|  |  |
| --- | --- |
|  | 密级：内部 |
| 版本：A/0 |
| 状态： |
| 文件授权管理软件  设计说明书  LS JS(1)-WJSQGLRJ-SDD  北京连山科技股份有限公司  2020年12月 | |

|  |  |  |  |
| --- | --- | --- | --- |
| 项目名称 | 文件授权管理软件 | 项目编号 | LS-WJSQGLRJ |
| 文件名称 | 软件设计说明书 | 页数 | 15 |
| 签署栏 | | | |
|  | 签名 | 日期 | 职务 |
| 编制 | 路国强 | 2020-12-17 | 软件工程师 |
| 校对 | 林玉超 | 2020-12-17 | 软件工程师 |
| 审核 | 阎威 | 2020-12-17 | 软件工程师 |
| 标审 |  |  |  |
| 会签 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 批准 |  |  |  |
| 摘要：  本文档针对文件授权管理软件的各项软件功能需求进行了分析,提出了满足需求的各种具体软件设计方法 | | | |

文件修改记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 修改内容 | 修改人 | 修改日期 | 备注 |
| A/0 | 创建文档 | 路国强 | 2020.12.17 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[1 软件标识 1](#_Toc59702005)

[2 系统概述 1](#_Toc59702006)

[3 系统级设计决策 1](#_Toc59702007)

[3.1 系统功能、行为设计 1](#_Toc59702008)

[3.2 系统界面设计 3](#_Toc59702009)

[3.3 系统安全性设计 9](#_Toc59702010)

[3.4 系统保密性设计 9](#_Toc59702011)

[4 系统体系结构设计 9](#_Toc59702012)

[4.1 架构设计与系统逻辑部件组成 10](#_Toc59702013)

[4.2 接口设计 11](#_Toc59702014)

[5 详细设计 14](#_Toc59702015)

[5.1 硬件通信库 14](#_Toc59702016)

[5.2 管理员软件 14](#_Toc59702017)

[5.3 用户软件 14](#_Toc59702018)

[6 注释 15](#_Toc59702019)

# 软件标识

1) 软件名称：文件授权管理软件

2) 软件标识号：LS-WJSQGLRJ

3) 软件版本号：V1.0

# 系统概述

文件授权管理软件，是提供文件加密存储的软件，通过本软件，用户可以把需要发送给对方的软件，使用对方的公钥进行加密，从而保证加密文件只有对方可以打开。

# 系统级设计决策

## 系统功能、行为设计

### 管理员软件

#### 管理员初始化

管理员初始化即，管理员软件第一次使用时，对管理员进行初始化的操作。初始化时，会要求输入管理员密码，软件会自动对密码进行MD5加密后，保存到本地。完成以上操作后，即完成了管理员初始化。

#### 管理员登录

管理员登录即，管理员输入登录密码，进行登录的操作。只有登录成功后，管理员才可以进入主界面进行用户管理、密码修改等操作。

管理员刚初始化完成后的登录密码，即为初始化时的密码。

#### 生成密钥对

管理员需要对所有用户的密钥信息进行管控，因此所有的公私钥对，应当在管理员软件中生成，然后分发到各个用户中。

目前，生成密钥对时，会自动生成1024对公私钥对。

#### 用户管理

用户管理即对用户的添加、更新、删除、查看等操作。

* 添加用户：插入UKey，输入用户名，点击添加用户按钮，即可添加一个用户。用户添加完成后，默认用户名为6个0。
* 更新用户：插入UKey，输入用户名，点击更新用户名按钮，即可对用户的用户名进行修改。
* 删除用户：插入UKey，点击删除当前用户按钮，即可删除该UKey对应的用户。
* 刷新用户：插入UKey，点击刷新用户信息按钮，即可查看到当前用户的用户名。

#### 修改密码

密码修改即对管理员的密码进行修改的操作。用户输入原密码、新密码，点击修改密码，即可完成密码修改。

### 用户软件

#### 用户登录

用户登录即，用户输入UKey的PIN码，进行登录的操作。管理员添加一个用户后，默认密码为6个0，因此用户第一次登录时，应当输入6个0，稍后用户即可对用户密码进行修改。

#### 授权分发

授权分发即，用户把需要分发的文件，使用指定接收者的公钥，进行加密的操作，加密后的文件，只有指定接收者使用其私钥可以解密，其他用户（包括发送者）都无法解密该文件。

#### 解密阅读

解密阅读即，用户把分发给自己的文件，使用自身的私钥进行解密阅读的操作，只有发送给自己的文件，才可以解密成功，对于不是发送给自己的文件，直接解密失败。

#### 更新配置

更新配置即，更新用户UKey中保存的其他用户信息的操作。管理员添加用户时，前面分发的用户，没有保存后面分发的用户的信息，这时需要前面的用户通过更新配置操作，把后面分发的用户的信息（主要包括姓名、公钥等信息）保存到自身的UKey中。这样前面分发的用户，就获得了所有用户的信息，从而可以发送文件到任何给任意一个接收者。

#### 修改密码

密码修改即对用户的密码进行修改的操作。用户输入原密码、新密码，点击修改密码，即可完成密码修改。

## 系统界面设计

### 管理员软件

#### 管理员初始化

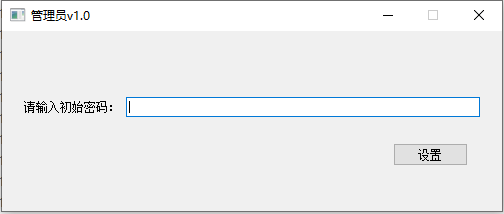


图 1 管理员密码初始化

#### 管理员登录

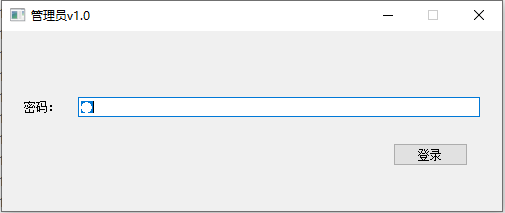


图 2 管理员登录

#### 生成密钥对



图 3 管理员生成密钥对

#### 用户管理

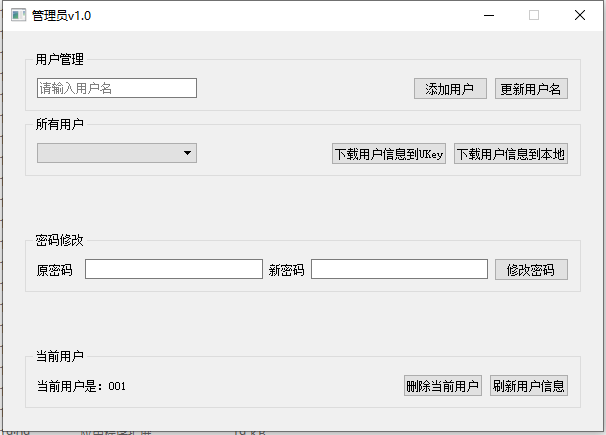


图 4 用户管理

#### 修改密码

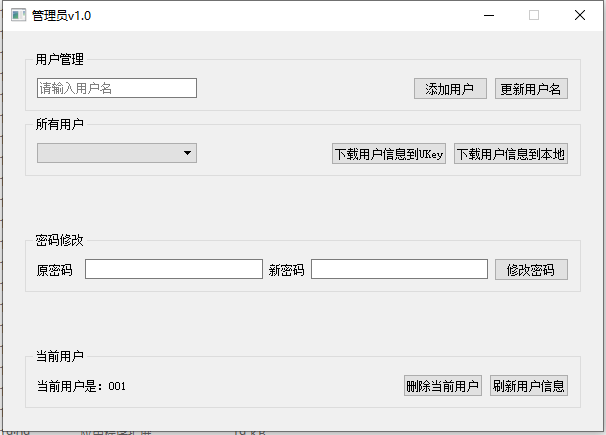


图 5密码修改

### 用户软件

#### 用户登录

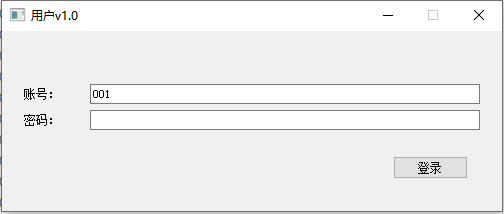


图 6 用户登录

#### 授权分发



图 7 授权分发

#### 解密阅读



图 8 解密阅读

#### 更新配置



图 9 更新配置

#### 修改密码



图 10 修改密码

## 系统安全性设计

本系统属于数据安全类产品。本软件采用软加密数据的方式对数据进行保护，运行期间只会读写特定的加解密文件，因此不会对用户的其他数据和计算机吞吐量造成不良影响；软件登录需要输入用户密码，保证了数据的安全性。

## 系统保密性设计

本项目为内部级项目，系统开发所涉及人员均将在安全控制范围内，严格遵守相关保密条例。

# 系统体系结构设计

管理员软件主要用于对用户（用户）的管理。主要功能包括密钥对的生成，对用户的添加、更新、删除、查看等。

## 架构设计与系统逻辑部件组成

管理员第一次使用本软件时，需要初始化密码。初始密码即为以后管理员登录使用的密码。

用户输入初始密码后，点击设置按钮，即可完成密码的初始化。

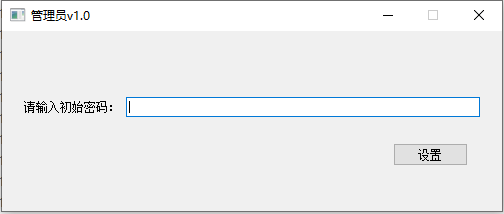


图 11 管理员密码初始化

### 基本架构

#### 硬件通信库

硬件通信库，为与硬件进行通信的Windows动态库。该通信库负责直接与硬件进行通信。管理员软件和用户软件通过此通信库与硬件进行通信。

#### 管理员软件

管理员软件负责对密钥对、用户进行统一的管理。包括生成密钥对，添加用户时把密钥对填充到UKey，导入用户信息到UKey等功能。

#### 用户软件

用户软件用于对文件进行授权分发以及解密阅读。

授权分发时，软件会生成一个随机密钥，使用随机密钥加密文件，然后使用接收者的公钥对此随机密钥进行加密，最后把加密后的随机密钥以及加密后的文件数据，写入一个文件。

解密阅读时，软件会先读取待解密文件中的随机密钥部分，然后使用私钥对随机密钥进行解密，最后使用随机密钥解密加密的文件数据，导入明文文件。

### 硬件环境

本软件对硬件环境无特殊要求，普通的个人电脑即可运行本软件。

## 接口设计

### 通信库接口

#### 获取设备列表

LS\_ERROR DEVAPI LS\_EnumDev(OUT LPSTR name\_list,

IN OUT ULONG\* size);

#### 连接设备

LS\_ERROR DEVAPI LS\_ConnectDev(IN LPSTR dev\_name,

OUT HANDLE \*dev\_handle);

#### 断开设备连接

LS\_ERROR DEVAPI LS\_DisConnectDev(IN HANDLE handle);

#### 生成随机数

LS\_ERROR DEVAPI LS\_GenRandom(IN HANDLE handle,

OUT BYTE\* random,

IN ULONG random\_len);

#### 导出SM2 公钥

LS\_ERROR DEVAPI LS\_ExportPublicKey(IN HANDLE handle,

OUT BYTE\* public\_key,

IN OUT ULONG\* public\_key\_len);

#### 导入 SM2 密钥对

LS\_ERROR DEVAPI LS\_ImportKeyPair(IN HANDLE handle,

IN BYTE\* public\_key,

IN ULONG public\_key\_len,

IN BYTE\* private\_key,

IN ULONG private\_key\_len);

#### 非对称加密

LS\_ERROR DEVAPI LS\_AsymEncrypt(IN HANDLE handle,

IN BYTE\* data,

IN ULONG data\_len,

OUT BYTE\* encrypted\_data,

IN OUT ULONG\* encrypted\_data\_len);

#### 非对称解密

LS\_ERROR DEVAPI LS\_AsymDecrypt(IN HANDLE handle,

IN BYTE\* encrypted\_data,

IN ULONG encrypted\_data\_len,

OUT BYTE\* data,

IN OUT ULONG\* data\_len);

#### 校验PIN码

LS\_ERROR DEVAPI LS\_VerifyPIN(IN HANDLE handle,

IN BYTE\* pin,

IN ULONG pin\_len,

OUT ULONG \*retry\_count);

#### 修改PIN码

LS\_ERROR DEVAPI LS\_ChangePIN(IN HANDLE handle,

IN BYTE\* old\_pin,

IN ULONG old\_pin\_len,

IN BYTE\* new\_pin,

IN ULONG new\_pin\_len,

IN ULONG max\_retry\_count,

OUT ULONG\* retry\_count);

### 管理员接口

#### 设置PIN码

int SetPIN(const std::vector<BYTE>& pin);

#### 验证PIN码

int VerifyPIN(const std::vector<BYTE>& pin);

#### 导入密钥对

int ImportKeyPairToUKey(const SM2KeyPair& keypair);

#### 写入存储区

int WriteToUKey(int sector\_offset, const std::vector<BYTE>& data);

#### 写入私有区

int WritePrivate(int offset, const std::vector<BYTE>& data);

### 用户接口

#### 读取存储区

int ReadFromUKey(int sector\_offset, int sector\_size, std::vector<BYTE>& data);

#### 读取私有区

int ReadPrivate(int offset, int bytes, std::vector<BYTE>& data);

#### 获取公钥

int GetPublicKey(std::vector<BYTE>& pubkey);

#### SM2加密

int SM2Encrypt(const std::vector<BYTE>& pubkey,

const std::vector<BYTE>& in,

std::vector<BYTE>& out);

#### SM2解密

int SM2Decrypt(const std::vector<BYTE>& in, std::vector<BYTE>& out);

#### SM4加密

int SM4Encrypt(const std::vector<BYTE>& key, const std::vector<BYTE>& in, std::vector<BYTE>& out);

#### SM4解密

int SM4Decrypt(const std::vector<BYTE>& key, const std::vector<BYTE>& in, std::vector<BYTE>& out);

# 详细设计

## 硬件通信库

硬件通信库负责直接与硬件进行通信，其中包括设备相关的设备的查找、连接、断开， PIN码相关的验证PIN码、修改PIN码，加解密相关的对称加密、对称解密、非对称加密、非对称解密。

管理员软件以及用户软件通过通信库与底层软件进行通信。

## 管理员软件

管理员软件主要包括管理员初始化、管理员登录、生成密钥对、用户管理、修改密码等功能。

* 管理员初始化：管理员第一次使用本软件时，需要初始化密码。初始密码即为以后管理员登录使用的密码。软件会把管理员密码计算哈希后，保存在本地的文件中保存。
* 管理员登录：管理员每次打开软件，都需要进行登录操作，登录完成后，才可以使用管理员软件的相关功能。
* 生成密钥对：因为管理员需要管理所有的用户，因此管理员需要保存一定数量的公私钥对，以分发给各个用户。管理员在第一次使用软件，进行初始化密码、登录操作后，软件会提示管理生成相关的密钥对。管理员点击生成密钥对按钮，即可生成一定数量的公私钥对。这些公私钥对用于分发给各个用户
* 用户管理：用户管理包括对用户的添加、更新、删除、查看操作。添加用户时，软件会自动把用户信息写入本地文件以及UKey中。
* 修改密码：管理员可以使用密码修改功能，对用户密码进行修改，用户输入原密码、新密码，然后点击修改密码按钮，即可完成对密码的修改操作。

## 用户软件

用户主要包括用户登录、授权分发、解密阅读、密码修改、更新配置四个功能。

* 用户登录：用户登录即，用户输入UKey的PIN码，进行登录的操作。管理员添加一个用户后，默认密码为6个0，因此用户第一次登录时，应当输入6个0，稍后用户即可对用户密码进行修改。
* 授权分发：授权分发，即对指定的文件，使用指定接收者的公钥，进行加密，保证加密后的文件，只能被接收者解密，其他用户无法解密。在待操作文件所在行，点击浏览按钮，选择需要授权分发的文件，然后在授权给标签后面，选择一个接收者，然后点击授权分发按钮，即可完成授权分发，文件加密完成后，会提供用户加密文件所在位置，用户把该文件发给接收者，接收者即可进行解密阅读。
* 解密阅读：解密阅读，即可用户授权分发的文件，进行解密阅读的功能。在待操作文件所在行，点击浏览按钮，需要接收到的授权分发文件，然后点击解密阅读按钮，即可对文件进行解密，文件解密完成后，会提示用户解密后的文件所在位置。
* 密码修改：用户可以使用密码修改功能，对用户密码进行修改，用户输入原密码、新密码，然后点击修改密码按钮，即可完成对密码的修改操作。
* 更新配置：由于管理员分配用户有前后关系，因此管理员前面分发的用户UKey中不包含之后分发的用户的相关信息。管理员录入所有用户后，可以下载用户信息到本地，然后分发给用户。用户在更新配置一栏，点击浏览按钮，选择管理员分发的用户信息文件，然后点击确定按钮，即可完成所有用户信息的导入。

# 注释

无。