**资金管理系统支持国家商用密码改造方案V1.1**

|  |  |  |  |
| --- | --- | --- | --- |
| **公司名称** | 深圳市金证科技股份有限公司 | **文档编号** |  |
| **文档名称** | 资金管理系统\_支付国家商用密码修改方案 | **文档版本** | 1.1 |
| **起 草** | 苏国兵 | **起草日期** | 2018.01.09 |
| **审 批** |  | **审批日期** |  |

**修订历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 日期 | 状态 | 修订人 | 摘要 |
| 1.0 | 2018.01.09 | C | 苏国兵 | 创建初稿 |
| 1.1 | 2018.04.16 | M | 高保君 | 调整“现状”、“改造方案”。 |
|  |  |  |  |  |
|  |  |  |  |  |

状态标识：C – Created A - Added M - Modified D - Deleted

目录

[1. 引言 4](#_Toc511749239)

[1.1. 目的 4](#_Toc511749240)

[1.2. 背景 4](#_Toc511749241)

[1.3. 项目目标 4](#_Toc511749242)

[1.4. 术语和定义 4](#_Toc511749243)

[2. 现状 4](#_Toc511749244)

[2.1. 资金管理操作员密码 5](#_Toc511749245)

[2.2. 各业务系统操作员密码 5](#_Toc511749246)

[2.3. 银行密码 5](#_Toc511749247)

[2.4. 资金密码 7](#_Toc511749248)

[2.5. 支付密码 8](#_Toc511749249)

[3. 改造方案 8](#_Toc511749250)

[3.1. 改造原则 8](#_Toc511749251)

[3.2. 资金管理操作员密码 8](#_Toc511749252)

[3.3. 各业务系统操作员密码 8](#_Toc511749253)

[3.4. 银行密码 9](#_Toc511749254)

[3.5. 资金密码 9](#_Toc511749255)

[3.6. 支付密码 9](#_Toc511749256)

[4. 改造范围 9](#_Toc511749257)

[4.1. 操作员密码 10](#_Toc511749258)

[4.2. 银行密码 10](#_Toc511749259)

[4.3. 资金密码 11](#_Toc511749260)

[4.4. 支付密码 12](#_Toc511749261)

[4.5. 外围配置 13](#_Toc511749262)

[5. 风险点 13](#_Toc511749263)

[6. 参考资料 13](#_Toc511749264)

# 引言

## 目的

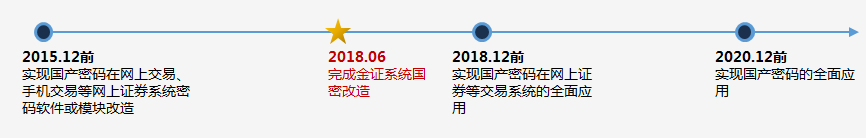
本方案是资金管理系统为支持国家商用密码进行改造的方案，描述资金管理系统密码现状、改造范围、改造方案、产品推进安排。

## 背景

为了保障商用密码安全，国家商用密码管理办公室制定了一系列密码标准。根据证信办[2014]157号文件《证券期货业国产密码应用推进规划方案》和国务院办公厅发布《金融领域密码应用指导意见》要求，公司发布会议，要求证券总部所有产品，使用的各种加密都要进行改造，会议内容见《【会议纪要】国密项目各系统方案沟通会会议纪要-20171222》。

## 项目目标

根据公司要求，在2018年6月前完成金证系统国密改造，2018年12前实现国产密码在网上证券交易系统全面应用。为此，资金管理系统目标在6月前完成国密改造，与各系统联调完成，并发布生产版本，版本同时支持新老两种密码加密方式。



## 术语和定义

国密：国家密码局认定的国产密码算法，即商用密码，也称为国家商用密码。

# 现状

目前资金管理系统有关的密码有资金管理系统操作员密码、各业务系统操作员密码、银行密码、各业务系统资金密码、支付密码、统一认证。

* 资金管理系统操作员密码

操作员密码由资金管理自主管理。使用场景有：

* WEB前端登录
* 其它业务系统调用资金管理系统功能时检查是否合法。
* 各业务系统操作员密码

在和业务系统交互时，各业务系统会校验操作员权限，目前访问各业务系统的操作员是固定的，连同操作员密码保留在配置表或配置文件中，各业务系统的操作员密码按照各业务系统要求的加密方式加密。

* 银行密码

银行密码发起方有外围、web客户端、账户系统、银行系统，发起方需要对银行密码进行加密操作。中间有三方交易网关连接资金管理到银行间的通道，银行密码由银行进行校验。

* 各业务系统资金密码

资金管理系统没有管理客户资金密码，处理业务需要校验资金密码时，向远程业务系统发送密码校验请求，由远程业务系统（集中交易、两融、期权）完成校验。

涉及到的业务有：券商端转账、银行端转账。

* 支付密码

支付密码由资金管理自主管理。用于校验支付业务密码，发起方有外围、web客户端、账户系统，需要对支付密码进行加密，资金管理接收到支付密码后校验。

* 统一认证

接入统一认证时，操作员密码和资金密码都到统一认证校验。

## 资金管理操作员密码

|  |  |  |  |
| --- | --- | --- | --- |
| **渠道** | **功能** | **入参** | **处理逻辑** |
| 资金管理Web前端  一柜通 | 密码校验 | KEY为操作员代码，采用AES加密，DLL：encrypt.dll 函数：AES\_ Encrypt1 | 数据库存储的密文采用AES加密 |
| 票据生成 |  | 标准KBSS票据生成算法 |
| 票据校验 | KBSS票据 | 标准KBSS票据校验算法 |

## 各业务系统操作员密码

柜员固定，密码固定，按各业务系统要求配置。

## 银行密码

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **发起渠道** | **资金管理** | | | | **外部系统** |
| **入参** | **内部处理** | | **出参** |
| W版外围 | 加密类型：’4’ AES算法，KEY采用资金账户  DLL：encrypt.dll  函数：AES\_Encrypt1 | 人民币：  不做处理 | | AES加密密文，KEY为资金账户 | 三方交易 |
| 外币：  用资金账户解密  DLL：encrypt.dll  函数：AES\_Decrypt1 | | 明文 |
| U版外围 | 银行密码：EXT\_ACC\_PWD | 用客户代码先解密，解密库CITICS\_CE.dll，解密函数UF\_CommDecrypt，再用外部机构加密  DLL：CITICS\_CE.dll  函数：UF\_CommEncrypt | | UF\_CommEncrypt加密密文，KEY为银行代码 |
| 期权外围 | KEY：资金账户  DLL：kbss\_encrypt.dll  函数：kbss\_comencrypt | 先用资金账户解密，解密库kbss\_encrypt.dll，解密函数kbss\_comdecrypt，再用资金账户加密，加密类型：’4’ AES算法，KEY采用资金账户  DLL：encrypt.dll  函数：AES\_Encrypt1 | | AES加密密文，KEY为资金账户 |
| 一柜通  Web3.5  账户系统 | 加密类型：’4’ AES算法，KEY采用资金账户  DLL：encrypt.dll  函数：AES\_Encrypt1 | 期权 | 不做处理 | AES加密密文，KEY为资金账户 |
| 对接W版 | 人民币不做转换 | AES加密密文，KEY为资金账户 |
| 外币用资金代码解密  DLL：encrypt.dll函数：AES\_Encrypt1 | 明文 |
| 对接U版 | 用资金代码解密，  用外部机构加密DLL：CITICS\_CE.dll  函数：UF\_CommEncrypt | UF\_CommEncrypt加密密文，KEY为银行代码 |

## 资金密码

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **发起渠道** | **资金管理** | | | **业务系统** |
| **入参** | **内部处理** | **出参** |
| W版外围 | 资金密码:fundpwd  加密类型:’3’W版外围算法 | 不做处理 | WIN版外围加密密文，KEY为资金账户 | W版 |
| U版外围 | 资金密码：AUTH\_INFO | 不做处理 | U版外围加密官文，KEY为客户代码 | U版 |
| 期权系统 | 资金密码:  加密类型：’4’ AES算法，KEY采用资金账户  DLL：encrypt.dll  函数：AES\_Encrypt1 | 不做处理 | 加密类型：’5’  AES加密密文，  KEY为资金账户 | 期权 |
| 一柜通  资金管理WEB客户端 | 加密类型：’0’ AES算法，KEY采用客户代码  DLL：encrypt.dll  函数：AES\_Encrypt1 | 用客户代码解密，  再重新加密，  KEY：资金账户  DLL：KDEncodeCli.dll  函数：KDEncode | WIN版外围加密密文，KEY为资金账户 | W版 |
| 用客户代码解密，  再重新加密，  KEY：客户代码  DLL：CITICS\_CE.dll  函数：UF\_CommEncrypt |  | U版 |
| 用客户代码解密，  再重新加密，  KEY：资金账户  DLL：encrypt.dll  函数：AES\_Encrypt1 | 加密类型：’5’ ，AES加密密文，KEY为资金账户 | 期权 |
| 三方交易 | 三方存管，写死密码类型’4’ AES算法，KEY采用资金账户  函数：AES\_Encrypt1 | 用资金账号解密，  再重新加密，  KEY：资金账户  DLL：KDEncodeCli.dll  函数：KDEncode | WIN版外围加密密文，KEY为资金账户 | W版 |
| 用资金账号解密，  再重新加密，  KEY：客户代码  DLL：CITICS\_CE.dll  函数：UF\_CommEncrypt | UF\_CommEncrypt加密密文，KEY为客户代码 | U版 |
| 不做处理 | 加密类型：’5’ ，AES加密密文，KEY为资金账户 | 期权 |

## 支付密码

采用AES加密，KEY作为客户代码。

# 改造方案

## 改造原则

资金管理系统自身没有周边系统，所以选择跟随策略，跟随WIN版集中交易、WIN版两融、期权系统升级进行变动。

资金管理系统进行国密改造升级后要保证：

* 仅资金管理系统升级，各业务系统不升级；
* 资金管理系统未升级，业务系统升级可部分升级或全部升级；
* 资金管理系统与相关系统同时升级；

系统正常运行。

## 资金管理操作员密码

* 密码算法

使用SM4代替AES、RC4；使用SM2代替RSA；使用SM3代替MD5。

* 升级策略

一次性实施升级、转换。

* 兼容性考虑

校验票据的功能，增加票据类型字段，‘0’-采用现有KBSS票据算法，‘1’-采用国密算法。其它系统国密改造后送‘1’，未改造不送，默认为‘0’。

校验操作员密码的功能，增加操作员密码类型字段，区分现有加密类型、国密加密类型。 -

## 各业务系统操作员密码

选择跟随策略，根据WIN版集中交易、WIN版两融、U版集中交易、U版两融、期权等系统国密改造方案进行适配。

## 银行密码

* 密码算法

使用SM4代替AES。

* 升级策略

资金管理内部环节一次性实施升级、转换。

* 兼容性考虑

目前银行密码各业务系统外围为明文形式，考虑后续可能会改为加密形式，所以此次增加银行密码加密类型字段，默认为‘0’-明文，后续根据需求扩充。

## 资金密码

* 密码算法

资金管理系统各自建渠道、三方交易渠道使用SM4代替AES算法。

调用各业务系统功能需送密码时，选择跟随策略，根据WIN版集中交易、WIN版两融、期权等系统国密改造方案进行适配。

* 升级策略

资金管理内部环节一次性实施转换，将AES转为SM4算法；

调用各业务系统功能需送密码时，根据业务系统升级情况，在配置中指定相应加密类型选择相应算法作加密处理。

* 兼容性考虑

对于各业务系统转发过来的请求，考虑目前业务系统计划采用分批切换资金密码，因此不同请求可能会选择不同密码算法，采用在配置中检查密码加密类型，转换为对应资金管理系统定义的加密类型传送到LBM中进行分类型处理。

现有资金密码类型需要进行扩充，增加对国密加密算法的类型定义。

## 支付密码

* 密码算法

使用SM4代替AES。

* 升级策略

资金管理内部环节一次性实施转换。

* 兼容性考虑

考虑增加密类型。

# 改造范围

根据改造方案，需要改造的密码包括操作员密码、银行密码、资金密码、支付密码。根据业务分析，需要改造的范围如下：

## 操作员密码

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **关联系统** | **涉及业务** | **改造范围** | **备注** |
| 操作员  密码 | 资金管理 | 1、用户认证信息校验L0000506  用户身份注册L0000507  用户密码管理L1100009  2、三方存管账户调整  资金密码校验  资金可取金额查询  客户资金划拨  客户资金划拨冲正  客户资金划拨流水查询  服务状态通知 | 1、远程调用配置表RPC2SPD\_PARAM\_CFG包含业务系统的操作员密码，业务系统包括集中交易、融资融券、个股期权、统一认证  2、操作员密码加解密方式需要修改  3、启用统一认证时，操作员密码需要到业务系统校验  4、需要使用工具，修改数据库中存量的操作员密码 |  |
| Web3.5 | 用户登陆  操作员密码设置  操作员密码修改 | 2、操作员密码加密方式需要修改 |  |

## 银行密码

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **关联系统** | **涉及业务** | **改造范围** | **备注** |
| 银行密码 | 资金管理 | 1、外围发起银证转账  外围发起查询银行账户余额  期权系统查询银衍交易配置信息  2、修改银行密码加解密处理，业务包括：  券商发起银行转证券  券商发起证券转银行  券商发起查询银行余额  券商发起银证开户  券商发起存管签约、  券商发起银证销户  券商发起同步客户资料  券商发起利息归本同步到银行  银行发起银行转证券  银行发起证券转银行  银行发起查询银行余额  银行发起银证开户  银行发起存管签约  银行发起银证销户  银行发起同步客户资料  银行发起变更银行账号 | 1、外围配置修改见4.5外围配置  2、代码涉及银行密码需要修改  3、发起方包括外围、账户系统、web系统，下游系统包括三方交易网关、银行 |  |
| 一柜通 | 券商发起银行转证券  券商发起证券转银行  券商发起查询银行余额  券商发起银证开户  券商发起存管签约、  券商发起银证销户  券商发起同步客户资料  券商发起利息归本同步到银行 | 银行密码加密需要修改 |  |
| Web3.5 | 券商发起银行转证券  券商发起证券转银行  券商发起查询银行余额  券商发起银证开户  券商发起存管签约、  券商发起银证销户  券商发起同步客户资料  券商发起利息归本同步到银行 | 银行密码加密需要修改 |  |

## 资金密码

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **关联系统** | **涉及业务** | **改造范围** | **备注** |
| 资金密码 | 资金管理 | 1、外围发起银证转账  外围发起查询银行账户余额  期权系统查询银衍交易配置信息  2、修改资金密码加解密处理，业务包括：  券商发起银行转证券  券商发起证券转银行  券商发起查询银行余额  券商发起银证开户  券商发起存管签约、  券商发起银证销户  券商发起同步客户资料  券商发起利息归本同步到银行  银行发起银行转证券  银行发起证券转银行  银行发起查询银行余额  银行发起银证开户  银行发起存管签约  银行发起银证销户  银行发起同步客户资料  银行发起变更银行账号  3、校验方为 | 1、外围配置修改见4.5外围配置  2、涉及资金密码需要修改  3、发起方包括外围、账户系统、web系统，下游系统包括三方交易网关、银行  4、校验方为集中交易（W版、U版）、融资融券（W版、U版）、个股期权 |  |
| 一柜通 | 券商发起银行转证券  券商发起证券转银行  券商发起查询银行余额  券商发起银证开户  券商发起存管签约、  券商发起银证销户  券商发起同步客户资料  券商发起利息归本同步到银行 | 资金密码加密需要修改 |  |
| Web3.5 | 券商发起银行转证券  券商发起证券转银行  券商发起查询银行余额  券商发起银证开户  券商发起存管签约、  券商发起银证销户  券商发起同步客户资料  券商发起利息归本同步到银行 | 资金密码加密需要修改 |  |

## 支付密码

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **关联系统** | **涉及业务** | **改造范围** | **备注** |
| 支付密码 | 资金管理 | 登陆  充值  提现  支付密码修改  支付密码重置  支付密码校验 | 1、外围配置需要修改  2、需要修改支付密码加解密  3、发起方包括外围、账户系统、自助服务，需要修改支付密码加密方式。  4、存量支付密码需要提供工具批量修改 |  |

## 外围配置

外围配置是通过TranslateForWWXT.xml文件转义银行密码和资金密码，通过修改配置文件，支持银行密码、资金密码转义。

# 风险点

国密加密库由网关提供，资金管理系统对提供的加密库、加密接口改造有依赖。

资金管理系统跟集中交易、融资融券、个股期权、统一认证联调资金密码，各系统提供资金密码改造联调时间对资金管理系统进度产生影响。

一柜通、账户系统与资金管理在银证开户时，需要依赖一柜通和账户系统改造后进行联调，对资金管理系统进度产生影响。

资金密码、银行密码改造后是否影响性能，需要性能测试后评估。

需要增加硬件加密方式处理，对硬件加密机有依赖，对资金管理系统进度产生影响。

资金密码改造对外围系统有影响，需要确认外围系统的改造时间。

不同券商对银行密码、资金密码上线需要沟通

# 参考资料

《国密算法V1.4.pptx》

《国密测试报告.xlsx》

《东进技术统一认证平台解决方案.docx》

《【会议纪要】国密项目各系统方案沟通会会议纪要-20171222》