

Frequently Asked Questions

General Questions

- [What are you doing now?](#) New
- [How can I register KryptoSpace?](#)
- [What can I do if I have lost my license?](#)

KryptoSpace

- [What happened to KryptoSpace?](#)
- [What encryption algorithm does KryptoSpace use?](#)
- [Why KryptoSpace and not Apple FileVault?](#)
- [Can I use KryptoSpace and FileVault at the same time?](#)
- [Why KryptoSpace and not another application?](#)
- [Should I store my passwords in the system KeyChain?](#)
- [Multiple Passwords?](#)
- [What about backups?](#)
- [What if I change machine?](#)
- [Is KryptoSpace Leopard ready?](#)

ShelfMenu

- [Is ShelfMenu Leopard ready?](#)
- [How much does ShelfMenu cost?](#)
- [Is ShelfMenu still maintained?](#)

General Questions

What are you doing now?

I am working hard for my day job!

Apart from that, I am writing on a technical blog, [OSOMac](#).



You can also follow me on Twitter, [@taglia](#)

How can I register KryptoSpace?

You can purchase a license for KryptoSpace from CeMacSoft [online store](#). You can pay using your [PayPal](#) account, or a credit card.

Once the payment is validated (usually within minutes), you will receive your license by email. Simply double click on the attached file to register the application.

What can I do if I have lost my license?

[Contact us](#) and we will resend you the license.

KryptoSpace

What happened to KryptoSpace?

Given the increasing workload of my day job, I cannot maintain and support KryptoSpace as I should, and I have decided to discontinue the product. This wasn't an easy decision, and most of all I didn't want to leave paying customers without an alternative solution.

The alternative solution is a new product called [Espionage](#); this product is similar to KryptoSpace, but it offers more features and it is better integrated with the system. I have contacted the developer of [Espionage](#), and he kindly agrees to give a discount to all the owners of KryptoSpace.

If you have purchased KryptoSpace on or after October 10, 2008, feel free to request a full refund.

What encryption algorithm does KryptoSpace use?

KryptoSpace is based on the same technology as Apple FileVault. Your data is encrypted using [AES-128](#); on Mac OS X 10.5 Leopard, it is possible to use [AES-256](#).

Why KryptoSpace and not Apple FileVault?

As all Apple products, FileVault is extremely easy to use and responds perfectly to the need of most users. That being said, if you want more flexibility, FileVault is not the ideal solution. The main disadvantages of FileVault are the following:

1. Your entire home folder is encrypted: as nothing is excluded, the disk image containing your data can be huge. If you do not log out and compact the FileVault regularly, you can quickly run out of space, with serious consequences for the operating system;
2. If you work with big media files (movies, music, raw photos, etc.), they will be encrypted as well, with a visible impact on the performance of your system;
3. Once you log into your account, the FileVault is open, and all your information is accessible. This can be a problem if somebody else has access to your account.

KryptoSpace allows you to encrypt only the information that you

want to protect. In this way you can protect data even though others can access your account, and the size of your encrypted data can be manageable.

Can I use KryptoSpace and FileVault at the same time?

Yes.

Why KryptoSpace and not another application?

The difference between KryptoSpace and other products to create and use encrypted disk images is the following: KryptoSpace can transparently *mount* your data in the same location where you expect them to be. This allows you to encrypt data folder used by every application and have these applications work seamlessly.

Consider the following example: you have confidential email messages in your mailbox, and you want to protect them. With KryptoSpace you can encrypt the email data, so that they will be invisible and inaccessible for other users, but will appear as usual for your mail application. In this way you can encrypt important data with minimum impact on your workflow.

Should I store my passwords in the system KeyChain?

It depends. If you store your passwords in the KeyChain, it will be easier to mount your encrypted folders (this can even be done automatically during the login), but people with access to your account will have access to all your encrypted data.

If you do not store your passwords in the KeyChain, you will have to manually authenticate every time you need to mount an encrypted folder, but nobody without the specific folder's password will be able to access the information.

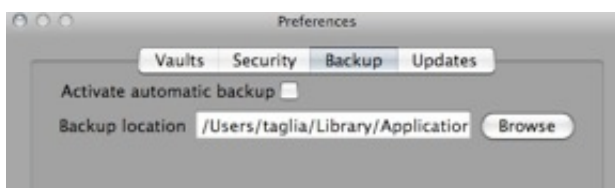
Can I use different passwords for different folders, and store only some of them in the system KeyChain?

You can use different passwords for your encrypted folders, and store some of them in the system KeyChain.

What about backups?

KryptoSpace can automatically back up your data. The backup files are encrypted and can be done on an external hard disk or on a networked volume.

FAQ



What if I change machine?

KryptoSpace can export your folders from your old machine and import them in the new one.

Is KryptoSpace Leopard ready?

Yes.

ShelfMenu

Is ShelfMenu Leopard ready?

Yes.

How much does ShelfMenu cost?

Nothing ShelfMenu is Freeware.

Is ShelfMenu still maintained?

The application is maintained, but we have no release date for a new version.

If you have any problem with the application, do not hesitate to [contact us](#).

If you can't find the answer to your question here, do not hesitate to [contact us](#).