Key Pad

Version 1.0

for Palm OS

Rolf Dümcke

Copyright © 2003 Rolf Dümcke, All rights reserved.

Palm, Palm OS und HotSync are registered trademarks of Palm, Inc. or its subsidiaries. All other product or brand names may be registered trademarks or trademarks of their respective owners.

Program Features

Key Pad stores **confidential information** using the **Advanced Encryption Standard (AES)** with 128 bit keys.

The information is accessed by entering a numerical key in a virtual key pad. Letters are associated with the digits as on a phone keyboard, therefore the user can enter a keyword which is easier to memorize.

The basic version, which can be used free of charge, stores up to 1000 characters in a single text field.

The registered version offers an unlimited number of text fields which are accessible from a list containing the titles of these text items. Furthermore, the keyword can be changed.

System requirements

The program runs on Palm OS systems starting with version 3.0. It uses 19 kB of memory.

Software installation

Unpack the zip file and and copy the file KeyPad.prc in the install directory of your Palm desktop software. In most cases a double-click on KeyPad.prc will do this job. After a HotSync you can start Key Pad on your handheld.

Registration

The unregistered version of Key Pad may be used for an indefinite time. If you register, you benefit from additional functionality. Information on registration sites is available at www.rduemcke.de.

To register, open the registration form by tapping on the "**Options/Registration**" menu entry. On the registration form you will find your personal username (HotSync username) which is required for registration. The registration server will ask for your username and provide a personal key (up to 5 digits). Enter the key in the empty field of the registration form and tap on the "**Register**" button. The label at the top of the registration form will change from "**Not Registered**" to "**Registered**". Tap on "**Ok**" after successful registration to return to the main form.

Using Key Pad

After starting Key Pad for the first time a key with up to 32 digits has to be entered which secures the secret information. It is advisable to use keys with a minimum of 12 to 16 digits.

After repeating the key, a text pad to enter confidential information is displayed. If the key entered and its repetition differ the key setup procedure has to be repeated.

When Key Pad is closed (by returning to the launcher with the home button or by starting another application with a hardware button) the text in the text field is encrypted and all clear text is erased.

On each start of Key Pad the access code is requested. You can try to enter the correct code as often as you like, however, after the fifth trial the handheld will block for 10 seconds.

The menu of the text field contains the following items:

Set Title: Enter a new title for the text field

Registration: Register Key Pad (see section Registration)

The Selection List

This form is available only in the registered version. To create a new text field tap on "**New**". An empty text field is displayed along with a form to enter a name for the new item. After filling in the name confidential information can be entered in the text field. When the "**Close**" button is hit the text will be encrypted and the display returns to selection list.

To view an item in the list, open the corresponding text field by tapping on the item. The items in the list are drawn in a large font to enable selection with fingers.

To delete an item from the list, open it and select the menu item '**Delete Item**". After a confirmation the item will be deleted and the display returns to the selection list.

Items can be moved in the selection list by putting the stylus down on an item and dragging it to the desired position.

The menu in the selection list includes the following entries:

Change Key: Change the access key for Key Pad. The new key has to be entered twice in the virtual key pad. If the repetitions of the key differ the old key will be retained. Otherwise the new key will be required for the next and subsequent invocations of Key Pad.

Registration: View the registration information.

Backup

On each HotSync operation a full backup of the database will be made. The database is fully encrypted and does neither contain any clear text nor keys.

Annex: Database format

In this appendix the format of the database which holds the encrypted information is described. The description should be detailed enough to allow the decryption of the confidential information when the access key is known. All encryption/decryption is done according to AES with 128 bit key and block sizes.

Record 0:

Bytes 0 – 15: contains information for access key validation (not described here)

Bytes 16 – 31: encrypted 128 bit key for decryption of records 1 and following.

Byte 32... : 32 bytes of title per text field encrypted in CBC mode. The key for decryption is obtained from the access key as described below. After decryption, each 32 bytes contain a null terminated string with the title of one text field. The nth string (n=1,2,3 ...) corresponds to record n.

Records 1 and following: a number of 16 byte groups holding the information for one text field encrypted in CBC mode. The decrypted byte chain holds a null terminated string with the clear text. The key for decryption is obtained from the access key as described below.

Key generation: Each digit entered on the virtual key pad is mapped to a half byte in a sixteen byte key starting with the low order half byte of the first byte. Unused half bytes are filled with 0. The half bytes are obtained by adding 1 to the digits entered. The resulting 16 byte quantity is used as a 128 bit key to decrypt bytes 16 – 31 in record 0 using ECB mode. The resulting 16 byte string is used as key to decrypt all other information in the database.

License Agreement

This license is the statement of agreement between Rolf Dümcke (“author”) and the user of the enclosed software product (“program”) in its evaluation (“shareware”) version and its registered version.

By installing, using, copying, or distributing the program, you agree to all terms of this License. If you do not agree to any of the terms of this License, then do not install, use, copy, or distribute the program.

The program is Copyright © 2003, Rolf Dümcke, All rights reserved.

Evaluation License

The program is distributed in an evaluation version, which is limited in the duration of use and/or in the program functions available.

Subject to the terms below, the user is hereby granted the non-exclusive right to install and use the evaluation version of the program free of charge on one Palm OS handheld under the restrictions described in the User's Guide. Any use of the evaluation version violating these conditions is not permitted.

The user is granted the right to distribute exact copies of the software (program code, user's guide, and license agreement) free of charge. Charging for program copies requires in any case the written permission of the author.

Grant of License for the registered version

By the act of registration the user obtains (after paying a fee) a personal key enabling him to transform the shareware version of the program into the registered version.

Subject to the terms below, the user is granted the non-exclusive right to use the registered version of the program on one Palm OS handheld. The user shall in no way copy the software (except for a backup copy created via HotSync), resell, lend, distribute, or make available the program to third parties. Furthermore, the user must not distribute, lease, rent, or lend the personal key.

Limited Warranty

The software, and all accompanying files, data and materials, are distributed “AS IS” and with no warranties of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The user takes full responsibility for the selection of the program to achieve his intended results, and for the use and results obtained from the program. The author does not warrant that the operation of the program will be uninterrupted or error-free.

Limitation of Liability

In no event shall the author be liable for any incidental, consequential, or punitive damages whatsoever relating to the use of the program (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption). Any liability of the author will be limited exclusively to refund of registration fee.

In no event does the author authorize the user to apply the software in environments or systems where its failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at the user's risk, and the user agrees to hold the author harmless from any claims or losses relating to such unauthorized use.

General

All rights of any kind in the program which are not expressively granted in this License are entirely and exclusively reserved to and by the author. The program may not be rented, leased, modified, translated, reverse engineered, decompiled, disassembled or be used in derivative works.

In the event that any provision of this Agreement should be or become invalid or if the Agreement is incomplete, the validity of the other provisions shall not be affected. In lieu of the invalid provision or in order to complete the Agreement, a reasonable provision shall be effective approaching to what parties would have agreed upon if they had considered that issue.

This Agreement is the complete statement of the Agreement between the parties on the subject matter, and merges and supersedes all other prior understandings, purchase orders, agreements and arrangements. This agreement shall be governed by the laws of the Federal Republic of Germany. Exclusive jurisdiction and venue for all matters relating to this Agreement shall be in courts and fora located in Berlin, Germany, and the user consents to such jurisdiction and venue.

Palm, Palm OS und HotSync are registered trademarks of Palm, Inc. or its subsidiaries.