ICS 03.060
CCS A 11

团　　体　　标　　准

T/AMAC 0002—2024

基金经营机构商用密码应用上线指南

Guide for launching of commercial cryptography applications in fund management institutions

2024-05-31 发布　　2024-05-31 实施

中国证券投资基金业协会　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国证券投资基金业协会提出并归口。

本标准主要起草单位：中国证券投资基金业协会、博时基金管理有限公司、易方达基金管理有限公司、南方基金管理股份有限公司、招商基金管理有限公司、中国银河证券股份有限公司、上海好买基金销售有限公司、大商所飞泰测试技术有限公司、北京信安世纪科技股份有限公司。

本标准主要起草人员：丁伯轩、梅亚雷、王德英、车宏原、莫崇慧、曾志、伍振河、陈朝昱、唐永鹏、李明、罗志灵、白开旭、李骏、李军锋、章栋兵、刘昌峻、谢冠彬、王志刚、魏自恩、刘伟东、胡长胜、马骥、刘军、庞彦广、刘进、隋文东、龙泉、李铭、陈锐。

基金经营机构商用密码应用上线指南

1　范围

本文件给出了基金经营机构开展密码应用上线的基本要求、主要程序、运行保障、应急管理等方面的要求。

本文件适用于基金经营机构新建商用密码应用和相关信息系统进行商用密码应用改造后的上线工作以及后续的重大变更操作。

2　规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

3　术语与定义

下列术语和定义适用于本文件。

3.1

商用密码 commercial cryptography

指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。

3.2

数字证书 digital certificate

指在互联网通讯中标志通讯各方身份信息的一个数字认证，人们可以在网上用它来识别对方的身份。

3.3

协同签名 collaborative signature

由多个密钥持有方共同完成的数字签名实现。

3.4

渗透测试 penetration test

一项在计算机系统上进行的授权模拟攻击，旨在对其安全性进行评估，是为了证明网络防御按照预期计划正常运行而提供的一种机制。

3.5

灰度发布 gray release

指在黑与白之间，能够平滑过渡的一种发布方式。在其上可以进行A/B testing，即让一部分用户继续用产品特性A,一部分用户开始用产品特性B,如果用户对B没有什么反对意见，那么逐步扩大范围，把所有用户都迁移到B上面来。

3.6

SSL 网关 secure sockets layer gateway

一种安全的网关设备，可以通过SSL和TLS协议，为网络应用提供加密连接和身份验证等服务。

3.7

CA 认证 certificate authority

即电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的活动。

3.8

抗抵赖性 no-repudiation

指防止网络信息系统相关用户否认其活动行为的特性。

3.9

加密机 encryption equipment

通过国家商用密码主管部门鉴定并批准使用的国内自主开发的主机加密设备。

4 基本要求

4.1 基本原则

4.1.1 确保系统正常运行。基金经营机构商用密码应用上线工作应以确保系统和业务的正常运行为前提。

4.1.2谨慎试点、新老并行、业务连续。并制定相关业务应急回退等方案。

4.2 组织保障

4.2.1 应组建专门的商用密码应用领导小组和商用密码应用工作小组,并明确其职责和分工,建立相应的工作机制。

注1：“商用密码应用领导小组”简称“领导小组”。

注2：“商用密码应用工作小组”简称“工作小组”。

4.2.2 领导小组的组成和职责如下：

a) 领导小组可指定相关职能团队来担任；

b) 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出任；

c) 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工作做到统一调度，统一处置。

4.2.3 工作小组的组成和职责如下：

a) 工作小组包含但不限于信息技术人员、相关业务人员、客服人员、法律合规人员、风险管理人员；

b) 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；相关制度、流程的合规性审定；以及业务影响评估、应急预案制定等工作。

4.3 经费保障

应为商用密码应用改造、上线、运维、扩容等做好经费及预算安排。

4.4 管理制度要求

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

a）人员管理，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；

b）密钥管理，至少包含密钥管理和口令管理等；

c）建设运行，至少包含密码应用方案和密码安全性策略等；

d）应急处置，至少包含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 主要程序

5.1 制定上线方案

商用密码应用上线时，应制定上线方案。内容包括但不限于测试方案、上线策略、上线方案、上线实施和回退方案。

5.2 系统测试

5.2.1 通用要求

商用密码应用上线或重大升级前，应进行系统测试。测试内容包括但不限于功能测试、性能测试、安全测试、场景对比测试。测试通过后应将测试结论形成报告存档备查。

5.2.2 功能测试

工作小组应制定详细的商用密码功能测试方案，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，以及协同签名流程、业务全链路场景。

5.2.3 性能测试

5.2.3.1 根据系统技术特点和承载业务类型，设定测试场景，制定性能测试方案，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。
5.2.3.2 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，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。

5.2.4 安全测试

5.2.4.1 在上线前针对商用密码应用制定详细的安全测试方案，执行相关测试并确保测试结果符合要求。
5.2.4.2 测试内容包括但不限于：

a）基线检查：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、技术决策（如开发模型等）进行安全功能检查；

b）代码审计：通过对软件源代码进行安全扫描和审计，检查代码规范、排查代码漏洞（若为外购类软件系统，可由开发商提供代码安全测试报告）；

c）漏洞扫描：通过自动化扫描等手段对指定系统进行探测与安全测试，发现应用或设备漏洞，并提供安全修复建议与方案；

d）渗透测试：以攻击者视角进行的模拟攻击测试，检测系统漏洞及安全弱点，从而获得对应用系统的安全评价并提供安全建议。

5.2.4.3 测试范围包含但不限于：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、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、组件安全、权限安全等。

5.2.5 场景比对测试

5.2.5.1 采集并比对应用系统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。
5.2.5.2 场景比对测试的结果评价应关注登录耗时、订单处理耗时等核心指标。在应用系统改造后，性能损耗应控制在设定的阈值之内，以保障用户的使用体验不受明显影响。

5.3 上线策略

正式上线前应通过试运行方式在生产环境做好相关功能的测试和验证。正式上线可采用灰度发布策略，通过流量逐步切换的方式实现应用升级。宜做好流量控制方案，提供紧急情况下基于流量控制的回退机制。上线期间实时监测用户使用情况，及时收集用户反馈。

5.4 上线方案

5.4.1 系统上线前审慎地制定完善的系统上线方案，经工作小组评审通过，并由领导小组审批。
5.4.2 上线方案包括上线相关参与方、具体参与人员、合理合适的上线时间、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。

5.5 上线实施

5.5.1 系统上线时应组织好具体参与人员，按照上线方案的操作步骤实施操作，并且做好相关的验证工作。
5.5.2 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。

5.6 回退管理

5.6.1 系统改造上线前，应制定上线回退方案，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。
5.6.2 回退管理包括但不限于：

a）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执行；

c）回退执行。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，回退操作完成后应进行相关业务验证测试。

6 运行保障

6.1 运行保障要求

商用密码应用上线前应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。

6.2 密码应用安全性评估

法律、行政法规和国家有关规定要求使用商用密码进行保护的信息系统在商用密码应用正式上线前，应聘请商用密码主管部门认可的安全评测机构开展密码应用安全性评估，确保达到国家密码主管部门相关标准要求。

6.3 上线后监控和质量保证措施

商用密码应用上线完成后，应将涉及的服务器、软件、网络设备、外部第三方服务（如CA服务）以及专有设备纳入监控和报警体系，并将应用性能、应用日志、证书有效期、服务器同步时间、系统容量、密码设备容量等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，并根据系统容量情况做好扩容准备。

7 应急管理

7.1 应按照《证券基金经营机构信息技术管理办法》中应急管理的统一要求，建立并完善商用密码应用应急管理内容。

7.2 当商用密码设备或者商用密码软件出现问题，无法在规定时间内排除时，商用密码应用应启动应急处理，保障业务连续性。建议通过流量控制方式，提供备用模式切换能力。

7.3 应急场景典型示例详见附录A。

附 录 A
（资料性）
应急场景典型示例

A.1 SSL网关故障

故障描述：SSL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网关建立连接，客户端的业务请求无法通过SSL网关转发至后台系统，导致业务功能无法完成。

处理建议：SSL网关采用多点部署模式，部分SSL网关设备无法正常提供服务，客户端会自动切换到其他SSL网关；若所有SSL网关故障，可采用相关旁路机制绕过SSL网关，使得客户端系统请求正常发送至后台应用服务器，保障业务的连续性。

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。在主备链路均无法连接CA提供服务的情况下，则按照应急流程进行功能回退。

A.3 协同签名系统服务器故障

故障描述：协同签名系统无法正常提供服务，可能造成的影响有：服务端不能完成用户终端注册、申请证书，导致不能为客户端下发证书；已申请密钥的客户端由于无法从协同签名系统中获取用户服务端密钥分量参数，无法实现协同签名运算，客户端将无法进行协同签名身份认证，也不能对基金申购、赎回等关键操作进行完整性、抗抵赖性保护。

处理建议：协同签名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。在主备协同签名系统均无法提供服务的情况下，客户端降级使用无证书认证和数据处理机制。协同签名系统支持负载均衡部署模式，可提供同机房或跨机房的横向扩展部署，而不仅限于主备部署。

A.4 加密机设备故障

故障描述：加密机无法正常提供服务，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：主备部署加密机设备，当主加密机无法提供服务时，自动切换到备加密机，继续提供服务，同时及时更换故障设备。当主备设备全部不可用时，则按照应急流程进行功能回退。

A.5 回退方案

当SSL网关、数字证书认证系统、协同签名系统、加密机等关键设备故障无法及时修复时，应按照应急流程启动回退方案，确保上线后系统的连续性和稳定性。

处理建议：通过流量控制方式，实现备用模式切换能力。紧急情况下可通过流量控制进行功能回退，启用商用密码SSL单向认证或旁路机制。

参考文献

[1] 《中华人民共和国密码法》
[2] 《商用密码管理条例》
[3] 《商用密码应用安全性评估管理办法》
[4] 《证券期货业网络和信息安全管理办法》
[5] 《证券基金经营机构信息技术管理办法》
[6] GB/T 37092-2018 信息安全技术 密码模块安全要求
[7] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[8] GM/T 0039-2015 密码模块安全检测要求
[9] GM/T 0028-2014 密码模块安全要求
[10] JR/T 0191-2020 证券期货业软件测试指南 软件安全测试
[11] JR/T 0175-2019 证券期货业软件测试规范
[12] JR/T 0099-2012 证券期货业信息系统运维管理规范
[13] JR/T 0060-2021 证券期货业网络安全等级保护基本要求