Tresør Manual v1.2

Laekery

March 19, 2011

Contents

List of Figures

1 Introduction

Nowadays everybody needs to remember a lot of secrets:

- Web logins,
- PIN numbers,
- WLAN passphrases,
- computer logins, and so on.

Password managers have come to help you with remembering your secrets. But unfortunately desktop password managers are bound to a location. Web password managers on the other side are too risky.

The solution: You have your cell phone always with you like your wallet! Tresør is a cell phone password manager using up-to-date cryptography to protect your secrets.

1.1 Features

The following is a list of the key features of the product:

- many different types of secrets:
  - file password,
  - WLAN keys,
  - web login,
  - EC card,
  - post card,
  - VISA card,
  - computer login,
  - messenger account,
  - free form.
- folders for grouping entries,
- fuzzy search
- strong cryptography (AES-256, SHA-256),
- optional password proposal avoids reusing passwords,

- optional field proposal avoids re-entering the same information over and over (for example username for websites),
- import/export to mobile phone filesystem for backups/migrations to new phones,
- multi-language: English and German,
- limited persistent undoing of changes,
- limited change tracking with entry modification and creation time stamps.

1.2 Requirements

You can check the requirements with your mobile phone manual or the mobile phone manufacturer:

- MIDP 2.0 compatible phone
- JSR 75 (PDA Optional Packages for the J2ME™ Platform)
- ca. 100 kB of memory

Almost all phones you can purchase today meet these requirements.

1.2.1 Demo version

You can verify that your phone works with the software by using our demo version. The demo version is restricted to 4 passwords. You can identify the demo version at the login screen where the word *demo* is written.

1.3 Security considerations

The security of your secrets is the highest priority of Tresør. This section lists the security advantages of Tresør.

Operational: The following are operational techniques that enlarge security of Tresør:

- Secrets are only stored *encrypted* in the phones persistent memory.
- Tresør logs you out after a period of 2 minutes of inactivity. This makes it very difficult for a thief to get access to the secrets even if you forget your phone in an unlocked state.

- Exported password files are still PIN *encrypted*. This means that if a thief even gets a password file, he still needs to break your PIN.
- Passwords are stored in a big chunk instead of smaller structures. This makes it harder to cryptoanalytically analyze the structures.
- No internet based password file backup/storage is done at the moment. This could simplify the operation of the program on one hand, but would also increase the risk of sending a password file with weak PIN over the internet on the other hand. The thief needs physical access to your device or hack it over the mobile network at the moment.

Technical: These technical or cryptographic techniques make Tresør secure. Please don't be frustrated if you don't understand the technical terms:

- Tresør uses *strong cryptography* (AES-256, SHA-256). AES is the first publicly accessible and open cipher approved by the NSA[1] for top secret information.
- The AES algorithm is used in CBC mode with a *random* 128 bit IV.
- No message digest (i.e. SHA-256) of the PIN itself is stored. This makes it impossible for a *rainbow table* attack to succeed.

2 First steps

This section describes the steps to make Tresør working for the first time.

2.1 Installation

Setup on your mobile phone heavily depends on your mobile phone operating system. You need to consult your mobile phones user manual or your phones manufacturer customer support for details on installing Java ME software applications.

You should consider the following hints when installing the Tresør application:

- Your phone should meet the requirements (see 1.2).
- Installing the application in internal phone memory is safer in regards of software operation and security.

[1] The *National Security Agency*/Central Security Service (NSA/CSS) is a cryptologic intelligence agency of the United States government, administered as part of the United States Department of Defense.

- Allow the application read and write access for password file import/export to the phones file system with the appropriate phone menus.

2.2 First start

When you start Tresør first you are queried for the password key ring PIN[2]. This is the code you'll need in the future to access your passwords. If you lose the PIN there's no way to access your passwords. You can change the again PIN later.

Please refer to the table on page 17 for a discussion about PIN lengths.

Some further PIN hints:

- Don't use your or someone elses birth date.
- Don't use your or someone elses phone number.
- Don't use your or someone elses information that is known to someone besides you.
- Don't write the PIN down.
- Don't store the PIN disguised as a phone number in the phones address book.
- Don't forget the PIN. A short unsafe PIN you can remember is better than a long secure PIN you'll forget.
- Remove the backups after a PIN change.

3 Usage

The normal usage cycle of the application is as follows:

1. start Tresør,
2. enter master PIN (see figure 1),
3. change folders and passwords,
4. exit Tresør.

You should exit Tresør as soon as possible. The time the password key ring is unlocked with your PIN, an attacker might spy on your secrets by watching your phone. To disable this attack Tresør will exit after two minutes of inactivity.

[2]personal identification number

Figure 1: Entering the PIN at the start

4 Screens & Commands

This section describes the screens and commands of that are most important for using Tresør.

4.1 Folders screen

The folders screen (see figure 2) is responsible for selecting, adding and deleting folders. It shows a list of all folders and the number of entries in each folder after the folder name. Assigning a folder to an entry is not done here, it is done in the per-entry view. There is only *one* hierarchy level for folders to increase maintainability.

There is always a folder called *General*. This is the default folder you can't delete. It has always the first position in the folder list.
Commands:

Edit: Brings you to a screen to edit the current folder name.

Delete: Deletes the current folder. The *General* folder *can't* be deleted. The command moves all entries into the General folder if the folder to delete is not empty.

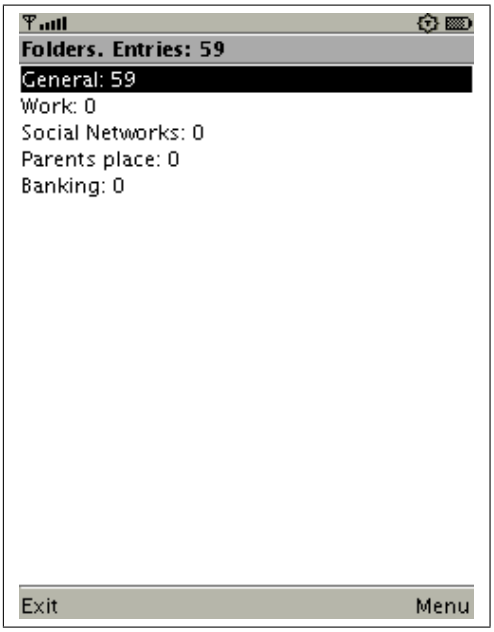

Figure 2: The folders screen

Warning: There is no confirmation dialog. The reason is that you can always revert to a previous state using *Revert*. See section 4.7.

New folder: Brings you to a screen to enter the new folder name, and creates a new empty folder.

Maintenance: Brings you to the maintenance screen that is described in section 4.7.

Sort: Sorts the folder names in alphabetical case-insensitive order. The General folder will stay at the top position because it plays a special role in other scenarios.

Search: Search for an existing password. See section 4.3 for more on this topic.

4.2 Password list screen

The password list screen (see figure 3) is responsible for selecting, adding and deleting password entries. It shows a list of all password entries inside a certain folder (or a search result).
Commands:

Edit: Brings you to a screen to edit the current password entry.

Figure 3: The password list screen

Delete: Deletes the currently marked password entry.

> **Warning:** There is no confirmation dialog. The reason is that there's the option to revert to a previous state using *Revert*. See section 4.7.

New password: Brings you to a screen to enter a new password entry.

Maintenance: Brings you to the maintenance screen that is described in section 4.7.

Sort: Sorts the entry names in alphabetical case-insensitive order. Sorting affects *all entries* in *all folders*.

Search: Search for an existing password. See section 4.3 for more on this topic.

4.3 Search

The search can be used from the folders screen (see 4.1) and the password list screen (see 4.2). You can search for passwords by *exactly* entering the search string with character case being ignored.

A more fancy search is to use the so-called *fuzzy search* that kicks in if exact search has no results. Fuzzy search uses *character equivalence classes* based on the numeric keypad layout (see figure 4). All letters on one key are treated like the same. So it doesn't matter if you search for:

- ’hello’,
- ’4elln’,
- ’ifkko’ or
- ’43556’.

Every search query above has the same sequence of keys on the numeric key pad (see figure 4). All search queries above return the same results.

You can quickly type the search string by just hitting each numeric key *once* instead of hitting the numeric keys in the required sequence to get the exact letters or using T9 to get the correct search term.

Fuzzy search also works with proposals from the T9 text input helper of your cell phone. A Nokia phone with German locale will propose ’Helln’ instead of ’hello’, but it doesn’t matter because search is fuzzy.

The key advantage of fuzzy search is that you can type the search term more quickly. The disadvantage is that you may get more search results than you requested.

1	2 abc	3 def
4 ghi	5 jkl	6 mno
7 pqrs	8 tuv	9 wxyz

Figure 4: The numeric keypad layout

4.4 Entry view screen

The password entry view screen (see figure 5) lets you view a password entry with all of its details. The first thing displayed is the entry kind with its icon (in case of figure 5 a web login), the entry details and the entry time stamps.

The entry time stamps help you manage your entries better. You can synchronize your entry creation time stamp with your e-mails to look for registration e-mails. You can use the modification date to track the age of an entry and change the password after a certain period of time.
Commands:

Edit: Brings you to a screen to edit the current password entry.

Back: Goes to the folder overview (see section 4.1).

Figure 5: The password entry view screen

4.5 Entry editor screen

The password entry editor screen (see figure 6) lets you modify a new or existing password entry with all of its details.

The first thing displayed is the entry kind with its icon (in case of figure 5 a web login). After this you select the folder to store the entry in. Following this are the entry-kind specific fields.

4.5.1 Password proposal

If you create an entry you're proposed a new generated password in the password field. This is to help you choose secure passwords instead of reusing the same password over and over again. If one of the reused passwords get stolen or eavesdropped, the thief can easily crack all your other accounts. Of course you can ignore the proposal and enter your own password. Note: The auto-generation is only done if it makes sense for this password kind. You usually can't chose your credit card PIN, you have to live with the one given by the credit card company.

Depending on the kind of password, password proposal uses different character sets for password generation. For textual passwords, password proposal uses all lower case and upper case letters and all digits with the following exceptions:

l (ell): Can be mistaken for 1 (one) or I (Ireland).

1 (one): Can be mistaken for l (ell) or I (Ireland).

I (Ireland): Can be mistaken for 1 (one) or l (ell).

O (Oscar): Can be mistaken for 0 (zero).

0 (zero): Can be mistaken for O (Oscar).

The exceptions from above are not used to use only easily distinguishable characters.

4.5.2 Field proposal

Besides password proposal there's also a feature called field proposal. There are certain fields for example user names that are reused by most users, for example the user names in social communities[3]. Tresør marks the proposed fields labels with the 'proposal' word to indicate that the fields are auto-generated and you're not editing an old password by mistake because you see well-known data.

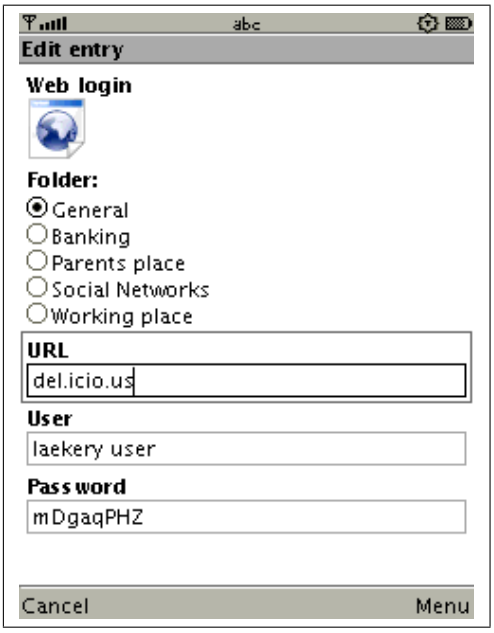

Figure 6: The password entry editor screen

Commands:

Store: Commits the password entry change and stores it in the password key ring.

[3]Note that reusing user names is also a security risk. It's much less dangerous than reusing passwords.

Generate secret: Goes to a screen where you can generate a new password. Generated passwords contain more entropy (=secureness) than human generated passwords. Please see section 4.6 for the description of this screen.

Cancel: Aborts the editing of the entry without storing the changes.

Change kind: Changes the kind (i.e. web login, computer login, EC card) of the entry. Only certain kind changes make sense. No data is lost when changing the password kind, but it may get hidden unintentionally if the target kind has less entries.

4.6 Password generator screen

The password generator screen (see figure 7) lets you create secrets with sophisticated algorithms. Generated passwords contain more entropy (=secureness) than human generated passwords.

When you first enter the screen the old password is displayed. You need to explicitely generate a secret to go on. The characters of the passwords are determined by the password entry kind. Credit cards only have numerical secrets, web passwords have usually alphanumerical characters.

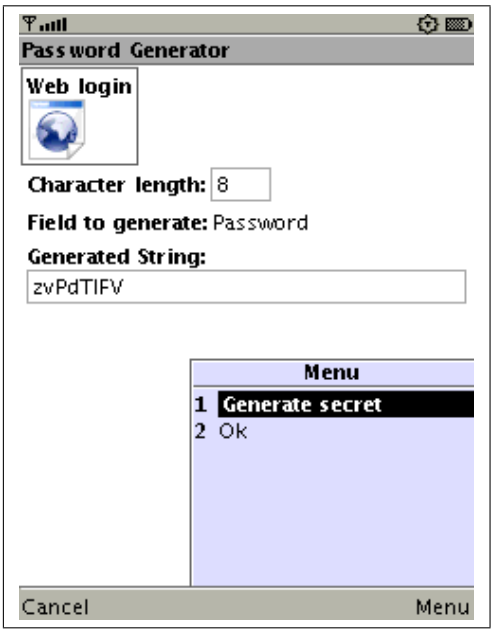

Figure 7: The password generator screen

Commands:

Generate secret: Creates a new secret and displays it. Nothing will be stored with this operation. You can view the password and take a look at it if it is okay for you. Because some phone fonts may have indistinguishable characters for 0 (zero) and O (Oh) or 1 (one) and l (el), these characters are left out of the random selection process.

Ok: Take over the password into the password entry editor screen (see section 4.5). The password is still not stored, it must be stored in the password entry editor screen.

Back: Goes back to the entry editor without taking over the generated password.

4.7 Maintenance screen

The maintenance screen (see figure 8) is for all actions that affect maintaining your password key ring. The screen itself shows some statistics about the currently active password key ring. The date given in *Written at* is in ISO 8601[4] format.

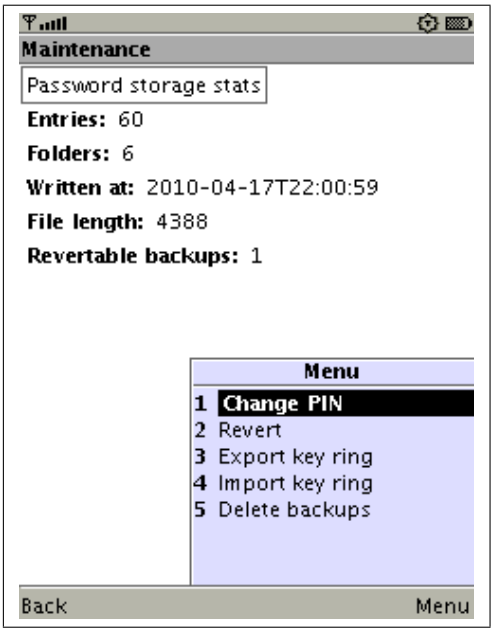

Figure 8: The maintenance screen

Commands:

Change PIN: Brings you to a screen to change your master PIN. See section 4.9.

[4]For a discussion of the ISO 8601 format please navigate to The ISO introduction to ISO 8601

Revert: Lets you go back in the list of changes you did to the password key ring. This technique is comparable with the well known *undo* operation desktop applications provide. Please see section 4.10 for more on the screen this command leads you to.

Export key ring: Exports the password key ring to the phones file system using the JSR 75 functionality. The exported file is still PIN-encrypted and can be backed up to a computer.

Note: The export command won't be shown if there's nothing to export.

Import key ring: Imports a password key ring from the phones file system using the JSR 75 functionality. Reading the imported file requires the PIN it was encrypted with. This PIN may be different to the PIN of your current password key ring!

Delete backups: Deletes all unnecessary backups of your password key ring. You remove the undoable backups you could *revert* to with this command.

4.8 Export screen

After chosing the destination folder you can enter the export file name on the export screen (see figure 9) . A file name including the current date is proposed by default. The date is given in ISO 8601 format.

You get some details about the file like the file size in bytes and the files cryptographic MD5 message digest. The message digest can be used to verify on your desktop computer that storing and file transfer worked and you have a valid file. On Unix systems there's often the command line utility `md5sum`. There are also many free utilities for other computer platforms.
Commands:

Export key ring: Writes the password key ring file to the phones file system. After successful writing a short info is displayed on the screen for feedback.

Cancel: Cancels the operation without saving.

4.9 Change PIN screen

The PIN changing screen (see figure 10) you can change the master PIN for your password key ring. You need to enter the old PIN to verify that you're authorized to change the PIN. Out of that you need to enter the new PIN twice.
Commands:

Figure 9: The export screen

Figure 10: The change PIN screen

Store: Stores the password key ring encrypted with the newly chosen PIN. Note that your backup password key rings are still encrypted wit the old PIN. After successful storing you need to login with your new PIN the program starts up next.

Cancel: Cancels the operation without saving.

4.10 Revert screen

The revert screen (see figure 11) lets you go back in the history of changes you made to your password key ring. This is comparable to the *Undo* function many desktop applications offer. The number of stored backup copies is limited due to security considerations and resource economy on a mobile device. The oldest copies get removed when new backups are stored.

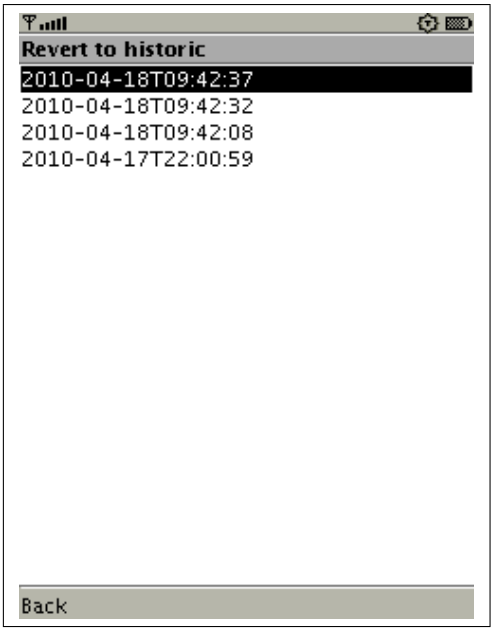

Figure 11: The revert screen

The screen allows you to chose a certain copy that is labeled with the time stamp of the copies writing. When you load a reverted copy it gets loaded but *not marked the current copy*. You need to modify something [5] in order to make it the current copy.

This means if you load a reverted copy and exit the application without saving, you'll still see your most current password key ring when you start Tresør again.

[5] For example edit and store a folder name.

You need to use your mobile phones *select* button to chose the desired backup entry. If your backup password key ring was stored with a *different PIN*, then you'll be queried for the old PIN you used.

5 Troubleshooting

This section tries to help with problems or questions that arise when using Tresør.

5.1 Frequently asked questions

In the following we'll address frequently asked questions about the Tresør application.

1. **Question:** PIN storing doesn't work! I see something with RecordStoreException!
   Answer: On some phones you need to move the application to the phones internal memory.

2. **Question:** Importing and exporting password files (JSR 75) doesn't work.
   Answer: On most phones you need to give the application the right/permission to read and write data before import and export works. Out of that, check with your phone manufacturer that your phone supports the optional JSR 75 (PDA Optional Packages for the J2ME™ Platform) functionality.

3. **Question:** Why exits the application after 2 minutes?
   Answer: It's a security function to exit the application after 2 minutes of inactivity. This protects your data in case you leave your phone with the application started and PIN entered somewhere unwatched.

4. **Question:** The backlight of the display goes off before I can finish copying my password. Can you change that?
   Answer: There is no manufacturer independent way to accomplish this. You'd have to change the general display or power saving settings of your phone.

5. **Question:** How can I protect myself from data loss?
   Answer: Export your passwords often to your micro SD storage and/or to your desktop computer.

6. **Question:** How can I migrate my data to a new phone?
   Answer: Follow these steps:

(a) Export your passwords on the old phone,

(b) move the export file to your new phone (using your PC),

(c) install Tresør on the new phone,

(d) import the file on the new phone using the newly installed Tresør application.

7. **Question:** How easily can my master PIN be cracked?
   Answer: The longer your PIN is the better. Internal testing in 2010 with current consumer hardware has given the following numbers for a brute-force-attack:

PIN digits	Time to crack
6	10 seconds
7	111 seconds
8	20 minutes
9	223 minutes
10	41 hours
11	18 days
12	207 days
13	6 years

   Please note that the numbers may differ in a big magnitude if the attackers have good equipment and good IT skills.

8. **Question:** How many digits should my PIN have?
   Answer: If you lose your cell phone or it gets stolen you should have enough time to disable your bank and web accounts. Take a look at the table above and add some extra safety.

9. **Question:** I've forgotten my PIN. Can you help me?
   Answer: It's our policy to not crack or help cracking PINs and break laws.

10. **Question:** How secure are my passwords?
    Answer: The passwords are encrypted using the AES-256 algorithm with a random initialization vector and SHA-256-hashed PIN. The PIN hash itself is not stored to disable rainbow table attacks.

11. **Question:** Can a thief extract the (encrypted) passwords to his PC without the PIN?
    Answer: It depends on your mobile phone implementation. You should calculate that he can. A good precaution is storing Tresør in the phones internal memory.

12. **Question:** Why is the PIN numeric? An alphanumeric PIN would be more difficult to break.
    Answer: That's right. Restricting the PIN to be numeric speeds up application usage on numeric keypad phone models. On this type of phones the risk of mistyping alphanumeric PINs is much larger.

13. **Question:** Are the passwords encrypted?
    Answer: Yes. They are stored in encrypted form in the phones persistent memory and are only decrypted when you're working with the passwords.

14. **Question:** Are the non-password informations also encrypted?
    Answer: Yes.

15. **Question:** Can I send the exported password ring file using the mobile phones e-mail client?
    Answer: Yes. You should ensure that your PIN is strong enough (see question 7) before doing so because in the internet there's the chance of eavesdropping and man-in-the-middle attacks.

16. **Question:** Chosing an export folder doesn't work!
    Answer: You need to chose the folder, when it's under the cursor press 'ok'. Then you'll have the chance to enter the file name. This is somehow different than this works on desktop computers.

17. **Question:** What if my question isn't answered here?
    Answer: Customers can reach the customer support at the address given in section 5.2.

5.2 Contacting customer support

For all questions not covered in the above FAQ (section 5.1) the customer support can be reached at the following e-mail address:

`support@laekery.com`

Please describe your problem as detailed as possible so our support can help you quickly: The software version number (shown at the startup screen), error codes, error messages and the actions that led to an error are of importance for us to reconstruct your problem.

6 Legal

All trademarks used in this document and the application besides *Laekery* belong to the appropriate owners.

6.1 Tresør license

You can obtain a license of Tresør by buying a copy of the software from a contract dealer of Laekery.

The license for Tresør (the software) has the following terms:

§1 **Usage:** You may use the software on devices that are your property. You may not sell devices containing the software without first deleting the software.

§2 **Backups:** You may make as many backup copies of the software as you like of the software as long as it stays in your property and on devices that are your property.

§3 **Access:** You may *not* give access to someone else to the software or files written by it.

§4 **Reverse Engineering:** You may *not* reverse engineer the software or files written by it.

§5 **Alteration:** You may *not* alter the software or files written by it without the authors permission.

§6 **Distribution:** You may *not* distribute, sell or rent the software without the authors permission.

§7 **No Warranty:** The software is provided *as is*. You have no right for the correct operation and data integrity.

§8 **No Compensation:** You have *no* right for compensation in case of data loss, data theft, information theft, money theft, credit card fraud or other damage in direct or indirect conjunction with the software.

§9 **Other Contracts:** The software does not affect other contracts you have. If there are other licenses affecting software, this license supersedes them (with the exception of the code listed in section 6.2).

§10 **Custom Development:** The licensee can contact the licensor for different license models that cover new features or special software versions.

§11 **Limited Support:** You have *no* right for response times or accuracy of the responses of customer support.

6.2 Subportions licenses

6.2.1 LWCrypto

This software uses code from the bouncy castle lightweight crypto API. The license for this subportion of the software is given in the following passage:

> Copyright © 2000-2009 The Legion Of The Bouncy Castle (`http://www.bouncycastle.org`)
>
> Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ”Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
>
> The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
>
> THE SOFTWARE IS PROVIDED ”AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

6.2.2 Icons

The icons were taken from public domain sources. The license given in 6.1 does not affect the icons inside the program except the Tresør (yellow key) icon.

Index