ICS 03.060
CSS A11

团　　体　　标　　准

T/ZQX 0002—2024

期货公司商用密码
应用上线指南

Guide for launching of commercial cryptography applications in futures company

2024－07－01 发布　　2024－07－01 实施

中国期货业协会发布

目　　次

前　言

本文件依据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》的规则起草。

本文件由中国期货业协会提出、归口。

本文件起草单位：中国期货业协会、兴证期货有限公司、浙商期货有限公司、中泰期货股份有限公司。

本文件主要起草人：杨光、王颖、王曦、任永胜、杨胜利、裴英剑、艾青、廖海山、杨林国、李嘉盛、郑杰、李腾飞、康明涛、李庆。

引　言

近年来，《中华人民共和国密码法》和 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》相继发布实施。为贯彻落实国家和监管部门有关要求，期货行业积极推进商用密码技术应用。由于商用密码应用上线环节多、影响范围大，存在一定的技术风险，为指导期货公司做好商用密码应用上线工作，降低商用密码应用试错成本，加速期货公司商用密码应用推广，特编制本文件，供各期货公司自愿参照执行。

本文件中的“密码”是指《中华人民共和国密码法》中所规定的“商用密码”。

期货公司商用密码应用上线指南

1. 范围

本文件主要对期货公司网上交易系统商用密码应用上线的主要环节做出指导和示范。

本文件适用于期货公司贯彻落实《中华人民共和国密码法》规定，结合 GB/T 39786《信息安全技术 信息系统密码应用基本要求》，开展网上交易系统商用密码应用的上线工作。

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。

GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》

JR/T 0099-2012 《证券期货业信息系统运维规范》

JR/T 0060-2021 《证券期货业网络安全等级保护基本要求》

3. 术语和定义

下列术语和定义适用于本文件。

3.1

风险 risk

对目标不确定性的影响。

[JR/T 0099-2012,定义 3.13]

3.2

身份鉴别 identity authentication

证实一个实体所声称身份的过程。

[GB/T 39786-2021,定义 3.8]

3.3

问题 problem

一个或多个事件的未知的潜在原因。

[JR/T 0099-2012,定义 3.9]

3.4

真实性 authenticity

一个实体是其所声称实体的这种特性。

注：真实性适用于用户、进程、系统和信息之类的实体。

[GB/T 39786-2021,定义 3.3]

3.5

机密性 confidentiality

保证信息不被泄露给非授权实体的性质。

[GB/T 39786-2021,定义 3.1]

3.6

完整性 integrity

数据没有遭受以非授权方式所作的改变的性质。

[GB/T 39786-2021,定义 3.2]

3.7

密钥 key

控制密码算法运算的关键信息或参数。

[GB/T 39786-2021,定义 3.6]

3.8

密钥管理 key management

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、恢复和销毁等密钥全生存周期的管理。

[GB/T 39786-2021,定义 3.7]

3.9

访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

[GB/T 39786-2021,定义 3.11]

3.10

加密 encipherment

对数据进行密码变换以产生密文的过程。

[GB/T 39786-2021,定义 3.5]

3.11

交易终端 transaction terminal

用于进行期货交易的软件系统或设备，允许用户通过电子方式进行交易。

3.12

数字证书 digital certificate

由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

注:按类别可分为个人证书、机构证书和设备证书,按用途可分为签名证书和加密证书。

[GB/T 38636-2020,定义 3.1]

3.13

密码模块 cryptographic module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

注：密码模块根据其组成，可分为硬件密码模块，固件密码模块，软件密码模块以及混合密码模块。

[GB/T 37092-2018,定义 3.13]

3.14

渗透测试 penetration testing

以未经授权的动作绕过某一系统的安全机制的方式，检查数据处理系统的安全功能，以发现信息系统安全问题的手段。

[JR/T 0191-2020,定义 3.2]

3.15

模糊测试 fuzz testing

通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞的技术。

[JR/T 0191-2020,定义 3.3]

3.16

网络与信息安全事件 network and information security incident

突发事件的一种，也被称为信息安全事件。由单个的或一系列的有害或意外信息安全事态组成，具有损害业务运作和威胁信息安全的极大可能性。

[JR/T 0099-2012,定义 3.17]

3.17

中继网关 relay gateway

用于连接交易终端和网上交易系统进行交易。

4. 工作要点

4.1 基本原则

确保系统正常运行的原则。期货公司网上交易系统商用密码应用上线工作涉及面广、衔接性强、实时性要求高，实施操作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，可按照实际需要编制相关业务应用推广和应急回退等方案。

4.2 组织保障

为保障商用密码信息系统上线正常运行，可以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”），明确责任分工，并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需要履行全局协调、整体指挥的职责。对系统上线涉及到的所有业务做到统一调度，发现问题统一排查、解决。领导小组负责人建议由首席信息官或分管信息技术的公司高级管理人员担任。

工作小组主要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，以及相关制度、业务流程的合规性审定等工作。同时，对业务人员开展交易者咨询、应急情况交易者响应等培训。工作小组建议至少包含信息技术人员、相关业务人员、客服人员、财务人员、合规人员、风险管理人员等。

4.3 经费保障

为保障项目顺利实施及为上线后运维、扩容等事项预备必要的经费，可为商用密码应用上线预留充足的预算。制定预算方案，费用包含软硬件采购、项目实施、密评费用、后期维护等。预算方案经领导小组审定后，工作小组需做好预算的管控，保障项目的正常实施。

4.4 技术要点

4.4.1 身份鉴别

身份认证的真实性保护。使用密码算法、数字签名机制等密码技术，对通信双方身份进行认证，保障接入用户的身份真实性。身份认证过程包括但不限于交易终端与网上交易系统服务端之间，运维管理终端与密码设备、网上交易系统相关的业务服务器、数据库服务器、堡垒机等设备之间，重要机房访问等。

4.4.2 数据传输

数据传输的机密性和完整性保护。交易终端与网上交易系统服务端之间的数据传输需采用合规的密码技术进行安全保护，保障数据机密性、完整性，防止数据泄露和被篡改。数据传输过程包括但不限于交易终端与网上交易系统服务端之间、运维管理终端与各类应用服务器设备、密码设备之间等。

4.4.3 数据存储

数据存储的机密性和完整性保护。重要数据采用合规的密码技术对机密性和完整性进行保护，防止数据被窃取和被篡改。重要数据包括但不限于密钥信息、机房电子门禁系统进出记录、视频监控信息等。

4.5 管理要点

管理要点由管理制度、人员管理、建设运行、应急处置四个密码应用管理维度构成，具体如下：

a) 管理制度：密码应用安全管理相关制度的制定、发布、修订的规范性要求；根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中的相关要求，需配套制定或遵循密钥管理、口令管理、硬件管理、运维管理、密码人员管理、应急处置、密码软硬件及介质管理等相关制度；根据密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥全生存周期制定相关密钥管理制度；为做好

对密码设备访问控制及运行情况的管理，上线过程中遵循既有的变更和应急事件[1]相关管理制度；

b) 人员管理：设立密码相关安全人员角色，明确密码安全意识以及关键密码安全岗位员工的密码安全能力培养要求，人员工作流程要求等；根据需求设定密钥管理员、密钥操作员、密钥保管员、密钥安全审计员角色，其职责互相制约互相监督。各角色按照密钥管理要求进行分工，确保密钥安全合规，密码相关系统正常运行。其中，密钥安全审计员岗位不可与密钥管理员、密钥操作员兼任；

c) 建设运行：编制切实可行的密码应用方案，包含密码的需求分析、系统密码技术方案、安全管理方案、上线前测试、上线变更、运行监测等部分。同时，上线前需要进行商用密码应用安全性评估，确保商用密码上线后系统安全稳定；

d) 应急处置：制定应急预案和应急处置报告流程，有效预防和处置密码应用安全相关的应急突发事件。对于商用密码应用上线、运行过程中，可能出现的异常场景制定专项应急处置流程，明确应急报告流程，并定期进行演练。

5. 需求分析

5.1 系统现状分析

目前期货交易者主要借助交易终端，通过互联网通道进行期货交易。现有交易终端的存在形态和方式较为多样和复杂，终端类型可分为移动端和 PC 端两类，对于同一终端类型，期货公司也会根据交易者使用习惯提供不同的交易软件。

网上交易系统作为期货交易主入口，一端衔接互联网，一端衔接期货公司内网的网上交易后台系统，在数据传输安全保护上提出了非常高的要求。

期货公司需要对标 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，根据系统架构、交易接入环境、交易终端使用情况、运维管理情况等现状进行分析，确定商用密码应用上线范围。

[1] JR/T 0099-2012 《证券期货业信息系统运维规范》

5.2 安全需求分析

网上交易系统的主要风险点为冒用他人身份进行恶意交易，泄露关键信息，非法窃取密钥，篡改交易数据，以及以非法占有为目的的交易数据恶意修改等。交易终端和网上交易系统的服务端通过互联网进行数据通信，经过各级网络设备进行数据转发，应用数据存在被非法窃取、篡改以及丢失的风险。由于网络环境的复杂性，很难通过网络层处理来保障应用数据的安全性。网上交易系统可采用商用密码技术对通信过程中的敏感数据进行加密保护，保障数据传输安全性。

5.3 密码需求分析

网上交易系统商用密码应用基于密码技术的安全机制以消减风险点。商用密码算法是保障信息安全的核心技术，建议使用国家密码管理局公布的商用密码算法进行升级改造。采用合规的密码协议，建立安全的数据通信通道，保障数据传输过程中的机密性、完整性。通过使用协同签名技术及数字证书认证系统进行用户强身份认证。密钥数据存储使用分段式存储方式，分别使用算法加密存储在交易终端及协同签名服务端，进一步提升密钥安全性。

6. 方案选型

6.1 选型原则

商用密码方案选型的原则主要包含如下几点：

a) 方案合规性。采购的密码设备需要通过商用密码产品检测认证，CA 服务及采用的密码算法、通信协议等需要符合法律、法规和密码相关国家标准、行业标准；

b) 方案可行性。不同期货公司具有不同的物理环境、网络架构、系统分布等，选择适合本公司实际情况的上线方案，方案选型要求可落地、可实施；

c) 系统可维护性。要确保方案具备较高的可维护性，包括但不限于硬件管理、密钥管理、数字证书维护等；

d) 系统高可用性。确保整体改造后具备高可用性。充分考虑冗余设计、容错设计、容量设计、负载控制等因素，可采用主备或多活等模式提高系统的抗风险能力；

e) 系统可拓展性。目前，期货公司网上交易系统大多呈现多机房、多系统、多站点、

多终端的特点，系统整体改造可使用逐步上线、分批上线的方式，良好的系统可拓展性有利于商用密码应用分批落地，降低上线风险。

6.2 方案选型

商用密码应用方案是以合规的密码协议为基础，通过交易终端、SSL 与协同签名、密码卡、网上交易系统前置等软硬件结合的手段，最终实现在安全通道下进行交易通信的过程。基本应用流程包括：终端有效性数字证书校验，交易者身份有效性校验，终端与网上交易系统服务端单向 SSL 通道建立，交易者数字证书申请，最终实现交易者与网上交易系统服务端建立双向 SSL 安全通道。

行业主流方案：在终端层→接入层→网上交易系统层的基础结构上进行改造，通过在终端层与接入层之间增加商用密码安全层，参见附录 A 方案选型参考模式一，或者在接入层采用旁路架构，增加密码卡或密码机配合协同签名服务，最终实现商用密码安全三层结构，参见附录 B 方案选型参考模式二。各公司可结合自身系统架构，选择合适的方案。

7. 联调测试

7.1 系统测试

7.1.1 业务功能测试

制定详细的网上交易系统商用密码应用测试方案和测试用例，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安全密码模块、密码卡、数字证书认证系统以及各接入交易终端。

测试场景包括但不限于数字证书查询、申请、延期、注销，以及业务委托报单等业务全流程场景。

7.1.2 安全测试

网上交易系统商用密码应用上线前，要根据实际需求编制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（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；

d) 渗透测试：以攻击者视角进行黑盒测试，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、输入数据安全、存储数据安全、算法安全、运行环境安全等。

7.1.3 对比测试

根据业务场景，对商用密码应用上线前后的系统，对比交易者使用体验、时延变化等情况，分析和评估对交易者应用操作和实际体验的影响。包括但不限于登录、委托报单、撤单、成交回报，以及持仓、资金等信息查询全业务流程。

7.1.4 冗余测试

根据行业特性，为保障业务连续性，网上交易系统商用密码应用建设要充分考虑系统冗余性，采用多活或冷备等模式部署，提高系统健壮性。

在商用密码应用上线后，对系统冗余情况进行充分测试，检测在节点异常情况下，备份系统能否正常承载日常业务。

7.1.5 压力测试

根据自身网上交易系统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，测试完成后形成压力测试报告存档备查。网上交易系统的性能容量、响应时间和系统资源利用率等控制在合理范围内，确保容量满足业务开展需要。

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，指标将从数据自交易终端到网上交易系统前置流转时间，及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：包括商用密码设备、服务器主要硬件资源（CPU、内存、磁盘等）的利用率，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）的使用情况等。

7.2 中继接入测试

7.2.1 架构设计

网上交易系统商用密码应用上线涉及到交易者接入方式的调整，根据柜台系统架构、密码应用架构、机房部署、线路设备情况等综合考虑，设计合适的交易终端中继接入架构。

7.2.2 可用性调试

根据实际情况进行架构设计，部署新的交易终端中继，或调整接入配置，做好交易中继版本升级，并进行数据包转发测试。如涉及互联网通信，则需检查中继通信过程中数据加解密的情况。

7.3 交易终端联调测试

7.3.1 功能测试

根据实际情况制定针对交易终端模块的测试方案和测试用例，测试内容至少包括登录（申请数字证书）、延期、重置 PIN 码、数字证书锁定、委托报单、修改账户密码等场景。不同场景设置不同输入值，例如交易者身份认证机制、数字证书有效期内或数字证书过期后的数字证书相关操作、重置 PIN 码的验证机制、首次与非首次登录等，多维度测试交易终端的健壮性，保障交易者在任何业务场景下的正常使用。

7.3.2 体验优化

根据交易者类型与使用特性，做好交易终端体验优化，尽最大可能保障交易者使用的便捷性，例如默认 PIN 码、自动延期、不同交易终端复用数字证书、数字证书管理功能优化等。

优化区分交易柜台系统、安全密码模块、数字证书认证系统的报错提示，以便进行故障定位。

7.3.3 合规性测试

交易终端上线前进行商用密码应用安全性评估，对数字证书认证机制、交易终端与网上交易系统服务端之间通信过程进行合规性测试，确保交易终端密码模块中密码算法以及通信协议的合规性。

8. 系统上线

8.1 上线实施

8.1.1 上线前置条件

a) 网上交易系统已完成技术准备，商用密码应用已完成部署，与现有系统已完成集成，已通过经商用密码主管部门认可的安全性评估机构开展的商用密码应用安全性评估；
b) 通过系统功能测试、压力测试、冗余测试等，确保系统容量、性能达到要求；
c) 上线交易终端完成基础功能测试，确保无影响正常业务进行的问题，并符合商用密码应用安全性评估标准；
d) 相关运维人员已完成上岗培训，熟悉商用密码应用的安全操作规范，明确人员分工职责，包括操作人员、维护人员、管理人员等；
e) 对公司内部业务、客服等相关人员做好统一培训，培训内容包括但不限于改造后各交易终端使用方法，所有客服人员熟练掌握交易者咨询、投诉等非现场服务处理流程。

8.1.2 上线前准备

a) 确定上线具体参与人员，做好上线实施工作及上线后的监控工作人员安排，并根据上线情况，向领导小组进行报告；
b) 制定上线计划，按步骤编写实施方案，方案包含但不限于具体实施步骤、业务验证方案、测试用例等，并做好相关验证工作；
c) 制定应急回退方案，包括回退工作的具体操作步骤、回退指标、后续检验步骤等。在上线前进行系统回退演练，确保方案切实可行。

8.1.3 上线实施

组织具体参与人员，按照上线方案的操作步骤实施，在开盘前完成切换操作，并调整好系统监控项。切换完成后，做好相关验证工作，使用测试交易终端进行基础业务测试，确保系统功能正常、数据准确无误。

8.1.4 上线跟踪

相关信息技术人员持续对上线后的系统进行状态监控，包括商用密码安全密码模块和数字数字证书认证系统的运行状态，以及各上线交易终端的交易者在线情况。收集交易者反馈，针对反馈问题制定后续优化方案。

在触发异常且已达到相关指标时，工作小组启动回退决策流程，报告领导小组。由领导小组决策是否继续上线工作，或启动回退方案。操作完成后针对相关问题开展扩展分析，并研究制定可行的解决方案，必要时可组织外部专家进行问题分析评估，避免相同问题再次发生。

8.2 投入运行策略

8.2.1 商用密码应用系统上线

网上交易系统商用密码应用上线，可按照实际情况采取逐个站点更换，新老站点并行等策略，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。

逐个站点更换策略：对交易者接入的前置、代理、中继等接入点，逐个进行部署替换，

切换时保留原有接入点，做好应急回退方案。

新老站点并行策略：网上交易系统各接入站点更换上线时，保留原有接入站点，并行观察一定时间，确保商用密码站点的稳定性。

8.2.2 交易终端上线

根据交易者交易终端使用占比情况，可使用从少到多、交易终端分批上线、交易终端灰度推送升级等策略，上线过程中加强风险控制，对可能出现的风险点进行分析、分类，制定应急处置措施。

上线后要做好系统运维保障，做好紧急情况下的回退方案，如正常站点升级包推送、混合地址终端（商密接入地址和非商密接入地址同时打包）启用应急接入地址等措施，并及时收集交易者反馈，做好交易者安抚工作。

9. 运行保障

9.1 日常操作

a) 商用密码应用上线后将相关密码设备纳入日常巡检设备清单，确保设备正常运转；
b) 制定协同签名系统、数字证书认证系统等相关密码系统启停计划，纳入日常操作规程；
c) 定期做好相关密钥数据备份，按照要求做好数据保存；
d) 定期对网上交易系统进行漏洞扫描，对发现的系统漏洞及时修复；
e) 系统运维人员严格执行系统操作流程，完整、准确、详细的记录并定期分析网上交易系统运行日志；
f) 如运行期间发生异常，详细记载发生异常情况的时间、现象、处理方式等内容并妥善保存有关原始资料。

9.2 系统监控

网上交易系统商用密码应用涉及的服务器、软件、网络设备和商用密码专有设备，以及应用性能、应用日志、关键业务场景指标等要纳入监控和报警体系，应用监控包括但不限于协同签名系统、API 服务（包括认证、申请数字证书等）、TCP 服务、HTTP 服务、CA 服务等，

关键业务场景监控指标包括但不限于身份认证登录、数字证书申请、交易者在线情况等，定期分析各项指标，确保相关指标在预期范围内。

9.3 升级变更

网上交易系统商用密码应用上线后，期货公司根据法律法规、自律规则和行业相关标准的要求，结合公司实际情况，制定系统升级变更实施细则，并严格按照细则进行升级变更操作，使系统升级变更能够安全、合规、高效进行，避免因升级变更给公司正常业务运行带来风险。

10. 应急管理

10.1 应急准备

a) 建立健全网上交易系统商用密码事件的应急处置组织体系，明确网络与信息安全事件的应急指挥决策机构和执行机构，负责商用密码安全事件相关的预防预警、应急处置、报告和调查处理工作；
b) 制定应急处置联络手册，明确详细的联络方式，并及时更新；
c) 制定应急预案及应急演练场景，定期进行应急演练、开展应急培训。

10.2 应急处置

a) 期货公司发现商用密码可能导致异常的风险隐患时，要尽快核实，立即采取必要的防范措施。如有重要情况按照有关规定进行预警报告，解除预警后，按相同路径进行报告；
b) 发生商用密码相关网络安全事件后，立即启动相应应急预案，迅速采取应急措施，尽快恢复信息系统正常运行；
c) 按有关规定报告事件情况，并报送密码管理局，直至系统恢复正常运行。报告要素要完备、及时、准确；
d) 事件处置完成后，组织运维人员、外部专家及相关人员进行事件复盘，跟进完成复盘提出的整改措施，并形成事件总结报告，报送相关单位。

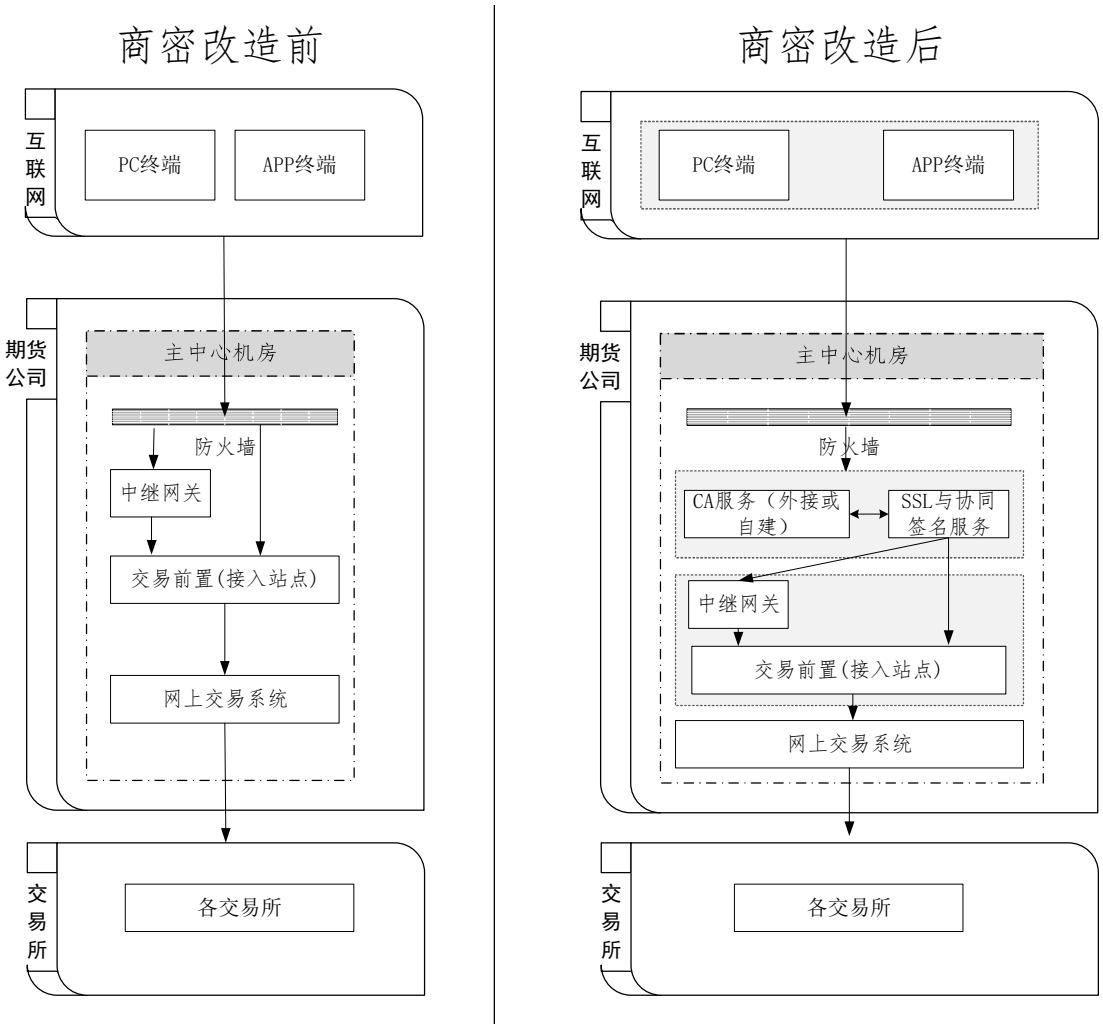
10.3 典型应急场景

本指南收录的应急场景典型案例参见附录C。

附 录 A
（规范性附录）
方案选型参考模式一

A.1 系统架构参考

以行业主流交易系统架构：终端层→接入层→网上交易系统层进行改造，在终端层与接入层之间新增商用密码安全层，改造后整体基础架构为：终端层→商用密码安全层→接入层→网上交易系统层，其系统结构如下:



图一：商用密码应用方案一

以上示意图灰色部分为改造重点，涉及如下环节：

a) 交易终端改造。商用密码应用引入了商用密码安全层，交易终端需要集成数字证书申请、协同签名、SSL 安全通道等服务，实现交易信息的安全传输以及交易用户的

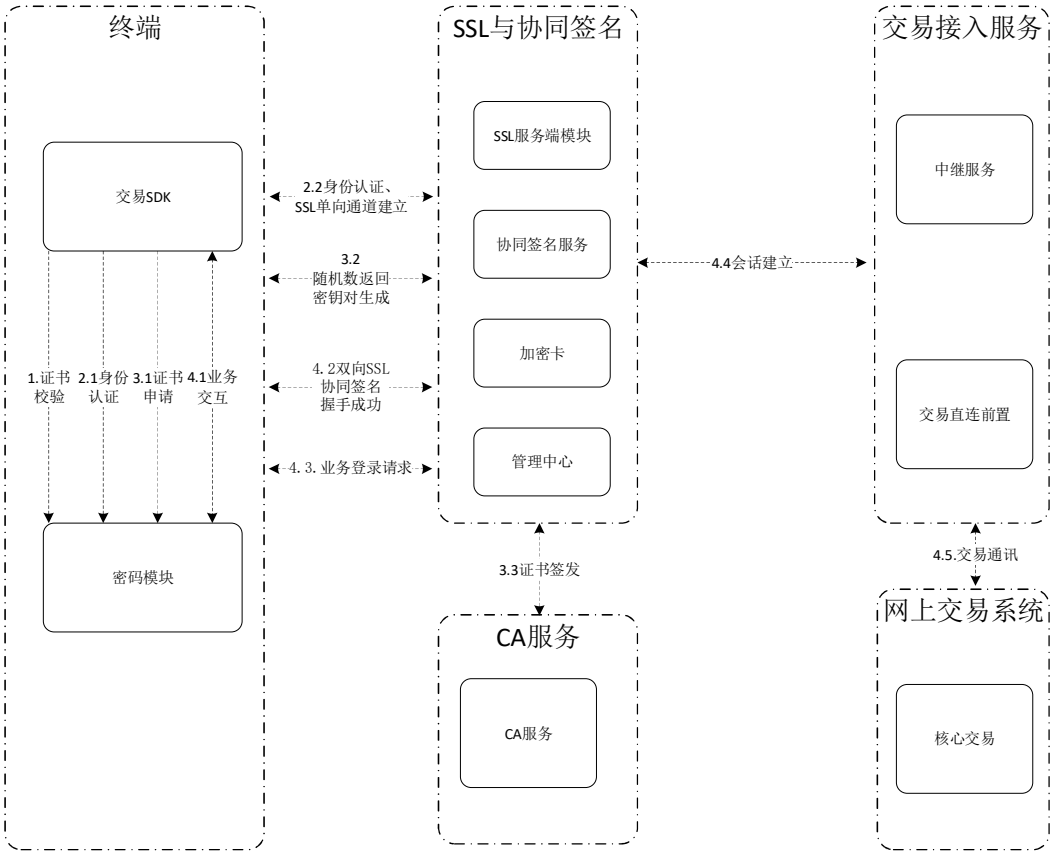
真实性保护；

b) 接入层改造。交易前置（接入站点）变更为商用密码安全层，用户通过交易终端向商用密码安全层发起接入请求。部分接入终端需要使用中继网关，在终端与中继网关通信过程中使用互联网链路通信，期货公司可根据自身系统架构、机房部署情况等综合考虑中继部署方案，图一所示为中继与交易核心在同一机房部署的参考模式；

c) 商用密码应用。使用密码卡或密码机、SSL 接入网关、协同签名系统和 CA 服务（数字证书认证系统）进行改造，主要用途为提供硬件随机数、建立安全通信协议通道、密钥管理、数字证书等服务，实现身份认证以及数据传输机密性、完整性保护。

A.2 对应密码应用方案

本章节描述的是方案一模式认证与安全通道建立过程总览，阐释交易终端通过商用密码安全层接入的工作流程和工作机制：



图二：网上交易系统商用密码方案一应用流程图

a) 终端交易 SDK 服务调用终端内嵌的密码模块进行本地数字证书校验，若本地端无有效数字证书则进行数字证书申请；

b) 交易 SDK 协同密码模块进行身份认证，交易者通过账号密码等有效性方式进行身份确认；

c) 终端密码模块与商用密码安全层建立 SSL 单向加密通道，对用户进行身份信息认证，认证通过则返回至 SSL 与协同签名，SSL 与协同签名发起数字证书签发申请请求；

d) 交易终端 SSL 通信模块与协同签名服务协同生成密钥对，并生成数字证书请求，发送给 CA 服务进行数字证书申请；

e) CA 服务校验有效性后，将给合法的用户签发请求进行数字证书的签发，并返回给 SSL 与协同签名服务。此时 SSL 与协同签名服务得到完整公钥，SSL 与协同签名服务返回公钥信息及数字证书私钥片段给终端密码模块，另一部分私钥片段则存储于协同签名服务端；

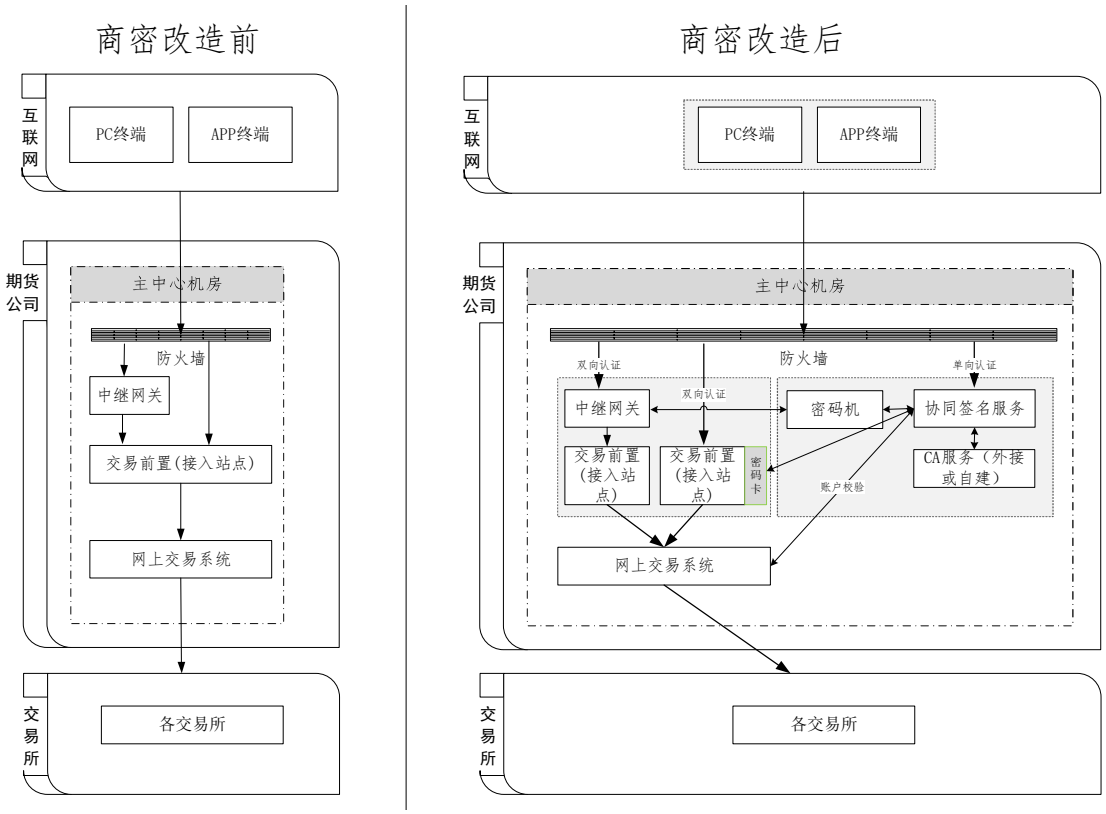
f) 终端密码模块收到相关信息后进行摘要处理并发起双向 SSL 通道建立请求，商用密码安全层收到相关请求并进行数字证书片段与密钥对校验，最终 SSL 双向通道建立；

g) 双向 SSL 通道建立成功，客户可以进行正常登录与交易操作。

附 录 B
（规范性附录）
方案选型参考模式二

B.1 系统架构参考

以行业内主流方案：终端层→接入层→网上交易系统层进行改造，在接入层采用旁路架构，新增密码卡或密码机配合协同签名服务，最终实现符合商密安全的三层结构。其结构示意图如下：



图三：商用密码应用方案二

以上示意图灰色部分为改造重点，涉及如下环节：

a) 终端改造。商用密码应用引入了商用密码安全层，交易终端需要集成协同签名模块，实现数字证书申请、协同签名、加解密、HMAC（散列运算消息认证码）等服务，实现交易终端接入身份真实性、数据传输的机密性和完整性要求；

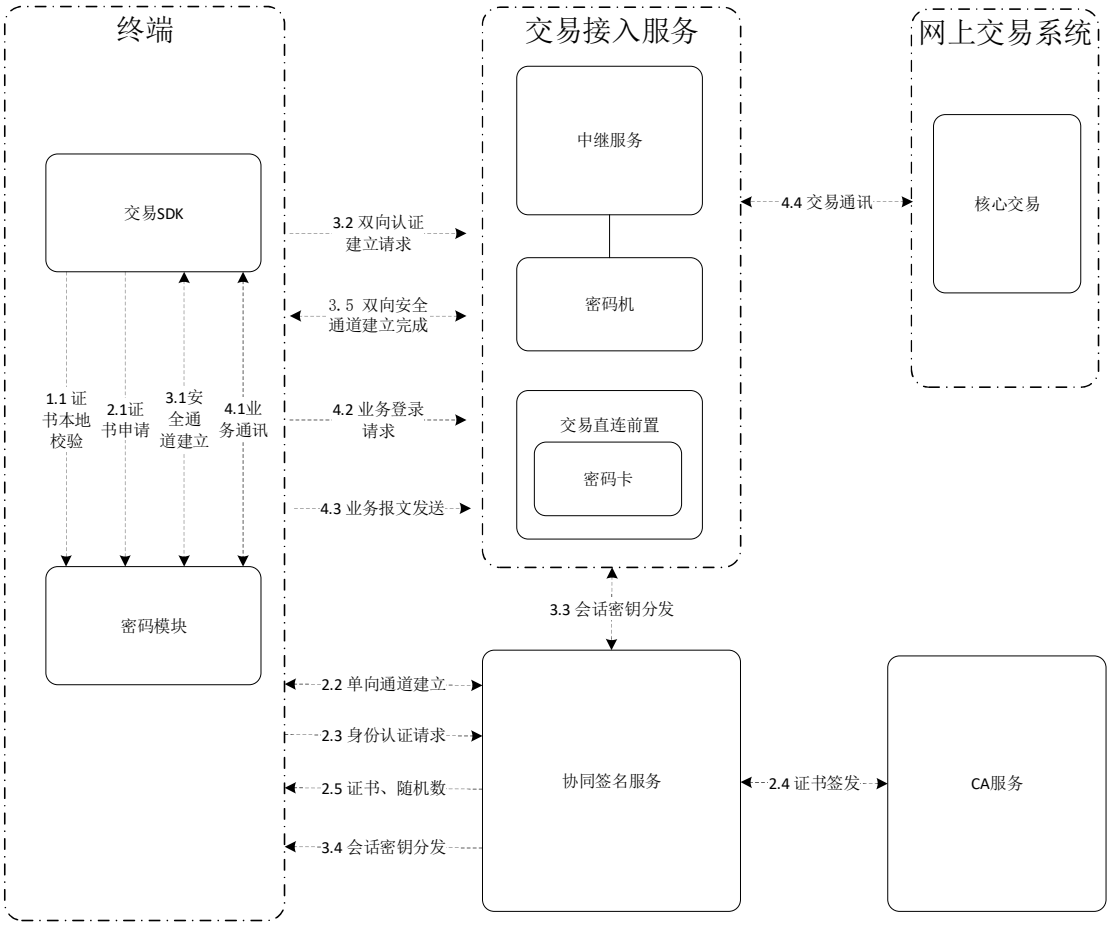
b) 接入层改造。可以在交易前置（接入站点）设备上加装密码卡，同时进行应用改造，实现数据加解密服务；中继网关通过应用改造，与密码机对接，实现数据加解密服

务；

c） 商用密码应用。使用应用接入层平行部署的密码机或密码卡、协同签名服务、CA 服务，主要用途为提供数据加解密、身份鉴别、数字证书等服务，实现身份认证以及数据机密性、完整性保护。

B.2 对应密码应用方案

本章节描述的是方案二模式改造后，其认证与安全通道建立过程总览，阐释交易终端通过商用密码安全层接入的工作流程和工作机制：



图四：网上交易系统商用密码方案二应用流程图

a） 终端交易 SDK 调用协同密码模块进行本地数字证书校验，若本地终端无有效数字证书则需进行数字证书申请；如果存在有效数字证书，则直接跳到（f）；

b） 申请数字证书需要先验证身份，终端 SDK 调用协同密码模块与协同签名服务器进

行单向认证，通过后建立 SSL 单向加密通道；

c） 交易者输入账号口令，通过 SSL 安全信道传输到协同签名服务器进行认证，认证通过则发起数字证书签发申请请求；

d） 终端密码模块和协同签名服务器协同产生密钥对，并产生数字证书申请报文，发给 CA 服务进行数字证书签发；

e） 数字证书签发完成后，协同签名服务返回数字证书至终端；

f） 交易 SDK 调用终端密码模块向交易端发起双向认证请求，双向认证通过后，协同签名服务器产生会话密钥，并分别分发给终端与交易前置完成密钥协商；

g） 双向认证安全信道建立成功；

h） 客户在双向认证安全信道内进行业务数据传输。

以上介绍的改造参考方案仅针对现有期货核心交易系统主机房部分，对于可能存在的异地前置、云站点、异地中继网关等情况，各期货公司可根据自身结构进行拓展。

附 录 C
（规范性附录）
应急场景典型示例

C.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：交易终端无法与SSL接入网关建立连接，交易终端的业务请求无法通过SSL接入网关转发至网上交易系统，导致业务功能无法完成。

处理建议：接入网关采用高可用集群模式部署，当部分接入网关设备无法正常提供服务，交易终端自动切换到其他接入网关；若所有接入网关故障，可采用将网络映射到后置的网上交易系统前置（网上交易系统原接入端）的方式，采用交易终端直接对接网上交易系统的办法，绕过SSL接入网关，让交易终端直连网上交易系统应用服务器，保证交易的连续性。

C.2 密码卡（密码机）故障

故障描述：密码卡（密码机）故障，可能导致相关接入前置无法正常工作。

处理建议：关闭使用这个密码卡（密码机）的接入前置，让流量切换到正常密码卡（密码机）的接入前置。同时做好记录，通知厂商更换密码卡（密码机）。若所有密码卡（密码机）损坏，可以采用旁路机制，保障业务持续运行。

C.3 数字证书认证系统（CA服务）故障

故障描述：CA服务无法正常提供服务，可能造成的影响有：交易终端无法申请签名数字证书和加密数字证书。

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。如有同时对接不同的CA服务机构，可切换CA服务接入。在主备CA服务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。

C.4 协同签名系统故障

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：服务端产生的协同签名密钥分量无法存储到协同签名系统，导致SSL接入网关不能提供协同签名密钥生成服务；未申请密钥的交易终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。已申请密钥的交易终端，由于无法从协同签名系统中获取用户服务端密钥分量，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：协同签名系统支持主备或多活部署模式，在主节点或单节点异常的情况下，支持服务切换到备份节点，继续提供服务。在主备或多活协同签名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。

参考文献

[1] 《中华人民共和国密码法》2019 年 10 月 26 日十三届全国人大常委会第十四次会议审议通过，自 2020 年 1 月 1 日起施行。

[2] 《信息安全技术 SM3 密码杂凑算法》2016 年 8 月 29 日由中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会发布，自 2017 年 3 月 1 日起施行。

[3] 《信息安全技术 SM4 分组密码算法》2016 年 8 月 29 日由中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会发布，自 2017 年 3 月 1 日起施行。

[4] 《信息安全技术 SM2 椭圆曲线公钥密码算法》2016 年 8 月 29 日由中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会发布，自 2017 年 3 月 1 日起施行。

[5] 《信息安全技术 SM2 密码算法使用规范》2017 年 12 月 29 日由中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会发布，自 2018 年 7 月 1 日开始施行。

[6] 《信息安全技术 密码模块安全要求》2018 年 12 月 28 日由国家市场监督管理总局、中国国家标准化管理委员会发布，自 2019 年 7 月 1 日起施行。

[7] 《信息安全技术 网络安全等级保护基本要求》2019 年 5 月 10 日由国家市场监督管理总局、中国国家标准化管理委员会发布，自 2019 年 12 月 1 日起施行。

[8] 《信息安全技术 传输层密码协议（TLCP）》2020 年 4 月 28 日由国家市场监督管理总局、中国国家标准化管理委员会发布，自 2020 年 11 月 1 日起施行。

[9] 《证券期货业软件测试指南 软件安全测试》2020 年 7 月 10 日由中国证券监督管理委员会发布，自 2020 年 7 月 10 日起施行。