Toysoft Inc.
mobile and software development

SecureX™ 1.3
User Documentation

www.toysoft.ca

Table of Contents

1. Introduction

SecureX™ is a robust and the most advanced PalmOS® security application today. SecureX™ implements the industry standard AES 256 bits encryption algorithm and SHA1 hashing technologies. Application databases are encrypted and decrypted transparently without any user intervention. The PalmOS® handheld is locked until the correct passphrase is entered before the handheld is unlocked. All passphrase entries are masked from the public view. SecureX™ has the traditional text passphrase entry and the new randomized keypad passphrase entry.

SecureX™ can be used to protect application from launch and requires user authentication before the application or control panel is launched. This is a great way to share your handheld with others if you do not want others to launch private applications or view private data.

Application alarms are handle properly by SecureX™ and with the SecureX™ reminder alarm feature you can be sure that you will never miss your alarms. SecureX™ is the only security application that can handle alarms. All other security applications with encryption do not allow alarms and thus you miss important appointments.

SecureX™ is compatible with PalmOS® 3.5 and higher including PalmOS® 5.0 and the Treo® 600 and 650 smart phones.

1.1 Why use SecureX™?

Information stored on your Palm® handheld is not secure. Data are not encrypted and can easily viewed and stolen. It only takes a few seconds to beam your entire Address Book to another device. Even if your Palm handheld is locked there are ways to get the data. By using encryption it gives you a new level of security and piece of mind.

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

- SecureX ™ uses the AES 256 bits encryption that works with PalmOS® 5.0 and higher
- Compatible with PalmOS® 3.5 and higher.
- Records are encrypted and not just masked.[1]
- SecureX ™ is the only security application that works properly with all alarms. Even if the databases are encrypted[2] and not just one application.
- 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 gain access to the device without a valid passphrase.
- Passphrase entries are masked[3]
- Transparent encryption
- Restore from any backup copies from the external card
- Application database filters and Application Launch Protections.
- Compatible with Palm® Treo® 600/650/700p/680
- Intuitive user interface

[1] On the built-in PalmOS® security application records are not encrypted.

[2] Most security applications do not encrypt databases that have alarms set or do not support alarms.

[3] Passphrase in the Owner information and viewing private records are not masked.

2. System Requirement

- PalmOS® 3.5 and higher
- 150K of free main memory.

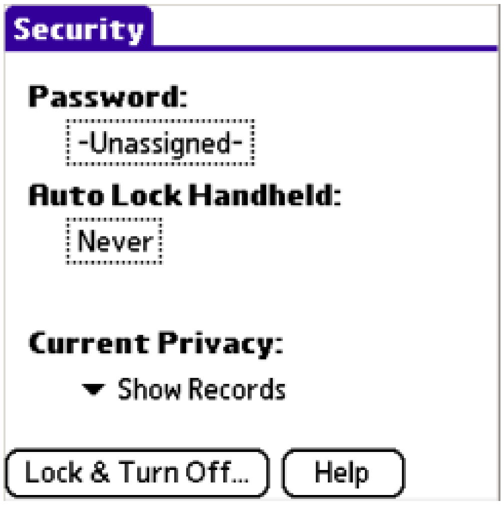
2.1 Compatibility

- Palm® Treo® 600/650/700p/680
- Palm® IIIc, Palm® Vx, Palm® M500/M505, Palm® Zire 21/22/71/72 series, Palm® W, C, Tungsten E/E2/T/T2/T3/T5/TX series, Palm® LifeDrive
- SonyClie® with PalmOS® 3.5 and higher
- Handspring® with PalmOS® 3.5
- All other Palms with PalmOS® 3.5 and higher

3. Installation

3.1 De-activate PalmOS® Security Application

Before you install SecureX™ make sure the Palm® Security application is not active. Please make sure the Palm® Security application looks like the following diagram.



Security

Password:
-Unassigned-

Auto Lock Handheld:
Never

Current Privacy:
▼ Show Records

Diagram 1: Palm®OS Security

3.2 PalmOS® 3.5, 4.x, Treo® 600/650/700P/680 and Sony Clie® and Non Palm Devices

Using the HotSync® install program add Security.prc file to the queue in the **Others** folder.

- Security.prc - SecureX ™ PalmOS® application

3.3 PalmOS® 5.x Tungsten E/E2/T/T2/T3/T5/TX, C and Zire 21/22/71/Zire72 and LifeDrive®

Using the HotSync® install program add the following files to the queue in the **Tungsten** folder.

Security.prc	- SecureX ™ PalmOS® application
SecureXPanel.prc	- SecureX ™ Panel application
Contacts-PAdd.PRC	- Contacts Template
Calendar-PDat.PRC	- Calendars Template

3.4 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.

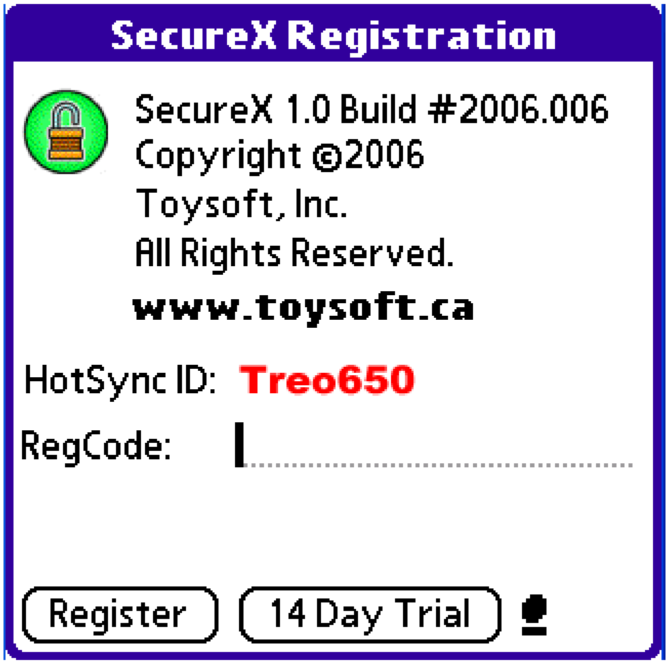
Security.prc, AESLib.prc and SHALib.prc must be installed to main memory and cannot be installed to the external card.

4. Registering SecureX™ After You Purchased SecureX™

After you have installed all the files, launch SecureX 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 **SecureX** 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.



SecureX Registration

SecureX 1.0 Build #2006.006
Copyright ©2006
Toysoft, Inc.
All Rights Reserved.
www.toysoft.ca

HotSync ID: Treo650

RegCode:

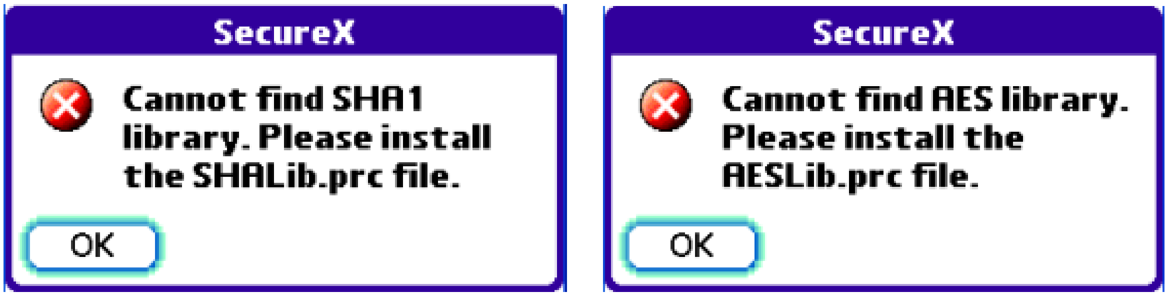
Diagram 2: SecureX registration

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

5. Launching SecureX™

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

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



SecureX

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

SecureX

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

Diagram 3: Encryption library errors

6. User Interface

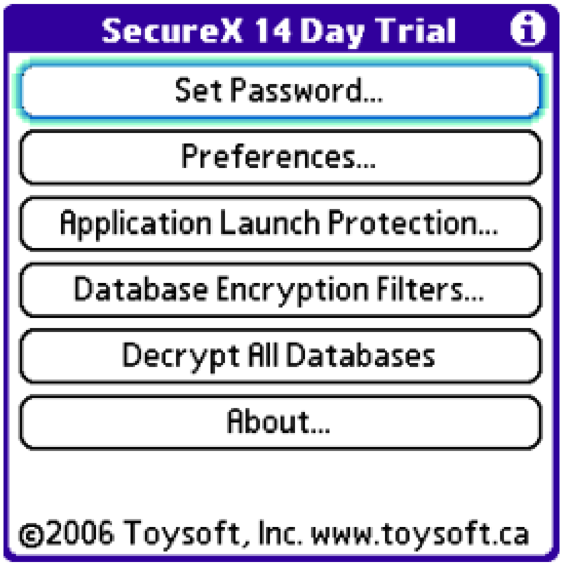
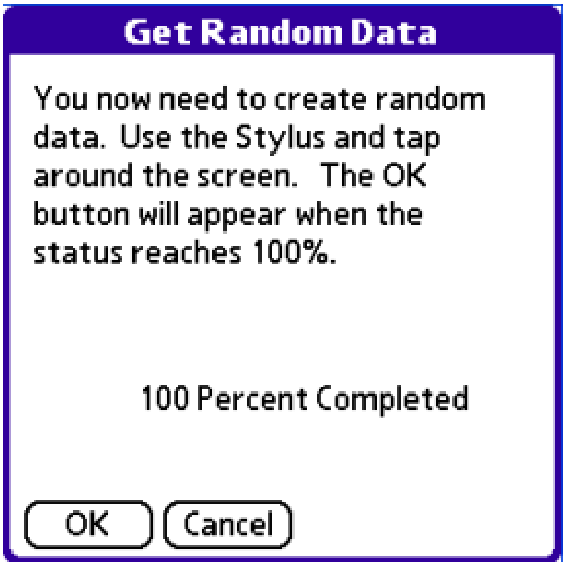

SecureX 14 Day Trial
Set Password...
Preferences...
Application Launch Protection...
Database Encryption Filters...
Decrypt All Databases
About...
©2006 Toysoft, Inc. www.toysoft.ca

Diagram 4: Main Screen.

Buttons	**Description**
Set Password…	Create a new password or change the current password
Preferences…	Open SecureX™ preferences screen
Application Launch Protection…	Control which application and panels can be launched
Database Encryption Filters…	Select the application database to encrypt
Decrypt All Databases	Decrypt all the databases and are encrypted
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

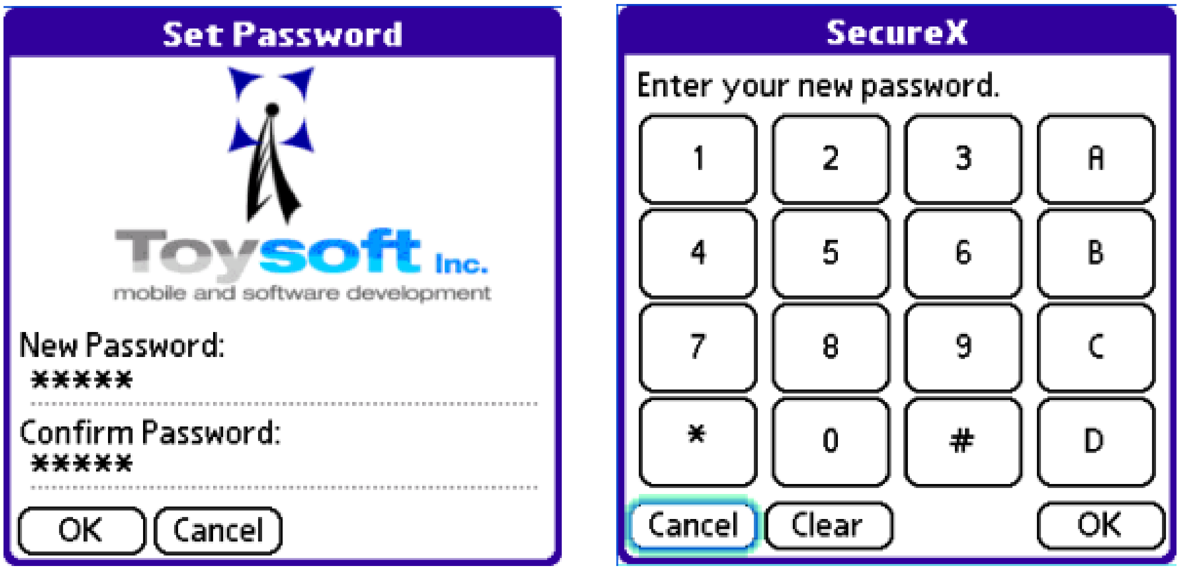
Diagram 5: Create random key

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 6: 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.

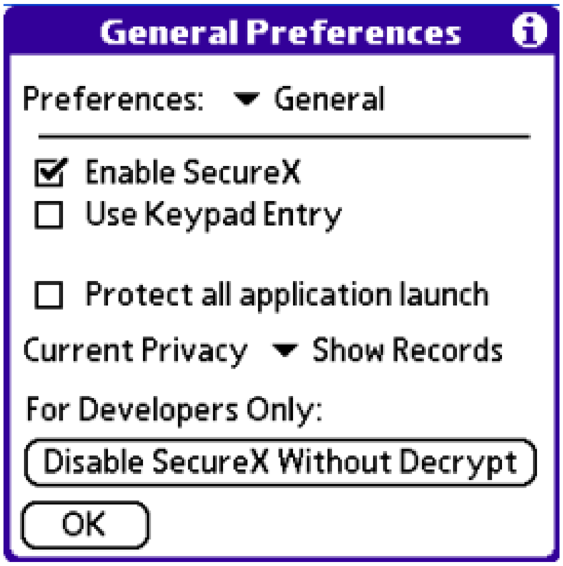
When choosing your private password make sure it is not easily guessed. Do not use password like your birthday, important dates, your favorite pet's name, your bank PIN, phone number etc… Mix the password with characters and digits. Make your password at least 6 characters long.

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 SecureX

□ Use Keypad Entry

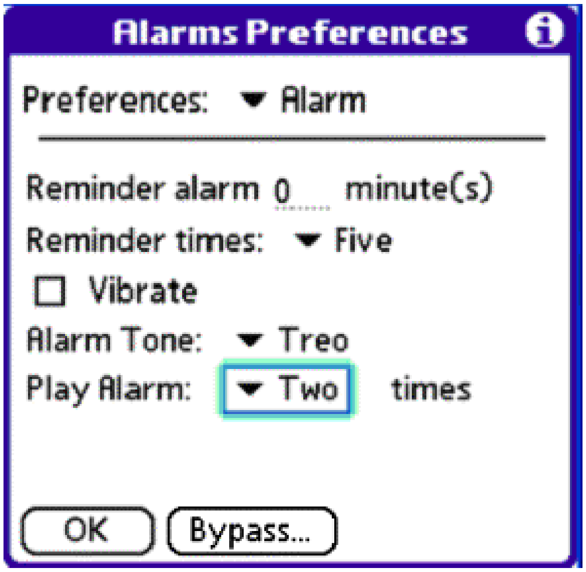
□ Protect all application launch

Current Privacy ▼ Show Records

Diagram 7: General Preferences

Controls	Descriptions
☑ Enable SecureX	To enable SecureX check the checkbox. To uninstall SecureX 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. SecureX 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.
□ Protect all application launch	If this is checked all application and control panel launch will be password protected. You can use the Application Protection screen to filter the application and control panels.

8.2 Alarms Preferences



Preferences: ▾ Alarm

Reminder alarm 0 minute(s)

Reminder times: ▾ Five

□ Vibrate

Alarm Tone: ▾ Treo

Play Alarm: ▾ Two times

Diagram 8: Alarms Preferences

Alarms are a important feature in SecureX™. All of the 3rd party security applications for the PalmOS® do not handle application alarms properly when the device is locked especially when the application's databases are encrypted. Most of the times alarms are disabled or not supported by the 3rd party security applications.

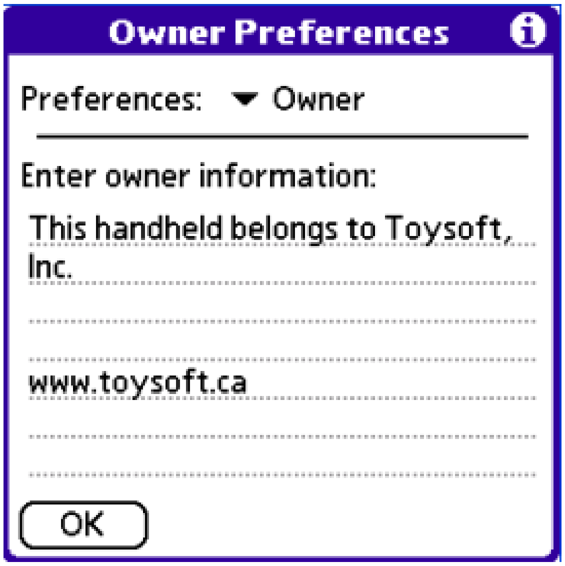
With SecureX™ application alarms are handled differently. SecureX™ will delay the application's alarm until you logon. When the alarm is triggered you can tell SecureX™ to play the regular alarm sound or specify a ring tone sound on the Treo® 600 and 650. You can even tell SecureX™ to keep reminding you of the alarm.

In the System Logon screen you can easily view all the triggered alarms and see which application and time without unlocking the device.

Controls	**Description**
Reminder alarm 0 minute(s)	Set the number of minutes for the reminder alarm. Set 0 to disable.
Reminder times: ▾ Five	Set the number of times to remind you of the alarm.
□ Vibrate	If you want to vibrate check it.
Alarm Tone: ▾ Treo	On the Treo® 600/650 you can select the alarm ring tone.

Play Alarm: ▾ Two times	On the Treo® 600/650 you can set the number of times to play the alarm ring tone.
	Set application with alarms to bypass SecureX. For system backup and email programs you should add them to the bypass list so that they can be run during the night.

8.3 Owner Preferences



Preferences: ▾ Owner

Enter owner information:

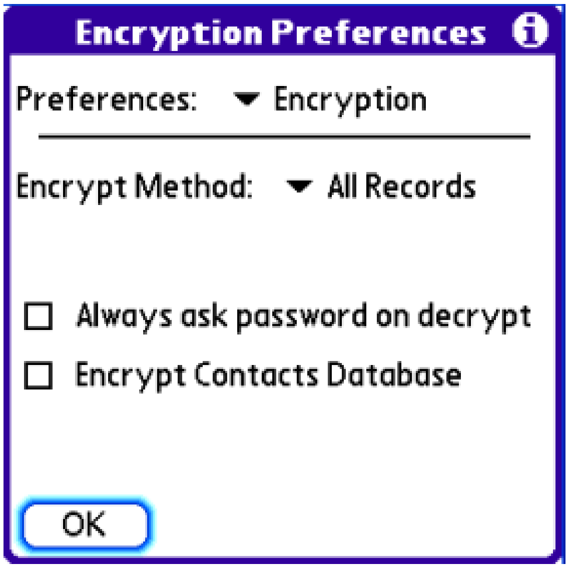
This handheld belongs to Toysoft, Inc.

www.toysoft.ca

Diagram 9: Owner Preferences

The owner information screen is displayed when you tap on the Owners button in the System Logon screen. If the device is lost or stolen you can put a lost and found message here.

8.4 Encryption Preferences



Encryption Preferences

Preferences: ▾ Encryption

Encrypt Method: ▾ All Records

□ Always ask password on decrypt

□ Encrypt Contacts Database

Diagram 10: Encryption Preferences

If you use SecureX™ to encrypt application databases you can control the type of records to encrypt. Currently SecureX™ supports All Records, Private Records or No Encryption.

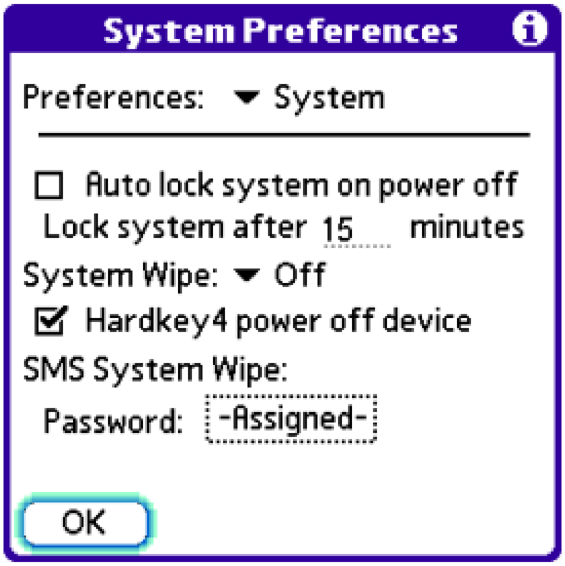
Private Records are records that you marked "Private". Typically private records are hidden or masked from viewing until you manually select the record for viewing or editing.

8.4.1 Encryption Contacts Database on the Treo® Smart phone

If you want to encrypt the Contacts database them check the □ Encrypt Contacts Database checkbox. SecureX will then ask you to create a new random key.

Note: When you have the Contacts database encrypted and when you get a phone call SecureX will need to decrypt the Contacts database. If you have a very large Contacts database it will delay the ringing of the ring tone.

8.5 System Preferences



System Preferences

Preferences: ▾ System

□ Auto lock system on power off

Lock system after 15 minutes

System Wipe: ▾ Off

☑ Hardkey4 power off device

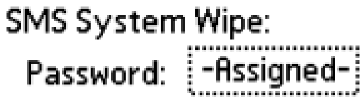
SMS System Wipe:

Password: -Assigned-

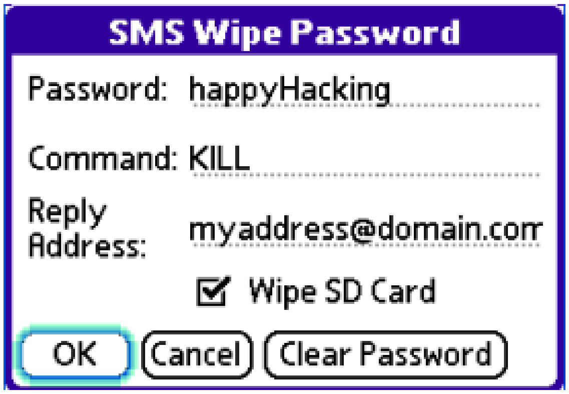
Diagram 11: System Preferences

System Preferences controls locking the system during power off, System Wipe if password is entered incorrectly for specified times and SMS System Wipe for the Treo® 600/650.

Controls	**Descriptions**
□ Auto lock system on power off	Lock down the system during power off if this is checked.
Lock system after 15 minutes	Lock down the system after a specified time. This is useful if you use the Palm often and do not want to keep entering the password.
System Wipe: ▾ Off	Perform System Wipe if password is entered incorrectly for specified number of times. System Wipe will delete all the application and databases on the device but leave SecureX™ active. Use this feature carefully.
☑ Hardkey4 power off device	On the Treo® 650 you can tell SecureX™ to treat the HardKey 4 as power off button. When SecureX™ locks the device no hard keys are accessible. Since the Treo® 650 doesn't have dedicated power button you must tell SecureX™ to allow to power off. Also the hardkey4 is used to hang up the call for a voice call.

 SMS System Wipe: Password: -Assigned-	On the Treo® 600/650 you can specify a password and command to perform System Wipe. This feature is usefully if your Treo® is lost or stolen and you didn't want anyone to access the data. Note: This feature is only available if SecureX™ is still installed. If you have lost the Treo® and the user had performed a cold reset and this feature will not work.

8.5.1 SMS System Wipe Preferences



SMS Wipe Password

Password: happyHacking

Command: KILL

Reply Address: myaddress@domain.com

☑ Wipe SD Card

Diagram 12: SMS System Wipe

If your Treo® is lost or stolen you can immediately send a SMS System Wipe command to SecureX™. You will need to assign a password and command. Reply address is optional. After SecureX™ has performed the System Wipe it will send you back a SMS notification. Optionally you can wipe the SD card.

Sending the SMS Message

The SMS message must be in the following format. The password and command are case sensitive.

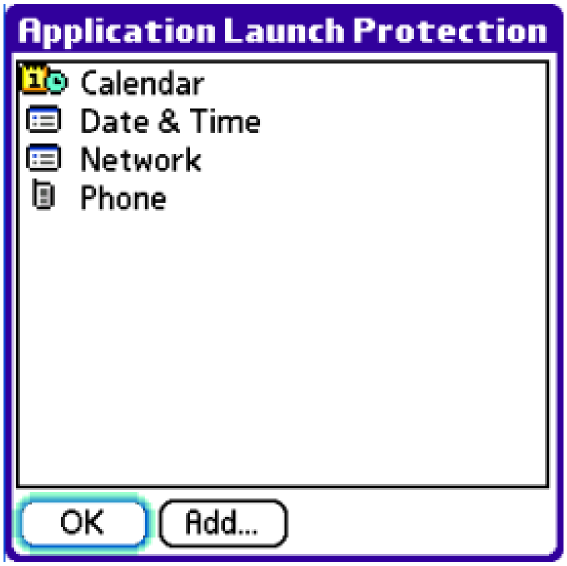
[PWD: xxx]
[CMD: yyy]

where xxx is the password you have assigned in SecureX™ and yyy is the command.

Example from the above diagram. In the SMS body message type the following and then Send it.

[PWD: happyHacking]
[CMD: KILL]

9. Application Launch Protection


Application Launch Protection

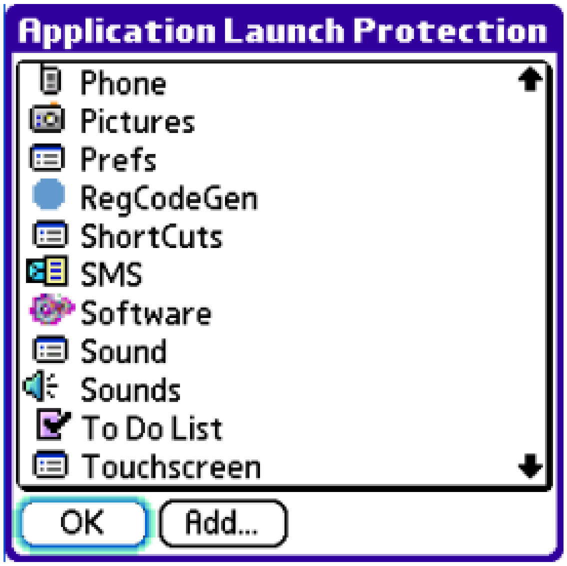
Calendar
Date & Time
Network
Phone

Diagram 13: Application Protection

Application Launch Protection lets you password protect applications and control panels from being launched. If you have private or sensitive information and don't want others to access then you can limit their access. Application Launch Protection is useful for multi-users who use your handheld. A good example is if you let your kids use your Palm and you only allow games to be launched.

9.1 Add Protected Application or Control Panel

To add an application or Control Panel to the protected database select the **Add…** button. The following screen will be opened.



Application Launch Protection

Phone
Pictures
Prefs
RegCodeGen
ShortCuts
SMS
Software
Sound
Sounds
To Do List
Touchscreen

Diagram 14: Select Protected Application or Control Panel

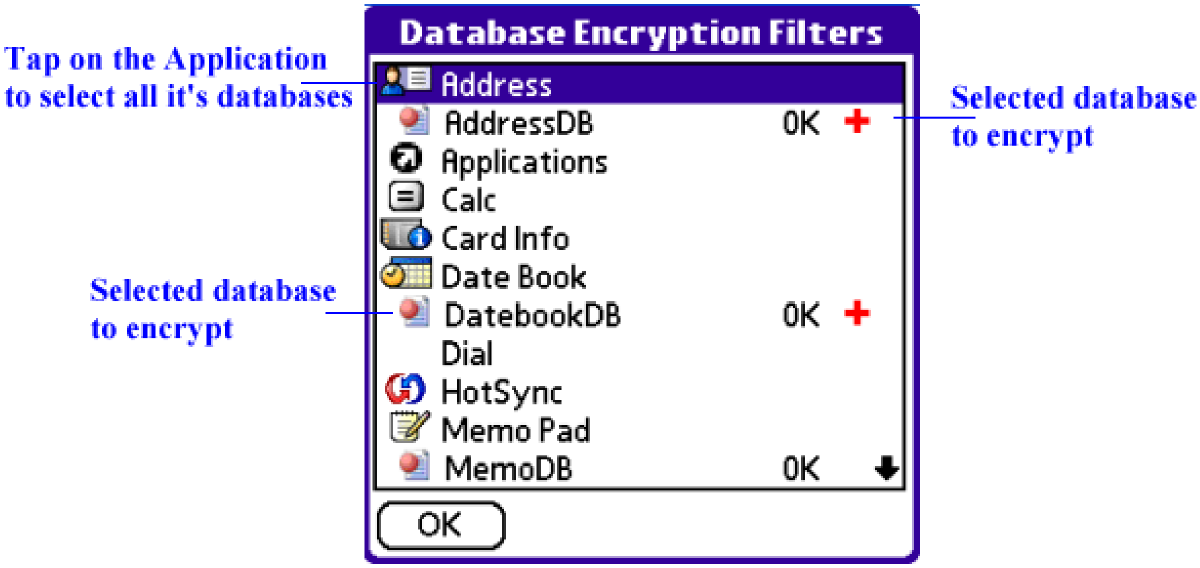
Tap on the application or control panel to add. The selected item will then be added to the protected database.

9.2 Global Application Protection

To protect application launch globally go to the **General Preferences** and check the item
☐ Protect all application launch

If the checkbox is checked then SecureX™ will password protect all applications and control panels from being launched. But if you have any applications or control panels in the Protected database then SecureX™ will allow those applications to be launched. If you uncheck the checkbox then application and control panels in the Protect database will be protected.

10. Database Encryption Filters



Database Encryption Filters

Address		
AddressDB	OK	+
Applications		
Calc		
Card Info		
Date Book		
DatebookDB	OK	+
Dial		
HotSync		
Memo Pad		
MemoDB	OK	

Tap on the Application to select all it's databases
Selected database to encrypt
Selected database to encrypt
OK

Diagram 15: Database Encryption Filters

Database Encryption Filters is a powerful feature in SecureX™. It enables you to encrypt any database on device with strong AES encryption. You can select any one database or all of the application's databases for encryption. SecureX™ will only decrypt the database that the application opens and leave others encrypted. Transparent encryption is one of the major features of SecureX™ that stands out from the competition. There are no limitations on the number of databases SecureX™ can encrypt.

10.1 Encrypt All vs Encrypt Private Records

In the Encryption Preferences you can specify how SecureX™ will encrypt database records. You can select Encrypt All which the entire database is encrypted or select encrypt Private records only. Private records are marked with the private flag when you edit the record such as in the Memo application. Typically private records are masked from the viewing and requires authentication to view. With SecureX™ authentication is not required since SecureX™ does not use the Palm® security.

If you do not use encryption to set the Encryption Method to "No Encryption" in the Encryption Preferences.

10.2 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 System Preferences. In either case SecureX™ always encrypt all the databases in the Database Encryption Filter database when it locks the device.

10.3 Orphaned Databases

Orphaned databases are databases that do have belong to any application. Sometimes multiple applications access the same database as the database is shared. If you want to encrypt Orphaned databases then select the ones you want from the database list. All the Orphaned database are shown on the bottom of the list in the Encryption Database Filter screen and they are not shown to belong to any application.

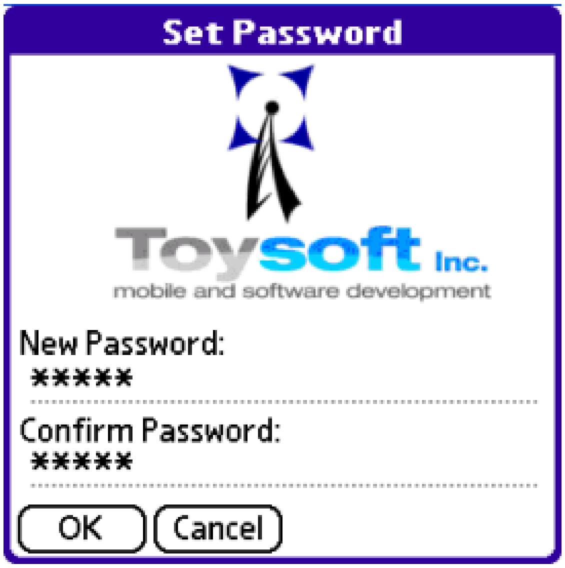
11. Decrypt All Databases

To quickly decrypt all the databases you can tap on the Decrypt All Databases button on the SecureX™ main screen. This feature is mostly used when you do a Warm Boot to recover from an endless reset loop. By decrypting all the databases and doing a soft reset it usually clears up the problem with encrypted records.

12. Password Authentication Screens

SecureX™ has two authentication screens.

12.1 Text Entry Screen



Set Password

New Password:
*****

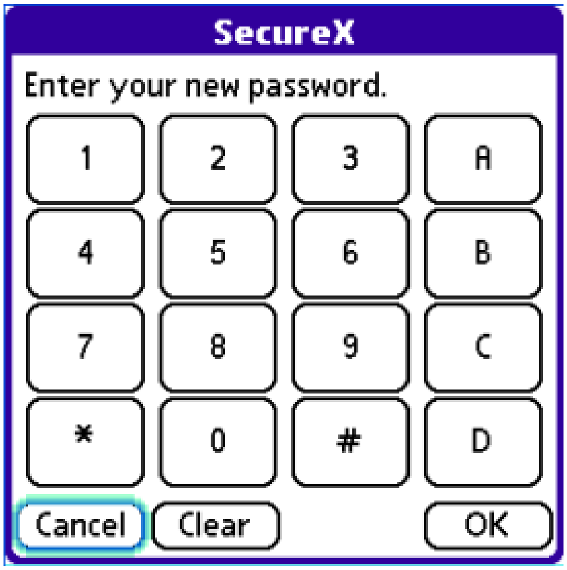
Confirm Password:
*****

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.

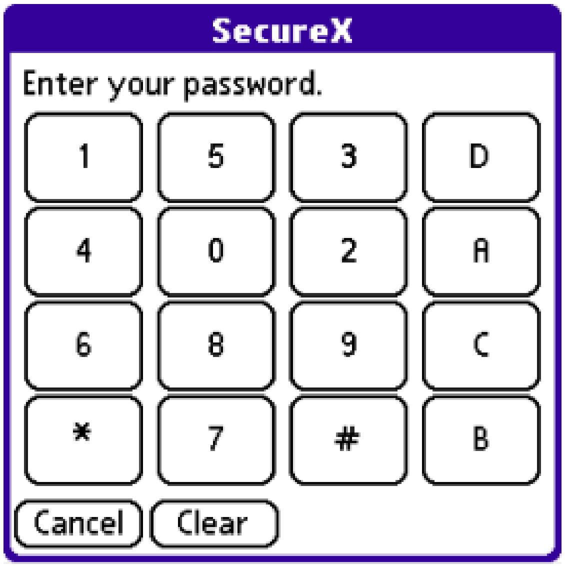
During authentication all hard keys and system events are disabled until you have successfully authenticated. This includes external card insertion or removal, incoming IR beam and application launch.

12.2 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 SecureX™ will validate the password as you enter the password. If you had made a mistake then tap on the **Clear** button and restart again.

12.2.1 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.

13. Application Alarms and Reminder Alarms

SecureX™ handles application alarms differently when the Palm handheld is asleep. When an application triggers an alarm such as the DateBook the next alarm in the DateBook will not be set. Therefore, any alarms that you may have set will not be triggered. SecureX ™ will not allow any alarms to be displayed when the device is locked. SecureX ™ considered this as a security risk.

This is because the data is encrypted and the handheld is not authenticated yet. There is no way to get your passphrase to decrypt the record with. In any case, regardless if the database is encrypted or not encrypted no new alarm will be set for the triggered application.

This is where SecureX ™ Reminder Alarms comes in. In the Alarms Preferences you set the reminder period. Whenever an alarm is triggered during the sleep state, SecureX ™ will continue to remind you by sounding the alarm sound. This will continue until you attend to the alarm by logging on to the Palm. When you log on to your Palm all previously triggered alarms will be displayed to you. If you do not want reminder alarms then you can turn it off in the Alarms Preferences screen.

Note: If you have many alarms set and you have not logged on to your Palm for days you will get many alarms being displayed when you log on to your Palm.

13.1 View Triggered Alarms

In the logon screen there is an Alarm button. If you need to quickly see which alarm has been triggered tap on it. SecureX ™ will display all the recently triggered alarms with their application names and the time it was triggered. This is very useful if you do not need to logon to the Palm.

14. Treo® 600/650/700P/680 Smart phones

The Treo® smart phone operates differently from traditional Palms such as the Tungsten®. A lot of problems can occur when encryption is involved and you need to know why.

When SecureX™ locks the Treo® internet and phone communication are still active and the Treo® is constantly pulling data. When you get a voice call the Phone application actually searches the Contact application to retrieve caller ID information and picture ID.

14.1 SMS and Voice Phone Calls

When SecureX™ locks the Treo® you can still receive SMS text message, MMS, IM chat and voice calls. For SMS you will get the popup dialog window. If you don't want the popup to show up then you can go to SMS or Messaging application and check the **Privacy Mode (hide text)** checkbox in the **Message Preferences**.

You cannot view the SMS or MMS message until you are authenticated.

When you get a phone call you can answer, ignore and hang up the call as normally but you cannot launch any application until you are authenticated.

15. 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.

15.1 Enterprise License and SecureX™ Customization

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

We can customize SecureX™ 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
- Application and data wipes
- Reject new applications that are installed on to the handheld

16. SecureX™ Limitations

The following are limitations in SecureX™

- SecureX ™ does not encrypt external cards such as SD/MMC®, Compact Flash® and Memory Stick®. We have a product called mEncryptor™ for media encryption.
- SecureX ™ does not mask the passphrase in the set owner information in the Prefs and when you are viewing a private record.
- If your device is reset or a system crash occurred during encryption and decryption, SecureX ™ will not recover any data lost. Eg: if SecureX ™ 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

17. Uninstalling SecureX™

To uninstall SecureX ™ do the following:

1. Launch SecureX™ and tap on the **Preferences** button.
2. You will be prompted, authenticate. Tap on the **Enabled SecureX** checkbox. SecureX™ 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 **Security** name in the list. Select it and then tap on the **Delete** button.
5. Look for the SHALib and AESLib and delete them.

18. Upgrading SecureX™

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

19. HotSync®

During the HotSync® process SecureX™ decrypts all the databases. This is needed because desktop conduits cannot handle encrypted databases.

20. 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 SecureX™

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

PalmOS® AES Library used in SecureX™

21. 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.

22. 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.

23. 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.

24. 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

25. Technical Support

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