**金证股份•<**OTC系统-国密改造 **>**

**概要设计说明书**

|  |  |  |  |
| --- | --- | --- | --- |
| **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** | OTC系统-国密改造概要设计说明书 | **文档版本** | 0.1 |
| **起 草** | 余跃 | **起草日期** | 2018-04-10 |
| **审 批** |  | **审批日期** |  |

**修订历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 日期 | 状态 | 修订人 | 摘要 |
| 0.1 | 2018-04-10 | C | 余跃 | 起草 |
|  |  |  |  |  |
|  |  |  |  |  |

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

**阅读指南**

|  |  |
| --- | --- |
| 单位/人员 | 建议阅读内容 |
|  |  |
|  |  |
|  |  |
| …… |  |

目录

[1 引言 5](#_Toc511144056)

[1.1 目的和范围 5](#_Toc511144057)

[1.2 背景 5](#_Toc511144058)

[1.3 术语和定义 5](#_Toc511144059)

[1.4 参考资料 5](#_Toc511144060)

[2 需求概述 5](#_Toc511144061)

[3 设计概述 5](#_Toc511144062)

[3.1 设计策略 5](#_Toc511144063)

[3.2 系统架构 5](#_Toc511144064)

[3.2.1 改造前 5](#_Toc511144065)

[3.2.2 改造后 5](#_Toc511144066)

[3.3 主要业务流程 5](#_Toc511144067)

[3.3.1 登陆 5](#_Toc511144068)

[3.3.2 质押确认 6](#_Toc511144069)

[3.3.3 到期回购 7](#_Toc511144070)

[3.3.4 其他业务 7](#_Toc511144071)

[3.4 后台服务 8](#_Toc511144072)

[3.4.1 数据字典 8](#_Toc511144073)

[3.4.2 主要数据表 8](#_Toc511144074)

[4 功能及处理流程 11](#_Toc511144075)

[4.1 报价交易 11](#_Toc511144076)

[4.1.1 参数设置 11](#_Toc511144077)

[4.2 三级清算 11](#_Toc511144078)

[4.2.1 清算数据采集 11](#_Toc511144079)

[4.2.2 清算数据导入 11](#_Toc511144080)

[5 接口及处理流程 11](#_Toc511144081)

# 引言

## 目的和范围

## 背景

## 术语和定义

## 参考资料

《证券期货业国产密码应用推进规划方案》 证信办[2014]157号

# 需求概述

2018.06 完成OTC系统国密改造

# 设计概述

## 设计策略

* 支持向下兼容、逐步切换

新老算法由于存在过渡期，所以支持向下兼容逐步切换

* 支持批量切换

支持柜员通过批量菜单全部更新客户存储密码

* 支持存储加密个性化算法

支持不同的券商采用不同的加密算法，以及个性化密钥

* 统一认证模式，修改密码由统一认证校验密码

当前版本报价交易在修改柜员密码时，先在报价对密码做校验，然后发布到统一认证；

后继修改密码时远程调用统一认证的功能，由统一认证校验。

* 外围系统0改动

切换算法的过程中外围程序不需要进行程序的修改

## 系统架构

### 改造前



### 改造后



## 主要业务流程

### 用户登陆



### 修改密码



### 重置密码



## 改造步骤

1. OTC系统更新框架程序。
2. OTC系统所有KCBP（统一认证单独处理）更新框架、新加解密库、新老密码转换库。涉及需要改造的子系统做改造。
3. OTC系统其他应用程序（KCBP程序以外）替换encrypt.dll。
4. OTC系统与集中交易有关的中转BP，更新集中交易提供的新加密库。
5. 发布程序，通知OTC外围系统替换encrypt.dll。

## 后台服务

### 数据字典

* 修改字典

认证类型（AUTH\_TYPE） 增加‘8-国密’

* OTC框架与统一认证，新增公共参数

个性化密钥串：默认为空

是否兼容旧(KBSS)加密方式：默认为1

# 功能及处理流程

## OTC框架

### 用户密码维护（L1100009包含新增、修改、重置）

* **后台处理流程**

1. 入参：无变化
2. 出参：无变化
3. 处理逻辑：（只描述需要修改部分）
   1. 不使用统一认证（REGISTRY.REGKEY\_ID = 'USE\_UNIAUTH\_INFO' 值为0）
      1. 重置密码、新增密码：AES解密后，使用国密码加密算法，认证类型修改为‘8-国密’
      2. 修改密码：将原有的密码校验方法更新为新的密码校验方法，参考4.1.5 用户密码校验
   2. 使用统一认证（REGISTRY.REGKEY\_ID = 'USE\_UNIAUTH\_INFO' 值为1）
      1. 远程调用统一认证的密码更新接口

### 认证信息查询（新增功能）

* **相关说明**

查询认证信息

* **前端处理流程**

柜台前端支持输入：用户代码、用户角色、使用范围、认证类型(默认‘0’)。

查询列表输出：用户代码、用户角色、使用范围、认证类型、设置日期

界面添加“国密处理”按钮，支持对查询结果进行单选、全选、反选。点击“国密处理”按钮时，前端启用多线程对选择的记录逐条进行处理（调用认证信息国密化功能）。

* **后台处理流程**

1. 入参：用户代码、用户角色、使用范围、认证类型、分页起始记录号、分页记录数量；
2. 出参：用户代码、用户角色、使用范围、认证类型、设置日期；
3. 处理逻辑：
   1. 检查用户权限，只有总部柜员有此权限。
   2. 不使用统一认证（REGISTRY.REGKEY\_ID = 'USE\_UNIAUTH\_INFO' 值为0）根据输入条件，在本地查询出认证信息，返回第二结果集；
   3. 使用统一认证（REGISTRY.REGKEY\_ID = 'USE\_UNIAUTH\_INFO' 值为1）根据输入条件，远程调用统一认证接口，查询出认证信息，返回第二结果集；

### 认证信息国密化（新增功能）

* **相关说明**

认证信息国密码化

* **前端处理流程**

柜台前端输入：用户代码、用户角色、使用范围、认证类型。

* **后台处理流程**

1. 入参：用户代码、用户角色、使用范围、认证类型；
2. 出参：用户代码、用户角色、使用范围、认证类型；
3. 处理逻辑：
   1. 检查用户权限，只有总部柜员有此权限。
   2. 不使用统一认证（REGISTRY.REGKEY\_ID = 'USE\_UNIAUTH\_INFO' 值为0），根据入参查找数据库中的记录；认证类型非‘0-密码’不处理；认证类型等于‘0-密码’：

b1)调用KBSS解密库进行解密

b2)调用国密加密库进行加密，将认证类型修改为‘8-国密’，认证信息更新为新的密文

b3)使用范围是登陆的（使用范围等于公共参数“UNIAUTH\_USE\_SCOPE”的值）同步给统一认证（远程调用）

* 1. 使用统一认证（REGISTRY.REGKEY\_ID = 'USE\_UNIAUTH\_INFO' 值为1），远程调用统一认证功能，做认证信息国密化
  2. 写用户操作日志
  3. 返回结果集并提交

### 封装用户密码校验方法

* + - 封装一个新的密码检验方法,处理逻辑如下

1. AES解密密文，获取密文的密码类型
2. 密码类型KBSS。
   * 1. 数据库认证类型为‘0-密码’，使用原有方式校验密码；
     2. 数据库认证类型为‘8-国密’，将密文做转换后再校验，如果设置了“是否兼容旧(KBSS)加密方式”为0则校验失败。
3. 密码类型SM4。
4. 数据库认证类型为‘0-密码’，将密文做转换后再校验，检验成功后更新本地数据库“认证类型”“认证数据”；
5. 数据库认证类型为‘8-国密’，用国密方法校验密码

## OTC报价交易

### 用户密码设置（L2610018）

* **后台处理流程**

1. 入参：无变化
2. 出参：无变化
3. 处理逻辑：
   1. 认证类型‘0-密码’修改为‘8-国密’
   2. 订阅发布更新为远程调用

备注：快速赎回还款申报（L2620331）密码送的是明文，需要修改为密文

## OTC账户子系统

### 客户设置、修改、重置密码（L3604030）

* **后台处理流程**

1. 入参：无变化
2. 出参：无变化
3. 处理逻辑：

认证类型‘0-密码’修改为‘8-国密’（已经是远程调用）

## OTC统一认证

### 生成票据（T0000102）

* **后台处理流程**

1. 入参：无变化
2. 出参：无变化
3. 处理逻辑：（只描述需要修改部分）
   1. AES解密后，判断密文的密码类型

a1)存储密文的加密因子增加一个固定串，该串从公共参数中读取，默认为空

a2)密码类型KBSS。数据库认证类型只有‘0-密码’，使用原有方式校验密码；数据库认证类型有‘8-国密’，将密文做转换后再校验，如果设置了“是否兼容旧(KBSS)加密方式”为0则校验失败。

a3)密码类型SM4。数据库认证类型只有‘0-密码’，将密文做转换后再校验，检验成功后在本地新增一条认证类型有‘8-国密’的认证数据；数据库认证类型为‘8-国密’，用国密方法校验密码

### 更新认证信息（T0000316，T0000317，T0000318）

* **后台处理流程**

1. 入参：无变化
2. 出参：无变化
3. 处理逻辑：（只描述需要修改部分）

增加密码校验，与票据校验调用同一个方法

### 认证信息查询（新增功能）

* **后台处理流程**

1. 入参：用户代码、用户角色、使用范围、认证类型、分页起始记录号、分页记录数量；
2. 出参：用户代码、用户角色、使用范围、认证类型、设置日期；
3. 处理逻辑：
   1. 根据输入条件查询(存在认证类型0且不存在认证类型8的数据)，查询出的认证信息以第二结果集返回；

### 认证信息国密化（新增功能）

1. 入参：用户代码、用户角色、使用范围、认证类型；
2. 出参：用户代码、用户角色、使用范围、认证类型；
3. 处理逻辑：
   1. 根据入参查找数据库中的记录；
   2. 存在认证类型0且不存在认证类型8的数据：

b1)调用KBSS解密库进行解密

b2)存储密文的加密因子增加一个固定串，该串从公共参数中读取，默认为空

b3)调用国密加密库进行加密，增加认证类型 ‘8-国密’的认证信息。

* 1. 返回结果集并提交

## OTC WEB

### 替换DES.JS/AES.JS脚本

### 替换KBSS加密库、集中交易的加密库

# 接口及处理流程

无