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

**金证股份 •金证券商经纪业务支持系统**

**一柜通系统**

**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** | 一柜通系统\_支持国家商用密码修改方案 | | |
| **文档编号** |  | **文档版本** | 1.00 |
| **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 | 刘青 |  |
|  |  |  |  |  |
|  |  |  |  |  |

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](#_Toc505023086)

[1.1 编写目的 4](#_Toc505023087)

[1.2 背景 4](#_Toc505023088)

[1.3 基线 4](#_Toc505023089)

[1.4 范围 4](#_Toc505023090)

[1.5 缩略语 4](#_Toc505023091)

[1.6 参考文档 4](#_Toc505023092)

[2 需求描述 5](#_Toc505023093)

[3 系统现状 5](#_Toc505023094)

[3.1 登录 5](#_Toc505023095)

[3.2 通讯协议层 5](#_Toc505023096)

[3.3 请求字段 5](#_Toc505023097)

[4 改造方案 5](#_Toc505023098)

[4.1 登录 5](#_Toc505023099)

[4.2 通讯协议层 6](#_Toc505023100)

[4.3 请求字段 6](#_Toc505023101)

[5 工程实施 6](#_Toc505023102)

[6 推进计划 6](#_Toc505023103)

# 引言

## 编写目的

本说明书是证券一柜通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

## 范围

## 缩略语

* KJDP

Kingdom Java Develop Platform，金证Java EE开发平台。

## 参考文档

一柜通系统概要设计说明书.doc

# 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，一柜通系统目标在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。

# 系统现状

目前一柜通使用密码的业务场景主要有以下几个方面。

## 登录

登陆时前端将操作员密码使用DES加密，请求数据到达后端时Java程序使用DES解密得到明文，再使用kbss\_encrypt加密明文，最后比较kbss\_encrypt加密得到的密文是否和数据库中存储的一致。

## 通讯协议层

http请求从前端发出时使用AES加密请求包内容。

## 请求字段

请求包中某些敏感信息如银行密码，资金密码等字段使用DES加密，后端Java程序使用DES解密。

# 改造方案

一柜通系统前后端加解密使用的是统一的API处理，由于分前后端两种不同语言的实现，一柜通系统需要网关产品部提供两种语言的算法（JavaScript，Java）。

为了保持现有生产数据的兼容性，老的加解密算法不能直接去掉，加密的API直接替换成新的算法处理即可，但解密时应先使用检测方法检测是否为国密的密串，如果是则使用新的算法解密，否则使用老的算法处理。

## 登录

前端JavaScript使用最新的算法加密，后端Java程序使用最新算法解密，得到柜员密码明文后再使用国密改造版的kbss\_encrypt对柜员密码加密，处理完成后和数据库的密文比较，相同则认证通过，否则认证失败。

## 通讯协议层

前端JavaScript发送http请求时使用最新的算法加密，后端Java程序使用最新算法解密，得到请求包明文后再进行相应的业务处理。

## 请求字段

前端JavaScript使用最新的加密算法对字段加密，考虑到数据库中的存量数据，后端解密时需优先使用最新算法解密，如解密失败则尝试使用老算法处理。

# 工程实施

操作员表中的数据需使用产品部门提供批量修改密码的工具将操作员密码修改。

# 推进计划

整体开发计划按公司国密项目进度要求开展，一柜通系统国密改造工作将在2月份开始，3月份底完成初步版本，并与相关系统进行联测。