|  |  |
| --- | --- |
| 机密 | |
| **密级** | **一** |

**金证股份 •金证券商经纪业务支持系统**

**股票期权系统**

**支持国家商用密码修改方案**

|  |  |  |  |
| --- | --- | --- | --- |
| **研制单位** | 深圳市金证科技股份有限公司 | | |
| **文档名称** | 股票期权系统\_支持国家商用密码修改方案 | | |
| **文档编号** |  | **文档版本** | 1.01 |
| **文档状态** | 🗹 草稿 🞏 完成 | | |
| **审 批** |  | **审批日期** |  |

**修改记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **文档版本** | **文档状态** | **修订日期** | **修订作者** | **修订内容** |
| 1.00 | C | 2018/01/13 | 陆明其 | 新编制 |
| 1.01 | M | 2018/04/16 | 王成明 |  |
|  |  |  |  |  |

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

**阅读指南**

|  |  |
| --- | --- |
| **人员／部门** | **建议阅读内容** |
|  |  |
|  |  |
|  |  |

目录

[1 引言 4](#_Toc515383619)

[1.1 编写目的 4](#_Toc515383620)

[1.2 背景 4](#_Toc515383621)

[1.3 基线 4](#_Toc515383622)

[1.4 范围 4](#_Toc515383623)

[1.5 缩略语 4](#_Toc515383624)

[1.6 参考文档 4](#_Toc515383625)

[2 需求描述 5](#_Toc515383626)

[3 总体需求概述 5](#_Toc515383627)

[4 系统现状 5](#_Toc515383628)

[4.1 股票期权管理系统 7](#_Toc515383629)

[4.1.1 操作员密码 7](#_Toc515383630)

[4.1.2 交易密码 8](#_Toc515383631)

[4.1.3 资金密码 9](#_Toc515383632)

[4.1.4 银行密码 11](#_Toc515383633)

[4.2 股票期权订单系统 12](#_Toc515383634)

[4.3 股票期权风控系统 12](#_Toc515383635)

[4.4 股票期权web系统 12](#_Toc515383636)

[5 改造方案 13](#_Toc515383637)

[6 关键改动点： 14](#_Toc515383638)

[6.1 外围算法库encrypt.dll 14](#_Toc515383639)

[6.2 柜台算法库KDStorageCrypt.dll 14](#_Toc515383640)

[6.3 校验逻辑修改 15](#_Toc515383641)

[7 推进计划 15](#_Toc515383642)

[8 周边系统升级影响 15](#_Toc515383643)

# 引言

## 编写目的

本说明书是证券经纪业务股票期权交易系统描述支持国家商用密码修改方案。

编写此文档旨在为系统业务模块的编码、测试、工程实施以及维护提供指导与依据。项目成员可参考下表进行重点阅读部分章节。

表1.1阅读指引

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 章节\角色 | 分析师 | 架构师 | 项目经理 | 开发人员 | 测试人员 | 工程人员 | 维护人员 |
| 第1章 | ★ | ★ | ★ | ★ | ★ | ★ | ★ |
| 第2章 |  |  |  |  |  |  |  |
| 第3章 |  |  |  |  |  |  |  |
| 第4章 |  |  |  |  |  |  |  |
| 第5章 |  |  |  |  |  |  |  |

## 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》。

## 基线

设计基线是《股票期权研发项目\_用户需求说明书.doc》。

## 范围

## 缩略语

## 参考文档

表1.2 缩略语

|  |  |  |
| --- | --- | --- |
| 缩略词 | 全称 | 说明 |
| KCXP | Kingdom Communication eXchange Platform | 金证通讯交换平台 |
| KCBP | Kingdom Core Business Platform | 金证核心业务平台 |
| KBSS | Kingdom Broker Supplied System | 金证券商经纪业务支持系统 |
| KSTS | Kingdom Security Trade System | 金证证券订单系统 |
| KMAP | Kingdom Multi-Active Platform  Kingdom Microkernel ArchitecturePlatform | 金证多活基础平台  金证微内核架构平台 |

# 需求描述

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，股票期权系统目标在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。

# 总体需求概述

本次改造总的设计原则是与股票期权对接的周边系统，仅通过增加底层加密算法库KDStorageCrypt.dll、更新encrypt.dll外围通讯加密算法库完成升级，业务接口不做任何改动。

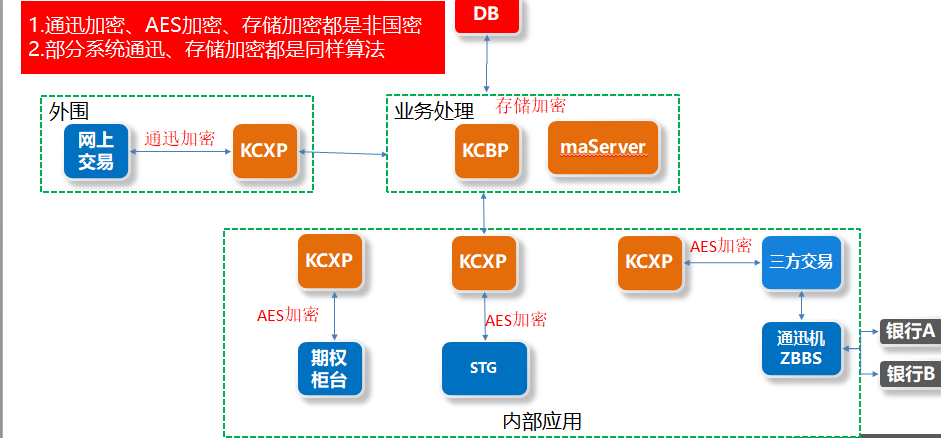
股票期权本身要实现升级前后的兼容处理，一方面在检查外部系统传入的密码时，要能正确加解密，并适配后台存量密码的加密算法进行正确转换，另一方面，对存量的客户数据，要能做到分阶段、分批次，增量切换到国密算法。

# 系统现状

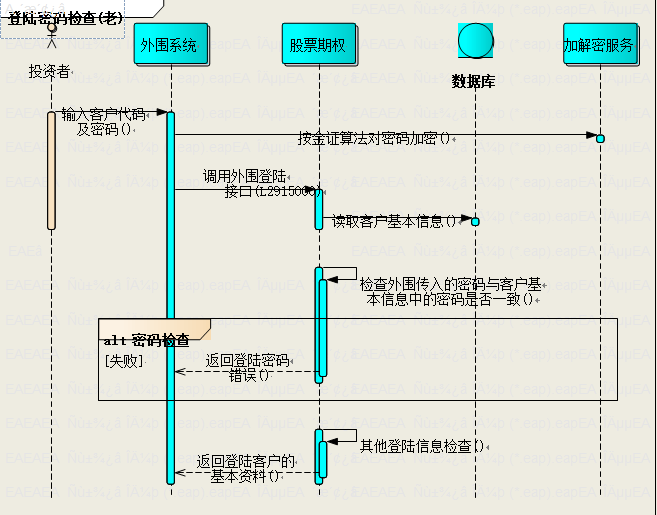
在股票期权系统中，大部分加解密算法都是对应国密算法的SM4对称加密算法。但是也有个别存在md5等非对称加密算法，该场景目前出现在申万宏源北京股票期权系统中。

|  |  |  |  |
| --- | --- | --- | --- |
| **DLL名称** | **DLL版本** | **导出函数** | 用途 |
| encrypt.dll |  | kbss\_comencrypt | 用于外围通信加密 |
| kbss\_comdecrypt | 用于外围通信解密 |
| AES\_Encrypt1 | 用于柜台、账户、三方交易通信加密 |
| AES\_Decrypt1 | 用于柜台、账户、三方交易通信解密 |
| MD5\_Digist | 用于登陆生成票据、申万宏源顶点加解密 |
| Base64\_Encode | 用于金仕达加密 |
| Base64\_Decode | 没用到 |
| RC5\_Encrypt | 用于登陆生成票据 |
| RC5\_Decrypt | 用于登陆票据解密 |
| RSA\_Encrypt | 用于登陆生成票据 |
| RSA\_Decrypt | 没用到 |
| kbss\_encrypt1 | 用于数据存储加密 |
| kbss\_recrypt1 | 没用到 |
| kbss\_recrypt2 | 没用到 |

**当前系统现状**：



改造前时序图：



## 股票期权管理系统

### 操作员密码

系统的操作员密码是存在数据库中，在管理系统本地校验用户登录；

具体内容如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **系统** | **涉及业务** | **详细信息** | **备注** |
| 操作员  密码 | 管理系统 | 1、用户认证信息校验L0000506  用户身份注册L0000507  用户密码管理L1100009 | 1、操作员密码存在股票期权管理系统数据库中  2、操作员密码通过AES\_Decrypt1解密后再用kbss\_encrypt加密 | 本系统 |
| Web4.0 | 用户登陆  操作员密码设置  操作员密码修改 | 采用Jni调用C++加密算法 | 前端 |
| 统一认证 | 用户认证 | 启用统一认证时，到统一认证校验操作员密码 |  |
|  |  |  |  |
| 股票期权管理系统 | 三方银衍账户调整  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 | 对接股票期权管理系统涉及校验柜员密码 |  |

### 交易密码

交易密码在股票期权管理系统以存储加密方式将密文保存在数据库中；

具体如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **关联系统** | **涉及业务** | **详细信息** | **备注** |
| 交易密码 | 股票期权  管理系统 | 客户修改交易密码  客户重置交易密码 | 1、股票期权管理系统对资金密码进行解密再加密后传给业务系统交易 | 本系统 |
| 外围系统（银衍） | 外围发起银衍转账  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 | 外围系统发起银衍转账，资金密码由外围加密后传入股票期权管理系统 |  |
| 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料 | 资金密码加密后传入股票期权管理系统 | 前端 |
| Web4.0 | 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料 | 资金密码加密后传入股票期权管理系统 | 前端 |
| 账户系统 | 客户开户设置交易密码  客户修改交易密码  客户重置交易密码 | 资金密码加密后传入股票期权管理系统 | 关联系统 |
| 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  银行发起银衍开户  银行发起银衍签约  银行发起银衍销户  银行发起同步客户资料  银行发起变更银行账号 | 资金密码由银行加密传入 | 发起方 |
| 三方交易网关 | 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  银行发起银衍开户  银行发起银衍签约  银行发起银衍销户  银行发起同步客户资料  银行发起变更银行账号 | 三方网关采用AES加密方式传送资金密码密文 | 网关 |
| 外围 | 外围登陆  外围密码修改  外围登陆（申万宏源） |  |  |
|  |  |  |  |  |

### 资金密码

资金密码在股票期权管理系统以存储加密方式将密文保存在数据库中；

具体如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **关联系统** | **涉及业务** | **详细信息** | **备注** |
| 资金密码 | 股票期权管理系统 | 客户修改资金密码  客户重置资金密码  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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  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  银行发起银衍开户  银行发起银衍签约  银行发起银衍销户  银行发起同步客户资料  银行发起变更银行账号 | 1、股票期权管理系统对资金密码进行解密再加密后传给业务系统交易 | 本系统 |
| 外围系统（银衍） | 外围发起银衍转账  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 | 外围系统发起银衍转账，资金密码由外围加密后传入股票期权管理系统 |  |
| 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料  券商发起利息归本同步到银行 | 资金密码加密后传入股票期权管理系统 | 前端 |
| Web4.0 | 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料  券商发起利息归本同步到银行 | 资金密码加密后传入股票期权管理系统 | 前端 |
| 账户系统 | 客户开立资金账户设置资金密码  客户修改资金密码  客户重置资金密码 | 资金密码加密后传入股票期权管理系统 | 关联系统 |
| 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  银行发起银衍开户  银行发起银衍签约  银行发起银衍销户  银行发起同步客户资料  银行发起变更银行账号 | 资金密码由银行加密传入 | 发起方 |
| 三方交易网关 | 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  银行发起银衍开户  银行发起银衍签约  银行发起银衍销户  银行发起同步客户资料  银行发起变更银行账号 | 三方网关采用AES加密方式传送资金密码密文 | 网关 |
|  |  |  |  |

### 银行密码

银行密码发起方有外围、web客户端、账户系统，三方银衍网关，需要对银行密码进行加密操作，通过三方交易网关发到到银行，由银行进行校验。具体如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **密码** | **关联系统** | **涉及业务** | **详细信息** | **备注** |
| 银行密码 | 股票期权  管理系统 | 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  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  银行发起银衍开户  银行发起银衍签约  银行发起银衍销户  银行发起同步客户资料  银行发起变更银行账号 | 1、W版外围通过AES\_Encrypt1加密银行密码  2、外围转义配置对外围发起业务的银行密码进行加密 | 本系统 |
| 外围系统（现货）  外围系统（信用）  外围系统（银衍） | 外围发起银衍转账  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 | 期权银行密码由外围加密进来  其他外围到外围转义配置 | 外围系统 |
| 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料 | 一柜通使用AES\_Encrypt1加密银行密码 | 前端 |
| Web4.0 | 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料 | Web客户端使用AES\_Encrypt1加密银行密码 | 前端 |
| 账户系统 | 券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料 | 账户系统进行银衍开销户时、同步客户资料、单账户结息归本同步银行时，使用AES\_Encrypt1加密银行密码 |  |
| 银行 | 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料 | 银行校验银行密码是否正常  银行发起业务将银行密码加密后，传入新三方交易网关 | 校验 |
| 三方交易网关 | 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  券商发起银衍开户  券商发起银衍签约、  券商发起银衍销户  券商发起同步客户资料  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  银行发起银衍开户  银行发起银衍签约  银行发起银衍销户  银行发起同步客户资料  银行发起变更银行账号 | 券商发起业务，网关对银行密码解密在加密后传给银行  银行发起业务，网关对银行密码进行解密加密后，发送给股票期权管理系统 | 关联系统 |

## 股票期权订单系统

股票期权订单系统也以加密的方式，在数据库中保存了客户交易密码密文和资金密码密文。

交易校验资金密码、客户登陆接口（L293000）密码校验。

## 股票期权风控系统

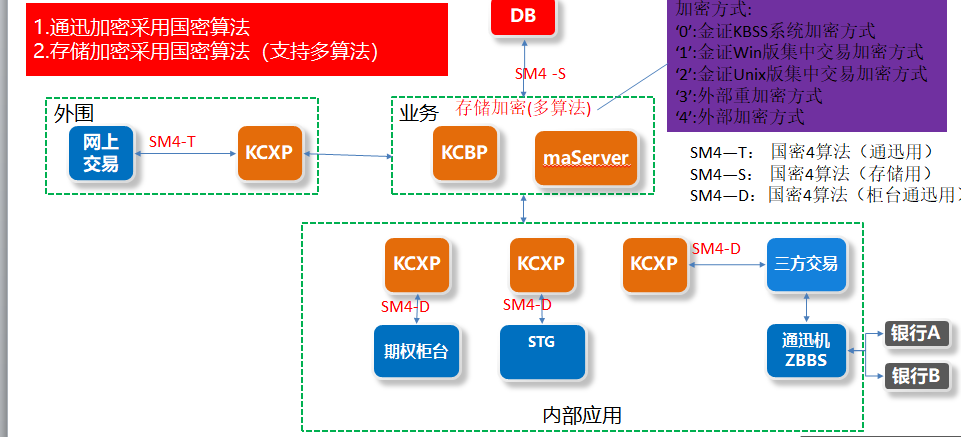
本次不涉及修改。

## 股票期权web系统

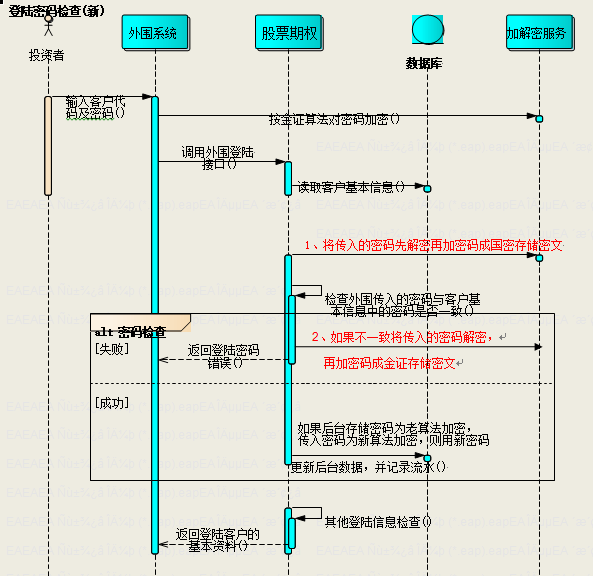
# 改造方案

股票期权系统中采用了一个统一封装的加密算法库，目前算法库名称为encrypt.dll。建议由网关产品使用国密算法，封装一个国密的加密算法库，统一给产品部门使用。原来加解密函数名和出入参不变，业务系统调用原函数，变动无感知。在正式切换到国密算法后，后台数据库中存储的密码需要逐步切换到新的加密算法。

**改造后：**



**改造后时序图：**



# 关键改动点：

## 外围算法库encrypt.dll

请网关将原有算法库encrypt.dll中的外围通信加解密（kbss\_comencrypt/kbss\_comdecrypt）封装为国密算法，出入参数不变。外围厂商只需更新encrypt.dll动态库，仍然调用原来的加密码函数。

## 柜台算法库KDStorageCrypt.dll

请网关提供新算法库KDStorageCrypt.dll，增加一套国密加解密函数，外围通信加解密函数（kbss\_GM\_comencrypt/kbss\_GM \_comdecrypt）、柜台通信加解密函数（AES\_GM \_Decrypt1/AES\_GM \_Encrypt1）、存储加解密函数（kbss\_GM \_encrypt1/kbss\_GM \_decrypt1）、密码转换函数（kbssCipherTextToGMCipherText）、密码类型查询函数（QueryType）。

## 校验逻辑修改

* 旧逻辑：

1、先将通信密文解成明文

2、再把明文加密成金证的存储密文，同数据库客户信息中的密文比较，如果一致，校验通过。如果不一致，则报密码错误

* 新逻辑：

1、先调用密码识别函数

2、根据密码标识将通信密文解成明文

3、再把明文加密成国密存储密文后同数据库客户信息中的密码比较，如果一致，则返回成功。

4、如不一致，再将明文加密成金证旧的存储密文，同数据库客户信息中的密文比较，如果一致，则将数据库客户信息中的密文更新为国密。如果不一致，则报密码错误

# 新增公参

CUBSB\_ENCRYPT\_TYPE '对接银衍网关密码类型（0-非国密，1-国密），用于控制期权系统向银衍网关发送的密码类型。当期权升级国密后，银衍网关还未升级，可通过此参数控制向银衍网关发送的密码类型

# 字典定义

**加密类型[ENCRYPT\_TYPE]**

|  |  |  |
| --- | --- | --- |
| 字典项代码 | 字典项名称 | 字典项说明 |
| 0 | 非国密 |  |
| 1 | 国密 |  |

# 表结构修改

**认证信息（AUTH\_INFO）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段代码 | 数据类型 | 主键 | 说明 |
| 用户代码 | USER\_CODE | BIGINT | √ |  |
| 用户角色 | USER\_ROLE | CHAR(1) | √ |  |
| 使用范围 | USE\_SCOPE | CHAR(1) | √ | 0:登录/交易  1:资金业务 |
| 认证类型 | AUTH\_TYPE | CHAR(1) | √ | 0:密码  1:证书  2:指纹 |
| 认证数据 | AUTH\_DATA | VARCHAR(256) | √ |  |
| 设置日期 | SET\_DATE | INTEGER | √ |  |
| 出错次数 | FAIL\_NUM | SMALLINT | √ |  |
| 锁定时间 | LOCK\_TIME | TIMESTAMP | √ |  |
| 最后登录时间 | LAST\_LOGIN\_TIME | TIMESTAMP | √ |  |
| 最后登录站点 | LAST\_LOGIN\_SITE | VARCHAR(256) | √ |  |
| 最后登录渠道 | LAST\_LOGIN\_CHNL | CHAR(1) | √ |  |
| 复核标志 | CHK\_FLAG | CHAR(1) | √ | 新开户或临柜重置后设置为1  临柜修改或外围修改后设置为0 |
| 加密类型 | ENCRYPT\_TYPE | CHAR(1) | √ | 初始为0（0-非国密，1-国密） |

增加字段：加密类型（ENCRYPT\_TYPE）初始为0（0-非国密，1-国密），当密码由非国密变为国密的同时，需要将该字段更新为“1”（当密码为非国密，且密码类型不为:**4-外部传入密文**

，当密码修改、重置、校验时会将密码更新为国密，将该字段更新为“1”）

# 国密批量转换菜单

**管理系统国密批量转换接口**

* 功能编号：L2940594
* 功能名称：国密批量转换
* 功能类型：事务功能
* 功能入参：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 列名 | 列代码 | 列类型 | 必输 | FIX域 | 说明 |
|  |  |  |  |  |  |

* 功能出参：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 列名 | 列代码 | 列类型 | FIX域 | 说明 |
|  |  |  |  |  |
|  |  |  |  |  |

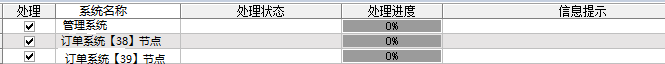
用于将后台数据库中存放的非国密密码（ENCRYPT\_TYPE=0），通过密码转换函数（kbssCipherTextToGMCipherText）转换为国密加密方式。注意：对后台数据库中存放的顶点、金仕达、外部密文的密码不做转化

**订单系统国密批量转换接口**

*待补充*

## 界面元素

1. 转换按钮
2. 复选框 | 系统名 | 进度条 (第个系统一条，多个订单系统分多条)



复选框：默认全选

系统名：订单系统（订单系统+节点名）、管理系统

进度条：参照清算任务进度条

# 推进计划

整体开发计划按公司国密项目进度要求开展，股票期权系统国密改造工作将在5月底开始，6月初底完成初步版本，并与相关系统进行联测。

# 周边系统升级影响

期权对接的上游系统：账户系统、一柜通、外围、资金系统、web前端。

期权需要先于对接的上游系统升级国密。期权系统兼容上游系统分批升级国密，例如：WEB前端升级国密，其他系统未升级国密。同一客户可通过web前端登陆（密文为国密），也可通过外围客户端登陆（官方为非国密）

期权对接下游系统：三方交易

通过共参控制：CUBSB\_ENCRYPT\_TYPE '对接银衍网关密码类型（0-非国密，1-国密）