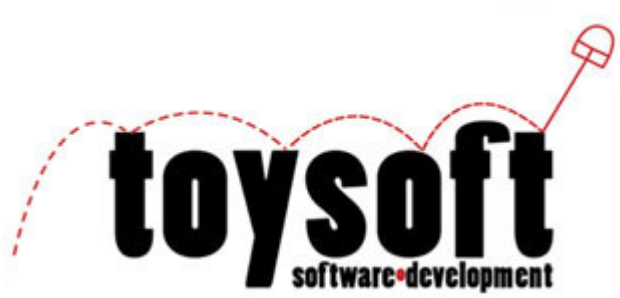


mEncryptor™ 1.4
User Documentation

www.toysoft.ca

Table of Contents

1. Introduction

mEncryptor™ is robust and advanced PalmOS® file media encryption application. mEncryptor™ implements the industry standard AES 256 bits encryption algorithm and SHA1 hashing technologies. mEncryptor™ supports the following external medias: SD/MMC®, Compact Flash® and Sony Memory® stick. mEncryptor™ does not do transparent encryption. mEncryptor™ can encrypt individual files or the entire directory including subdirectories on the card. A secure folder can be setup when the Palm goes to sleep mEncryptor™ will automatically encrypt all the files. When the Palm awakes mEncryptor™ will authenticate you before it will decrypt all the files in the secure folder.

Original file is wiped after encryption. This eliminates anyone from recovering the original file using restore utilities.

mEncryptor™ has the traditional text passphrase entry and the new keypad passphrase entry. mEncryptor ™ is compatible with PalmOS® 3.5 and higher including PalmOS® 5.0 Palm® Tungsten T and Sony® NX.

2. System Requirement

- PalmOS® 3.5 and higher.
- Virtual File System manager is required for Handspring® Visors.
- External card is required.
- 200K of free memory.

2.1 Compatibility

- Palm® Tungsten T, Palm® Tungsten W, Palm® M125, Palm® M130, Palm® M500, Palm® M505, Palm® M515 and Palm® i705, Treo® 600/650, LifeDrive
- Handspring® Visor, Prism and Treo series. (Visor and Prism requires Virtual File Manager installed)
- Sony Clie® series
- HandEra®
- Kyocera® with external card
- Samsung®
- Legend®
- Acer®

3. Installation

To install mEncryptor double click on the files mEncryptor.prc, AESLib.prc and SHALib.prc

Press the HotSync® button on the cradle. The HotSync® manager will install the files on to your Palm.

4. Launching mEncryptor™

Look for the mEncryptor™ icon mEncryptor in the Launcher. If you cannot find it, scroll down using the down arrow.

5. User Interface

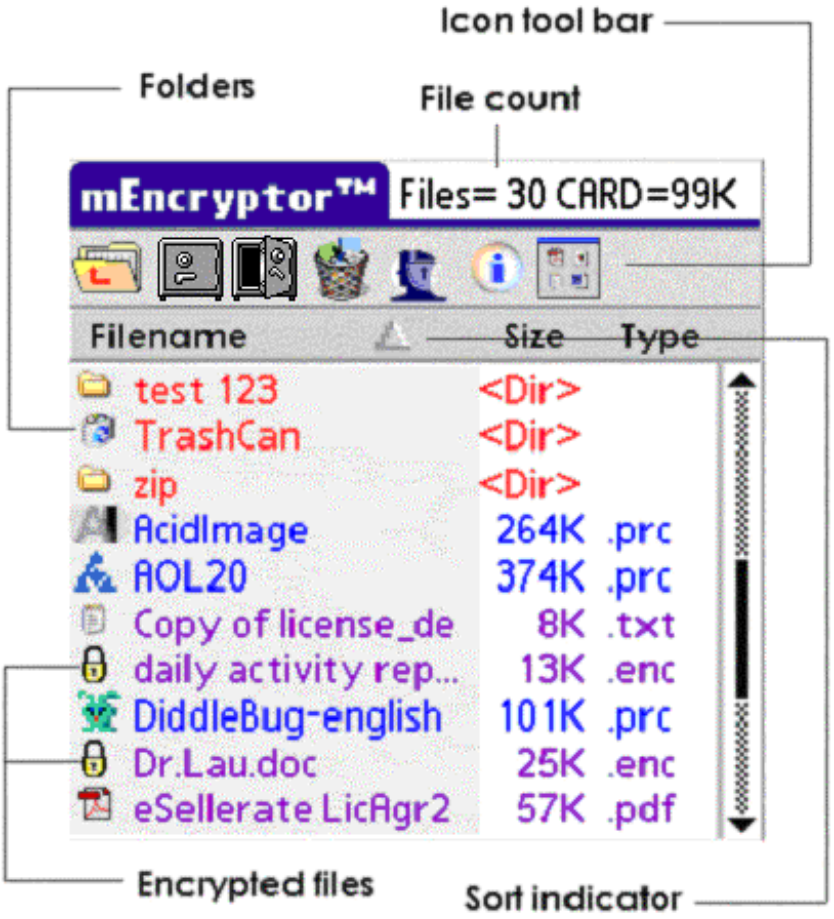


Diagram 1: Main screen.

5.1 Icon Tool bar

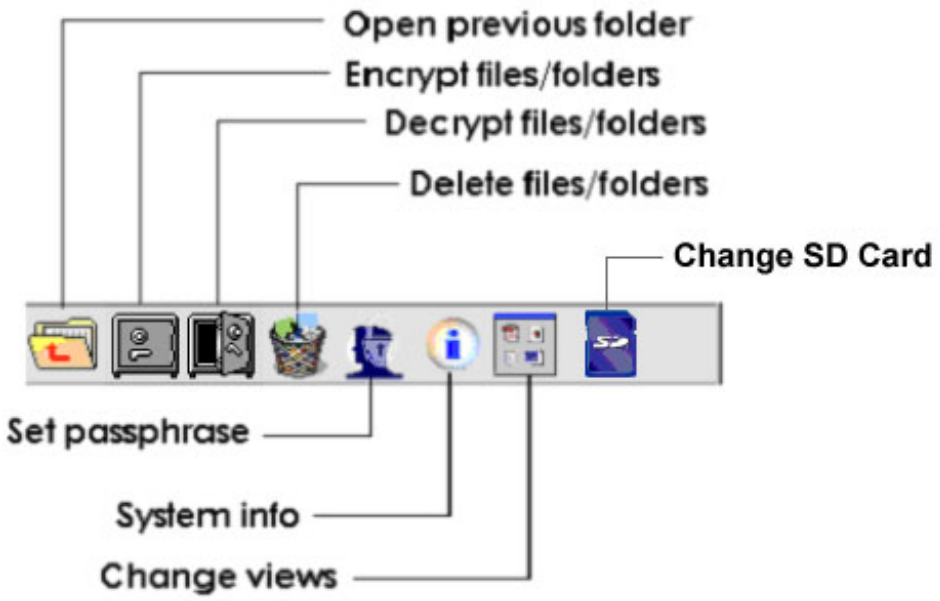


Diagram 2: Icon tool bar.

 **Previous Folder** – Open the previous folder. This only works if you are browsing files on the card.

 **Encrypt** – Encrypt all the selected files or folders. Sub folders will also be encrypted. The original files will be deleted.

 **Decrypt** – Decrypt all the selected files or folders. Sub folders will also be decrypted. The original files will be deleted.

 **Delete Files** – Delete all the selected files or folders. When deleting a folder on the card all subfolders will be deleted. Be careful when deleting folders on the card.

 **Passphrase** – To set or change your passphrase. When you change your passphrase the entire card will be scanned and encrypted files will be decrypted with your current passphrase first.

 **System Info** – Get information about your Palm device such as RAM left and card memory.

 **View Types** – To switch to different view types. You can also sort by type and creator id. Its useful to sort all zipped files by type.

 **Media Card** – To switch to a different media card tap on the icon. On Palms with 5-way d-pad you can select the Center button to select media card. The media feature is available on devices that have multiple cards such as Treo® 650, Tungsten T5/TX and LifeDrive.

5.2 mEncryptor ™ Menus

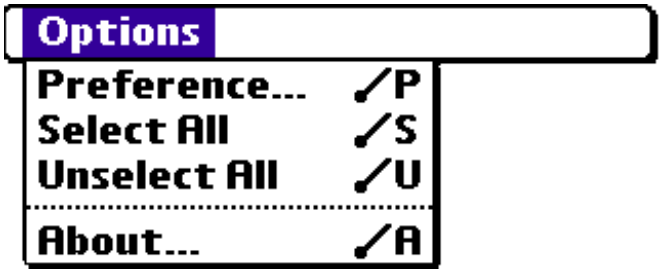


Diagram 3: Menus

5.2.1 Preferences

Diagram 4: Preference

☐ Turn on icon help

If checked whenever you tap on an icon, a help text will be shown.

☑ Prompt when deleting files

If checked you will be prompted before files are deleted.

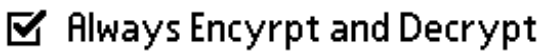
☑ Use Keypad

If checked the Keypad passphrase entry dialog will be used. mEncryptor™ will decrypt all the files on the card first. This process could take several minutes. (Depends how large the external card is and the amount of encrypted files)

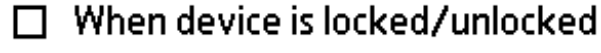
☐ Encrypt the headers only

If this is checked mEncryptor will only encrypt the first 1K of the header file. This is lazy encryption. This feature isn't very useful but it does protect image files from loading and viewing such as JPG, BMP ,MP3 and movies files.

If this is checked mEncryptor will wipe the original file after the file encrypted. This will protect you from people trying to recover the original file. Without wiping the file the original file may be still somewhere on the card. When deleting the file the PalmOS® just changes the file attribute and return the space back to the file system. With a file recovery utility on the Desktop computer you can recover deleted files.



If checked then you must select a secure folder by tapping on the toggle button. A window will be opened to let you select the secure folder. Whenever the Palm goes to sleep mEncryptor™ will encrypt all the files in the secure folder. When the Palm awakes you must authenticate before mEncryptor™ will decrypt all the files in the secure folder.



If this is checked mEncryptor will only encrypt the files in the secure folder if the system security locks the device down. You will need to have entered a passphrase in the Security application for this feature to work. This feature is useful if you use your Palm often during the day and only lock the device after hours.

If your Palm has multiple cards then you can select which card to default the Secure folder.

Select the Secure folder to use. The entire folder including sub folders will be encrypted.

6. Assigning and changing your Passphrase

The first step in configuring mEncryptor™ is to assign your secret passphrase. Your secret passphrase must be at least 3 characters long. Your passphrase may contain any characters, digits, symbols, punctuations, or non-printable characters. Do not use any passphrase like your birthday, bank account PIN number, your telephone number etc… Your secret passphrase should contain mixture of characters and digits.

6.1 Create Random Data

There are two steps in assigning your passphrase. The first step is you must create some random data. The random data is the key that will be used to encrypt and decrypt all the files. The random data (key) will then be encrypted with your secret passphrase.

Diagram 5: Create random key

To create the random data you must tap around the screen until the status displays **100 Percent Completed** and the **OK** button is shown. Try not to tap on the same area on the screen. Use the entire screen. To cancel the passphrase change, select the **Cancel** button.

6.2 Set Passphrase

When changing your passphrase, first you must be authenticated. mEncryptor™ will prompt you for your current passphrase. You have three chances to get your passphrase correctly. Once you are authenticated the following screen will be shown.

Diagram 4: Set passphrase

Enter your secret passphrase in the field **Passphrase:**, you will be required to verify your passphrase in the **Verify:** field. Tap the **OK** button when you are done. To cancel the passphrase change, tap on the **Cancel** button.

Tap on the  or  softkey to display the system keyboard if you need it to.

If both fields are the same mEncryptor™ will hash your passphrase using SHA1. Your secret passphrase is **never** saved anywhere on your Palm. Only the hash of your secret passphrase is saved. The hash is used for authentication only, such as when you launch mEncryptor™.

The key will be saved on the card in the *Palm/Launcher* folder called mEncryptor.key. Do not delete or modify the key file. If the key is corrupted or is missing your data will not be decrypted properly.

7. Keypad Passphrase Dialog

The Keypad is an alternative passphrase entry to the traditional text passphrase entry. The Keypad will be used if it's selected in the Options screen. The Keypad has a limited numbers of combinations. The Keypad uses the following keys [0,1,2,3,4,5,6,7,8,9,*,#] therefore the secret passphrase to choose may not be as secure as the one with the traditional text passphrase. When assigning your passphrase using the Keypad do not use a pattern passphrase. Eg: the L (147*0#), 7 (12369#). It is too easy to guess.

Diagram 5: Keypad Passphrase Dialog

8. mEncryptor™ Browser

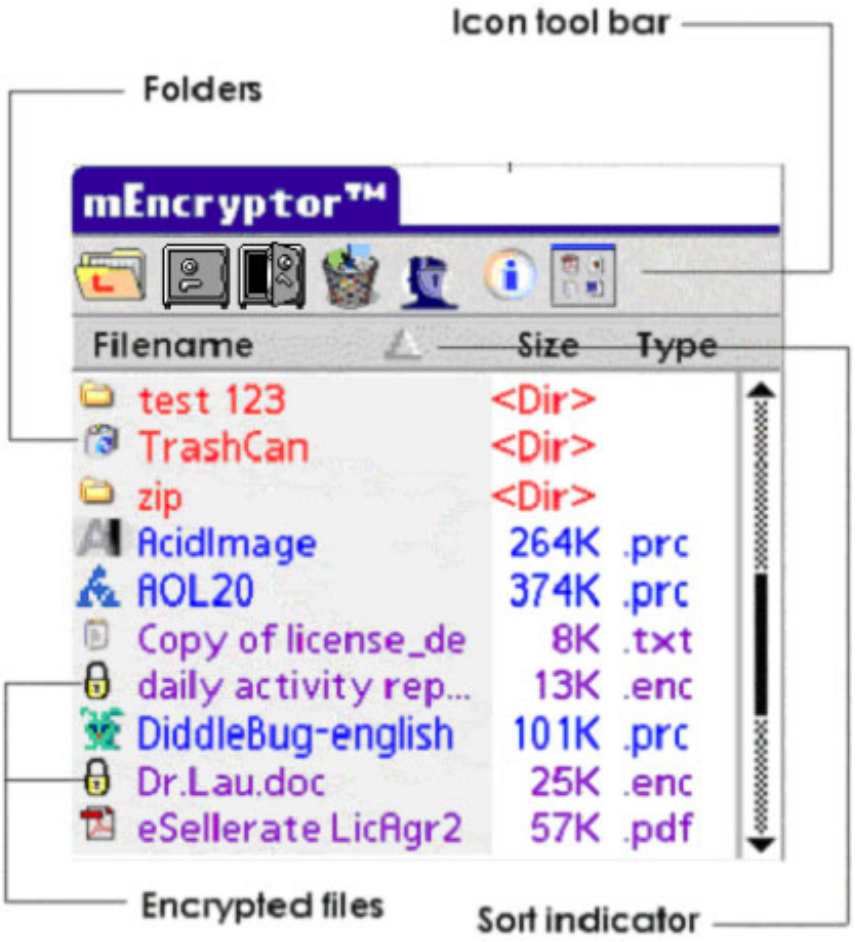


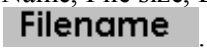
Diagram 6: Browser

When a file is encrypted  the file extension for be **.enc**. This indicates the file is encrypted. Also the icon will be changed to the locked icon  .

When a file is encrypted on the card the file extension .enc will be added to the original file. Eg: Dr.Lau.doc.prc will become Dr.Lau.doc.prc.enc.

Note: do not change the extension name or modify the file. If file becomes corrupted mEncryptor™ will not be able to decrypt it correctly.

8.1 Sorting

By default the browser is sorted by Name. You can sort by Name, File size, Date, Creator Type and Creator ID. To sort the browser list, tap on the column title 

. The arrow  indicates sort is in ascending. To sort in descending  order tap on the sort column title again. To sort by Creator Type or Creator ID select the View icon  .

8.2 Folders

To open a folder, double tap on the folder. You can encrypt the entire folder. All the files in the folder and subfolders will be encrypted.

8.3 Quick key

To quickly jump to a file you can press or enter the first letter of the file name and mEncryptor will scroll to there.

8.4 Go to Previous Folder

To go back to the previous folder you can press the Left arrow key on the 5-Way.

9. Secure Folder

If you have information that you access regularly on the card and want to secure it then you can use the Secure Folder feature. Any files and subfolder in the secure folder will be encrypted when the Palm goes to sleep. When the Palm awakes you will be prompted to authenticate before mEncryptor™ will decrypt all the files in the secure folder. If you failed to authenticate then the secure folder will remain encrypted. You will have to manually select the files or folder to decrypt using the mEncryptor™ application.

If you have many files in the secure folder it will take time to encrypt and decrypt when the Palm shuts down and starts up. You should only put files in the secure folder that you will use daily.

Do not recommend you to set the secure folder to /Palm or any root folder.

10. mEncryptor™ Limitations

The following are limitations in mEncryptor™

- mEncryptor™ does not do transparent encryption/decryption. You must manually select the files to encrypt.
- If your device is reset or a system crash occurred during encryption and decryption, mEncryptor™ will not recover any data lost. Eg: if mEncryptor™ is encrypting a record and you do a reset. Half of the record will be encrypted and the other half is not. This could cause application fatal errors when the application tries to read the corrupted data.

11. Cryptographic References

ADVANCED ENCRYPTION STANDARD (AES)

http://csrc.ncsl.nist.gov/encryption/aes/aesfact.html

SECURE HASH STANDARD

http://csrc.ncsl.nist.gov/publications/fips/fips180-2/fips180-2.pdf

PalmOS® SHA1 Library by Duncan Shek Wong used in mEncryptor™

http://www.ccs.neu.edu/home/ahchan/wsl/PalmCryptoLib/SHA/

PalmOS® AES Library used in mEncryptor™

12. Copyright

Ownership rights and intellectual property rights in and to the Software shall remain in Toysoft, Inc. The Software is protected by the copyright laws of Canada and international copyright treaties. This License gives you no rights to such content.

13. Disclaimer

(a)DISCLAIMER OF WARRANTY. The Software is provided on an "AS IS" basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement.

(b)You and not Toysoft, Inc. assume the entire cost of any service and repair. In addition, mechanism implemented by the Software may have inherent procedural limitations, and you must determine that the Software sufficiently meets your requirements.

(c)This disclaimer of warranty constitutes an essential part of the agreement.

(d)Due to the nature of encryption Toysoft, Inc. is not responsible for data lost.

14. Limitation of Liability

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT, OR OTHERWISE, SHALL TOYSOFT, INC. OR ITS SUPPLIERS OR RESELLERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES.

15. Termination of License

This license will terminate automatically if you fail to comply with the limitations described above. On termination, you must destroy all copies of the Software

16. Technical Support

For technical support please send email to support@toysoft.ca or visit our website at www.toysoft.ca