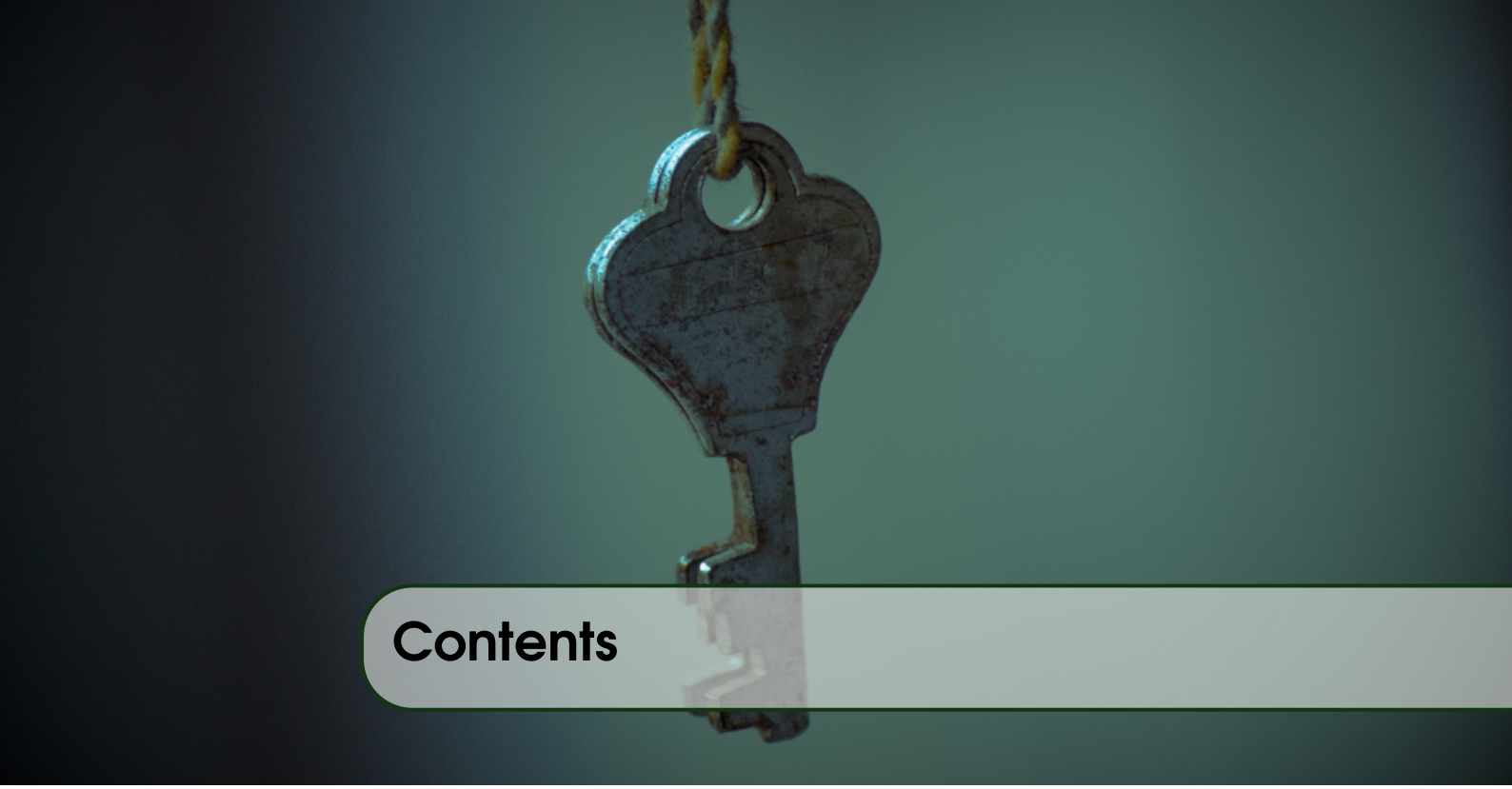
GostCrypt User Guide

Laboratoire de Cryptologie et de Virologie Opérationnelles - ESIEA

Copyright © 2014 Laboratoire de Cryptologie et de Virologie Opératoinnelles - ESIEA

GOSTCRYPT.ORG



Contents

1 Using GostCrypt volumes 5

1.1 File container encryption 5

1. Using GostCrypt volumes

GostCrypt allows you to encrypt data using three different methods:

1. File container encryption
2. Partition encryption
3. Full disk encryption

The following sections will explain how these methods work.

1.1 File container encryption

Creating a encrypted file container is the easiest way to encrypt data in GostCrypt. In this process, you will create an encrypted file of a size you specify. Once this file has been created, you can open it as a storage device in which you can store your sensitive data.

Creating the volume

In order to encrypt data on your system, you will first need to create a new GostCrypt volume. To open the GotsCrypt Volume Creation Wizard, click on the “Create Volume” button on the main screen of GostCrypt (as seen in figure 1.1).

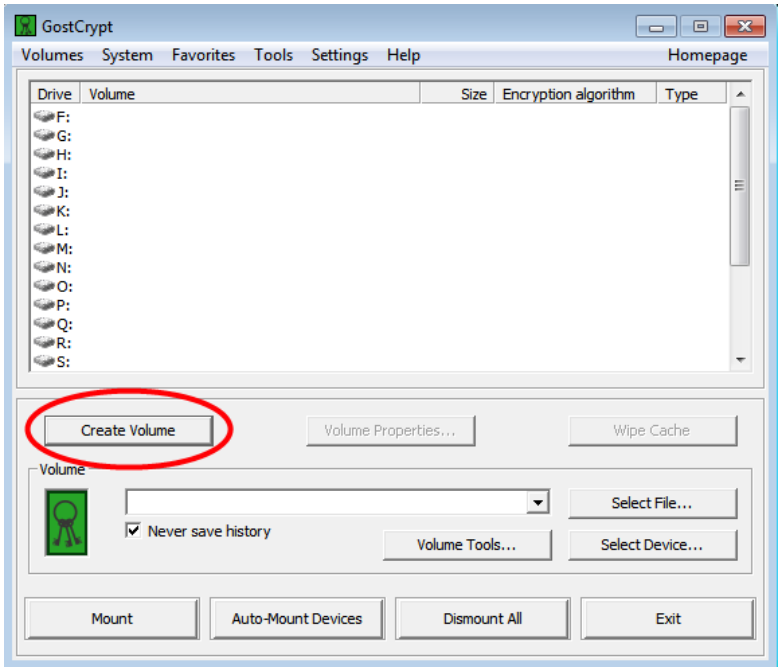


Figure 1.1: GostCrypt main window

In the GostCrypt Volume Creation Wizard, select the “Create an encrypted file container” option and click next.

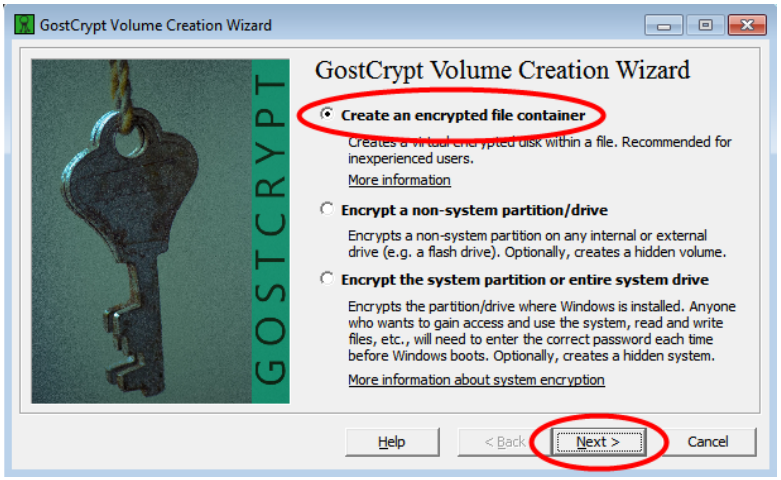


Figure 1.2: Select encrypted file container

In the next screen, you are asked to choose between the creation of a standard GostCrypt volume and a hidden GostCrypt volume. For this exercise, select “Standard GostCrypt volume”. For hidden volumes, see chapter **??**.

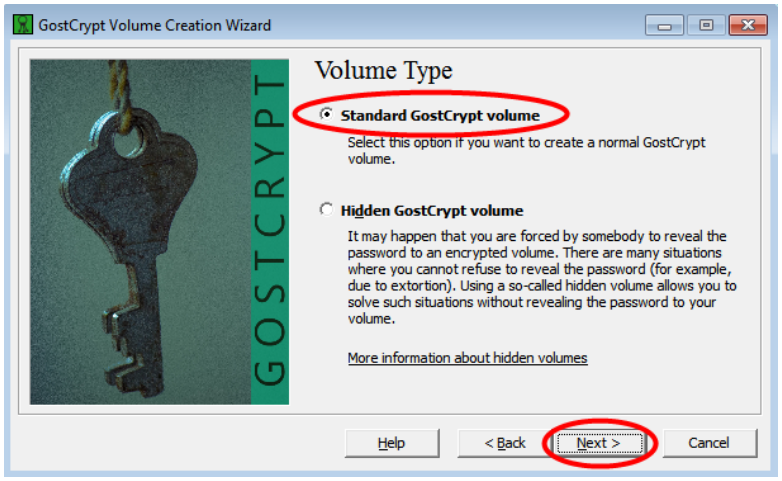


Figure 1.3: Select standard GostCrypt volume

In the next dialog, provide GostCrypt with the location where you want the file container to be created.

Figure 1.4: Provide GostCrypt with a file location

By clicking the “Select File...” button, you can specify where you want to save your file container in an easy manner.

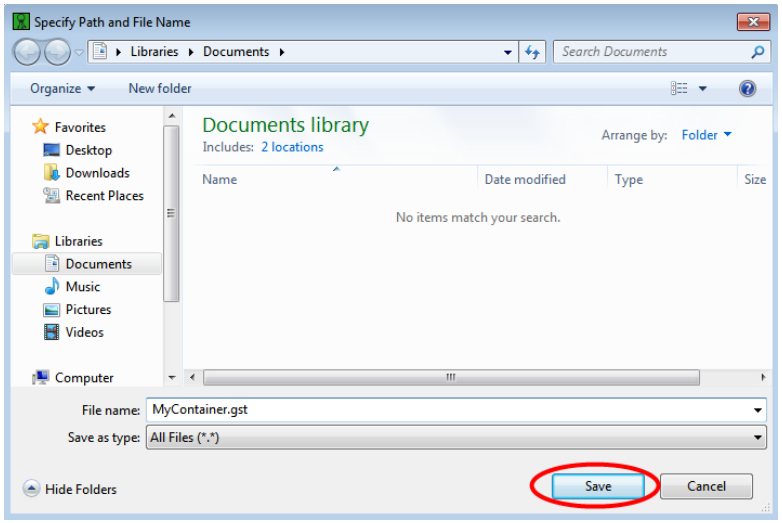


Figure 1.5: Use the "Save file" dialog for easy navigation

In the next dialog, the encryption algorithm and hash algorithm used to encrypt the file container can be chosen. This dialog also allows you to navigate to the "Test vector" dialog and "Benchmark" dialog (see chapter **??**). If you are unsure of the differences in the available algorithms, you can leave them as is and proceed to the next dialog.

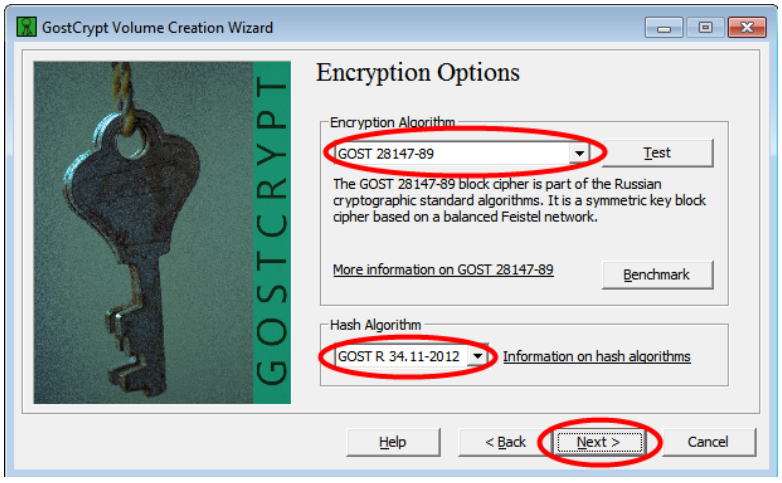


Figure 1.6: Select the preferred algorithms

You can now specify the size you want the file container to be. Specify a size in KB, MB or GB and click Next.

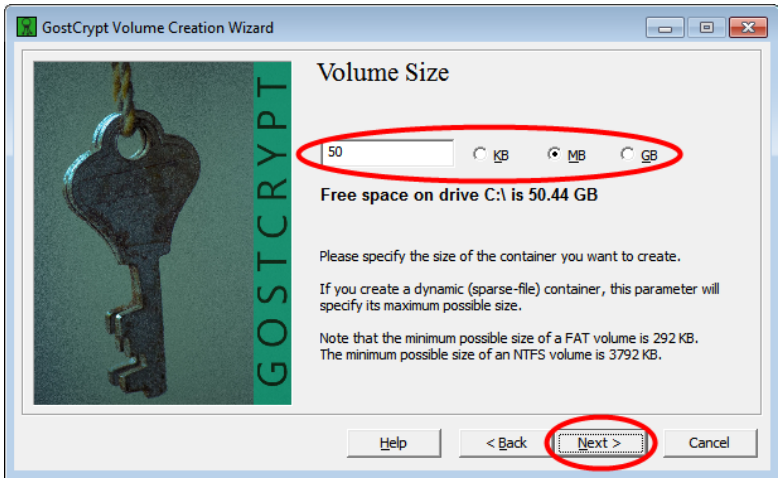


Figure 1.7: Specify the file container size

In the next dialog, you will be asked to enter the volume password. This is the password that will be used to calculate the volume header key. Make sure to follow the instructions this dialog provides on choosing a good password. You can also specify a keyfile here. For more information on keyfiles, see chapter **??**.

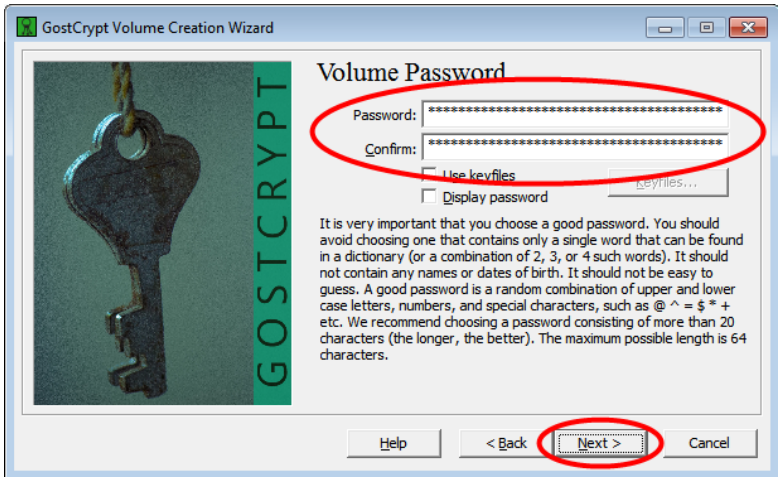


Figure 1.8: Volume password

The Volume Format dialog is the final step in creating an encrypted file container. Here, you can specify the filesystem you want to use, as well as the cluster size. If you saved the file container on an NTFS filesystem, you also have the option to make the file container “dynamic”. Using this mode, the file container will not take up much disk space at first. Instead, it will grow as you write more data to it. Note that this mode makes the resulting GostCrypt volume slower in operation. It also allows adversaries to see how much data is in your GostCrypt volume, as it grows when data is added. If you are unsure about which options to choose here, the default settings will suffice for most use cases.

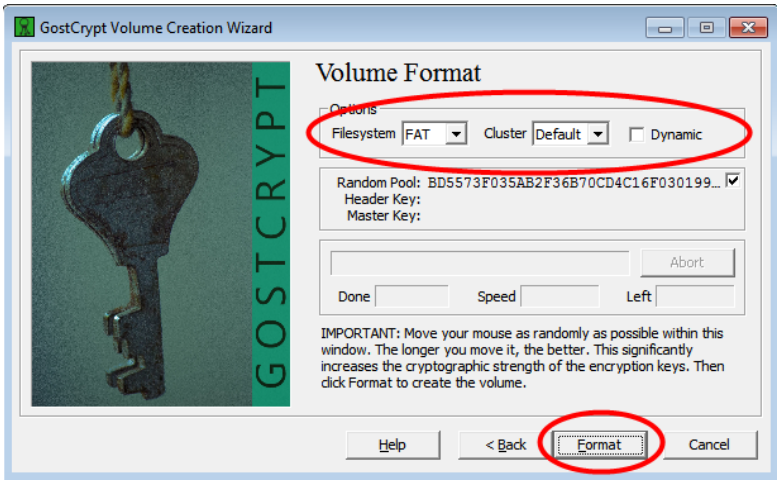


Figure 1.9: Volume format

The encrypted file container has now been created and you can exit out of the GostCrypt Volume Creation Wizard.

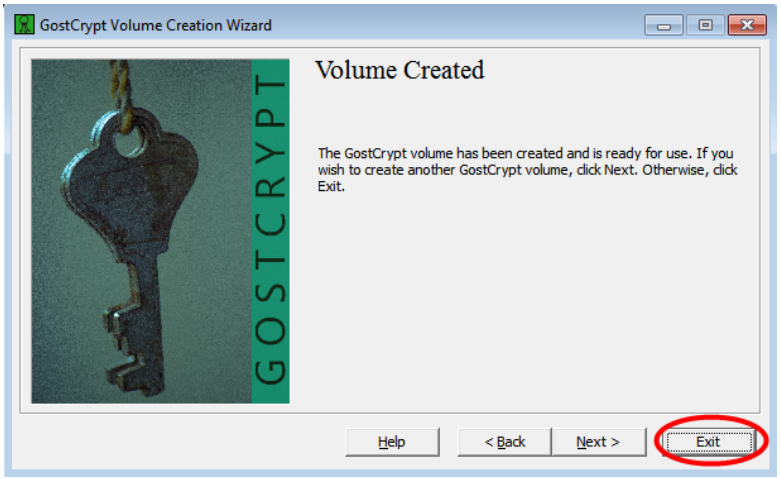


Figure 1.10: Volume created

Volume mounting

In order to start using the encrypted file container, go back to the starting window of GostCrypt. Here, you can select a free drive letter that GostCrypt will use for this file container. Next, click the “Select File” button and open the file container. Finally, click the “Mount” button.

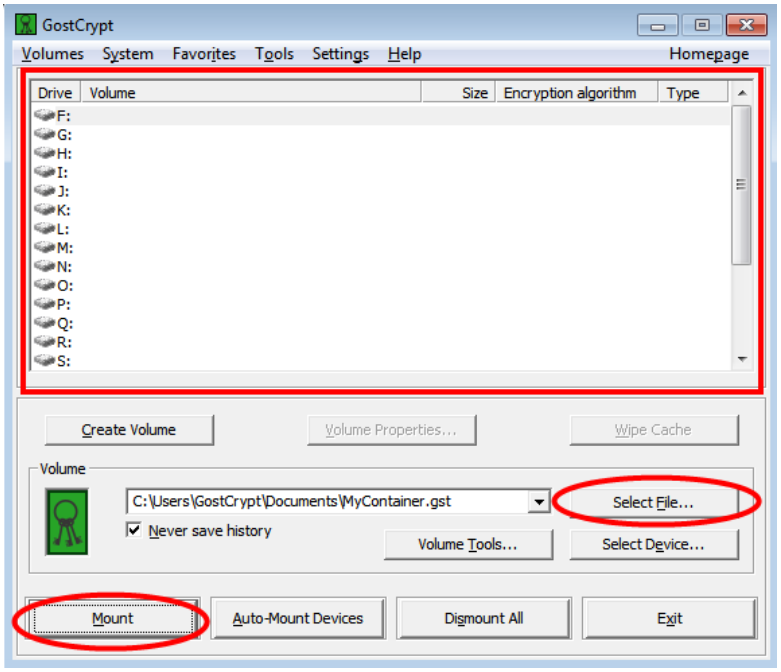


Figure 1.11: Mounting an encrypted file container

A dialog pops up which asks for the user password associated with the volume. Enter your previously specified password here. You can click "OK" to mount the volume. Chapter **??** explains the mount options that allow you to modify GostCrypt's behaviour for this volume.

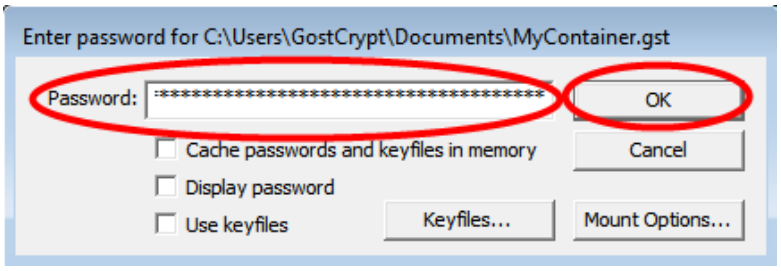


Figure 1.12: Volume mounting password dialog

The encrypted file container can now be accessed like a normal partition.

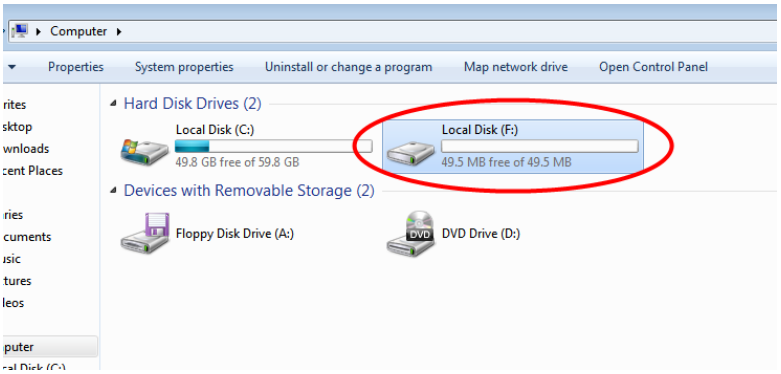


Figure 1.13: Encrypted file container mounted