Toysoft Inc.
mobile and software development

SecureCard™ 1.0
User Documentation

www.toysoft.ca

Table of Contents

1. Introduction

SecureCard™ is a robust and the most advanced PalmOS® transparent media encryption application today. SecureCard™ implements the industry standard AES 256 bits encryption algorithm and SHA1 hashing technologies. Files are encrypted and decrypted transparently without any user intervention. Files are encrypted until the correct passphrase is entered before it is decrypted. All passphrase entries are masked from the public view. SecureCard™ has the traditional text passphrase entry and the new randomized keypad passphrase entry.

SecureCard™ can encrypt any type of files stored on the SD/MMC/MS/CF such as .doc, .xls, .pdf, .txt, .jpg, etc.

A powerful Files Filter database enables to you select only important files to be encrypted or you can create single or multiple secure folders. Any files in the secure file and the sub folders are automatically encrypted and decrypted transparently.

SecureCard™ is compatible with PalmOS® 5.0 and higher including the Treo® 600 and 650 smart phones.

1.1 Why use SecureCard™?

Information stored on external memory card is not secure. Data are not encrypted and can easily viewed and stolen. Anyone can remove your external memory card and read it on the desktop computer with a card reader. By using encryption it gives you a new level of security and piece of mind.

What makes SecureCard™ better than the PalmOS® Security application and all other 3rd party security applications on the market?

- SecureCard™ uses the AES 256 bits encryption that works with PalmOS® 5.0 and higher
- Compatible with PalmOS® 5.0 and higher.
- Files are encrypted on the external card.
- SecureCard™ is the only encryption application that supports secure folders.
- Keypad passphrase entry for quick access with randomized keypad. Hackers will not be able to guess your passphrase from your finger markings on the screen.
- Impossible to view the encrypted file without a valid passphrase.
- Passphrase entries are masked

- Transparent encryption
- Compatible with Palm® Treo® 600 and 650
- Intuitive user interface

2. System Requirement

- PalmOS® 5.0 and higher
- 150K of free main memory
- External card such as SD/MMC/Compact Flash/Memory Stick

2.1 Compatibility

- Palm® Treo 600 and Treo® 650
- Palm® Zire 21/22/71/72 series, Palm® C, Tungsten E/E2/T/T2/T3/T5/TX series, Palm® LifeDrive
- SonyClie® with PalmOS® 5.0 and higher
- All other Palms with PalmOS® 5.0 and higher

3. Installation

Using the HotSync® Quick Install program add the following file to the Hotsync queue.

- SecureCard.prc - SecureCard™ PalmOS® application

3.1 SHA1 and AES Libraries

You will also need to install the encryption libraries in the **Libs** folder.

- AESLib.prc - AES encryption library
- SHALib.prc - SHA1 hashing

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

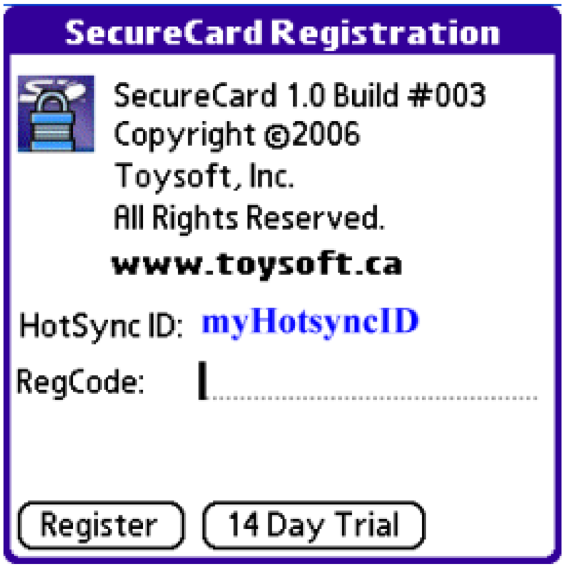
SecureCard.prc, AESLib.prc and SHALib.prc must be installed to main memory and cannot be installed to the external card.

4. Registering SecureCard™ After You Purchased SecureCard™

After you have installed all the files, launch SecureCard and you will see the following screen below.

You will need to write down your **HotSync® ID** to use for generation of your Registration Key. Send your HotSync ID to support@toysoft.ca for your registration key.

When you get your Registration Key, launch the **SecureCard** application again and enter the Registration Key into the RegCode: input area and tap the **Register** button. You will only have to do this once.



SecureCard Registration

SecureCard 1.0 Build #003
Copyright ©2006
Toysoft, Inc.
All Rights Reserved.
www.toysoft.ca

HotSync ID: myHotsyncID

RegCode:

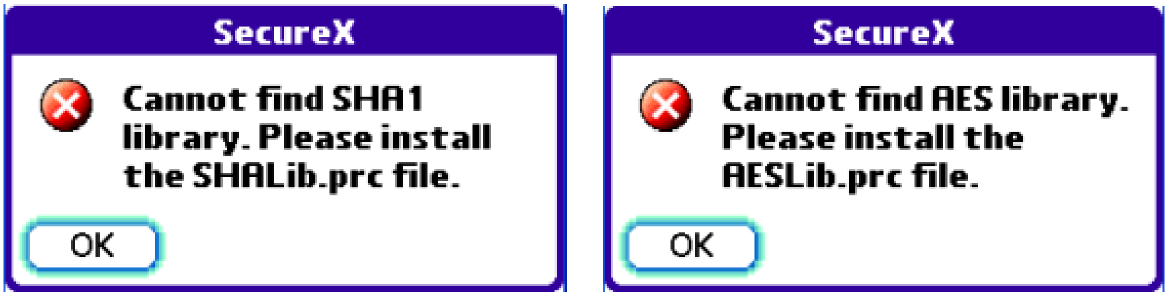
Diagram 1: SecureCard registration

For a 14 day trial tap on the 14 Day Trial button.

5. Launching SecureCard™

To launch SecureCard™, look for the icon SecureCard on the Launcher and tap on it.

If you get the following error messages after you have launched SecureCard™, then you did not install all the encryption libraries correctly. Refer to section 3. Installation.



Cannot find SHA1 library. Please install the SHALib.prc file.

Cannot find AES library. Please install the AESLib.prc file.

Diagram 2: Encryption library errors

6. User Interface

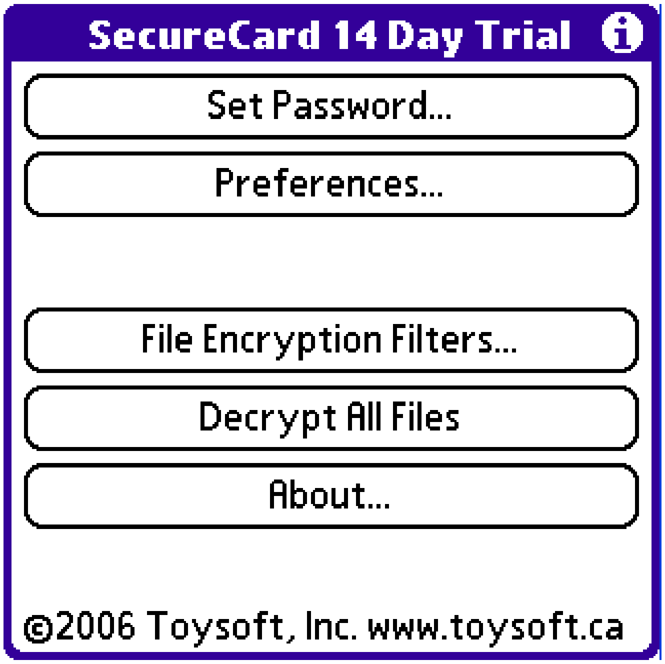
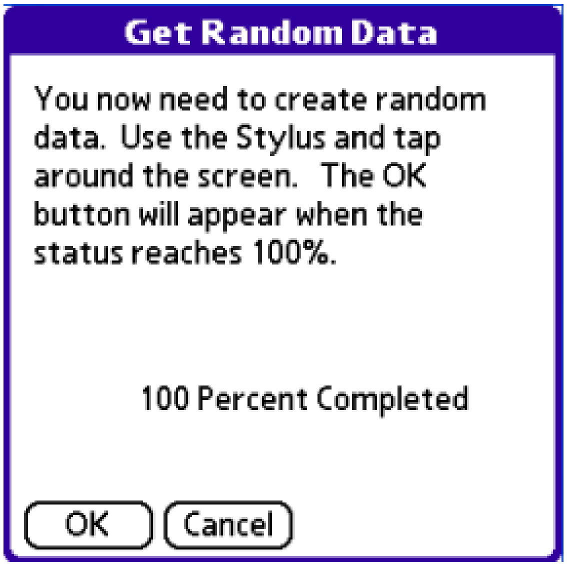


Diagram 3: Main Screen.

Buttons	**Description**
Set Password…	Create a new password or change the current password
Preferences…	Open SecureCard™ preferences screen
File Encryption Filters…	Select the files to encrypt or set secure folders
Decrypt All Files	Decrypt all the files in the Encryption Filter db
About…	Show the About screen

7. Set and Change Password

To set a new password or change your current password, tap on the Set Password... button. If you are changing your password then you must authenticate first. The following screen will appear.



Get Random Data

You now need to create random data. Use the Stylus and tap around the screen. The OK button will appear when the status reaches 100%.

100 Percent Completed

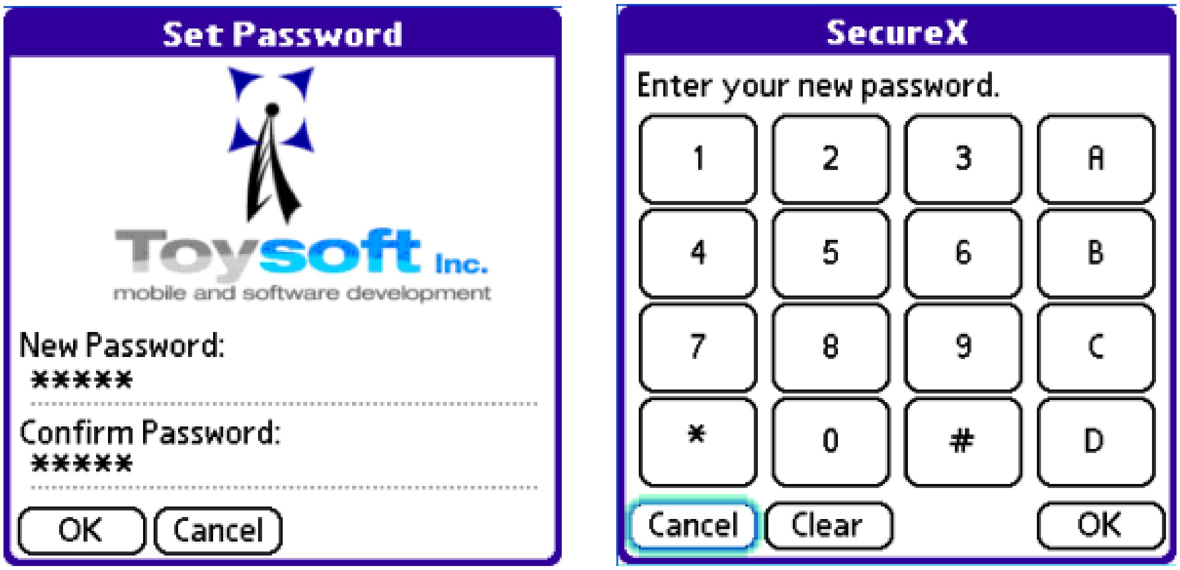
Diagram 4: Create random key

7.1 Create random key

The first thing you must do is to create the random key. The random key is used to encrypt and decrypt data. The random key is never exposed to anyone. It is always stored in encrypted form when it not used.

To create the random key, use the Stylus and tap around the screen until the OK button appears and then tap on the OK button continue.

7.2 Assigning a Private Password



Set Password

New Password:
*****

Confirm Password:
*****

SecureX

Enter your new password.

Diagram 5: Assign private password. Text and Keypad entries

The final step is to assign your private password. This is the password you will use for all authentications. Enter the private password in the New Password: field and then enter the password again in the Confirm Password: field.

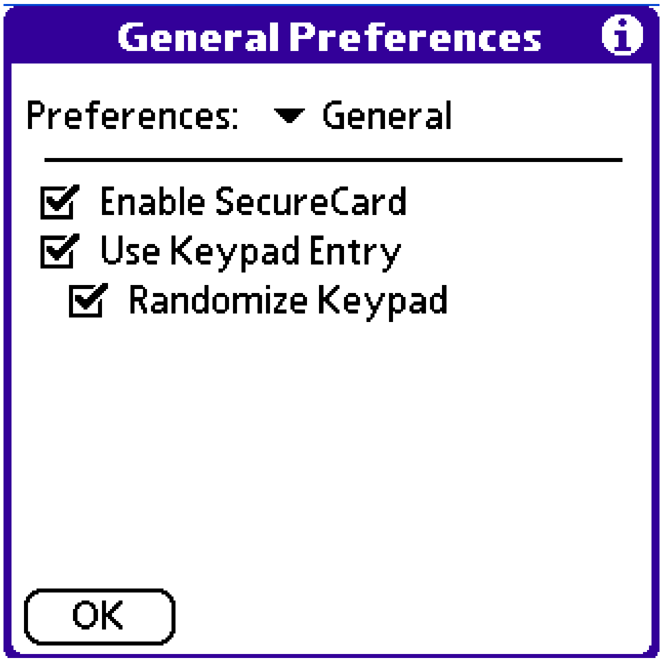
When choosing your private password make sure it is not easily guessed. Do not use password like your birthday, important dates, your favorite pet's name, your bank PIN, phone number etc… Mix the password with characters and digits. Make your password at least 6 characters long.

After you have assigned or changed your password do not give your password to anyone or forget it. If you forget you will not be able to unlock your Palm® and you must do a cold reset and lose all the data and must restore from your last HotSync® backup.

Note: Once you have assigned your password you can change the text entry to the keypad entry in the General Preferences.

8. Preferences

8.1 General Preferences



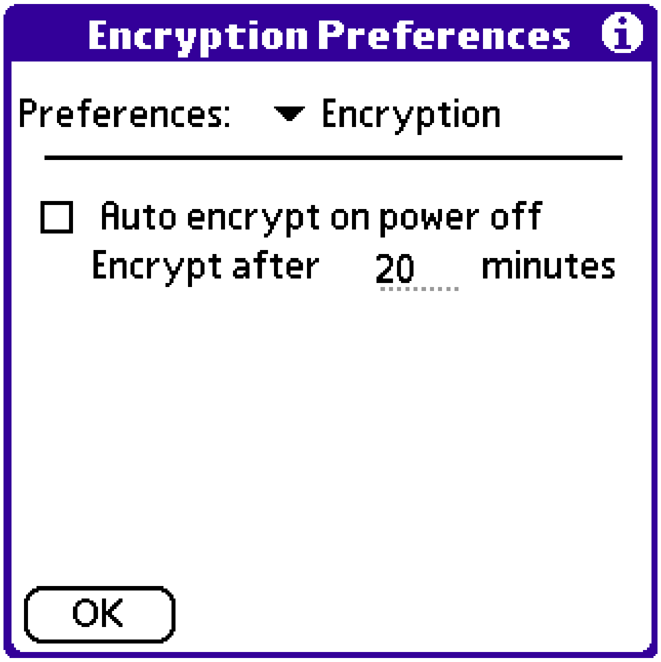
Preferences: ▾ General

☑ Enable SecureCard
☑ Use Keypad Entry
☑ Randomize Keypad

Diagram 6: General Preferences

Controls	**Descriptions**
☑ Enable SecureCard	To enable SecureCard check the checkbox. To uninstall SecureCard uncheck the checkbox.
☑ Use Keypad Entry	Check to use the keypad password entry instead of the text entry. The keypad entry has limited combinations and is not as flexible as the text password entry.
☐ Randomize Keypad	If you want randomize keypad keys then check the checkbox. SecureCard will then mix the keypad buttons so that the buttons are not in the same static place each time. This avoid hackers looking at your finger prints on the screen to guess your password.

8.2 Encryption Preferences



Encryption Preferences

Preferences: ▾ Encryption

□ Auto encrypt on power off

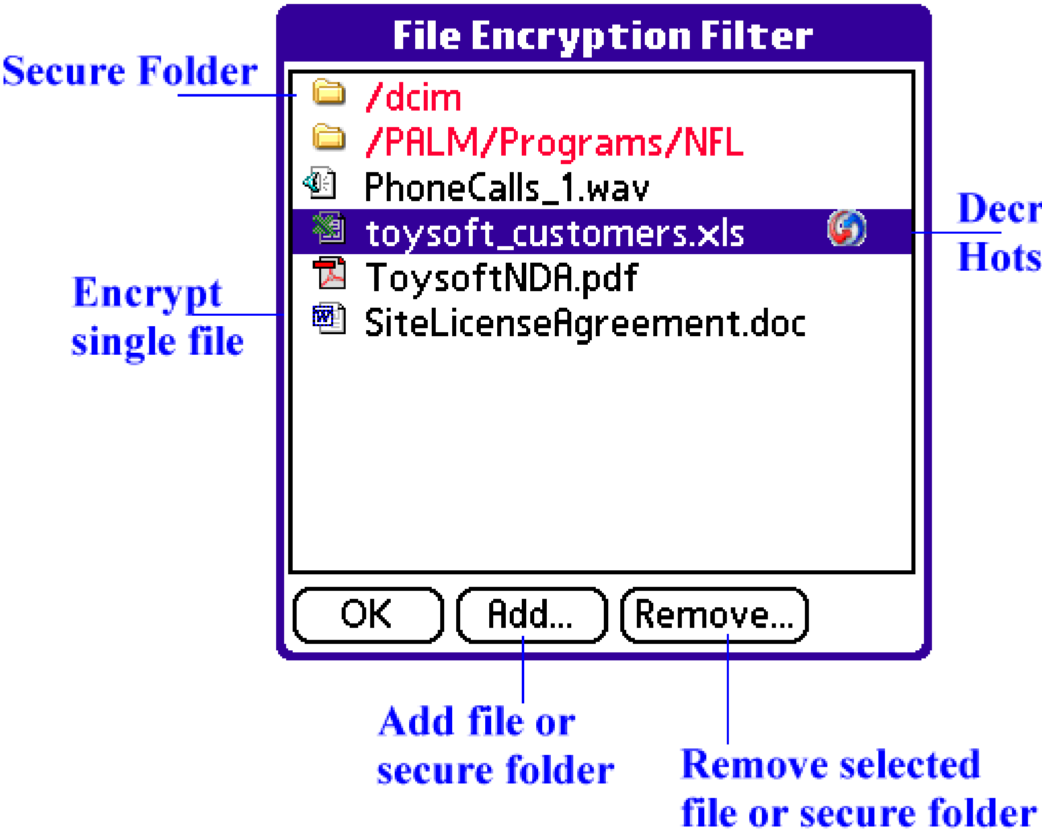
Encrypt after 20 minutes

Diagram 7: Encryption Preferences

Controls	Description
☑ Auto encrypt on power off	Set to auto encrypt when the device is turned off.
Encrypt after 20 minutes	Set to auto encrypted after a specified delay time.

To automatically encrypt all the files and secure folders whenever you turn off the device then check the ☑ Auto encrypt on power off checkbox. If you want to encrypt on a timed event then set the minutes in the Encrypt after 20 minutes field. SecureCard will only encrypt when the device has been idled for the specified amount of time.

9. File Encryption Filters



File Encryption Filter

/dcim

/PALM/Programs/NFL

PhoneCalls_1.wav

toysoft_customers.xls

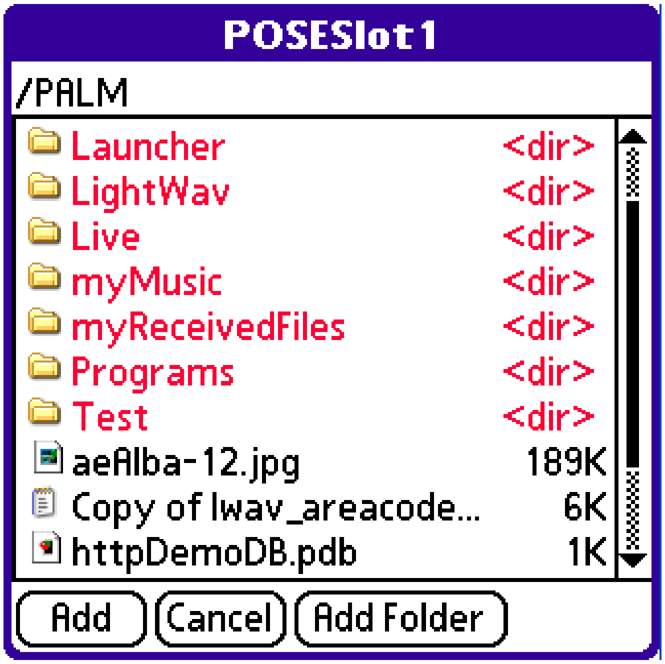
ToysoftNDA.pdf

SiteLicenseAgreement.doc

Diagram 15: File Encryption Filters

File Encryption Filters is a powerful feature in SecureCard™. It enables you to encrypt any file or secure folder on external card with strong AES encryption. SecureCard™ will only decrypt the file that the application opens and leave others encrypted. Transparent encryption is one of the major features of SecureCard™ that stands out from the competition. There are no limitations on the number of files SecureCard™ can encrypt.

To add a file or secure folder tap on the Add… button and the following window will be opened.



POSESlot1

/PALM

Launcher	<dir>
LightWav	<dir>
Live	<dir>
myMusic	<dir>
myReceivedFiles	<dir>
Programs	<dir>
Test	<dir>
aeAlba-12.jpg	189K
Copy of lwav_areacode...	6K
httpDemoDB.pdb	1K

Diagram 15.1: File Encryption Filters

Use the browser to select the file to encrypt or select the folder and then select **Add Folder** button to add it as a secure folder.

You can only select a single file at time to add to the encryption database.

9.1 HotSync® Process

If desktop synchronization is require then you must select the file and then set the Hotsync® flag. Tap on the file or the secure folder and then select **Decrypt on Hotsync...** item.

If the Hotsync flag is not set then during Hotsync process the files on the external card will be synced to the desktop encrypted. Desktop application such as Microsoft® Words will not be able to open the encrypted file.

9.2 Encryption Process

Encryption happens when you turn off the device. This also depends if you have selected to auto lock the device on power off or time delay in the Encryption Preferences. In either case SecureCard™ always encrypt all the files in the File Encryption Filter database when it locks the device.

10. Decrypt All Files

To quickly decrypt all the files you can tap on the Decrypt All Files button on the SecureCard™ main screen.

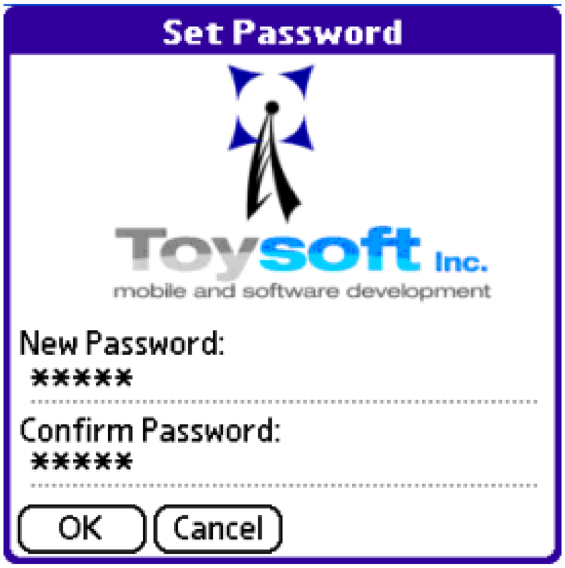
10.1 Encryption and Decryption Speeds

Encryption speeds vary from CPU to CPU among different devices. Also external card speed is another concern. Encrypting the same file in main memory vs external card will result in different speeds. Main memory will always be faster. There are overheads in external card encryption as such data read and write, writing to temp files and wiping the original file. All this contributes to the encryption and decryption speed.

11. Password Authentication Screens

SecureCard™ has two authentication screens.

11.1 Text Entry Screen



New Password: *****

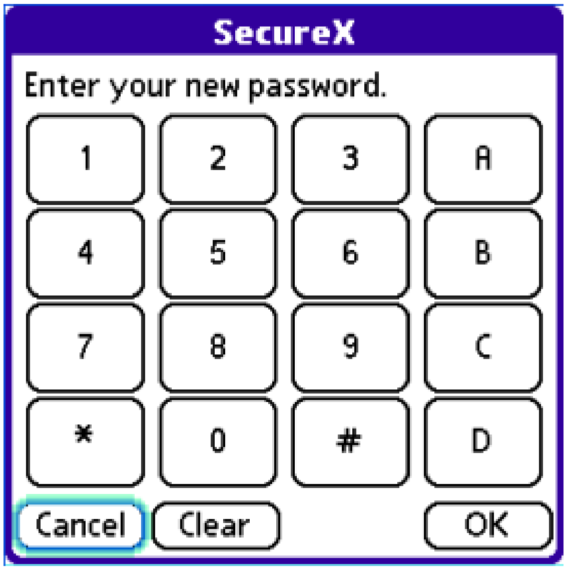
Confirm Password: *****

Diagram 16: Text Entry Screen

The Text Entry screen is the most common screen. You can use any characters in the alphabet, digits 0 to 9 and the punctuations. PalmOS® built in virtual keyboard is not supported because it poses security risks.

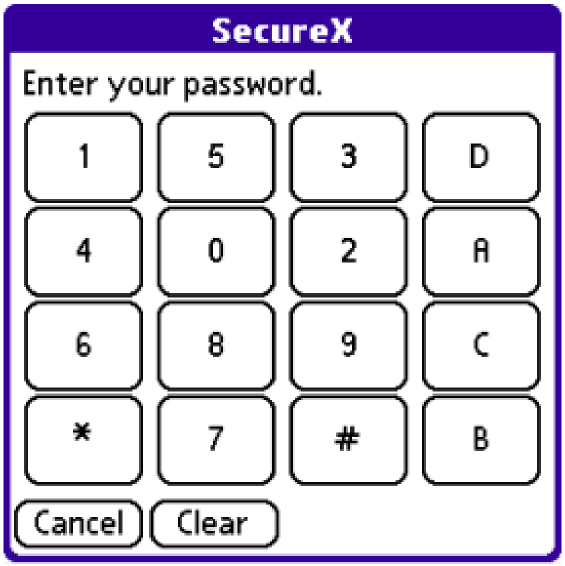
During authentication all hard keys and system events are disabled until you have successfully authenticated. This includes external card insertion or removal, incoming IR beam and application launch.

11.2 Keypad Entry Screen


SecureX

Enter your new password.

Diagram 17: Keypad Entry


SecureX

Enter your password.

Diagram 18: Randomized Keypad Entry

The Keypad entry is not as secure as the Text entry because it only has 16 usable characters but it is easy to enter the password.

When authenticating with the Keypad it works differently than the Text entry because there is no **OK** button. When you enter your password SecureCard™ will validate the password as you enter the password. If you had made a mistake then tap on the **Clear** button and restart again.

11.2.1 Keypad Keyboard Short Cuts

On the Treo® 600/650 you can use the keyboard to enter the password and thus you don't leave your finger markings on the display screen for others to guess your password. You do not need to enter capital letters for ABCD. Just press the abcd keys.

12. Secure Folder

If you have common files you can create a secure folder and put all the files in the secure folder. Any files in the secure folder and sub folders will be encrypted and secured.

Also any files that are created in the secure will be automatically encrypted during shutdown.

Once the files are in the secure folder you do not have to worry about encryption and decryption. SecureCard will handle this transparently in the background. When an application accesses the encrypted file SecureCard will determine if authentication is needed or not. Typically when the device is turned off and you turn if back on authentication is required to access any encrypted files on the external card.

You can create and add as many secure folders as you like. The only drawback is when the device is turned off and SecureCard must encrypt all the files in the secure folder. If there are many files then the encryption will take sometime the first time it encrypts the files.

13. User License

(a) Toysoft Development, Inc. Hereby grants you a non-exclusive license to use its accompanying software product ("Software") according to the following agreement:

(b)You may: Distribute the Software if your application is freeware.

(c) You may not: Distribute the Software if your application is shareware or commercial.

(c)You may not: permit other individuals to use the Software except under the terms listed above; modify, translate, reverse engineer, de-compile, disassemble, or create derivative works based on the Software; copy the Software (except for back-up purposes); rent, lease or otherwise transfer rights to the Software; or remove any proprietary notices or labels on the Software.

Toysoft Development, Inc. reserves all rights not expressly granted to Licensee.

13.1 Enterprise License and SecureCard™ Customization

Please contact Toysoft, Inc. for Enterprise license, customization and volume discounts.

We can customize SecureCard™ to your needs. Here are some of the customization features.

- Have your own corporate logo on the System Logo screen.
- Set minimum passphrase length
- Admin. Policy editor to maximize your corporate security
- File wipes
-

14. SecureCard™ Limitations

The following are limitations in SecureCard™

- If your device is reset or a system crash occurred during encryption and decryption, SecureCard™ will not recover any data lost. Eg: if SecureCard™ is encrypting a record and you do a reset. Half of the record will be encrypted and the other half will not. This could cause application fatal errors when the application tries to read the corrupted data.
- Does not support the Palm® virtual keyboard for passphrase entry.

15. Uninstalling SecureCard™

To uninstall SecureCard™ do the following:

1. Launch SecureCard™ and tap on the **Preferences** button.
2. You will be prompted, authenticate. Tap on the **Enabled SecureCard** checkbox. SecureCard™ will decrypt all the secured databases and will do a soft reset.
3. After the soft reset is completed, go to the Launcher and from the **App** menu select **Delete…** menu item.
4. Look for **SecureCard** name in the list. Select it and then tap on the **Delete** button.
5. Look for the SHALib and AESLib and delete them.

16. Upgrading SecureCard™

To upgrade SecureCard™ to the newer version first you must uninstall SecureCard™. This will disable SecureCard™. You can then install and HotSync® the new version.

17. HotSync®

During the HotSync® process SecureCard™ decrypts all the files that are marked for HotSync®. This is needed because desktop conduits cannot handle encrypted databases.

18. 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 SecureCard™

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

PalmOS® AES Library used in SecureCard™

Copyright (c) 2006, Copera, Inc.,
Mountain View, CA, USA.
All rights reserved.

19. Copyright

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

20. 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.

21. 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.

22. 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

23. Technical Support

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