliability, simplicity, and security of smartcards and cryptographic tokens without the hassle and cost of a reader.

Depending on the token you are using, please go to the corresponding chapter:

Aladdin R2 and PRO token ….. chapter 11.1.b

Eutron WebIdentiy token …….. chapter 11.1.a
Eutron CryptoIdentiy token…..... chapter 11.1.b

Rainbow 1000/1032 token ..…... chapter 11.1.a
Rainbow 2000/3000 token..…... chapter 11.1.b

Other PKCS #11 compliant token….. chapter 11.1.b

11.1.a Use of a Rainbow iKey 1000/ 1032 or Eutron WebIdentiy Token

In order to use the token, please make sure it has been correctly inserted in the USB port, and the LED on the token has been turned on. Furthermore, make sure that the driver of the token has been installed.

> **Note:** When programming the USB-Token for DriveCrypt, the token to be used must be the ONLY one connected to the PC or the FIRST key to be found by the operating system. If in doubt, please remove other USB-tokens.

First mount all the volumes you would like to be able to access through the USB Token (for more information see the chapter “Mounting Encrypted Volumes”)

> **Note: The Rainbow i-Key 1000 only has a capacity of 8 Kb, and therefore you can only store keyfiles of up to 3 volumes.**

On the DriveCrypt main screen click on **File->Create DKF access file**

Tick off the box “***Save DKF file into Rainbow I-Key***” or “**Eutron WebIdentity Token**” and press ***Next.***

You can also impose further restrictions on the keyfile, such as the expiration date (key is valid only for X days), and/or the time during which it should be possible to use. (Example: Key may be used only during office hours, such as from 9:00h to 18:00h).

> In order to have the keyfile expire after a certain amount of days, please enable the ***EXPIRE AFTER*** box, and enter the amount of days you wish the keyfile to be valid for.
>
> To restrict the keyfile use during certain hours of the day, tick off the box: ***Allow mounting of disks only between certain times***.

Enter the hour and minutes, when the keyfile is to be initiated.
Enter the timeframe, (in hours and minutes), during which the keyfile is to be operational.

Press ***Next*** to continue.

Now please ***enter the I-Key Password*** and ***confirm it***. Press ***Next*** to continue…..

Your keyfile will then be written on the USB token.
Subsequently, please press ***Finish*** to return to the main screen of DriveCrypt.

11.1.b How to Program a PKCS #11 Compliant Token :

First of all make sure that your DriveCrypt is configured to work with your specific PKCS#11 hardware.

Please go to: ***OPTIONS-> Setup Security***

In the new dialog box, you can choose the pre-configured USB-Token you would like apply (Aladdin, Eutron or Rainbow).

If the hardware you are using is not listed, you can register your own PKCS #11 compliant device:

Simply browse down the hardware DLL list and position yourself in an empty slot, then press the button: **ADD PKCS#11 DLL**

You will be requested to instruct DriveCrypt where to find the PKCS#11 DLL in your system. Simply browse to your PKCS#11 DLL and press: **Select File**

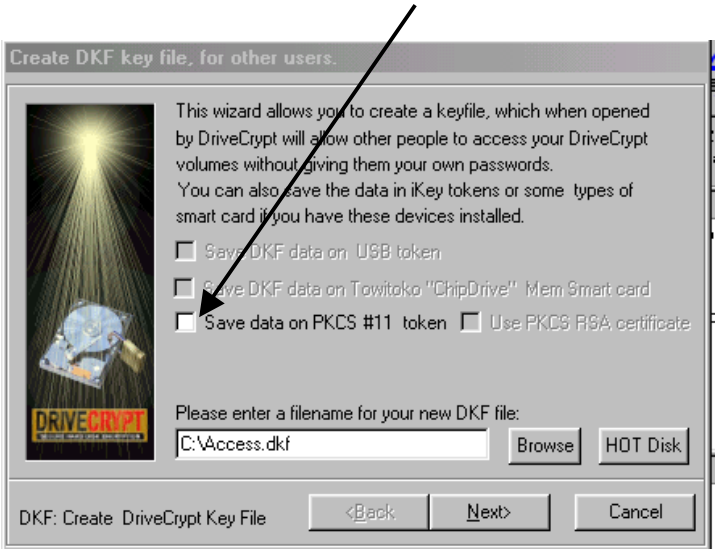
Once your new hardware device has been added to the device list, you can select: **Exit Setup Security** and confirm all changes with **UPDATE ALL**

Now your PKCS#11 device is ready to be programmed:

To program the device, first mount all the volumes you would like to access through the USB-Token token following the normal procedure (for more information see the chapter “Mounting Encrypted Volumes”)

On the DriveCrypt main Screen, click on **File->Create DKF access file**

This will bring up the following dialog box:
Please make sure the checkbox “**save data on PKCS #11 token**” has been enabled.



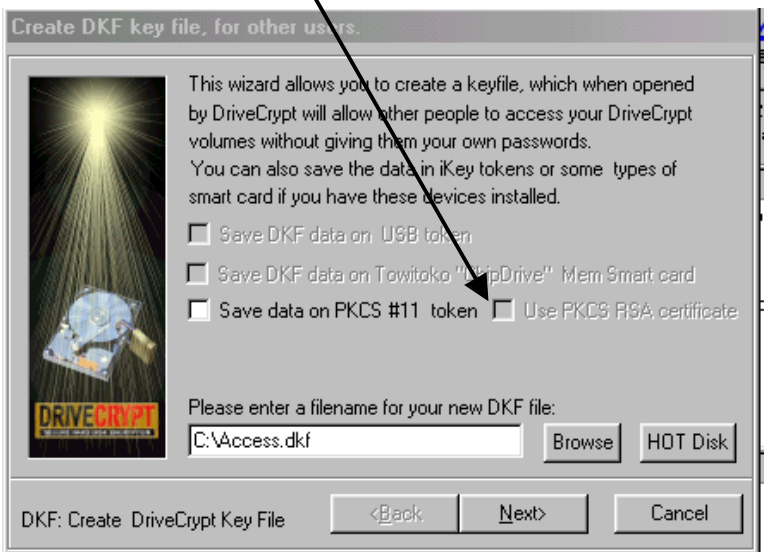
NOTE : This checkbox is only available if an installed and working token has been inserted into the computer. If the token has not been properly installed and inserted, this option will be greyed out.

At this point you can choose whether you want to encrypt your token with a user-selected password, or, if your token already carries X-509 certificates you can encrypt the DKF file using these PKI certificates.

> ***Note:*** If you are not working with certificates you can just ignore the parts referring to these as the token will just behave the same way as described in section 11.1.c

If you want to work with certificates, you need to make sure, first of all, that your token has a valid X-509 certificate on it. This implies that you need a certificate as well as a public and private key stored on the token. If no valid certificate is present on the token, the PKI checkbox will be greyed out.

Assuming you have a valid certificate on the token, please select the corresponding PKI checkbox in order to activate the PKI encryption.



11.1.c

After pressing ***Next*** You can impose further restrictions on the keyfile, such as the expiration date (key is valid only for X days), and/or the time during which it should be possible to use. (Example: Key may be used only during office hours, such as from 9:00h to 18:00h).

In order to have the keyfile expire after a certain amount of days, please enable the ***EXPIRE AFTER*** box, and enter the amount of days you wish the keyfile to be valid for.

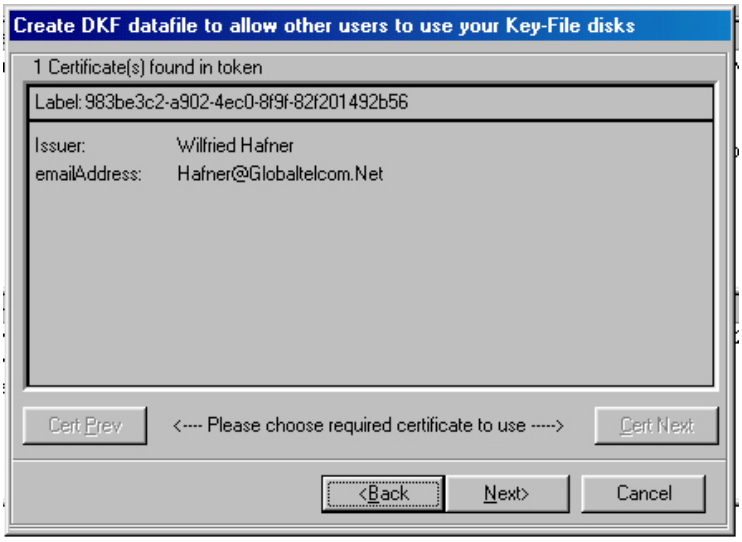
To restrict the keyfile use during certain hours of the day, tick off the box:
Allow mounting of disks only between certain times.

Enter the hour and minutes, when the keyfile is to be initiated.
Enter the timeframe (in hours and minutes), during which the keyfile is to be operational.

> **Note:** when the allowed timeframe is over, DriveCrypt will attempt to dismount the volumes.

Press ***Next*** to continue.

DriveCrypt will read the certificates on the token and show you the valid certificates found. Please press “Cert Prev” or “Cert Next” to select between all available certificates.



Once you have selected the desired certificate, please confirm with ***NEXT***
This will conclude the programming of the token, storing all the information on it.

NOTE: When using an Aladdin token, in order to be able to register data on the token, you will be required by the Aladdin drivers to enter the token PIN.

When all the data is saved successfully you will get confirmation.
You must wait for this confirmation before you remove the token.

11.1.d How to Mount /Dismount Volumes with the USB-Token :

In order to mount a volume with the USB-Token, just enter the token into the USB port of your computer. This will automatically open a password dialog box on your screen. Enter the keyfile password and confirm with Enter.

The keyfile will subsequently be mounted.

> **Note:** The FIRST key connected to the USB-Port with DriveCrypt data on it will be the one attempting to open the disks.

In order to dismount the Drive, simply take out the USB-Token from the USB port.

Note: By taking out the token from the USB port, a normal dismount will take place. If the dismount attempt fails due to the fact that an application is running on the mounted volume, you have 15 seconds to close that application. After 15 seconds a brutal dismount will take place.

11.2 SMART CARD Support (Towitoko Readers)

DriveCrypt supports the SmartCard Reader/Writer from Towitoko.

Towitoko ChipDrive Readers offer the reliability, simplicity, and security of smartcards in a very cost effective solution. In addition to this,Towitoko Readers support more than 40 different ChipCards.

How to Program the SmartCard :

In order to use the SmartCard, please make sure you have the SmartCard Reader correctly connected to your computer and that the SmartCard is fully inserted into the Card-Reader.

Mount all the volumes you would normally like access to through the ChipCard. (For more information see the chapter “Mounting Encrypted Volumes”)

On the DriveCrypt main screen click on **File->Create DKF access file**

Tick off the box “***Save DKF file on SmartCard***” and press ***Next***

> **Note:** DriveCrypt supports keyfile to mount up to 8 disks contemporaneously. However, **the keyfile needs 2kb per mounted disk**. Meaning: In case you want a SmartCard to mount one disk, you can use SmartCards with 2kb of memory. In case you want the SmartCard to mount 4 disks contemporaneously you will need at least 8kb of memory on the card. In case if you want to mount all 8 disks you need at least a SmartCard with 16 kb of memory.

You can also impose further restrictions on the keyfile, such as the expiration date (Card is valid only for X days), and/or the time during which it should be possible to use. (Example: Key may be used only during office hours, such as from 9:00h to 18:00h).

> In order to have the keyfile expire after a certain amount of days, please enable the ***EXPIRE AFTER*** box, and enter the amount of days you wish the keyfile to be valid for.

To restrict the keyfile use during certain hours of the day, tick off the box: ***Allow mounting of disks only between certain times***.

Enter the hour and minutes, when the keyfile is to be initiated.
Enter the timeframe (in hours and minutes), during which the keyfile is to be operational.

Press ***Next*** to continue.

Subsequently, ***enter the SmartCard Password*** and ***confirm it***.

Press ***Next*** to continue…..

Your keyfile will then be written on the SmartCard.
Once this is done, please press ***Finish*** to return to the main screen of DriveCrypt.

How to Mount /Dismount Volumes with SmartCards :

In order to mount a volume using SmartCards, just enter the card into the SmartCard reader. This will automatically open a SmartCard password dialog box on your screen. Enter the SmartCard password and confirm with Enter.

The keyfile will, subsequently, be mounted.

Dismount a Volume Mounted with a SmartCard

In order to dismount the drive, simply take out the SmartCard from the CardReader.

Note 1: *By taking out the SmartCard from the CardReader, a normal dismount will take place. If the dismount attempt fails due to the fact that an application is running on the mounted volume, you will have 15 seconds time to close that application. After 15 seconds a brutal dismount will take place.*

11.3 Fingerprint Reader Support (SecuGen Readers)

DriveCrypt supports the Fingerprint reader from SecuGen.



SecuGen offers cost effective, accurate, and durable fingerprint sensors designed to let your fingerprints act like digital passwords that cannot be lost or forgotten.

How to Use the Fingerprint Reader :

In order to use the SecuGen fingerprint reader, please make sure you have the device correctly connected to your computer and the device drivers are installed.

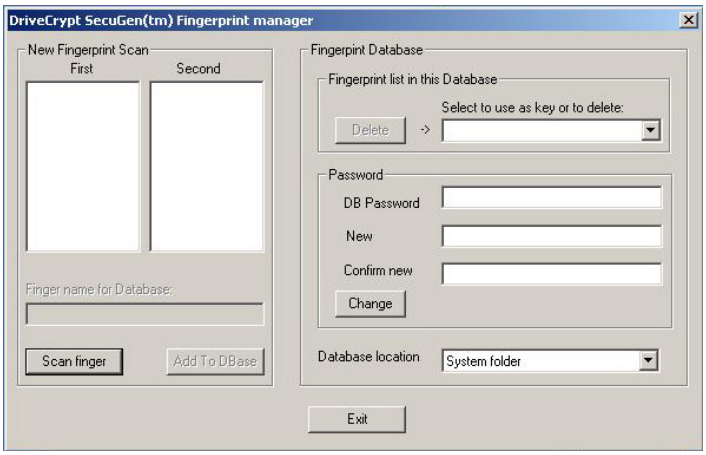
Note : Please run DriveCrypt AFTER the Fingerprint device has been correctly connected and installed, otherwise DriveCrypt will not be able to detectthe devices. If you need to close DriveCrypt in order to plug in the fingerprint device, please go to the DriveCrypt main screen and select: ***FILE->EXIT DriveCrypt***

Register Your Fingers :

Once the fingerprint reader has been installed and DriveCrypt is running, you have the possibility to register several fingers in the fingerprint database.

You can call the fingerprint database by selecting : ***FILE -> Fingerprint Manager***

This will bring up the following dialog:



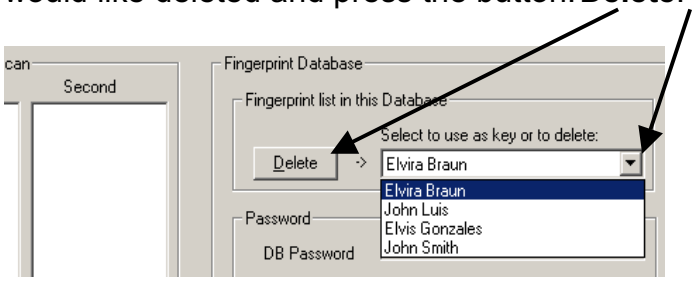
In order to register your finger, please press the button: ***Scan finger***
When the lens of the fingerprint reader starts flashing, it is ready to scan the finger.

At this point, you can place one of your fingers on the fingerprint reader, which will scan your finger and show the fingerprint in box “First”.
Remove your finger from the fingerprint reader for a few seconds and replace it on the device. The finger will be scanned again and its image will be displayed in box “Second”.

When the finger has been scanned twice and the software has detected that the fingerprint quality is acceptable, you will be able to name this fingerprint and store it in the database by pressing the “***Add to DBase***” button.

Delete a Finger from the Database:

If you need to delete a fingerprint from the database, please select the finger you would like deleted and press the button: **Delete**.



Secure Your Database:

DriveCrypt allows you to protect the database.
This prevents unauthorised people to delete fingerprints from the database and/or create a container securing it with someone else’s finger.

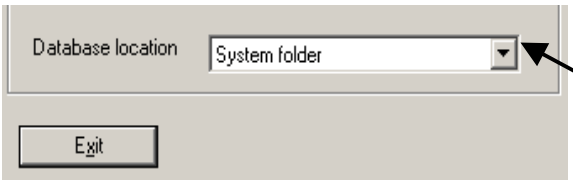
By default, the database is NOT password protected, however, you can define a password by entering it in the field: ***New*** and retype it in the field: ***Confirm New*** followed by the button: ***Change***

If the database is protected whenever you want to create a new keyfile using the registered fingerprints, you will have to enter the database unlock password in the field: ***DB Password*** of the fingerprint manager.

Database Storage :

Important Note: It is highly recommended to store the fingerprint database in a secure location. By default, DriveCrypt stores the encrypted database on the Windows System folder; it is, however, strongly recommended to create an encrypted container, and to use the possibility given by DriveCrypt to store the entire encrypted database on the encrypted container.

SecurStar does NOT assume any responsibility for an eventual security weakness derived from an improper fingerprint storage. It is the user's responsibility to protect the fingerprint database as good as possible (ideally on an encrypted DriveCrypt container).



To define where the database should be stored, please select the location in this window. Note that alternative locations are only available when an encrypted container has been mounted.

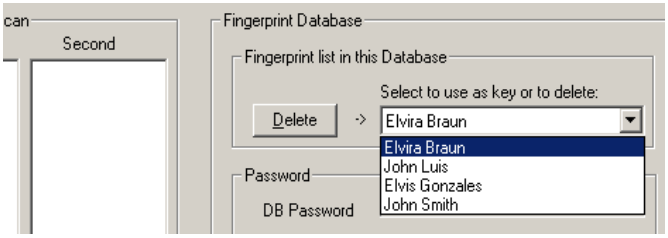
Note: If you choose to store the fingerprint database in an encrypted container, this container needs to be mounted every time you want DriveCrypt to be able to access that database.

Furthermore, please note that each database is able to store 100 fingerprints, but if you have mounted more containers at the same time each of them storing a database, the quantity of fingerprints you are able to store is 100 times the quantity of the mounted databases. DriveCrypt automatically scans all the mounted containers for a fingerprint database, and can handle a maximum of 800 fingers simultaneously.

Assign a Fingerprint to an Encrypted Volume

If you want to assign a finger to an encrypted container, firstly, you need to mount the container as usual using your password. At this point, create a keyfile for that container: ***File ->Create DKF Access File***

In the new dialog box, please select the button: ***FP Manager***
And select the fingerprint you would like to use by browsing the fingerprint database.
Once you have found the finger you would like to use, please highlight it and confirm by pressing: ***EXIT***



NOTE: Before you can access the list of registered fingers, if your database is password protected, you need to enter the unlock password in the line: ***DB Password***.

Once you are back in the DKF window, please press NEXT and finish the creation of the DKF file. (For more information about the creation of DKF files go to paragraph 6 of this manual)

Mounting a Fingerprint Protected DKF file

In order to mount an encrypted container if you have a fingerprint protected DKF file, simply double click the DKF file (or drag and drop it into the program). DriveCrypt will automatically make sure that a fingerprint password screen pops up. At this point you can place your finger on the fingerprint reader which will unlock the container.

Using the Fingerprint to Unlock the Lockout Screen

DriveCrypt also allows you to unlock the "console lockout screen" by using any registered finger in the fingerprint database in an easy way.

In order to activate the fingerprint device from the lockout console, simply press the ***ENTER*** key at the lockout password entry, or click on the button ***FingerPrint.***

NOTE: For security reasons, if there is any DKF file mounted with the fingerprint, then only the owner of that finger will be able to unlock the lockout screen using the fingerprint reader. It is, however, always possible to unlock the lockout screen by using the previously defined lockout-screen-password.

SecurStar GmbH

Les Balcons du Port, Bât 2
7 Allée des Phalènes
F-06600 Antibes – France

Web : www.securstar.de
E-Mail: info@securstar.de