

**<<密宝软件系统>>**

**需求规格说明书**



北京航空航天大学

2015-11

版本变更历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 提交日期 | 主要编制人 | 审核人 | 版本说明 |
| 1.0 | 2015.11.29 | 丁蔚然 | 丁蔚然 | 系统需求规格说明书初版 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

[1. 范围 1](#_Toc307900541)

[1.1 标识 1](#_Toc307900542)

[1.2 系统概述 1](#_Toc307900543)

[1.3 文档概述 1](#_Toc307900544)

[1.4 术语和缩略词 1](#_Toc307900545)

[2. 引用文档 1](#_Toc307900546)

[3. 功能需求 2](#_Toc307900547)

[4. 数据需求 2](#_Toc307900548)

[5. 非功能需求 2](#_Toc307900549)

[6. 运行需求 2](#_Toc307900550)

[6.1 硬件接口 2](#_Toc307900551)

[6.2 软件接口 2](#_Toc307900552)

[6.3 用户界面需求 3](#_Toc307900553)

# 范围

## 标识

文档标志号：A2015-00-01-00

文档标题：项目系统需求规格说明书

版本号：1.0

## 系统概述

随着互联网技术不断发展，人们需要管理的账号和密码越来越多，为了方便记忆，多数人只使用简单密码，或与个人信息有关的密码，或直接将多个不同账号的密码设为同一个，造成非常大的安全隐患，所以构建一个优秀的密码管理系统很有必要。

本系统结合当今快速发展的计算机网络，用于为广大上网者提供便利。网络飞速发展，而网站的登录方式还是一成不变，所以，这样一个密码管理系统应具备如下特点：

* 具有极强的稳定性、最高级别安全保密性：通过安全高效的权限访问控制、信息加密包含和完整性鉴定等一系列策略，以解决密码管理系统的安全性、保密性问题，软硬件结合，多重密钥保障，防止信息被盗和非法的入侵；
* 使用便捷：本系统颠覆传统密码模式，所以不仅从管理入手，操作上亦要保证简约到极致。简约却不简单，这是本系统的要义；
* 可扩展、可定制性：密码管理若便捷起来可以拓展到多个平台、多个领域，这对于信息之间的交流有着重大的意义。所以，密码管理的业务是动态和变化的，系统设计更要着重于软件的可扩展性、可定制性。在今后系统扩充升级时，能够利用和保护已有的系统，既能满足当前业务的需求，又为今后的扩充留有空间；
* 规范密码标准：利用此系统简化登录流程，可保障每个用户密码为最高级别并符合安全标准。必要时动态修改账户密码，保证一切对密码的操作均规范化；
* 系统简单、易维护、易使用：系统功能完备实用，界面UI友好清晰。网络结构简单明了，层次清楚，便于管理。

|  |  |
| --- | --- |
| 项目 | 说明 |
| 系统定位 | 跨平台全功能高级别密码管理系统 |
| 创新形式 | 告别一切繁琐，毋须记忆，颠覆传统密码管理形式 |
| 用户定位 | 所有网民，尤其是账户覆盖较广的用户 |
| 系统基本功能 | 无密码实现账户登录，关键文件云端同步校验，全平台运行 |

项目的需求方为广大账户较多的网民、用户为所有网民，开发方密宝软件开发团队，目前项目正处于开发过程中。

## 文档概述

本文档用于明确各部分功能及系统各类需求，包括系统总体结构设计与系统功能结构设计需求、数据加密技术实现需求、综合业务系统子程序实现需求、综合查询系统子程序实现需求、统计分析子程序设计需求与信息管理数据库设计需求。与此同时，此文档还将阐述系统设计结构，以及各子功能块之间的联系。除此之外对需要实现的接口进行说明，便于开发实现。

## 术语和缩略词

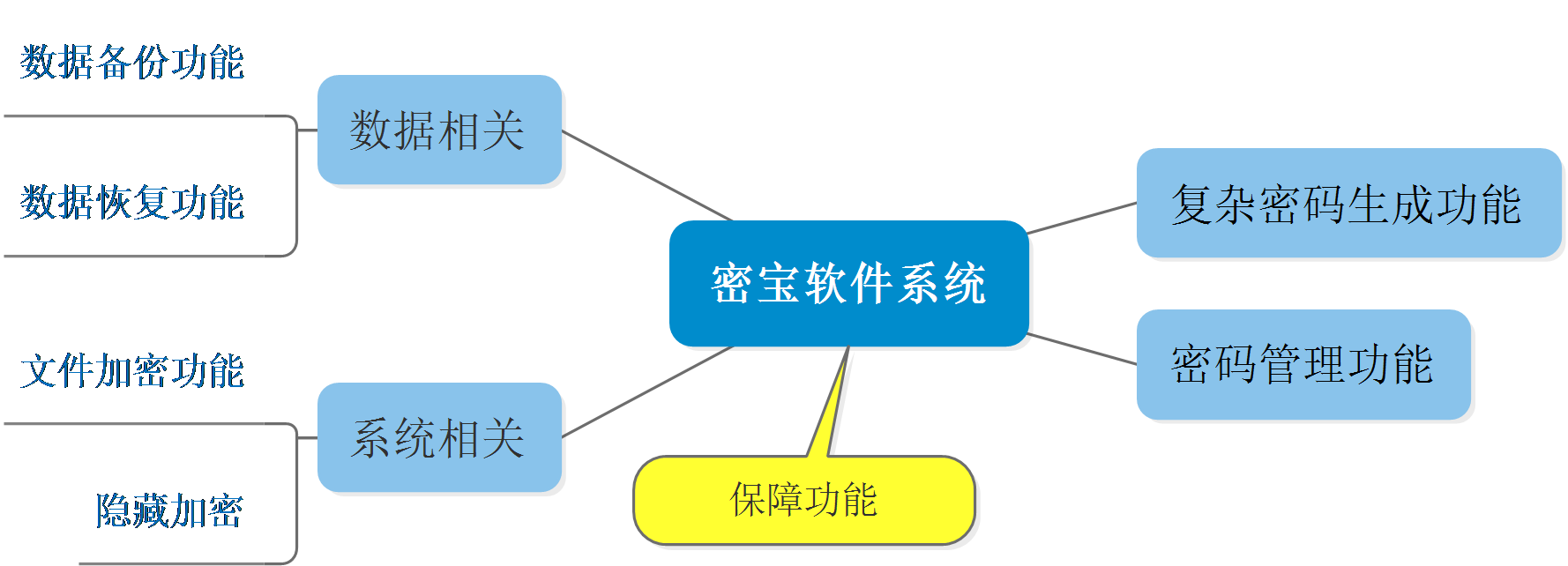
**SRS**：软件需求规格说明书（System Requirement Specification）

**IDE**：集成开发环境（Integrated Development Environment）

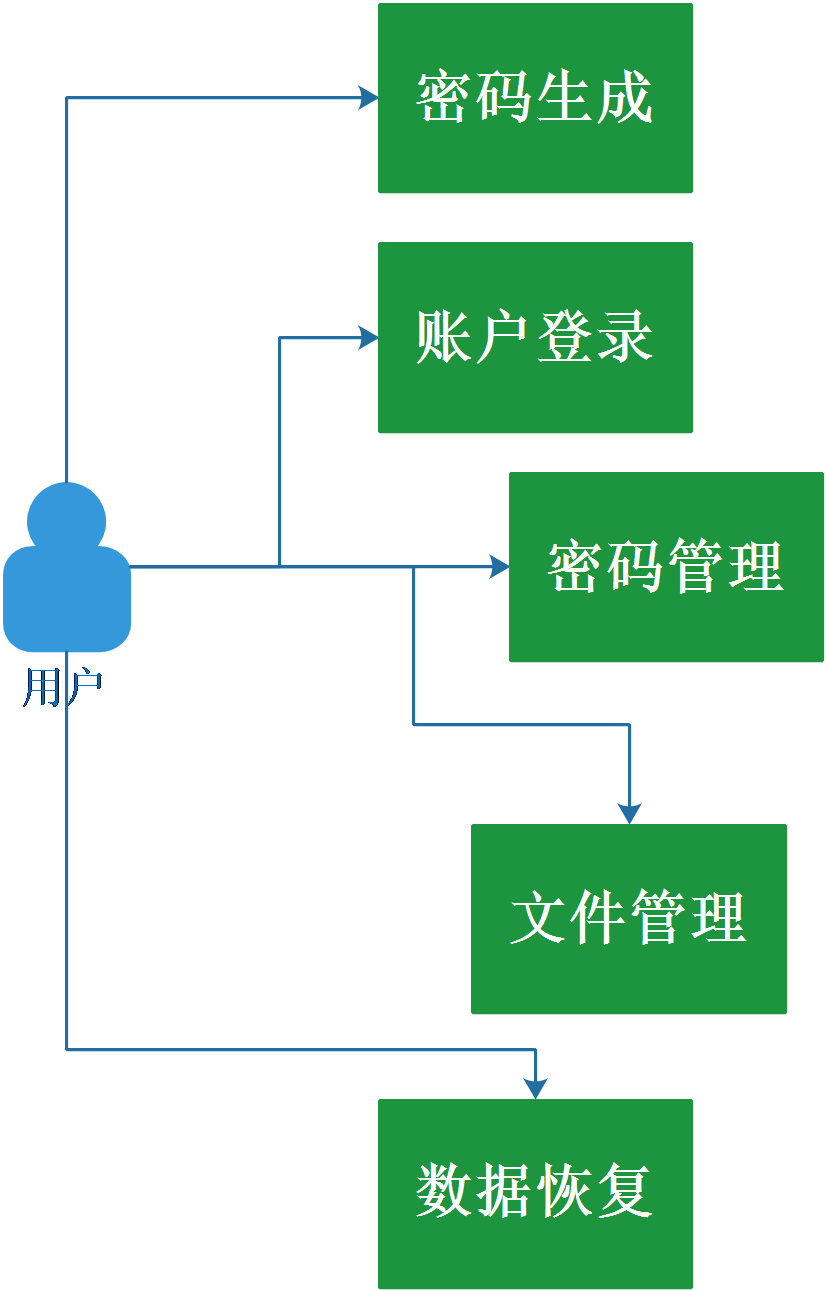
# 引用文档

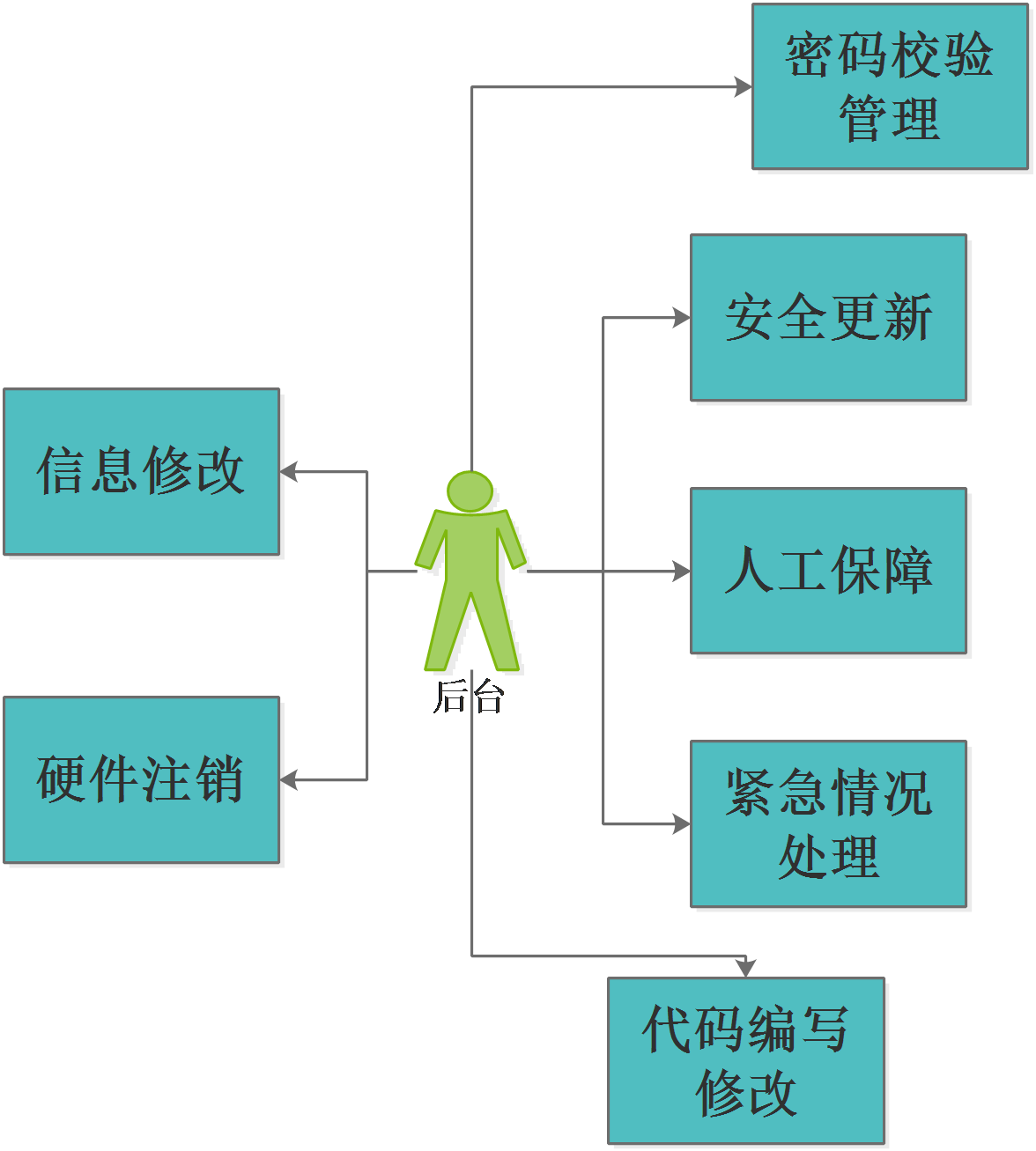
1. 密宝软件系统项目任务书
2. 密宝软件系统软件开发计划书
3. 徐孝成.基于Android的密码管理系统的设计与实现.北京林业大学.2013.
4. 王卓.基于网格的分布式密码管理系统设计与实现.解放军信息工程大学.2009.
5. 杨飞麟.银行动态密码管理系统的分析与设计.厦门大学.2013.
6. 彭家华.基于MD5的应用程序授权及密码管理系统.2009.
7. 邸鑫.批量密码管理子系统的设计与实现.吉林大学.2010.
8. 王刚.ATM动态密码电子锁管理系统的设计与实现.2013.
9. 戴欢.基于B/S模式的中学图书管理系统设计与实现.山东大学.2012.

# 功能需求



以上为团队整个系统的功能结构，面向的用户和后台的管理分别如下：





* 复杂密码生成功能

根据用户的需要，可选择大小写字母、数字、特殊符号等，生成用户指定的长度的伪随机字符串当作密码，默认为所有类型字符都包括。并且，对于多种类型字符的密码，须保证每种字符的个数较为平均。

* 密码管理功能

将用户的账号、密码、账号相关信息等列表并存入文件中。这个文件要有必要的加密、签名、冗余等，以提供保密性、数据完整性、可用性支持。给用户提供创建、增加、删除、修改、查询等接口，以管理这些账号信息。上文中“账号相关信息”包括注册这个账号时需要用户记住的诸如邮箱、电话号、保密问题等等，要给用户提供定义相关信息的接口，以方便用户加入其他的账号相关的信息。

* 数据备份功能

密宝需要给每个用户在云端提供一个小的在存储空间，用于在云端备份用户所要管理的账号密码等信息。同时，在本地也会在其他位置（用户指定或者系统默认）另外备份一份数据，并实时更新，以确保用户在重装系统、更换平台、更新软件、文件损坏等情况下，之前保存的数据可用。

* 数据恢复功能

在软件工作目录下的数据文件损坏、丢失或被恶意篡改时，用本地或者密宝云端中备份的数据文件恢复数据。

* 文件加密功能

用户可以使用密宝软件对任意文件加密，同时提供“隐藏加密”功能，即加密后的文件在用户的操作系统中看不到。加密时，用户可以选择加密算法、加密密钥等，也可以使用默认加密算法并使用密室硬件提供的密钥进行加密。同时，还给用户提供诸如文件 Hash 码验证、签名验证等辅助功能。

* 保障功能

如果用户的密宝硬件丢失或损坏，密宝团队需要给用户提供类似银行卡挂失的功能，使那个密宝硬件无效。当用户认为密宝硬件中保存的密钥不再安全时，或者密宝团队认为那个密钥使用时间过长必须更换时，要在人工参与的前提下更新密宝硬件中的密钥。当用户的身份信息发生变化时，密宝团队需要更新用户身份信息以保证系统的可用性。以上服务都必须有人工参与，以确保用户的身份得到确认。

# 数据需求(ER图)

描述该系统所涉及的数据实体。以ER图的方式给出基本的数据实体以及关系，再针对每个数据实体的数据项进行展开介绍。

# 非功能需求

## 系统可移植性

本系统应有良好的可移植性，不需要做大量代码修改就可完成软件的跨平台运行。要求少用系统特有的特性，如尽量不要使用WINDOWS的API。分离前后端，后端包括数据库、系统内部机制；前端通过后端提供的统一接口访问后端数据；在实现跨平台软件开发时，只用修改前端，减少对后端做出的修改。

## 系统安全性

建立完整的权限机制，以保证本系统的安全性。只有管理员才有权限直接修改后台数据，只有输入正确的口令，才能被授予管理员权限。商家和用户的权限较低，只能修改与自己有关的数据，数据可视范围也有限制；要实行这些权利，也需要通过口令获得授权。

## 系统可靠性

本系统的可靠性要求达到97%以上，能较快响应用户的操作。具有较高的容错性能，发生系统故障时不至于让系统崩溃，且能及时保存故障时的数据，保证后面的恢复工作顺利进行。

## 系统可扩展性

本系统应具备良好的可扩展性，保证以后能持续添加新的功能，满足日益复杂的用户需求。要求代码有良好的框架设计，保证接口统一且合理，减少后期对接口的修改，采用模块化编程的思想。

## 系统可维护性

系统编写时要求有20%以上的注释，以便当系统出现问题时，软件维护人员容易对软件进行修改。应当有特定的数据库维护人员对数据库进行及时的备份，以保证数据库的安全性。

## 系统易用性

要求系统提供良好的用户接口，易用的交互界面。常用功能应出现在界面易见位置，使用通俗易懂的文字描述，提供使用手册和在线帮助。系统要提供方便的手段供系统维护人员进行数据的备份，日常的安全管理，系统意外崩溃时数据的恢复等工作。

# 运行需求

## 硬件接口

密宝硬件系统，密码的生成管理等均需要密宝开发的硬件来支持。

## 软件接口

random.org真随机数接口，对于高级用户，密码安全性需求高时，可调用该随机数网站接口生成真随机数，并通过相关算法进行用户随机密码的生成；

DBMS（Database Management System），如Access、SQL Server、Oracle等，可以实现对数据的访问功能；

NET框架使用ADO. NET完成对数据库的访问：ADO. NET技术是一个基于标准的、面向创建的、分布式数据共享应用程序的编程模型。

应用层是应用程序和用户交互的层，将系统的业务功能在浏览器上显示出来，通过页面调用用户控件的方法，用户控件调用基础类的方法，基础类再调用SQL存储过程，实现用例；业务逻辑层将用户需求的信息转化为抽象的类和对象，在数据访问层调用存储过程，直接与数据库进行交互，实现具体的业务逻辑功能，处理应用层传输过来的用户响应，并将结果返回给应用层；数据层实现对数据的访问功能，在SQL Server上建立相应的数据库，数据库中包括若干张表。

## 用户界面需求

用户界面保证简洁明了，对于需求较小的用户直接不给出图形界面，只要硬件信息吻合，即获得登录准入。对于密码管理、删改等需求，可通过web界面列出，即保证不会有对于软件的篡改，同时保证用户登录页面的时候都是最新的版本，更大程度上保证了安全。