密码本

1. 背景

随着信息化的一步步走进人民的生活中，需要大家记住账号和密码的地方越来越多。绝大多数采取的方式都是生日、手机号、名字拼音等方式去组合，账号越来越多容易记错和混淆。修改密码造成的时间成本、金钱成本也越来越高。

现在各种云存储密码的方式确实能够解决此困惑，但是密码等数据存储在云端非常容易被云端技术公司和人员获取。绝大多数人对云端的存储解决方法是非常不信任的。

至此打造一款本地版本的密码钥匙扣呼之欲出，解决人们对密码存储的需求。用一组密码或者生物认证打开名下信任的密码账本。

密码钥匙扣需要具有以下的功能：随机密码生成、账号密码加密存储、账号密码找回机制、双密码认证机制、密码账本备份、定期更换密码提醒和一账号多组密码等功能。

1. 名词解释

|  |  |
| --- | --- |
| 名词 | 解释 |
| 主密码 | 由客户输入的用于解开存储密码本的密码。 |
| 副密码 | 针对特殊的密码本记录的密码，需要二次认证才能获取的解密密码。 |
| 物理密码 | 二次认证的系统自动分配一个加密的密文单独存储，方便解密使用。一般和主程序不同一地点存放。 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. 功能需求和设计
   1. 随机密码生成

随机的生成12位的字母和大小写字母组合的随机密码。用户也可以调整策略按需重新生成希望的密码。生成时自动规避用户提供的例如生日、手机号等屏蔽密码组合。

* 1. 账号密码加密存储

用户输入的密码等机密信息通过多重可逆加密方式进行存储，防止意外暴力方式破解。将主密码加入到加密计算过程中。更换主密码的时候全部重新加密所有密码存储数据。

加密过程和步骤前期设计的足够复杂后续不允许修订和调整。方便长期兼容各种版本。

* 1. 账号密码找回机制

用户忘记主密码，可以通过验证密保密码找回。找回密码密码如果指定计算机，将只能由固定的计算机和账号才能找回指定的密码。如果不指定计算机，则由任意的计算机和账号都能找指定的密码。

* 1. 双密码认证机制

对于特殊的密码除了主密码外，允许输入副密码双重认证。副密码通过字符密码、物理密码、邮箱验证码或手机验证码方式认证。

* 1. 密码账本备份还原

将完整的数据备份打包备份到另外的地方。方便公司和家庭多地存储。后续做用户数据云端存储。

* 1. 定期更换密码提醒

每次打开程序提供用户更新密码，更新周期默认三个自然月，也可以由用户自行设定更新密码周期。

* 1. 一账号多组密码

一个账号允许用户存储多组密码。例如：银行的账号有登陆密码、U盾密码、手机密码和一网通密码等。