国密改造需求说明书

文件修订历史

修订时间	修订说明	作者	审核
2022/04/15	初稿	高英	

目 录

1. 需求概述

为贯彻落实中办、国办的方针思想和《密码法》关于信息系统密码应用的要求，基金行业在 2021 年启动密码应用升级改造工作，通过对基金 APP 客户端应用场景在功能上和性能上的国密密码算法改造。我司积极响应国家和证监会的号召，开展针对直销 APP 系统的国产密码算法改造工作。

2. 国密改造需求

APP 作为公司网上交易系统移动端应用，主要为直销客户提供基金产品查询、基金交易、资产查询、交易记录查询等各类业务功能。

APP 传输信息种类主要包含客户的个人信息（包括个人身份信息、个人金融信息）、交易指令、交易流水、资产记录、基金产品数、基金公告等。其中个人的身份信息、个人金融信息、交易指令、交易流水等属于重要、敏感信息。基金产品数据、基金公告等为公开的非敏感信息。

2.1. 网络和通信

在本系统统一外联区部署符合密码相关国家、行业标准要求的 SSL 应用安全网关，建立安全 HTTPS 加密通道。

2.2. 应用和数据

交易数据安全加固，对基金交易环节的重要数据采用数字信封技术保证数据传输的机密性，对于扣款指令、对账单数据进行传输机密性、完整性保护，实现互联交互数据防窃取和防篡改保护。

2.3. 业务安全

同时兼容 APP 旧版本的访问，核心产品需同时支持国产商用密码算法和国际双算法，具有灰度发布和平滑过渡的方案和数据灾备恢复手段。

2.4. 合规性要求

本次项目聚焦在直销 APP，在网络和通信、应用和数据层面进行密码应用的设备、

算法、协议等需符合国家主管部门要求。即产品需具备《商用密码产品认证证书》、使用国产商用密码算法、使用符合规范的密钥交换协议、SSL 协议等。