

# In Dubio

## Table of Contents

Introduction.....	1
User Guide.....	1
Daily usage.....	1
Setup.....	2
Maintaining items and entries.....	3
Background.....	4
Roadmap.....	5
Disclaimer.....	6

## Introduction

In Dubio is an application which is meant to be a reference for assisting access to personal information of any kind. Everyone has passwords, accounts any kind of information which is great to have at hand all the time. In Dubio means "in doubt" and the idea is to have a software for reference when you're in doubt of whether you remember the information correctly.

For this purpose it maintains a list of items with a undefined number of information lines to it, e.g. a bank account might contain Branch and Account number, PIN, Telephone Banking contact etc., whereas a mail account contains user name, password, pop server name, smtp server name etc.. Because every matter is so individual, the application does not force categorisation but simply provides a facility to add rows of information in a non-predetermined way.

Instead, focus has been put into ensuring that the contents stored within the application are secure in such a way that if your phone/pod gets into someone else's hands or that you install some spyware (which I have not seen so far, but who knows ...) will not be usable. All data is saved using AES (Advanced Encryption Standard).

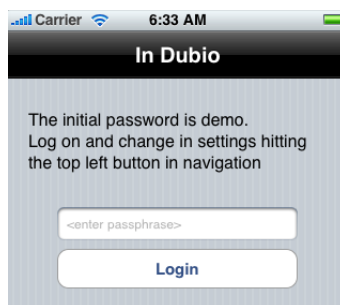
The backside of this is, that if you loose the password for this application, you won't be able to recover the information that you stored – and neither will even be the developer.

THEREFORE IT IS HIGHLY RECOMMENDED TO ALSO FIND AN ALTERNATE SOLUTION TO KEEPING THIS INFORMATION, THIS PRODUCT SOLELY SUPPORTS YOU IN CARRYING SECRET INFORMATION SAVE FROM UNWANTED ACCESS.

## User Guide

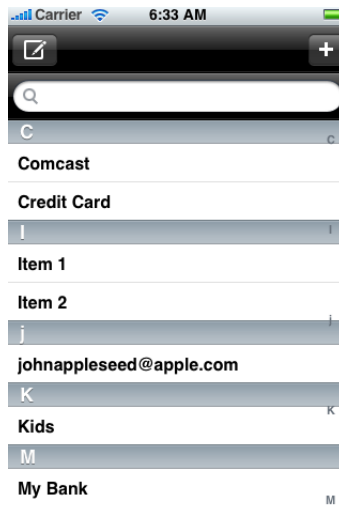
### *Daily usage*

After install, InDubio sets up an initial settings table and demo items. Log in using "demo" as passphrase.



After log in, you are presented with the main item list. There is a search function at the top,

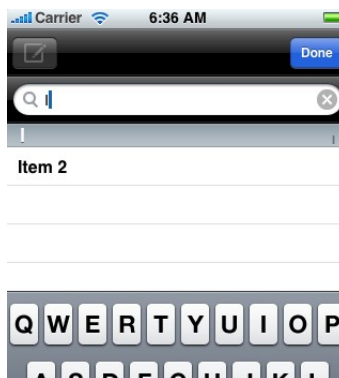
filtering your list, and you can navigate using the letters on the right.



To select an item, tab it.



This displays the entries that are stored against the item. As you can see, this is simply a list of text lines – plus a group definition for future versions.



The main screen allows you to search through the list and filter the entries. Click on the search bar and enter your search string. Click done to hide the keyboard.

## Setup

Navigate to the main screen and hit the compose button on the top left.

Enter a new passphrase, confirm and enter your previous passphrase (initially "demo").

The 2 sliders determine how high the rows in the main and detail view are for selecting. Some

people might prefer a low number (many lines but harder to hit), some a higher number (easier to hit but less lines at a time).



Press "Save" to store the settings.

### ***Maintaining items and entries***

This section will guide you through the usage of the application for creating and editing information.

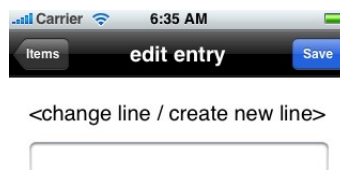
To maintain an item, tab it in the main list. You will see the detail screen. Click "Edit" at the top right:



Similar to the application "Contacts" on the device, you can edit the entries. Let's first look at deleting the entire item. Click the "Trash" Icon in the top left corner. There is no confirmation. The item is gone and your back in the main menu.

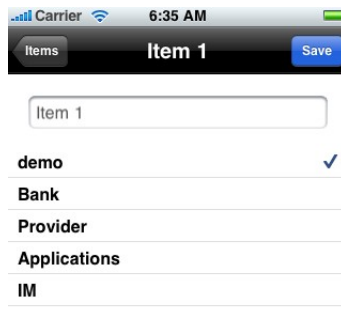
There are 2 sections in the details, one for the lines themselves and one for a group. Items can be grouped so a future version of the application can alternatively show items by group (e.g. all "bank" related items).

Clicking a line in the first section (an existing or a new line) brings you to this screen:



Change the value and press "Save" or go back to cancel.

When you click on the group section of the item, you can edit the item group and it's name:



To select a group, just tab it. Group maintenance is not included in this version.

To delete a single row of information, use the standard deletion mechanism by hitting the red icon and then the "delete" button next to the line.



## Background

This simple application ensures that the data is stored safely on the iPhone by encrypting the content in the applications file. The password is stored as : user password + application internal passcode, the two together are hashed and the resulting binary hash (SHA1) is stored as string, resulting in something like Ebd#ô #Úκ., 1òÊV# ' ¶ #ò.

The data itself is encrypted with part of this hash as symmetric key, using AES128 encoding (American Encrypting Standard) which is also used in Open SSL, the result looks to the user and other applications like this

#Ê¬%oêeaâſç\_W\*°#†≈ìXoË«##Æ`mìØÕx•î# #u°âdì™Pi«-.C· ÓñÿôYf#IhΠO<À#Ìç¬h, ,√á4♣Ω±\_èÑ#âi/5¬Gc%[Π[μO#sà` }Ë` ®◊Õ°êâf...àv≤°B∞,H#Úkè#XêZ.«G”≥,, -c»

etc. anyway, ... you get the picture.

With the key being part of the hash which again is generated from password and other letters, it's reasonably secure.

# Roadmap

If the application becomes a success, we'd like to add a handful of features to it, to enhance usability:

1. **Timer:** if the iPhone is left with the application running, the access to the data is open except the PIN unlocking is set for the phone. Alternatively the application could utilise a timer and lock itself, requesting you to put in the password again after a certain amount of idle time.
2. **Backup facility:** as the iPhone is backed up with the iTunes synchronisation, your data file is backed up. If you restore, you'll have to use the password which was in place at the time of the backup, not the latest. We might add the following: Prior to backup, the settings allow you to save the data in plain text. If then the sync is run, you'll have a readable copy on the computer – the iPhone version can be deleted again using the application settings.
3. **PC / Mac client for simplifying maintenance.** This sounds great, contradicts though the the current guarantee of the product, which is that the production is not able to ring home, anyone else, etc. A peer product would mean that networking is possible and thus transmission of your secure data. (only to the windows version of course, but nevertheless ...)
4. Navigation using the **group** information
5. **Favourites** – another contradiction. Has an entry become a favourite it would mean you use it often. But then – you most likely won't have to look it up any more. This is why the priority of this feature is quite low.

# Disclaimer

Refer to Apple's APP store terms and conditions.

## I . DISCLAIMER OF WARRANTIES; LIABILITY LIMITATIONS.

a. SHTH DOES NOT GUARANTEE, REPRESENT, OR WARRANT THAT YOUR USE OF THE PRODUCT WILL BE UNINTERRUPTED OR ERROR-FREE, AND YOU AGREE THAT NO SUPPORT SERVICE EXISTS FOR THE PRODUCT.

b. YOU EXPRESSLY AGREE THAT YOUR USE OF, OR INABILITY TO USE, THE PRODUCT IS AT YOUR SOLE RISK. THE PRODUCT IS PROVIDED "AS IS" AND "AS AVAILABLE" FOR YOUR USE, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, THE ABOVE EXCLUSION OF IMPLIED WARRANTIES MAY NOT APPLY TO YOU.

c. IN NO CASE SHALL SHTH, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, PRINCIPALS, OR LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING FROM YOUR USE OF THE PRODUCT OR FOR ANY OTHER CLAIM RELATED IN ANY WAY TO YOUR USE OF THE PRODUCT, INCLUDING, BUT NOT LIMITED TO, ANY ERRORS OR OMISSIONS IN ANY CONTENT, OR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF THE PRODUCT, EVEN IF ADVISED OF THEIR POSSIBILITY. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR THE LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES OR JURISDICTIONS, SHTH'S LIABILITY SHALL BE LIMITED TO THE EXTENT PERMITTED BY LAW.

d. SHTH DOES NOT REPRESENT OR GUARANTEE THAT THE PRODUCT WILL BE FREE FROM LOSS, CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, OR OTHER SECURITY INTRUSION, AND SHTH DISCLAIMS ANY LIABILITY RELATING THERETO.

II. WAIVER AND INDEMNITY. BY USING THE PRODUCT, YOU AGREE TO INDEMNIFY AND HOLD SHTH, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, PRINCIPALS, AND LICENSORS HARMLESS WITH RESPECT TO ANY CLAIMS ARISING OUT OF YOUR BREACH OF THIS AGREEMENT, YOUR USE OF THE PRODUCT, OR ANY ACTION TAKEN BY SHTH AS PART OF ITS INVESTIGATION OF A SUSPECTED VIOLATION OF THIS AGREEMENT OR AS A RESULT OF ITS FINDING OR DECISION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS MEANS THAT YOU CANNOT SUE OR RECOVER ANY DAMAGES FROM SHTH, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, PRINCIPALS, AND LICENSORS AS A RESULT OF ITS DECISION TO REMOVE OR REFUSE TO PROCESS ANY INFORMATION OR CONTENT, TO WARN YOU, TO SUSPEND OR TERMINATE YOUR ACCESS TO THE PRODUCT, OR TO TAKE ANY OTHER ACTION DURING THE INVESTIGATION OF A SUSPECTED VIOLATION OR AS A RESULT OF SHTH'S CONCLUSION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS WAIVER AND INDEMNITY PROVISION APPLIES TO ALL

VIOLATIONS DESCRIBED IN OR CONTEMPLATED BY THIS AGREEMENT.

III. CHANGES. SHTH reserves the right, at any time and from time to time, to update, revise, supplement, and otherwise modify this Agreement and to impose new or additional rules, policies, terms, or conditions on your use of the Service.

IV. NO WARRANTY: YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE LICENSED APPLICATION IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE LICENSED APPLICATION PROVIDED ARE PROVIDED "AS IS" AND "AS AVAILABLE", WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND LICENSOR HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE LICENSED APPLICATION AND ANY SERVICES, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. LICENSOR DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE LICENSED APPLICATION, THAT THE FUNCTIONS CONTAINED IN, THE APPLICATION WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE APPLICATION WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE APPLICATION WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY LICENSOR OR ITS AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE APPLICATION PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

f. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL LICENSOR BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE APPLICATION, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Licensor's total liability to you for all damages exceed the amount of 1 dollar (\$1.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.