**国产密码算法改造**

**产品立项申请报告**

|  |  |  |  |
| --- | --- | --- | --- |
| **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** | 产品立项报告 | **版 本 号** | V0.1 |
| **起 草** | 高世博 | **起草日期** | 2018-05-25 |
| **审 批** | <审批人> | **审批日期** |  |

**修订历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 日期 | 状态 | 修订人 | 摘要 |
| 1.0 | 2018.5.24 | C | 高世博 | 新建 |
| 2.0 | 2018.5.25 | M | 高世博、冉丽君 | 新增各产品方案，修改文档排版 |
|  |  |  |  |  |

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

目录

[1 产品概述 4](#_Toc455497642)

[1.1 产品定义 4](#_Toc455497643)

[1.2 产品开发背景 4](#_Toc455497644)

[1.3 产品主要功能和特色 4](#_Toc455497645)

[1.4 产品范围 4](#_Toc455497646)

[2 产品描述 4](#_Toc455497647)

[2.1 系统简介 4](#_Toc455497648)

[3 市场分析 5](#_Toc455497649)

[4 技术分析 5](#_Toc455497650)

[5 可行性分析 5](#_Toc455497651)

[6 风险及不确定因素分析 5](#_Toc455497652)

[7 职责与任务 6](#_Toc455497653)

[8 项目计划和成本分析 6](#_Toc455497654)

[8.1 项目团队 6](#_Toc455497655)

[8.2 主要软件硬件资源估计 7](#_Toc455497656)

[8.3 成本估计 8](#_Toc455497657)

[9 成本效益分析 8](#_Toc455497658)

[9.1 生产规划 8](#_Toc455497659)

[9.2 收益 8](#_Toc455497660)

[9.3 收益/投资比 8](#_Toc455497661)

[9.4 投资回收周期 8](#_Toc455497662)

[10. 总结 9](#_Toc455497663)

# 产品概述

## 产品定义

为配合国产密码的应用改造，金证公司对W/U版交易系统、KBSS系统、JAVA系统、平台等系统做了相应的升级改造。将原密码升级为国产级别密码。

## 产品开发背景

国务院办公厅转发《金融领域密码应用指导意见》（国办发[2014]6号文件）要求“建立以国产密码为主要支撑的金融信息安全保障体系，实现金融领域信息安全核心产品及系统的自主可控，力争2015年初步实现国产密码在重点领域的广泛应用，到2020年实现国产密码在金融领域的全面应用”。

《证券期货业国产密码应用推进规划方案》 证信办[2014]157号文件要求“2015.12前实现国产密码在网上交易、手机交易等网上证券系统密码软件或模块改造,2018.12前实现国产密码在网上证券等交易系统的全面应用,2020.12前实现国产密码的全面应用”。

为适应国产密码应用的，各券商须对系统进行相应的改造升级

## 产品主要功能和特色

根据各类监管机构的相关政策与规定，金证公司目标将目前已经部署在各金融企业中的金证IT应用系统、以及今后新建的金证IT应用系统，其中所使用到的非国产密码算法，如RES,RSA,MD5,AES等，全部替换为国产密码算法。

## 产品范围

金证公司此次改造升级范围包括：

* W版交易系统：W版集中交易、W版融资融券
* U版交易系统：U版集中交易、U版融资融券
* KBSS系统：统一账户、期权、资金、订单、转融通
* Java系统：一柜通、影像档案、清算系统、PIF、做市
* 平台系统：STG、方存管、统一认证、综合机构网关、MID等。

# 产品描述

## W版交易系统

### 2.1.1兼容处理

不同兼容方案的优缺点分析，兼容方案的核心问题是如何识别新老加密算法，主要思路为：

* 通过引入标识字段进行区分
* 通过加密密文本身的特性进行区分
* 不做兼容，上线时所有系统一刀切

以下为各方案的优缺点比较：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 识别方法 | | 优点 | 缺点 | 备注 |
| 引入标识字段 | | 简单，方便后期维护 | 影响范围大，所有对接的外部系统都需要配合修改，数据库也需新增字段 | 公共入参中引入新的字段 |
| 通过密文本身特性区分 | 长度 | 外部系统升级仅替换加密库即可，业务代码无需修改，影响范围小 | 当原始密码设置超过15个字符时，无法区分 | 老算法密文长度固定为24、28或32，新密码密文长度与原文相同，在密码长度较短时，通过长度的差异可进行识别 |
| 增加特殊头部信息 | 需要修改加密算法，密码字段需要扩位 | 密文通过BASE64处理后，只会出现特定的64个字符，剩下还有30多个可见字符未使用，通过在密文开头引入标识字符，可达到对密文进行识别的效果 |
| 一刀切 | | 简单，方便后期维护 | 影响范围大，所有对接的外部系统都需要配合升级 | 适合柜台本身的升级，不适合外部对接的系统 |

备注：加密库提供的接口有用来标识不同加密算法的入参（第1个参数nEncode\_Level），但柜台未使用，固定传的6，“引入标识字段”的方案，与底层加密库的设计贴合得更加紧密，便于后期维护。

而通过加密内容本身进行区分的方案，或多或少都要修改加密算法本身，在密文中增加标识信息以达到区分的目的，这样会破坏原始数据。

**后文使用方案三，通过在密文中增加特殊头部信息，达到兼容的目的，由于生产中的密码普遍设置的6个字符，因此，不做扩位处理，同时，功能号入参中不加标识字段，但数据库中涉及到密码的字段增加加密类型字段，用于区分不同的加密算法。**

### 2.1.2密码检查逻辑调整

**改造前登陆检查时序图**

****

**改造后登陆检查时序图**



国密升级后，将通讯密码和存储密码进行分离，外围系统传给柜台的密码使用通讯密码加密，柜台将通讯密码重加密为存储密码后，再存入后台数据库进行存储。

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，切换条件如下：

* 如果数据库中的密码为老算法加密，传入密码为新算法加密，则用新密码更新后台数据库，并记录操作流水
* 如果数据库中的密码为老算法加密，传入密码为老算法加密，则不修改后台数据
* 如果数据库中的密码为新算法加密，不管传入的密码是用的何种加密算法，均不修改后台数据

### 2.1.3周边系统升级

本次改造，集中交易对外公开的接口并未作调整，因此，与集中交易对接的周边系统业务代码无需做任何修改，但调用的底层加密算法库需要替换为新的组件，涉及到需要升级的周边系统清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 系统名称 | 调用接口 | 影响字段 | 加密算法库 |
| 外围系统 | 外围接口 | trdpwd  newpwd  oldfundpwd  newfundpwd  fundpwd  outpassword | KDEncodeCli.dll |
| KBSS | 柜台接口 | g\_operpwd  g\_trdpwd  password  outpassword  inpassword  bankpwd |  |
| OTC | 柜台接口 | g\_operpwd fundpwd | KDEncodeCli.dll |
| PIF | 柜台接口 | g\_operway |  |
| QQ微平台 | 柜台接口 | g\_operpwd |  |
| STG | 柜台接口 | g\_operpwd | KDEncodeCli.dll |
| AutoOffer | 柜台接口 | g\_operpwd | CliEncrypt.dll |
| 个股期权 | 柜台接口 | g\_operpwd trdpwd | KDEncodeCli.dll |
| 机构综合业务网关 | 柜台接口 | 无 | |
| 快速订单 | 待确认 | | |
| 三方存管 | 柜台接口 | 待确认(初步评估感觉没影响) | |
| 深证通OES | 柜台接口 | g\_operpwd | KDEncodeCli.dll |
| 统一认证 | 待确认 | | |
| 账户系统 | 柜台接口 | g\_operpwd trdpwd fundpwd st\_trdpwd bankpwd operpwd |  |
| CIF系统 | TSPI | g\_operpwd | KDEncodeCli.dll |
| 资金系统 | TSPI | g\_operpwd fundpwd | KDEncodeCli.dll |
| 做市商系统 | 待确认 | | |
| 巨潮系统 | 柜台接口 | 待确认 | |
| VIP系统 | 待确认 | | |

备注：周边系统无需和集中交易同步升级，集中交易先升级，等运行稳定后，再更新周边系统的加密算法库即可。

**对于STG这类通用程序，交易系统、融资融券、快速订单等多个系统都会用到，如果部署环境中有同一个STG被多个系统公用的情况，请保证在对应系统全部升级到国密加密库后，才能升级STG的加密组件。**

**账户系统对接接口132001的出参包含operpwd字段，需账户系统评估是否有使用这两个字段，如果有使用，则两个系统如何配合升级有待评估。**

### 2.1.4密码旁路

针对从恒生系统或金仕达系统迁移过来的用户，柜台中存在密码旁路的处理逻辑，基本思路如下：

1. 检查柜台数据库中存储的密码是否为空，如果不为空，则按正常的逻辑校验，否则，执行第2步的处理；
2. 将客户输入的加密后的密码，解密成明文后，连同恒生或金仕达的机构编码、客户代码一起，发给对应系统的检查接口进行密码校验，如果验证成功，则用金证的密码更新后台数据库，否则，提示密码错误；

对于金仕达系统，其密码验证接口存放在影像库img中，由于影像库已经废弃，本次升级不做考虑。

**对于恒生系统，由于密码校验接口以及恒生密码均由恒生系统提供，金证系统升级无需考虑兼容性，但恒生系统自身升级时，需要考虑检查接口与其后台数据的一致性。**

### 2.1.5 KCXP登陆密码说明

KCXP API提供的登陆接口，密码以明文格式传入，KCXP内部通过调用kcbpcrypt.dll进行加密处理，与柜台的加密控件没有冲突。

在柜台内部，密码以密文格式存放在SpbClient.ini中，由于加解密处理均由柜台完成，且加密控件支持兼容处理，因此，本次升级过程SpbClient.ini以及KCXP程序均无需做调整。

### 2.1.6 extconfig表说明

extconfig中包含大量系统参数设置，其中，字段extconfig2、extconfig9、extconfig21与加解密有关，各字段值含义如下：

* extconfig2表示是否使用金证加密算法，为1表示金证加密，为0表示国君加密
* extconfig9表示使用哪种密钥对密码进行加密，为1表示使用1234567890加密，为2表示使用extconfig21的值加密，其他值按标准密钥加密

**本次升级过程中，需检查extconfig2是否配置为1，如果不为1，本次改造不做任何修改，需客户自行评估改造方案。**

### 2.1.7加密控件说明

|  |  |  |  |
| --- | --- | --- | --- |
| 控件名称 | 关联文件 | 调用程序/接口 | 说明 |
| KDEncodeCli.dll | KDEncodeCli.lib KDEncodeCli.h | KCBP 外围等周边系统 | 常规业务使用的加密算法库，与KDEncode.dll的区别是函数名以字符串的形式输出，提供了加密、重加密功能，未提供解密功能 |
| KDEncode.dll | 无 | KCBP | 函数以序号的形式输出，提供了加密、解密的实现，目前用于金仕达密码旁路处理及外围登陆功能中 |
| KDEnDelib.lib | KDEncode.h | KCBP | 加解密算法是通过静态库的方式提供，没有dll文件，提供了带EX后缀版本的加密、解密、重加密功能，目前用于恒生密码旁路处理 |
| CliEncrypt.dll | 无 | SpbClient AutoOffer | 柜台客户端用于密码加密，密码输入控件TCSPasswdEdit中使用 |
| CSEncrypt.bpl | 无 | SpbClient AutoOffer | 柜台客户端用于对SpbClient.ini中的密码进行加解密处理 |
| kcbpcrypt.dll | 无 | KCBPCli API | KCBPCli API用于对KCXP登陆密码进行加密处理，本次改造不调整 |

## U版交易系统

### 2.2.1 柜台加密控件改造

提供新版本的CITICS\_CE.dll，实现对国密加密算法的包装，柜台程序业务处理部分代码不做调整，通过替换CliEncrypt.dll实现对国密算法的升级。

### 2.2.2 密码检查函数改造

现有的密码检查处理逻辑，是拿外部传入的加密后的密码，与柜台数据库中记录的密码，直接进行比较，两者相同则检查通过，否则，校验失败，检查过程不涉及密码加解密的处理。本次改造，引入新的密码检查函数，其作用是做密码兼容处理，在检查通过后，更新后台数据库的数据。

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，切换条件如下：

* 如果数据库中的密码为老算法加密，传入密码为新算法加密，则用新密码更新后台数据库，并记录操作流水，此步骤是在后台自动进行，通过函数QueryType获取送入客户密码类型。
* 如果数据库中的密码为老算法加密，传入密码为老算法加密，则不修改后台数据
* 如果数据库中的密码为新算法加密，不管传入的密码是用的何种加密算法，均不修改后台数据

所有后台涉及到的UF\_Encrypt函数、UF\_CommDecrypt函数调用都涉及到修改。首先调QueryType函数，判断此密码是新密码类型，还是旧密码类型。

再查询数据库密码，通过QueryType函数校验密码类型。如果是旧密码类型，则转换为新密码进行业务操作。并且更新密码表为新密码。如果是新密码类型，则直接按照新密码类型转化后，进行业务比较。

涉及到功能点L0102015、L0102016、L0102017、L0102018、L0203015、L0206112、L0206021、L0204002。有AUTO\_INFO入参的都涉及到改动。另外注意统一认证也涉及到相关的改造。

### 2.2.3 外部系统接口调用

涉及外部系统的功能号调用，入参中的密码需做兼容处理数据库增加加密类型字段

针对数据库中所有包含密码字段的表，均需增加“加密类型”字段，初始值为6，表示对应的密码字段为老算法加密，密码字段本身的值不做调整。

有密码字段的表清单如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 状态 | 表名 | 描述 | 字段名 | 中文名 | 加密因子 |
| 使用中 | AUTHENTICATION | 用户认证信息表 | AUTH\_INFO | 用户密码 | USER\_CODE |

### 2.2.4 国密批量转换菜单

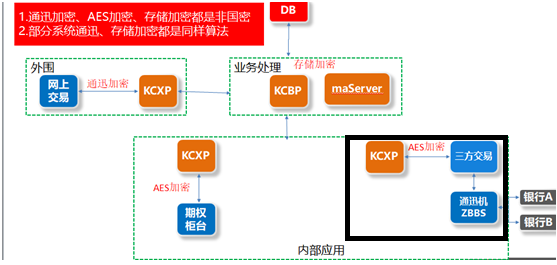
增加专门的菜单，用于将后台数据库中存放的密码，批量转换为国密加密方式。

## KBSS系统（账户）

### 2.3.1 系统现状（改造前）

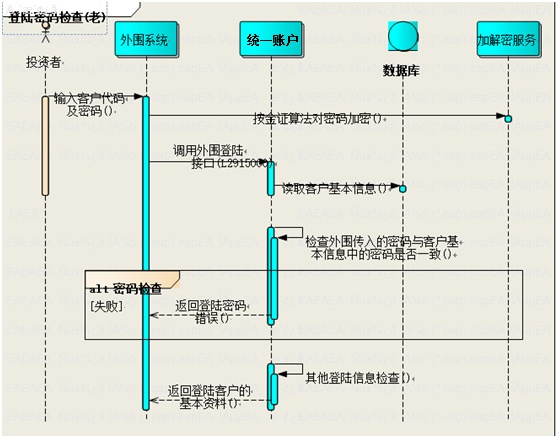
在统一账户系统(KBSS架构)中，大部分加解密算法都是对应国密算法的SM4对称加密算法。

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | 用于柜台系统、三方交易通信加密 |
| AES\_Decrypt1 | 用于柜台系统、三方交易通信解密 |
| MD5\_Digist | 未用到 |
| Base64\_Encode | 没用到 |
| 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 |



注:账户计划后续直接对接银行

### 2.3.2 时序图(改造前)



### 2.3.3 操作员密码

系统的操作员密码是存在数据库中，在统一账户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 | 统一账户系统 | 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、操作员密码存在统一账户系统数据库中  2、操作员密码通过AES\_Decrypt1解密后再用kbss\_encrypt加密 | 本系统 |
| 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 |  |

### 2.3.4 交易密码

交易密码在统一账户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 | 统一账户系统 | 客户修改交易密码  客户重置交易密码 | 1、统一账户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 |
| 股票期权系统 | 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统一账户系统 | 关联系统 |
| 银行(暂未对银证) | 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(暂未对银证) | 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） |  |  |

### 2.3.5 资金密码

资金密码在统一账户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 | 统一账户系统 | 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  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  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 | 1、统一账户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 |
| 股票系统 | 客户修改资金密码  客户重置资金密码 |  | 关联系统 |
| 三方交易网关 | 银行发起银衍开户  银行发起银衍签约  银行发起银衍销户 | 三方网关采用AES加密方式传送资金密码密文 | 网关 |

### 2.3.6 银行密码

银行密码发起方有外围、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 | 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 | 本系统 |
| 外围系统 |  | Web客户端等使用AES\_Encrypt1加密银行密码 | 前端 |
| 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，发送给统一账户系统 | 关联系统 |

## Java系统（一柜通）

### 2.4.1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。

### 2.4.2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。

### 2.4.3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。

## 平台系统

替换DLL文件

# 市场分析

当前使用金证集中交易系统的券商有33家，由于《证券期货业国产密码应用推进规划方案》的规定，券商需要跟随监管层的变化做相应的改造。因此，这次的改造在市场上可行。

# 技术分析

国产密码算法改造项目是在原有系统基础上的完善，将原有加密模式替换成符合监管要的加密模式，技术上没有太多新的难关。但需保障开发和测试人员的深度参与，以及券商的配合，技术上可行。

# 可行性分析

为了保障国产密码算法改造目按时完成，公司将保障预算中的人员及时到位。

技术上，在原有系统基础上进行替换，没有太多新的难关，但需要保障开发和测试人员的深度参与以及券商的配合，从技术层面来说是可行的。

市场上，金证有33家柜台券商需要根据监管要求做相应的系统改造，因此市场上可行。

综上所述，我们有必要迅速进行系统改造，现在技术条件和人员都已经具备，可以立即启动。

# 风险及不确定因素分析

* + 参与本系统的部分开发人员对业务相关的处理不熟悉，存在相关需求点能否完全覆盖的风险；
  + 网关进行升级改造，是一次新的尝试，能否能在约定时间内完成，是项目风险之一；
  + 市场方面，存在开发出的功能需求在对接异构系统时不通畅的情况，在短期内失去部分市场的风险；

# 职责与任务

*以下分别说明在本项目中各相关部门所应承担的职责和任务，以及具体的资源需求和人员安排。*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品线 | 开发 | 测试 | 项目人员合计 |
| 1 | **W版** | 万长久、刘伟、史磊 | 麦凤娟 | 5 |
| 2 | **U版** | 夏乔 | 罗秋姣 | 2 |
| 3 | **账户** | 李永洪 | 卢婷婷、陈彩 | 3 |
| 4 | **期权** | 陆明其、王成明 | 李元名 | 3 |
| 5 | **风控** | 雷文彬 |  | 2 |
| 6 | **网关** | 刘三高、张超、钟文升 |  | 3 |
| 7 | **资金** | 高保君 | 王会勤 | 2 |
| 8 | **OTC** | 张昌城 |  | 2 |
| 9 | **做市** | 谢晓生、隆烨 | 杨大贤 | 3 |
| 10 | **订单** | 何万刚、王敬普 | 刘昀 | 3 |
| 11 | **PIF** | 柳宗 | 高恬恬 | 2 |
| 12 | **一柜通** | 刘青 |  | 2 |
| 13 | **影像档案** | 雷勇 |  | 2 |
| 14 | **清算系统** | 许培华 |  | 2 |
| 15 | **转融通** | 朱文杰 | 王希意 | 2 |
| 16 | **MID** | 钟文升 |  | 2 |
| 17 | **加密DLL改造** | 李学 | 1 | 1 |

# 项目计划和成本分析

## 项目团队

**提示：**说明项目团队的角色、知识技能要求、建议人选、人数、工作时间，如下表所示。

|  |  |  |
| --- | --- | --- |
| 角色 | 知识技能要求 | 工作时间 |
| 领导小组 | 在战略层面对项目进行指导 |  |
| 项目经理 | 具备多年交易系统开发经验，组织协调能力突出 | 2016.5.27-2017.3.31 |
| 需求开发人员 | 具备多年交易系统开发、需求整合经验。 | 2016.5.27-2016.8.5 |
| 系统设计人员 | 具备多年交易系统设计、开发经验 | 2016.5.27-2016.8.5 |
| 编程人员 | 具备多年交易系统开发及相关的业务知识。 | 2016.5.27-2016.8.5 |
| 测试人员 | 具备多年交易系统测试及相关的业务知识 | 2016.6.18–2016.9.19 |
| 工程人员 | 具备多年项目现场实施经验 | 2016.6.18–2016.10.10 |

|  |  |  |  |
| --- | --- | --- | --- |
| 内容 | 范围 | 开始时间 | 完成时间 |
| 国密库开发 | 所有系统 | 2018.4.19 | 2018.5.18 |
| 第一轮国密开发 | 期权、账户、W版、一柜通 | 2018.5.28 | 2018.6.1 |
| 第二轮国密开发 | 所有系统 | 2018.6.4 | 2018.6.8 |
| 第一轮系统联测 | 期权、账户、W版、一柜通 | 2018.6.4 | 2018.6.15 |
| 第二轮系统联测 | 所有系统 | 2018.6.18 | 2018.6.29 |
| 工程上线演练 | 所有系统 | 2018.7.2 | 2018.7.13 |

## 主要软件硬件资源估计

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 产品线 | 资源名称 | 级别 | 详细配置 | 数量 | 获取方式 | 费用 |
| WIN版 | 操作系统 | 关键 | Windows server 2012 | 1 | 客户提供 | 无 |
| 数据库 | 关键 | SQL SERVER 2014 | 1 | 客户提供 | 无 |
| 电信网络 | 关键 | 万兆、低延时交换机 |  | 客户提供 | 无 |
| U版 | 操作系统 | 关键 | AIX 5.3/AIX 6.1 | 1 | 客户提供 | 无 |
| 数据库 | 关键 | ORACLE 10G/11G DB2 V8.2/V10.5 | 1 | 客户提供 | 无 |
| 电信网络 | 关键 | 万兆、低延时交换机 |  | 客户提供 | 无 |
| 账户2.0系统 | 操作系统 | 关键 | Windows、Linux、Aix | 1 | 客户提供 | 无 |
| 数据库系统 | 关键 | 最低数据库版本：IBM DB2 8.2、ORACLE 10g、MSSQL2005 | 1 | 客户提供 | 无 |
| 中间件平台 | 关键 | 各操作系统平台的KCBP、KCXP | 1 | 客户提供 | 无 |
| 电信网络 | 关键 | 万兆、低延时交换机 |  | 客户提供 | 无 |

## 成本估计

|  |  |  |
| --- | --- | --- |
| 条款 | 成本（人民币） | 备注 |
| 人力资源 | 40人\*44天\*3000=528万 | 包括专家分析诊断、开发实施等 |
| 软硬件资源 | 0元 | 厂商提供 |
| 差旅费 | 0万元 | 包括专家、开发、实施人员的差旅费，差旅费含酒店住宿费用与交通补贴费用，及每人2次往返机票预算 |
| 会议费 | 0万元 |  |
| 接待费 | 0万元 |  |
| 协作费 | 万元 |  |
| 合计 | 528万元 |  |

# 成本效益分析

## 生产规划

总投入30人每月左右进行产品的开发和测试。

## 收益

使用我们柜台系统的33家券商为了符合监管政策的要求，需要进行系统改造。

## 收益/投资比

整个产品生命期的收益／投资比值是3000: 465≈ 1:0.155（单位：万元）。

## 投资回收周期

投产后上线即可回收研发成本并产生利润，开发到上线时间为半年。投资回收周期最快为半年可收回成本。

# 10. 总结

在当今的市场情况下，此时进行国产密码算法统改造是非常可行的，由此可见，这个项目是具有较大的经济效益，在财务上是可行的。