File Encryption with Secure Key A1

Veracrypt and Secure Key A1

Secure strong file encryption with Free Software

Introduction

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key but, for a well-designed encryption scheme, considerable computational resources and

skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Historically, various forms of encryption have been used to aid in cryptography. Early encryption techniques were often utilized in military messaging. Since then, new techniques have emerged and become commonplace in all areas of modern computing.[1] Modern encryption schemes utilize the concepts of public-key and symmetric-key.[1] Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption.

Secure Key A1 & Veracrypt in a symmetric-key scenario

It is possible to use two or more Secure Key A1 to share the symmetric-key between two subjects, without sharing the original symmetric-key.

Prerequisites:

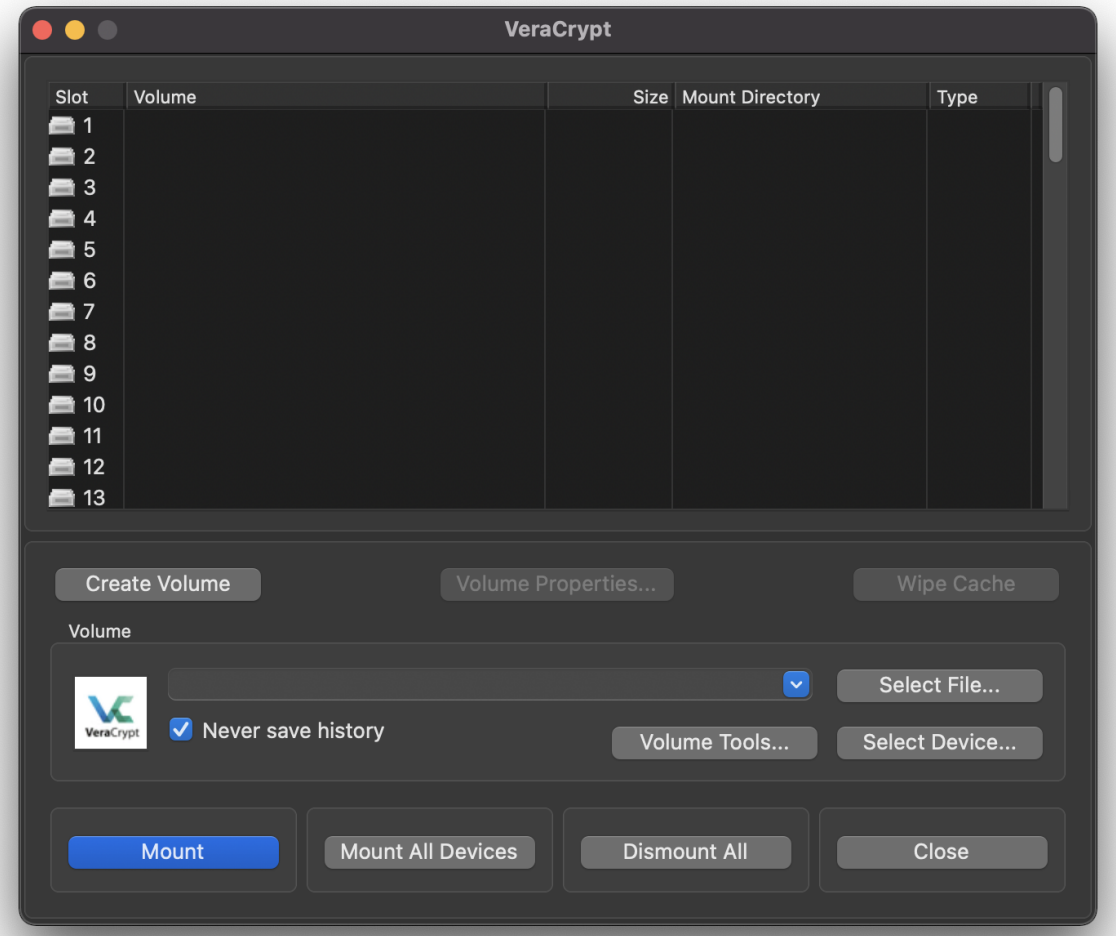
1) both the subject must install Veracrypt in their PC/Laptop
2) the two subjects must have the Secure Key A1 and share the Team PINs

Step 1: Veracrypt Installation

Download Veracrypt from the official web site https://www.veracrypt.fr/en/Downloads.html

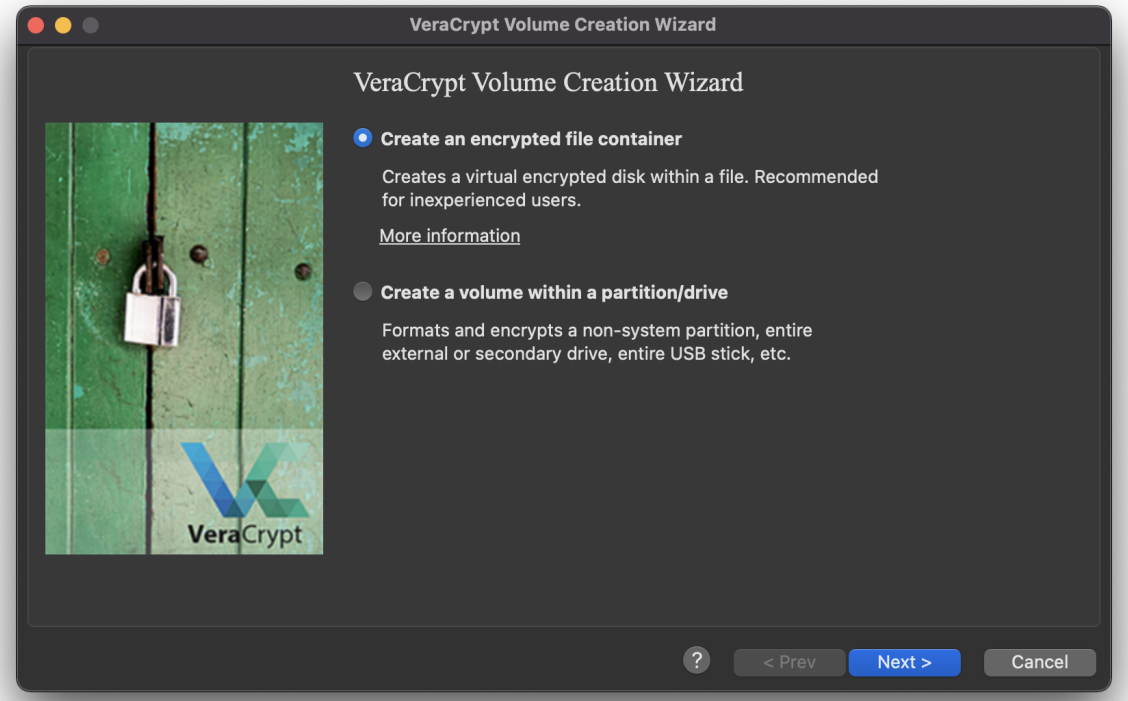
Step 2: Create an encrypted file

Press the button “Create Volume”



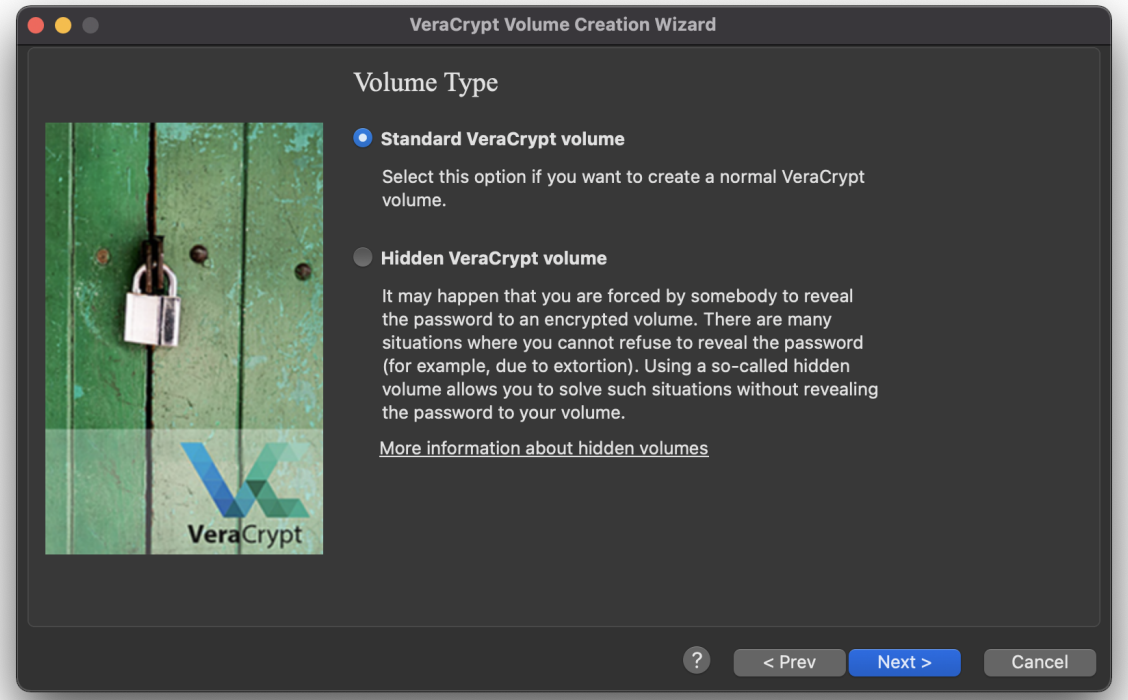
Step 3: Create an encrypted file

Select “Create an encrypted file container” and press “Next>”



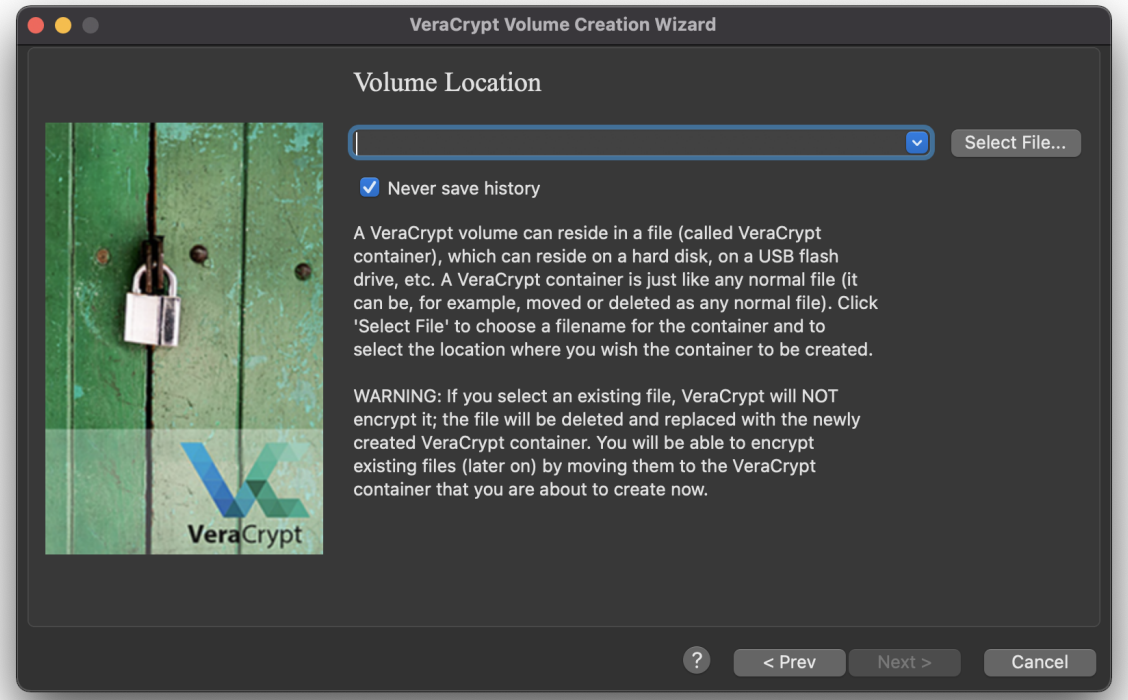
Step 4: Select the volume type

Select “Standard VeraCrypt volume” and press “Next>”



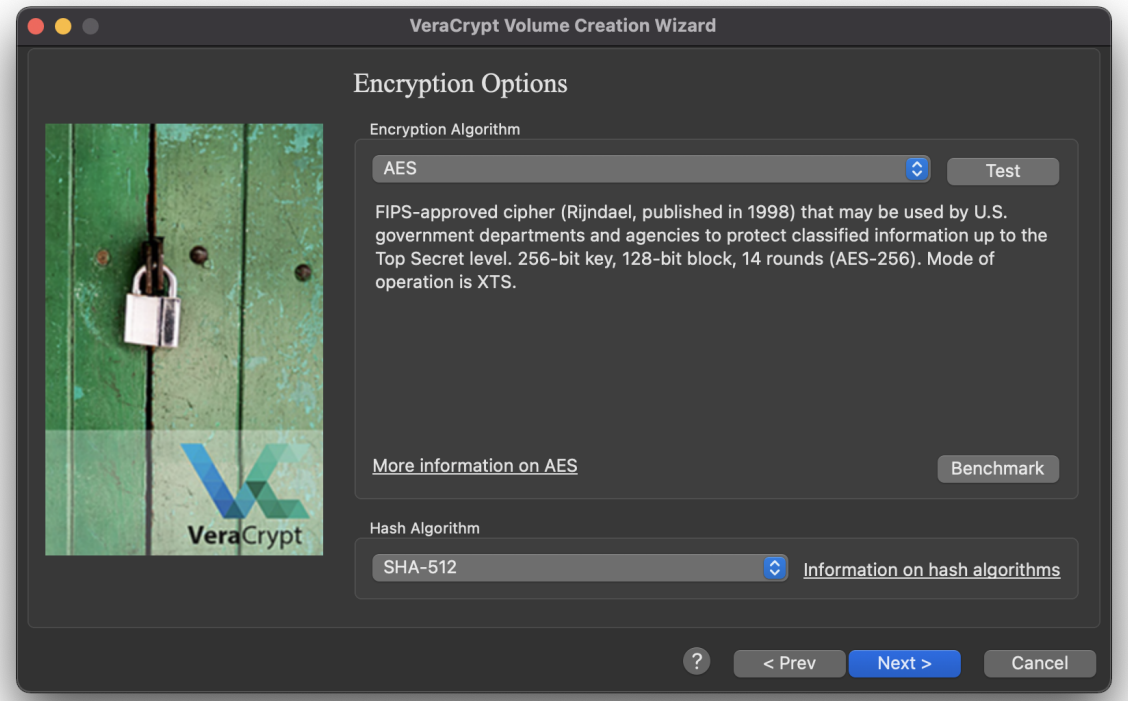
Step 5: Select the volume type

Select the location of the new encrypted file volume and press “Next>”



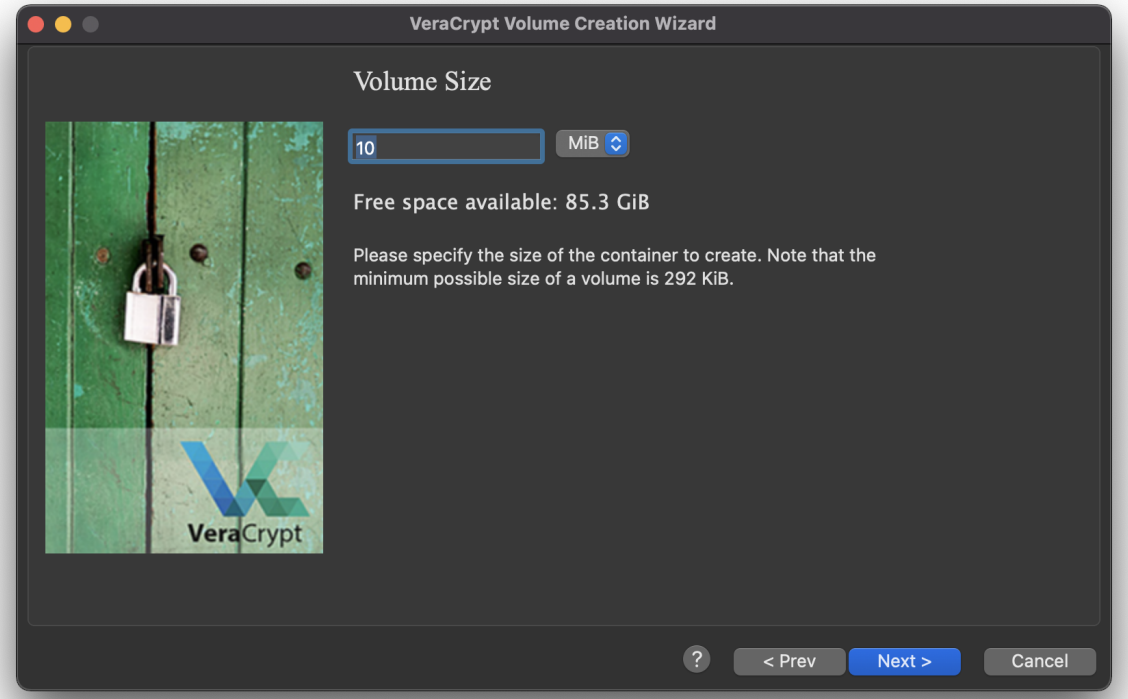
Step 6: Select the desired encryption algorithm

Check that the AES “Encryption Algorithm” and SHA-512 “Hash Algorithm” are selected and press “Next>”.



Step 7: Define the volume dimension

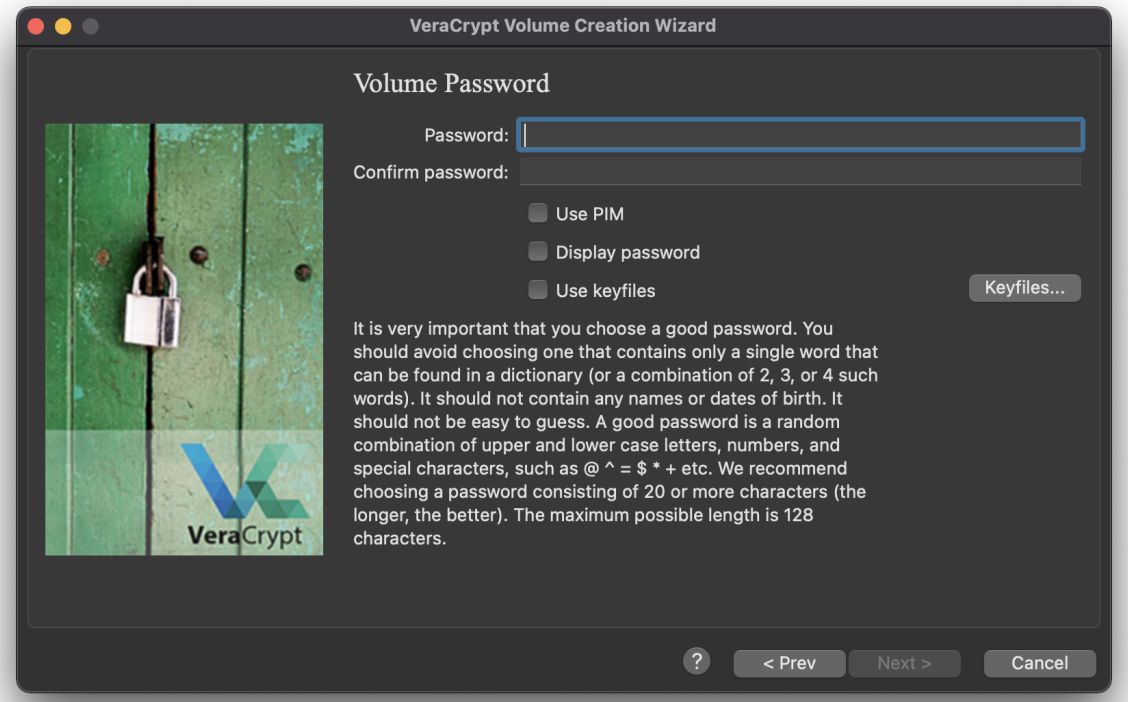
In the example a 10Mb Volume is going to be created, if you desire a bigger volume you can select the desired size and press “Next>”.



Step 8: Set the password with your Secure Key A1

Remember that Veracrypt accepts up to 128 character passwords. You have two different options to secure this file:

1) Share the password C password generated with Secure Key with one media transfer like the email and the D password with other messaging solution like Whatsapp
2) Share only the team **masked password** with some one the already has SecureKey A1 with the same team PINs



Step 9: Open/mount the encrypted file volume with your Secure Key A1

Select the file just created by clicking on “Select File…”, than insert the requested password. Now a new volume will be available on your operative system. Save and update the needed file inside the volume. Remember to unmount all the encrypted volumes with the button “Dismiss all” before shutdown the PC.