# BeanTresor

## Specifications

Kim D. Jeker
**kije-dev**

December 22, 2014

# Contents

# 1 Introduction

### The Problem(s)...

Today, every user has do deal with dozens or even hunderts of passwords daily. This often causes users to reuse the same password on multiple sites.

While this seems very convenient, it's very insecure and can be even dangerous[1], because if someone can retrive the password from one site, he is able to login to other sites where the user also has used this password.

One might argue, nowadays this isn't as much a problem as it was some years ago, since most Online Services started to hash[2] their user's passwords. While this is true, we need to acknowledge that breaking into a database is not the only way to get passwords from users. For example, an attacker can also spy on a user's connection, or he can simply brute-force the password.

Unfortunatelly, the use of a new password for every site (one-time passwords) will not prevent attackers from retriving passwords. But it will minimize the damage caused to the user in such a case.

An other problem is the strength of passwords. In order to remember a password, users often use the name of one of their friends, family members, pet, girl- or boyfriend etc...as their password, which isn't very secure.

### ...and the solution

To make it, nevertheless, easy and convenient for the user to create and use **secure** one-time passwords, we need password managers.

Such a password manager will be **BeanTresor**. It will be focused on a very user-friendly user interface and should be cross-platform and open-source.

[1] e.g. use the same password for `themaliciousshop.com` as for e-Banking
[2] Often also refered as "encrypt", but this is technically not quite correct