ICS 03.060
CCS A 11

团 体 标 准

T/SAC 003—2024

证券业商用密码应用上线指南

Guide for launching of commercial cryptography applications in securities industry

2024-05- 发布 2024-05- 实施

中 国 证 券 业 协 会 发布

目　　次

前　言

本文件按照GB/T　1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件起草单位：中国银河证券股份有限公司、广发证券股份有限公司、兴业证券股份有限公司。

本文件主要起草人：罗黎明、华阳、魏自恩、梅养真、魏振宇、鹿群、杜瑞罡、谈加虎、王金刚、樊丹、王栩。

证券业商用密码应用上线指南

1 范围

本文件给出了证券业机构开展密码应用上线的要求。本文件适用于证券业核心机构、经营机构等相关信息系统进行商用密码应用改造后的上线工作。

2 规范性引用文件

下列文件对于本指南的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本指南。凡是不注日期的引用文件，其最新版本适用于本指南。

《中华人民共和国密码法》

GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》

GB/T 22239—2019《信息安全技术网络安全等级保护基本要求》

GB/T 37092—2018《信息安全技术 密码模块安全要求》

JR/T 0060—2021 《证券期货业网络安全等级保护基本要求》

JR/T 0191—2020 《证券期货业软件测试指南 软件安全测试》

JR/T 0099—2012 《证券期货业信息系统运维规范》

GM/T 0115—2021 《信息系统密码应用测评要求》

GM/T 0116—2021 《信息系统密码应用测评过程指南》

GM/T 0039—2015 《密码模块安全检测要求》

GM/T 0028—2014 《密码模块安全要求》

GM/T 0024—2014 《SSL VPN 技术规范》

GM/T 0015—2012 《基于SM2密码算法的数字证书格式规范》

GM/T 0009—2012 《SM2密码算法使用规范》

GM/T 0004—2012 《SM3密码杂凑算法》

GM/T 0003—2012 《SM2椭圆曲线公钥密码算法》

GM/T 0002—2012 《SM4分组密码算法》

3 术语和定义

下述术语和定义适用于本文件。

3.1

密钥 key

控制密码算法运算的关键信息或参数。

3.2

密钥管理 key managenment

根据安全策略，对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥生存周期的管理。

4 基本要求

4.1 基本原则

确保系统正常运行的原则。证券业信息系统商用密码应用改造工作涉及面广、衔接性强、实时性要求高，实施操作必须要以确保系统和业务的正常运行为前提。

坚持“谨慎试点、新老并行、业务不中断”的原则，并制定相关业务应用推广和应急回退等方案。

4.2 组织保障

为保障商用密码应用上线正常运行，应成立专门的商用密码应用领导小组（以下简称“领导小组”）和商用密码应用工作小组（以下简称“工作小组”），明确相应职责和任务分工，建立定期汇报交流的工作机制。

领导小组在系统上线全过程中应履行全局协调、整体指挥的职责。对系统上线涉及到所有业务做到统一调度，发现问题统一排查、解决。领导小组负责人由首席信息官或分管信息技术的公司高级管理人员承担。

工作小组负责商用密码应用项目的技术方案论证、设计、系统建设、运维管理和技术保障，以及对相关制度、业务流程的合规性审定等工作。同时要对业务人员开展客户咨询、应急情况客户响应等培训。工作小组至少包含信息技术人员、相关业务人员、客服人员、法律合规人员、风险管理人员等。工作小组组织相关人员持续开展商用密码相关知识及标准规范学习培训，落实系统上线后的运维和管理保障工作。

4.3 经费保障

为保障项目顺利实施及上线后运维、扩容等预备必要的经费，应为商用密码应用改造预留充足的预算。

4.4 管理制度要求

按照GB/T 39786相关要求，制定密码应用、密码安全管理制度及安全操作规范。包括但不限于：

a) 采用密码技术提供物理和环境、网络和通信、设备和计算以及应用和数据的安全；
b) 人员管理制度，至少包含密码安全人员管理制度和密码安全人员岗位划分制度等；
c) 密钥管理制度，至少包含密钥管理和口令管理等；
d) 建设运行制度，至少包含密码应用方案和密码安全性策略等；
e) 应急处置制度，至少包括应急处理和报告制度。

4.5 产品资质要求

应使用国家密码主管部门认证核准的密码技术和产品，采用的密码服务符合国家密码主管部门的要求。

5 运行保障

为保障商用密码应用上线后安全、高效和稳定运行，上线前对其存在的风险点进行分析、分类，并对风险点做好应对策略，便于在发生安全事件时可以根据应对策略快速响应。

5.1 密码应用安全性评估

网络安全等级保护二级以下信息系统商用密码应用在正式上线前，可聘请商用密码主管部门认可的安全性评估机构开展密码应用安全性评估，并达到符合及以上要求。

网络安全等级保护二级信息系统商用密码应用在正式上线前，宜聘请商用密码主管部门认可的安全性评估机构开展密码应用安全性评估，并达到符合及以上要求。

网络安全等级保护三级及以上信息系统商用密码应用在正式上线前，应聘请商用密码主管部门认可的安全性评估机构开展密码应用安全性评估，并达到符合及以上要求。

5.2 上线后监控和质量保证措施

商用密码应用上线工作完成后，应将涉及的服务器、软件、网络设备以及专有设备纳入监控和报警体系，并且将应用性能、应用日志、系统容量、关键业务场景指标等纳入监控和报警体系，定期进行分析，确保相关指标在预期范围内。

6 系统上线

商用密码应用上线时，应制定完整的上线方案，内容包括但不限于测试方案、上线策略、部署方案、上线实施和回退方案，保障商用密码应用上线后安全、高效和稳定运行。

6.1 系统测试

商用密码应用改造上线或重要升级前进行严格的测试，测试内容包括但不限于功能测试、压力测试、安全测试和场景对比测试。

6.1.1 功能测试

工作小组制定详细的商用密码应用测试方案，对各系统模块以及系统整体进行测试。测试模块包括但不限于商用密码相关的协同签名模块、应用安全网关、数字证书、密码模块。测试场景包括但不限于证书申请、更新、注销，以及应用安全网关流程、协同签名流程、业务全链路场景。

6.1.2 压力测试

根据系统技术特点和承载业务类型，设定测试场景，制定测试方案，从系统处理能力、业务响应时间等方面设置测试指标，有序组织测试工作。信息系统的性能容量、响应时间和系统资源利用率等应控制在合理范围内并满足业务开展需要。测试完成后形成压力测试报告存档备查。

需重点关注以下两类指标：

a) 系统性能指标：包括吞吐量、并发数和响应时间等，指标将从单位时间、特定长度时间、数据从源端到目标端流转时间和数据请求发起到服务完成时间等不同角度反映被测系统处理数据的效率和能力；
b) 资源性能指标：包括服务器主要硬件资源（CPU、内存、磁盘等）的利用率和操作系统软件资源（进程数、网络连接数量、文件句柄占用数量等）的使用情况。

6.1.3 安全测试

在上线前针对商用密码应用编制详细的安全测试计划和测试用例，执行相关测试并确保测试结果符合要求。

测试内容包括但不限于：

a) 安全功能检查：通过人工检查、审核的方式对软件开发过程中涉及的安全策略、进度、技术决策（如开发模型等）进行安全功能检查；
b) 代码安全测试：通过对软件源代码进行安全扫描和审计，排除代码中的漏洞及恶意代码（如外购类软件系统，可由开发商提供代码安全测试报告）；
c) 漏洞扫描：通过扫描等手段对指定系统进行检测，发现可利用漏洞的一种安全检测行为；
d) 渗透测试：以攻击者视角进行的黑盒测试，从而获得对应用系统的安全评价；
e) 模糊测试：以向目标系统提供非预期输入的方式，提高应用程序的健壮性及抵御意外输入时的安全性。

测试范围包含但不限于多种安全类型：身份认证安全、口令安全、访问权限安全、会话管理安全、通信安全、业务逻辑安全、输入数据安全、存储数据安全、提示信息安全、个人信息保护安全、日志数

据安全、算法安全、安全审计、配置安全、拒绝服务、源代码数据安全、架构安全、运行环境安全、卸载安全、组件安全、权限安全、第三方库安全（若涉及）等。

6.1.4 场景对比测试

对比改造前后的使用体验、延迟变化，分析和评估对用户应用操作和实际体验的影响。

6.2 上线策略

可采用逐步替换或逐步切换流量的方式，做好系统开关控制方案的设计、评审和验证，实现通过系统参数控制功能或流量切换。提供紧急情况下通过系统参数进行的回退机制，并及时收集用户反馈。

6.3 上线方案

系统上线前审慎地根据系统部署方案，制定详尽的系统上线方案，经由工作小组评审通过，并由领导小组审批。

上线方案包括上线相关参与方、具体参与人员、合理的上线时间、应用备份工作、数据备份工作、前序工作检查步骤、上线详细操作步骤、检验步骤等。

6.4 上线实施

系统上线时组织好具体参与人员，按照上线方案的操作细节步骤实施操作，并且做好相关的验证工作。上线成功后，工作小组向领导小组进行报告，并启动上线后的监控工作和质量保证措施。

系统改造上线前，制定上线回退方案，保障商用密码应用上线过程中出现异常时，可回退到改造前系统状态。回退管理主要内容包括但不限于：

a) 回退方案：回退方案包括回退工作的具体操作步骤、后续检验步骤等。在上线前进行相应的系统回退演练，确保方案切实可行。
b) 回退触发：针对上线过程中可能会遇到的各种异常情况，制定相应的指标，在触发异常并且已达到相关指标时，工作小组启动回退的决策流程，并报告领导小组。经由领导小组决策后是否继续上线工作还是启动回退方案。
c) 回退执行：如果领导小组决策启动回退方案，工作小组执行系统的回退工作，终止本次商用密码应用上线工作，系统回退到上线前的系统状态。

7 应急管理

7.1 应急准备

a) 建立健全软硬件应急知识库，发生故障时及时向工作小组上报，工作小组协调技术人员进行事件评估与处置；
b) 准备充足的重要设备备品配件（包括但不限于密钥管理系统、SSL 接入网关等），并进行定期评估，检测和维护；
c) 对客服人员统一培训，所有客服人员熟练掌握应对投资者咨询、投诉等非现场服务处理流程；
d) 制定应急演练场景，定期进行应急演练，重点演练出现过的异常情况。

7.2 应急处理

a) 查找知识库信息，确认此软硬件事件是否有记录，若有记录则依据知识库现场恢复后验证有效性并上报事件信息；
b) 若知识库无记录此软硬件事件，需联系厂商人员提供远程技术支持，并联系厂商技术人员分析事故影响，厂商提供事件恢复方案，厂商需依据方案的时效性给出相应的替换方案，技术人员验证方案的有效性，上报事件问题和现场恢复状况，将恢复方案记录知识库；

c) 厂商无法远程恢复，需立刻上报工作小组并联系厂商负责人派遣专业人员到现场提供技术支持，联系厂商给出现状描述，并提供确保系统服务稳定的解决方案，事件恢复后厂商需提交报告说明情况，验证方案的有效性，将事件描述和恢复记录知识库；

d) 任何软硬件事件恢复现场后需持续监控修复后的软硬件运行状况，并按有关规定报告事件情况，对可能构成特别重大、重大网络安全事件的保持持续报告，直至系统恢复正常运行，报告要素应完备、及时、准确，不得迟报、漏报、谎报或瞒报；

e) 由客服中心统一处理投资者咨询和投诉。

7.3 调查处理

调查处理过程中,应对工作底稿进行有效保护,扩展分析相关问题及研究制定可行对应的解决方案，可适时组织外部专家进行会审，尽量避免相关问题再次发生。同时，工作小组根据事件响应和处理情况编制报告并上报领导小组。

7.4 典型应急场景

本指南收录应急场景典型案例参见附录A。

附 录 A
（资料性）
应急场景典型示例

A.1 SSL接入网关故障

故障描述：SSL接入网关设备无法正常提供服务，可能造成的影响有：客户端无法与SSL接入网关建立连接，客户端的业务请求无法通过SSL接入网关转发至后台系统，导致业务功能无法完成。
处理建议：接入网关采用多点部署模式，部分接入网关设备无法正常提供服务，客户端会自动切换到其他接入网关；若所有接入网关故障，可采用相关旁路机制绕过SSL接入网关，让客户端系统请求正常发送至后台应用服务器，保证交易的连续性。

A.2 数字证书认证系统故障

故障描述：CA无法正常提供服务，可能造成的影响有：客户端无法申请签名证书和加密证书。
处理建议：CA服务供应商提供备份线路，当主线路无法提供服务时，自动切换到备份线路，继续提供服务。在CA无法正常提供服务的情况下，启用商用密码SSL单向认证或旁路机制。

A.3 密钥管理系统（KMS）故障

故障描述：密钥管理系统（KMS）无法正常提供服务，可能造成的影响有：服务端产生的协同签名密钥分量无法存储到密钥管理系统，导致SSL接入网关不能提供协同签名密钥生成服务；未申请密钥的客户端将无法使用协同签名服务，无法完成商用密码SSL双向认证连接。已申请密钥的客户端由于无法从KMS中获取用户服务端密钥分量参数，无法实现协同签名运算，导致商用密码SSL双向认证失败。
处理建议：密钥管理系统支持主备部署模式，在主节点异常的情况下，支持服务切换到备份节点，继续提供服务。在主备密钥管理系统均无法提供服务的情况下，启用商用密码SSL单向认证或旁路机制。