



中华人民共和国金融行业标准

JR/T XXXXX—XXXX

证券期货业信息系统商用密码应用 测评要求

Testing and evaluation requirements for information system cryptography
application in the securities and futures industry

(征求意见稿)

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中国证券监督管理委员会 发布

目次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 通则 2

5 测评实施原则 3

6 通用测评要求 4

 6.1 密码算法 4

 6.2 密码技术 4

 6.3 密码产品 4

 6.4 密码服务 5

 6.5 密钥管理 5

7 技术测评要求 5

 7.1 物理和环境安全 5

 7.2 网络和通信安全 9

 7.3 设备和计算安全 14

 7.4 应用和数据安全 18

8 管理测评要求 24

 8.1 管理制度 24

 8.2 人员管理 26

 8.3 建设运行 29

 8.4 应急处置 31

9 特殊测评要求 33

 9.1 适用范围 33

 9.2 系统可用性 33

 9.3 系统压力 34

10 整体测评要求 39

 10.1 概述 39

 10.2 单元间测评 39

 10.3 层面间测评 39

 10.4 特殊测评要求 39

11 风险分析和评价 39

12 测评结论 40

附录 A（资料性） 密钥生存周期管理检查要点 41

附录 B（资料性） 典型商用密码应用场景案例 45

附录 C（资料性） 风险评价 47

参考文献 49

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。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC 180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：大商所飞泰测试技术有限公司、上海证券交易所、深圳证券交易所、大连商品交易所、上海期货交易所、中国证券登记结算有限责任公司、银河证券股份有限公司、国泰海通证券股份有限公司、海通期货股份有限公司、中信建投证券股份有限公司、中泰期货股份有限公司、深圳华锐分布式技术股份有限公司、杭州中焯信息技术股份有限公司、航天中认软件测评科技（北京）有限责任公司、北京海泰方圆科技股份有限公司、北京信安世纪科技有限公司、中国信息通信研究院。

本文件主要起草人：庞彦广、隋文东、李婷婷、杨慈航、韩大伟、谭浩通、张新帅、张勇、何飞、梅养真、方优、何铁军、张锋、康明涛、宿旭升、柳刚强、宋俊宇、王学进、李莹威、徐秀。

证券期货业信息系统商用密码应用测评要求

1 范围

本文件规定了证券期货业信息系统第一级到第四级密码应用的通用测评要求、技术测评要求、管理测评要求、特殊测评要求，并给出了整体测评要求、风险分析和评价、测评结论等测评环节的要求。

注：本文件描述的信息系统密码应用等级与 GB/T 39786—2021 规定的密码应用等级一致，其中第五级密码应用的测评要求不在本文件中描述。

本文件适用于指导、规范证券期货业信息系统密码应用安全性评估工作中的测评活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 37092—2018 信息安全技术 密码模块安全要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GB/T 43206—2023 信息安全技术 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/Z 4001 密码术语

JR/T 0347—2026 证券期货业信息系统密码技术应用指引

3 术语和定义

GB/T 25069—2022、GB/T 39786—2021、GB/T 43206—2023、GM/T 0116—2021和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

密码应用安全性评估人员 commercial cryptography application security evaluation staff

通过国家密码管理部门认可的考核或具有密码技术应用员、密码工程技术人员职业技能等级证书，从事密码应用安全性评估的人员。

简称“密评人员”。

[来源：GB/T 43206—2023，3.1]

3.2

核查 examine

密评人员对测评对象进行访谈、文档审查、实地查验和分析，以帮助密评人员理解、澄清或取得证据的过程。

[来源：GB/T 43206—2023，3.2]

3.3

测评单元 unit of testing and evaluation

一组相对独立和完整的测评内容，由测评指标、测评对象、测评实施和结果判定组成。

[来源：GB/T 43206—2023，3.3]

3.4

测评指标 index of testing and evaluation

测评单元中第一级到第四级密码应用测评的具体要求。

[来源：GB/T 43206—2023, 3.4]

3.5

测评对象 target of testing and evaluation

测评单元中密码应用的测评实施对象。

注：主要包括物理安防设施、通信信道、密码产品、通用设备、应用、重要数据、人员、制度文档等。测评对象基于密码应用方案和信息系统保护目标的实际安全需求确定，具体确定方法参考 GM/T 0116—2021。

[来源：GB/T 43206—2023, 3.5]

3.6

证券期货业信息系统 information system cryptography application in the securities and futures industry

指用于证券期货行业交易（交易所、经营机构）、结算与清算、风险监控与合规管理、资产管理与投资、开户、监管与报告、行情与信息披露等业务活动的信息系统。

3.7

业务连续性 business continuity

在业务运行过程中，需确保数据传输不中断且系统能正常处理数据。

3.8

证券期货业机构 securities and futures industry entity

包括中国证券监督管理委员会、证券交易所、期货交易所、证券登记结算公司、中国期货市场监控中心、中国证券金融股份有限公司、证券公司、期货公司、基金公司、基金估值与服务机构、基金业协会、证券业协会、期货业协会等行业核心机构与经营机构。

4 通则

本文件对证券期货业信息系统各密码应用等级的测评指标以“应”“宜”“可”方式进行描述，密评人员在开展实际测评时，按照如下方法确定是否纳入测评和结果判定范围。

- a) 对于“应”的条款，密评人员应按照第7章和第8章中相应的测评指标要求进行测评和结果判定。
如根据信息系统的密码应用方案和方案评估意见，密评人员应判定信息系统确实不存在与测评指标相关的密码应用需求，则相应测评指标为“不适用”；否则，相关条款纳入测评和结果判定范围。
- b) 对于“宜”的条款，密评人员应确认信息系统是否具有已通过评估的密码应用方案。
 - 1) 如信息系统没有通过评估的密码应用方案，或方案评估意见中未对“不适用”项作出明确说明，则“宜”的条款纳入测评和结果判定范围。
 - 2) 如信息系统有已通过评估的密码应用方案，且方案评估意见中对“宜”条款作出了明确说明，则密评人员应根据信息系统的密码应用方案和方案评估意见决定是否纳入测评和结果判定范围。
 - 如纳入测评和结果判定范围，则密评人员应按照第7章和第8章相应的测评指标要求进行测评和结果判定。
 - 如未纳入测评和结果判定范围，且判定信息系统确实不存在与测评指标相关的密码应用需求时，则相应测评指标为“不适用”。
 - 如未纳入测评和结果判定范围，但信息系统有与测评指标相关的密码应用需求，密评人员应根据信息系统的密码应用方案和方案评估意见，在测评中进一步核实该信息系统是

否满足密码应用方案描述的风险控制措施使用条件，且信息系统的实施情况与所描述的风险控制措施是否一致，并在密码应用安全性评估报告中体现核实过程和结果。如满足使用条件且风险控制措施一致，该测评指标为“不适用”；如不满足使用条件或风险控制措施不一致，密评人员应按照第7章和第8章中相应的测评指标要求进行测评和结果判定。

c) 对于“可”的条款，由信息系统责任方自行决定是否纳入测评和结果判定范围。

- 1) 如信息系统责任方确认纳入测评和结果判定范围，且密评人员经核实后判定信息系统不存在与测评指标相关的密码应用需求，则密评人员应在密码应用安全性评估报告中体现核实过程和结果，相应测评指标为“不适用”。
- 2) 如信息系统责任方确认纳入测评和结果判定范围，且密评人员经核实后判定信息系统存在与测评指标相关的密码应用需求，则密评人员应按照第7章和第8章中相应的测评指标要求进行测评和结果判定。

如证券期货业信息系统通过评估的密码应用方案要求高于其自身对应等级的测评指标要求，则密评人员应按照密码应用方案要求进行测评。例如，密码应用方案要求第三级的信息系统部分指标按照第四级进行规划、建设、运行，则对应指标按照密码应用等级第四级进行测评，并在密码应用安全性评估报告中记录。

信息系统的测评范围原则上应与信息系统网络安全等级保护定级范围及通过评估的密码应用方案中明确的系统范围保持一致，以确保测评对象覆盖该系统内所有需使用密码技术进行保护的信息系统组件，避免因范围不一致导致评估缺项。

5 测评实施原则

对信息系统开展商用密码应用安全性评估测评实施时，应遵循以下原则。在某些情况下，受限于具体场景的安全需求和各项条件，本文件给出的指导内容可能存在不适用情况，此时也应结合如下原则和信息系统的实际情况实施测评工作。

- a) 准确性原则：测评实施时，应结合 GB/T 43206 中的测评指标及相关内容开展工作，确保测评实施内容、取证结果和指标考查内容的一致性。
- b) 完备性原则：测评实施时，应考虑在不同检查点上获取证据并相互验证，以确保取证结果是完备的。例如，应用服务器调用密码机实现重要数据传输完整性保护场景中，在传输过程中对数据报文进行抓包分析的同时，还需采用诸如在调用密码机过程中对数据报文进行抓包分析或登录密码机查看日志记录等方式，以确认密码机调用情况和密码功能使用情况是否符合预期。
- c) 可靠性原则：测评实施时，应结合不同类型的测评方式获取证据并相互验证，以确保取证结果是可靠的。同时，鼓励采用通过更高可靠程度的方式获取到的证据作为结果判定的依据。例如，对采用基于 SM2 证书的数字签名实现真实性场景进行测评时，在查阅相关技术文档后，需进一步采用抓包分析等测评方式进行核查；核查时不仅要验证相关 SM2 数字证书及其证书链，还要关注 SM2 数字签名机制实现是否合规、正确和有效。
- d) 差异性原则：针对不同的密码实现方式，应在测评实施关注点上有所差异。
 - 1) 若密码技术由合规密码产品实现，检查重点在于密码产品是否被安全、正确地使用。例如，所处环境的风险控制措施是否与密码产品安全防护能力相匹配、是否按照相应安全等级要求被使用、是否配置为合规密码技术等。
 - 2) 若密码技术由非合规产品实现，检查重点在于密码实现（如开源密码库）是否是当前未发现明显安全问题的版本，以及密码技术实现和使用正确性、密钥管理措施安全性等方面。

6 通用测评要求

6.1 密码算法

6.1.1 测评指标

证券期货业信息系统中使用的密码算法符合法律、法规的规定、密码相关国家标准和行业标准以及证券期货业相关技术规范（适用于第一级到第四级）。

6.1.2 测评对象

证券期货业信息系统中使用的密码算法。

6.1.3 测评实施

了解证券期货业信息系统中使用的密码算法的名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查信息系统中使用的密码算法是否符合法律法规的规定、密码相关国家标准和行业标准以及证券期货业相关技术规范，或取得国家密码管理部门同意使用的证明文件。

6.2 密码技术

6.2.1 测评指标

证券期货业信息系统中使用的密码技术应遵循密码相关国家标准、行业标准以及证券期货业相关技术规范（适用于第一级到第四级）。

6.2.2 测评对象

证券期货业信息系统中使用的密码技术。

6.2.3 测评实施

了解证券期货业信息系统中使用的密码技术的名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查信息系统中使用的密码技术是否符合法律法规的规定、密码相关国家标准和行业标准以及证券期货业相关技术规范，或取得国家密码管理部门同意使用的证明文件。

6.3 密码产品

6.3.1 测评指标

证券期货业信息系统中使用的密码产品符合法律法规、密码相关国家标准和行业标准、证券期货业相关规范（适用于第一级到第四级）。

证券期货业信息系统中使用的密码产品如遵循密码模块相关标准，则应：

- 达到密码模块安全等级一级及以上安全要求（适用于第二级）；
- 达到密码模块安全等级二级及以上安全要求（适用于第三级）；
- 达到密码模块安全等级三级及以上安全要求（适用于第四级）。

6.3.2 测评对象

JR/T 0347—2026标准中推荐的产品，以及证券期货业信息系统中使用的其他密码产品。

6.3.3 测评实施

了解证券期货业信息系统中使用的密码产品的型号和版本等配置信息，核查密码产品是否经商用密码认证机构认证合格、是否符合证券期货业准入要求，并核查密码产品的使用是否满足其安全运行的条件，例如其安全策略或使用手册说明的部署条件。遵循了密码模块相关标准的密码产品，还要核查其是否满足密码模块相应安全等级及以上安全要求。此外，还应关注密码产品的性能、可用性是否满足证券期货交易等实时性要求较高的业务场景。

6.4 密码服务

6.4.1 测评指标

证券期货业信息系统中使用的密码服务符合法律法规以及证券期货业相关规范（适用于第一级到第四级）

6.4.2 测评对象

证券期货业信息系统中使用的密码服务。

6.4.3 测评实施

核查证券期货业信息系统中使用的密码服务是否符合法律法规、密码相关标准以及证券期货业相关规范。同时关注密码服务的性能、可用性是否满足证券期货交易等实时性要求较高的业务场景。

6.5 密钥管理

6.5.1 测评指标

本单元测评指标如下：

证券期货业信息系统密钥管理使用的密码产品、密码服务符合法律法规、密码相关国家标准和行业标准以及证券期货业相关规范（适用于第一级到第四级）；

证券期货业信息系统密钥管理应符合密码相关国家标准、行业标准以及证券期货业密钥管理规范（适用于第一级到第四级）。

6.5.2 测评对象

证券期货业信息系统密钥管理使用的密码产品、密码服务以及密钥管理实现。

6.5.3 测评实施

本单元测评实施如下：

- a) 核查密钥管理使用的密码产品、密码服务是否满足 6.3 和 6.4 的要求；
- b) 核查证券期货业信息系统密钥管理实现是否安全、正确、有效。例如：非公开密钥是否能被非授权访问、使用、泄露、修改和替换，公开密钥是否能被非授权修改和替换。对于涉及敏感交易数据加密的密钥，还应核查其产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节是否符合行业特殊规定。详细测评实施要点可见附录 A。

7 技术测评要求

7.1 物理和环境安全

7.1.1 身份鉴别

7.1.1.1 测评指标

本单元测评指标如下：

- 可采用密码技术进行物理访问身份鉴别，保证证券期货业信息系统机房等重要区域进入人员身份的真实性（适用于第一级）；
- 宜采用密码技术进行物理访问身份鉴别，保证证券期货业信息系统机房等重要区域进入人员身份的真实性（适用于第二级到第三级）；
- 应采用密码技术进行物理访问身份鉴别，保证证券期货业信息系统机房等重要区域进入人员身份的真实性（适用于第四级）。

7.1.1.2 测评对象

证券期货业信息系统主机房、灾备机房、多区域部署所涉及的机房等重要区域及其电子门禁系统（包括自建机房、第三方物理机房及其中有独立门禁的机笼、第三方云平台机房等）。

7.1.1.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；
- c) 核查所有测评对象电子门禁系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对重要区域进入人员进行身份鉴别，并验证进入人员身份真实性实现机制是否正确和有效。

7.1.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果7.1.1.3测评结果均为是，则该测评对象符合本单元的测评指标要求；如果7.1.1.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

针对被测信息系统部署在被测系统单位管辖范围之外的情形：若被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等开展了商用密码应用安全性评估且相应系统评估结果为“符合”或“基本符合”，云平台级别不低于行业信息系统的网络安全保护等级，密评报告为一年内出具的，在复核报告内容与实际情况相符后，可以复用商用密码应用安全性评估报告中“物理和环境安全”层面的相关测评结论。不可复用相关测评结论的情况包括：

- 被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等未开展商用密码应用安全性评估。
- 被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等开展了商用密码应用安全性评估，评估结论为“不符合”。
- 被测信息系统所在云平台级别低于行业信息系统的网络安全保护等级。
- 被测信息系统所在的IDC机房、运营商机房或云服务提供商机房虽开展了商用密码应用安全性评估且相应系统评估结果为“符合”或“基本符合”，但密评报告不是一年内出具的。

针对上述不可复用的情况，密评人员需现场取证；对于条件不允许的情况，可以通过系统建设方或租赁方要求IDC机房、运营商机房或云服务提供商机房等运维方提供相关说明文件和证据以支撑测评结论（如：报告、说明、证明等）。

7.1.2 电子门禁记录数据存储完整性

7.1.2.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证电子门禁系统进出记录数据的存储完整性（适用于第一级到第二级）；
- 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性（适用于第三级）；
- 应采用密码技术保证电子门禁系统进出记录数据的存储完整性（适用于第四级）。

7.1.2.2 测评对象

证券期货业信息系统主机房、灾备机房、多区域部署所涉及的机房等重要区域及其电子门禁系统（包括自建机房、第三方物理机房及其中有独立门禁的机笼、第三方云平台机房等）。

7.1.2.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；
- c) 核查所有测评对象是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对电子门禁系统进出记录数据进行存储完整性保护，并验证完整性保护机制是否正确和有效。

7.1.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果7.1.2.3测评结果均为是，则该测评对象符合本单元的测评指标要求；如果7.1.2.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

针对被测信息系统部署在被测系统单位管辖范围之外的情形：若被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等开展了商用密码应用安全性评估且相应系统评估结果为“符合”或“基本符合”，云平台级别不低于行业信息系统的网络安全保护等级，密评报告为一年内出具的，在复核报告内容与实际情况相符后，可以复用商用密码应用安全性评估报告中“物理和环境安全”层面的相关测评结论。不可复用相关测评结论的情况包括：

- 被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等未开展商用密码应用安全性评估。
- 被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等开展了商用密码应用安全性评估，评估结论为“不符合”。
- 被测信息系统所在云平台级别低于行业信息系统的网络安全保护等级。

——被测信息系统所在的IDC机房、运营商机房或云服务提供商机房虽开展了商用密码应用安全性评估且相应系统评估结果为“符合”或“基本符合”，但密评报告不是一年内出具的。

针对上述不可复用的情况，密评人员需现场取证；对于条件不允许的情况，可以通过系统建设方或租赁方要求IDC机房、运营商机房或云服务提供商机房等运维方提供相关说明文件和证据以支撑测评结论（如：报告、说明、证明等）。

7.1.3 视频监控记录数据存储完整性

7.1.3.1 测评指标

本单元测评指标如下：

- 宜采用密码技术保证视频监控音像记录数据的存储完整性（适用于第三级）；
- 应采用密码技术保证视频监控音像记录数据的存储完整性（适用于第四级）。

7.1.3.2 测评对象

证券期货业信息系统主机房、灾备机房、多区域部署所涉及的机房等重要区域及其视频监控系统（包括自建机房、第三方物理机房及其中有独立门禁的机笼、第三方云平台机房等）。

7.1.3.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；
- c) 核查所有测评对象是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对视频监控音像记录数据进行存储完整性保护，并验证完整性保护机制是否正确和有效。

7.1.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果7.1.3.3测评结果均为是，则该测评对象符合本单元的测评指标要求；如果7.1.3.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

针对被测信息系统部署在被测系统单位管辖范围之外的情形：若被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等开展了商用密码应用安全性评估且相应系统评估结果为“符合”或“基本符合”，云平台级别不低于行业信息系统的网络安全保护等级，密评报告为一年内出具的，在复核报告内容与实际情况相符后，可以复用商用密码应用安全性评估报告中“物理和环境安全”层面的相关测评结论。不可复用相关测评结论的情况包括：

- 被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等未开展商用密码应用安全性评估。
- 被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等开展了商用密码应用安全性评估，评估结论为“不符合”。
- 被测信息系统所在云平台级别低于行业信息系统的网络安全保护等级。

——被测信息系统所在的IDC机房、运营商机房或云服务提供商机房虽开展了商用密码应用安全性评估且相应系统评估结果为“符合”或“基本符合”，但密评报告不是一年内出具的。

针对上述不可复用的情况，密评人员需现场取证；对于条件不允许的情况，可以通过系统建设方或租赁方要求IDC机房、运营商机房或云服务提供商机房等运维方提供相关说明文件和证据以支撑测评结论（如：报告、说明、证明等）。

7.2 网络和通信安全

7.2.1 身份鉴别

7.2.1.1 测评指标

本单元测评指标如下：

- 可采用密码技术对通信实体进行身份鉴别，保证跨网络类型访问且涉及交易数据、个人敏感信息传输的证券期货业信息系统服务端通信实体身份的真实性（适用于第一级）；
- 宜采用密码技术对通信实体进行身份鉴别，保证跨网络类型访问且涉及交易数据、个人敏感信息传输的证券期货业信息系统服务端通信实体身份的真实性（适用于第二级）；
- 应采用密码技术对通信实体进行身份鉴别，保证跨网络类型访问且涉及交易数据、个人敏感信息传输的证券期货业信息系统服务端通信实体身份的真实性（适用于第三级）；
- 应采用密码技术对通信实体进行双向身份鉴别，保证涉及交易数据、个人敏感信息传输的证券期货业信息系统客户端与服务端通信实体身份的真实性（适用于第四级）。

7.2.1.2 测评对象

证券期货业信息系统与网络边界外通信实体建立的网络通信信道，包括交易所交易系统、经营机构交易系统、结算系统、业务办理系统、行业监管系统、风险监控系统等与网络边界外建立的通信信道，以及提供通信保护功能的设备或组件、密码产品等。

应根据实际网络部署与数据敏感程度，综合考量测评对象的选取范围。如信息系统中RA服务器与CA服务之间的网络通道、跨机构协作场景下（如银证转账、银期转账）系统之间建立的网络通道，一般应作为测评对象；采用socket协议的跨网络通信信道，一般应作为测评对象；对于因业务需求行业系统访问非中国大陆地区相关系统的情况，遵循外部机构接入规范所建立的网络通信信道，一般应作为测评对象；异地机房间通道需判断是否涉及中间的不可控和公共交换设备，在明确不涉及相关情况下可不作为测评对象，否则需进行测评；对于经营机构部署交易接入服务器于交易所托管机房，托管机房与交易所交易系统处于同一物理安全域（即同一建筑/园区内，且由同一组织机构实施统一的物理访问控制），且通信链路为不经过第三方公共交换设备的直连光纤，可不作为测评对象。

7.2.1.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；当被测对象涉及客户端部署于无管理、控制权限的计算环境时，客户端使用的密码模块安全等级要求可根据所部署计算环境须达到等级调整。如交易所交易网关部署于经营机构服务器时，其使用的密码模块安全等级要求遵循经营机构对接系统等级要求；
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对通信实体进行身份鉴别（适用于第一级到第三级）/双向身份鉴别（适用于

第四级），并验证通信实体身份真实性实现机制是否正确和有效；用户首次使用客户端时，如需从服务端获取绑定证书，应核查是否对用户进行口令及账户留存手机号短信验证等多因素方式认证。

7.2.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果7.2.1.3测评结果均为是，则该测评对象符合本单元的测评指标要求；如果7.2.1.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.2.2 通信数据完整性

7.2.2.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息的网络通道在通信过程中数据的完整性(适用于第一级到第二级)；
- 宜采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息的网络通道在通信过程中数据的完整(适用于第三级)；
- 应采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息的网络通道在通信过程中数据的完整(适用于第四级)；

7.2.2.2 测评对象

证券期货业信息系统与网络边界外通信实体建立的网络通信信道，包括交易所交易系统、经营机构交易系统、结算系统、业务办理系统、行业监管系统、风险监控系統、行情系统等与网络边界外建立的通信信道，以及提供通信保护功能的设备或组件、密码产品等。

应根据实际网络部署与数据敏感程度，综合考量测评对象的选取范围。如信息系统中RA服务器与CA服务之间的网络通道、跨机构协作场景下（如银证转账、银期转账）系统之间建立的网络通道，一般应作为测评对象；采用socket协议的跨网络通信信道，一般应作为测评对象；对于因业务需求行业机构访问非中国大陆地区交易所服务，遵循外部机构接入规范所建立的网络通信信道，一般应作为测评对象；异地机房间通道需判断是否涉及中间的不可控和公共交换设备，在明确不涉及相关情况下可不作为测评对象，否则需进行测评；对于经营机构部署交易接入服务器于交易所托管机房，托管机房与交易所交易系统处于同一物理安全域（即同一建筑/园区内，且由同一组织机构实施统一的物理访问控制），且通信链路为不经过第三方公共交换设备的直连光纤，可不作为测评对象。

7.2.2.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；当网络边界外通信实体部署于无管理、控制权限的计算环境时，客户端使用的密码模块安全等级要求可根据所部署区域计算环境需达到等级调整。如交

交易所交易网关部署于经营机构服务器时，其使用的密码模块安全等级要求遵循经营机构对接系统等级要求；

- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对通信过程中的数据进行完整性保护，并验证通信数据完整性保护机制是否正确和有效。对于交易客户端内嵌 VPN 模块的与服务端跨网络通信的建立网络通道，须核查其所使用的 VPN 密码模块等级是否符合对应等级要求。

7.2.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果7.2.2.3测评结果均为是，则该测评对象符合本单元的测评指标要求；如果7.2.2.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.2.3 通信过程中重要数据的机密性

7.2.3.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息的网络通道在通信过程中重要数据的机密性（适用于第一级）；
- 宜采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息的网络通道在通信过程中重要数据的机密性（适用于第二级）；
- 应采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息的网络通道在通信过程中重要数据的机密性（适用于第三级到第四级）。

7.2.3.2 测评对象

证券期货业信息系统与网络边界外通信实体建立的网络通信信道，包括交易所交易系统、经营机构交易系统、结算系统、业务办理系统、行业监管系统、风险监控系統、行情系统等与网络边界外建立的通信信道，以及提供通信保护功能的设备或组件、密码产品等。

应根据实际网络部署与数据敏感程度，综合考量测评对象的选取范围。如信息系统中RA服务器与CA服务之间的网络通道、跨机构协作场景下（如银证转账、银期转账）系统之间建立的网络通道，一般应作为测评对象；采用socket协议的跨网络通信信道，一般应作为测评对象；对于因业务需求行业机构访问非中国大陆地区交易所服务，遵循外部机构特殊接入规范所建立的网络通信信道，一般应作为测评对象；异地机房通道需判断是否涉及中间的不可控和公共交换设备，在明确不涉及相关情况下可不作为测评对象，否则需进行测评；对于经营机构部署交易接入服务器于交易所托管机房，托管机房与交易所交易系统处于同一物理安全域（即同一建筑/园区内，且由同一组织机构实施统一的物理访问控制），且通信链路为不经过第三方公共交换设备的直连光纤，可不作为测评对象。

7.2.3.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；

- b) 核查是否符合 6.3、6.4 和 6.5 的要求；当被测对象涉及客户端部署于无管理、控制权限的计算环境时，客户端使用的密码模块安全等级要求可根据所部署区域计算环境须达到等级调整。交易所交易网关部署于经营机构服务器时，其使用的密码模块安全等级要求遵循经营机构对接系统等级要求；
- c) 核查是否采用密码技术的加解密功能对通信过程中敏感信息或通信报文进行机密性保护，并验证敏感信息或通信报文机密性保护机制是否正确和有效。对于交易客户端内嵌 VPN 模块的与服务端跨网络通信的建立网络通道，须核查其所使用的 VPN 密码模块等级是否符合对应等级要求。

7.2.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.2.3.3测评结果均为是,则该测评对象符合本单元的测评指标要求；如果7.2.3.3 c)测评结果为否,则不符合本单元的测评指标要求；否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合；如果判定结果均为不符合,则本单元的测评结果为不符合；否则,本单元的测评结果为部分符合。

7.2.4 网络边界访问控制信息的完整性

7.2.4.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息网络通道网络边界访问控制信息的完整性(适用于第一级到第二级)；
- 宜采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息网络通道网络边界访问控制信息的完整性(适用于第三级)；
- 应采用密码技术保证跨网络类型访问且涉及交易数据、个人敏感信息网络通道网络边界访问控制信息的完整性(适用于第四级)。

7.2.4.2 测评对象

证券期货业信息系统与网络边界外通信实体建立的网络通信信道，包括交易所交易系统、经营机构交易系统、结算系统、业务办理系统、行业监管系统、风险监控系統、行情系統等与网络边界外建立的通信信道，以及提供网络边界访问控制功能的设备或组件、密码产品等。

应根据实际网络部署与数据敏感程度，综合考量测评对象的选取范围。如信息系统中RA服务器与CA服务之间的网络通道、跨机构协作场景下（如银证转账、银期转账）系统之间建立的网络通道，一般应作为测评对象；采用socket协议的跨网络通信信道，一般应作为测评对象；对于因业务需求行业机构访问非中国大陆地区交易所服务，遵循外部机构接入规范所建立的网络通信信道，一般应作为测评对象；异地机房间通道需判断是否涉及中间的不可控和公共交换设备，在明确不相关情况下可不作为测评对象，否则需进行测评；对于经营机构部署交易接入服务器于交易所托管机房，托管机房与交易所交易系统处于同一物理安全域（即同一建筑/园区内，且由同一组织机构实施统一的物理访问控制），且通信链路为不经过第三方公共交换设备的直连光纤，可不作为测评对象。

7.2.4.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C)：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；当被测对象涉及客户端部署于无管理、控制权限的计算环境时，客户端使用的密码模块安全等级要求可根据所部署区域计算环境须达到等级调整。如交易所交易网关部署于经营机构服务器时，其使用的密码模块安全等级要求遵循经营机构对接系统等级要求；
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对网络边界访问控制信息进行完整性保护，并验证网络边界访问控制信息完整性保护机制是否正确和有效。

7.2.4.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 7.2.4.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果

7.2.4.3 c) 测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。

本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.2.5 安全接入认证

7.2.5.1 测评指标

本单元测评指标如下：

- 可采用密码技术对从外部连接到证券期货业信息系统内部网络的设备进行接入认证，确保涉及交易数据、个人敏感信息传输的接入设备身份的真实性（适用于第三级）；
- 宜采用密码技术对从外部连接到证券期货业信息系统内部网络的设备进行接入认证，确保涉及交易数据、个人敏感信息传输的接入设备身份的真实性（适用于第四级）。

7.2.5.2 测评对象

证券期货业信息系统内部网络，以及提供设备入网接入认证功能的设备或组件、密码产品等。

7.2.5.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见 GB/T 43206-2023 中附录 B 和附录 C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对从外部连接到内部网络的设备进行接入认证，并验证安全接入认证机制是否正确和有效。

7.2.5.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果 7.2.5.3 测评结果均为是，则该测评对象符合本单元的测评指标要求；如果

7.2.5.3 c) 测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.3 设备和计算安全

7.3.1 身份鉴别

7.3.1.1 测评指标

本单元测评指标如下:

- 可采用密码技术对登录证券期货业信息系统所包含设备的用户进行身份鉴别,保证用户身份的真实性(适用于第一级);
- 宜采用密码技术对登录证券期货业信息系统所包含设备的用户进行身份鉴别,保证用户身份的真实性(适用于第二级);
- 应采用密码技术对登录证券期货业信息系统所包含设备的用户进行身份鉴别,保证用户身份的真实性(适用于第三级到第四级)。

7.3.1.2 测评对象

通用设备(如应用服务器、数据库服务器)、网络及安全设备、密码设备、数据库及其管理系统、堡垒机、各类虚拟设备、宿主机设备,以及对用户提供身份鉴别功能的密码产品等。

注:交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为本指标测评对象。

7.3.1.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023中附录B和附录C):

- a) 核查是否符合 6.1 和 6.2 的要求;
- b) 核查是否符合 6.3、6.4 和 6.5 的要求;
- c) 核查是否采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对设备操作人员等登录设备的用户进行身份鉴别,并验证登录设备的用户身份真实性实现机制是否正确和有效。

7.3.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.3.1.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果7.3.1.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.3.2 远程管理通道安全

7.3.2.1 测评指标

证券期货业信息系统设备进行远程管理时,应采用密码技术建立安全的信息传输通道(第三级到第四级)。

7.3.2.2 测评对象

通用设备（如应用服务器、数据库服务器）、网络及安全设备、密码设备、数据库及其管理系统、堡垒机、各类虚拟设备、宿主机设备，以及对远程管理通道提供安全的信息传输通道的密码产品等。

注：交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为本指标测评对象。

7.3.2.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；
- c) 核查远程管理时是否采用密码技术建立安全的信息传输通道，包括身份鉴别、传输数据机密性和完整性保护，并验证远程管理信道所采用的密码技术实现机制是否正确和有效。

7.3.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果7.3.2.3测评结果均为是，则该测评对象符合本单元的测评指标要求；如果7.3.2.3 c)测评结果否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

7.3.3 系统资源访问控制信息完整性

7.3.3.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证证券期货业信息系统设备的系统资源访问控制信息的完整性（适用于第一级到第二级）；
- 宜采用密码技术保证证券期货业信息系统设备的系统资源访问控制信息的完整性（适用于第三级）；
- 应采用密码技术保证证券期货业信息系统设备的系统资源访问控制信息的完整性（适用于第四级）。

7.3.3.2 测评对象

通用设备（如应用服务器、数据库服务器）、网络及安全设备、密码设备、数据库及其管理系统、堡垒机、各类虚拟设备、宿主机设备，以及对系统资源访问控制信息提供完整性保护功能的密码产品等。

注：交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为本指标测评对象。

7.3.3.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023中附录B和附录C）：

- a) 核查是否符合 6.1 和 6.2 的要求；
- b) 核查是否符合 6.3、6.4 和 6.5 的要求；

- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对设备上系统资源访问控制信息进行完整性保护，并验证系统资源访问控制信息完整性保护机制是否正确和有效。

7.3.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.3.3.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果7.3.3.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

对于具有合格商用密码产品认证证书的整机密码设备,且设备等级符合6.3的要求,本指标为符合。

7.3.4 重要信息资源安全标记完整性

7.3.4.1 测评指标

本单元测评指标如下:

- 宜采用密码技术保证证券期货业信息系统设备中的重要信息资源安全标记的完整性(适用于第三级);
- 应采用密码技术保证证券期货业信息系统设备中的重要信息资源安全标记的完整性(适用于第四级)。

7.3.4.2 测评对象

通用设备(如应用服务器、数据库服务器)、网络及安全设备、密码设备、数据库及其管理系统、堡垒机、各类虚拟设备、宿主机设备,以及对重要信息资源安全标提供完整性保护功能的密码产品等。

注:交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为本指标测评对象。

7.3.4.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见 GB/T 43206-2023 中附录 B 和附录 C):

- a) 核查是否符合 6.1 和 6.2 的要求;
- b) 核查是否符合 6.3、6.4 和 6.5 的要求;
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对设备中的重要信息资源安全标记进行完整性保护,并验证安全标记完整性保护机制是否正确和有效。

7.3.4.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.3.4.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果7.3.4.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

若系统设备中没有重要信息资源安全标记且通过评估的密码应用方案中已做出说明，本指标可判定为不适用。

7.3.5 日志记录完整性

7.3.5.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证证券期货业信息系统设备中日志记录的完整性(适用于第一级到第二级)；
- 宜采用密码技术保证证券期货业信息系统设备中日志记录的完整性(适用于第三级)；
- 应采用密码技术保证证券期货业信息系统设备中日志记录的完整性(适用于第四级)。

7.3.5.2 测评对象

通用设备（如应用服务器、数据库服务器）、网络及安全设备、密码设备、数据库及其管理系统、堡垒机、各类虚拟设备、宿主机设备，以及对日志记录提供完整性保护功能的密码产品等。

注1：交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为本指标测评对象；

注2：仅包含保护设备本身日志记录完整性的设备及组件，应用相关的日志保护如交易信息日志等不涉及。

7.3.5.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C)：

- a) 核查是否符合6.1和6.2的要求；
- b) 核查是否符合6.3、6.4和6.5的要求；
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对设备运行的日志记录进行完整性保护，并验证日志记录完整性保护机制是否正确和有效。

7.3.5.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.3.5.3测评结果均为是,则该测评对象符合本单元的测评指标要求；如果7.3.5.3 c)测评结果为否,则不符合本单元的测评指标要求；否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合；如果判定结果均为不符合,则本单元的测评结果为不符合；否则,本单元的测评结果为部分符合。

对于具有合格商用密码产品认证证书的整机密码设备，且设备等级符合6.3的要求，本指标为符合。

7.3.6 重要可执行程序完整性、重要可执行程序来源真实性

7.3.6.1 测评指标

本单元测评指标如下：

- 宜采用密码技术对证券期货业信息系统设备中重要可执行程序进行完整性保护，并对其来源进行真实性验证(适用于第三级)；
- 应采用密码技术对证券期货业信息系统设备中重要可执行程序进行完整性保护，并对其来源进行真实性验证(适用于第四级)。

注：重要可执行程序指运行在服务器端为应用提供重要服务的程序及其更新程序；

7.3.6.2 测评对象

通用设备（如应用服务器、数据库服务器）、网络及安全设备、密码设备、数据库及其管理系统、堡垒机、各类虚拟设备、宿主机设备，以及对重要可执行程序提供完整性保护和来源真实性功能的密码产品等。

注：交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为本指标测评对象。

7.3.6.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C）：

- a) 核查是否符合6.1和6.2的要求；
- b) 核查是否符合6.3、6.4和6.5的要求；
- c) 核查是否采用基于公钥密码算法的数字签名机制等密码技术及产品或服务对需安装在服务器端、为自身应用提供服务的重要可执行程序进行完整性保护并实现其来源的真实性保护；
- d) 验证重要可执行程序完整性保护机制和其来源真实性实现机制是否正确和有效。

7.3.6.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象，如果7.3.6.3测评结果均为是，则该测评对象符合本单元的测评指标要求；如果7.3.6.3 c)测评结果为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象，单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象，对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

对于具有合格商用密码产品认证证书的整机密码设备，且设备等级符合6.3的要求，本指标为符合。

7.4 应用和数据安全

7.4.1 身份鉴别

7.4.1.1 测评指标

本单元测评指标如下：

- 可采用密码技术对登录用户进行身份鉴别，保证证券期货业信息系统用户身份的真实性（适用于第一级）；
- 宜采用密码技术对登录用户进行身份鉴别，保证证券期货业信息系统用户身份的真实性（适用于第二级）；
- 应采用密码技术对登录用户进行身份鉴别，保证证券期货业信息系统用户身份的真实性（适用于第三级到第四级）。

7.4.1.2 测评对象

业务应用（终端用户登录交易所交易系统、经营机构交易系统、业务办理系统、业务管理系统、监控系统、结算系统等过程），以及提供身份鉴别功能的密码产品等。

7.4.1.3 测评实施

本单元测评实施如下（涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023中附录B和附录C）：

- a) 核查是否符合6.1和6.2的要求;
- b) 核查是否符合6.3、6.4和6.5的要求;
- c) 核查是否采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对应用登录用户进行身份鉴别,并验证应用系统用户身份真实性实现机制是否正确和有效。针对涉及证书签发的信息系统,用户首次使用客户端时,如需从服务端获取绑定证书,应核查是否对用户进行口令及账户留存手机号短信验证等多因素方式认证。

7.4.1.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.4.1.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果7.4.1.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.4.2 访问控制信息完整性

7.4.2.1 测评指标

本单元测评指标如下:

- 可采用密码技术保证证券期货业信息系统的访问控制信息的完整性(适用于第一级到第二级);
- 宜采用密码技术保证证券期货业信息系统的访问控制信息的完整性(适用于第三级);
- 应采用密码技术保证证券期货业信息系统的访问控制信息的完整性(适用于第四级)。

7.4.2.2 测评对象

业务应用(交易所交易单元/席位权限、经营机构系统用户权限、业务系统用户重要操作权限等访问控制信息),以及提供访问控制信息完整性保护功能的密码产品等。

7.4.2.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C):

- a) 核查是否符合6.1和6.2的要求;
- b) 核查是否符合6.3、6.4和6.5的要求;
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对应用的访问控制信息进行完整性保护,并验证应用的访问控制信息完整性保护机制是否正确和有效。

7.4.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.4.2.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果7.4.2.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.4.3 重要信息资源安全标记完整性

7.4.3.1 测评指标

本单元测评指标如下：

- 宜采用密码技术保证证券期货业信息系统的重要信息资源安全标记的完整性(适用于第三级)；
- 应采用密码技术保证证券期货业信息系统的重要信息资源安全标记的完整性(适用于第四级)。

7.4.3.2 测评对象

业务应用中包含的符合相关行业标准和自身安全要求的重要信息资源，以及提供完整性保护功能的密码产品等。

7.4.3.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C)：

- a) 核查是否符合6.1和6.2的要求；
- b) 核查是否符合6.3、6.4和6.5的要求；
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对应用的重要信息资源安全标记进行完整性保护，并验证安全标记完整性保护机制是否正确和有效。

7.4.3.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.4.3.3测评结果均为是,则该测评对象符合本单元的测评指标要求；如果7.4.3.3 c)测评结果为否,则不符合本单元的测评指标要求；否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合；如果判定结果均为不符合,则本单元的测评结果为不符合；否则,本单元的测评结果为部分符合。

若系统应用层无重要信息资源安全标记应用场景且通过测评的密码应用方案中已做出说明,本指标可判定为不适用。

7.4.4 重要数据传输机密性

7.4.4.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证证券期货业信息系统的重要数据在传输过程中的机密性(适用于第一级)；
- 宜采用密码技术保证证券期货业信息系统的重要数据在传输过程中的机密性(适用于第二级)；
- 应采用密码技术保证证券期货业信息系统的重要数据在传输过程中的机密性(适用于第三级到第四级)。

7.4.4.2 测评对象

业务应用跨网络的数据传输所包含的个人敏感信息(银行账户、姓名、联系方式、证件信息、生物特征等)、鉴别数据(口令)、重要审计数据、重要业务数据(交易委托数据、成交数据、含重要数据的监管报送数据等)以及提供重要数据机密性保护功能的密码产品等。

7.4.4.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C)：

- a) 核查是否符合6.1和6.2的要求；
- b) 核查是否符合6.3、6.4和6.5的要求；
- c) 核查是否采用密码技术的加解密功能对重要数据在传输过程中进行机密性保护，并验证传输数据机密性保护机制是否正确和有效。

7.4.4.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.4.4.3测评结果均为是,则该测评对象符合本单元的测评指标要求；如果7.4.4.3 c)测评结果为否,则不符合本单元的测评指标要求；否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合；如果判定结果均为不符合,则本单元的测评结果为不符合；否则,本单元的测评结果为部分符合。

7.4.5 重要数据存储机密性

7.4.5.1 测评指标

本单元测评指标如下：

- 可采用密码技术保证证券期货业信息系统的重要数据在存储过程中的机密性(适用于第一级)；
- 宜采用密码技术保证证券期货业信息系统的重要数据在存储过程中的机密性(适用于第二级)；
- 应采用密码技术保证证券期货业信息系统的重要数据在存储过程中的机密性(适用于第三级到第四级)。

7.4.5.2 测评对象

业务应用存储的个人敏感信息(银行账户、联系方式、证件信息、生物特征等,行情信息中包含的个人信息除外)、鉴别数据(口令)、重要业务数据:盘后结算数据(涉及到投资者数据的市场报表、对账数据)、持久化后的持仓数据,含重要数据的重要审计数据、监管报送数据等,以及提供机密性保护功能的密码产品等。

注:数据存储的对象指在证券期货行业信息系统中以持久化方式保留,存储时间超过一个完整交易日的业务数据或相关信息,不包括在单个交易日内生成、使用并于同一交易日内销毁的临时数据或过程性中间数据。

7.4.5.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见GB/T 43206-2023 中附录B和附录C)：

- a) 核查是否符合6.1和6.2的要求；
- b) 核查是否符合6.3、6.4和6.5的要求；
- c) 核查是否采用密码技术的加解密功能对重要数据在存储过程中进行机密性保护，并验证存储数据机密性保护机制是否正确和有效。

7.4.5.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.4.5.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果7.4.5.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.4.6 重要数据传输完整性

7.4.6.1 测评指标

本单元测评指标如下:

- 可采用密码技术保证证券期货业信息系统的重要数据在传输过程中的完整性(适用于第一级);
- 宜采用密码技术保证证券期货业信息系统的重要数据在传输过程中的完整性(适用于第二级到第三级);
- 应采用密码技术保证证券期货业信息系统的重要数据在传输过程中的完整性(适用于第四级)。

7.4.6.2 测评对象

业务应用跨网络的数据传输所包含的个人敏感信息(银行账户、姓名、联系方式、证件信息、生物特征等)、鉴别数据(口令)、重要审计数据、重要业务数据(交易委托数据、成交数据、含重要数据的监管报送数据等)以及提供重要数据完整性保护功能的密码产品等。

7.4.6.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见 GB/T 43206-2023 中附录 B 和附录 C):

- a) 核查是否符合 6.1 和 6.2 的要求;
- b) 核查是否符合 6.3、6.4 和 6.5 的要求;
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对重要数据在传输过程中进行完整性保护,并验证传输数据完整性保护机制是否正确和有效。

7.4.6.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果7.4.6.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果7.4.6.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.4.7 重要数据存储完整性

7.4.7.1 测评指标

本单元测评指标如下:

- 可采用密码技术保证证券期货业信息系统的重要数据在存储过程中的完整性(适用于第一级);
- 宜采用密码技术保证证券期货业信息系统的重要数据在存储过程中的完整性(适用于第二级到第三级);

——应采用密码技术保证证券期货业信息系统的重要数据在存储过程中的完整性(适用于第四级)。

7.4.7.2 测评对象

业务应用存储的个人敏感信息(银行账户、姓名、联系方式、证件信息、生物特征等,行情信息中包含的个人信息除外)、鉴别数据(口令)、重要审计数据、重要业务数据:投资者行为数据、盘后结算数据(涉及到投资者数据的市场报表、对账数据)、持久化后的持仓数据、含重要数据的监管报送数据等以及提供完整性保护功能的密码产品等。

注:数据存储的对象指在证券期货行业信息系统中以持久化方式保留,存储时间超过一个完整交易日的业务数据或相关信息,不包括在单个交易日内生成、使用并于同一交易日内销毁的临时数据或过程性中间数据。

7.4.7.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见 GB/T 43206-2023 中附录 B 和附录 C):

- a) 核查是否符合 6.1 和 6.2 的要求;
- b) 核查是否符合 6.3、6.4 和 6.5 的要求;
- c) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术及产品或服务对重要数据在存储过程中进行完整性保护,并验证存储数据完整性保护机制是否正确和有效。

7.4.7.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果 7.4.7.3 测评结果均为是,则该测评对象符合本单元的测评指标要求;如果 7.4.7.3 c) 测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

7.4.8 不可否认性

7.4.8.1 测评指标

本单元测评指标如下:

- 在可能涉及法律责任认定的应用中,宜采用密码技术提供证券期货业信息系统数据原发证据和数据接收证据,实现数据原发行为的不可否认性和数据接收行为的不可否认性(适用于第三级);
- 在可能涉及法律责任认定的应用中,应采用密码技术提供证券期货业信息系统数据原发证据和数据接收证据,实现数据原发行为的不可否认性和数据接收行为的不可否认性(适用于第四级)。

7.4.8.2 测评对象

业务应用,以及提供不可否认性功能的密码产品等。

7.4.8.3 测评实施

本单元测评实施如下(涉及的密码功能和密码产品应用的测评技术可分别见 GB/T 43206-2023 中附录 B 和附录 C):

- a) 核查是否符合 6.1 和 6.2 的要求;
- b) 核查是否符合 6.3、6.4 和 6.5 的要求;

c) 核查是否采用基于公钥密码算法的数字签名机制等密码技术及产品或服务对数据原发行为和接收行为等实现不可否认性, 并验证不可否认性实现机制是否正确和有效。

7.4.8.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象, 如果7.4.8.3测评结果均为是, 则该测评对象符合本单元的测评指标要求; 如果7.4.8.3 c)测评结果为否, 则不符合本单元的测评指标要求; 否则, 部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象, 单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象, 对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合, 则本单元的测评结果为符合; 如果判定结果均为不符合, 则本单元的测评结果为不符合; 否则, 本单元的测评结果为部分符合。

若业务应用没有不可否认性需求且通过评审的密码应用方案中已做出说明, 本指标可判定为不适用。

8 管理测评要求

8.1 管理制度

8.1.1 密码应用安全管理制度

8.1.1.1 测评指标

应具备密码应用安全管理制度, 包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度, 且制度内容满足行业监管要求(第一级到第四级)。

8.1.1.2 测评对象

安全管理制度类文档。

8.1.1.3 测评实施

核查各项安全管理制度是否包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度, 且制度内容符合证券期货业相关监管要求。

8.1.1.4 结果判定

如果8.1.1.3测评实施内容均为是, 则本单元的测评结果为符合; 如果8.1.1.3测评实施内容均为否, 则本单元的测评结果为不符合; 否则, 本单元的测评结果为部分符合。

8.1.2 密钥管理规则

8.1.2.1 测评指标

根据密码应用方案建立相应密钥管理规则(第一级到第四级)。

8.1.2.2 测评对象

密码应用方案、密钥管理制度及策略类文档。

8.1.2.3 测评实施

核查是否有通过评估的密码应用方案，并核查是否根据密码应用方案建立相应密钥管理规则（例如，密钥管理制度及策略类文档中的密钥全生存周期的安全性保护相关内容）且对密钥管理规则进行评审，以及核查信息系统中密钥是否按照密钥管理规则进行生存周期的管理。

8.1.2.4 结果判定

如果8.1.2.3测评实施内容均为是，则本单元的测评结果为符合；如果8.1.2.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.1.3 操作规程

8.1.3.1 测评指标

应对管理人员或操作人员执行的日常管理操作建立操作规程，操作规程应结合证券期货业特点，满足行业监管要求（第二级到第四级）。

8.1.3.2 测评对象

操作规程类文档。

8.1.3.3 测评实施

核查是否对密码相关管理人员或操作人员的日常管理操作建立操作规程，且操作规程符合证券期货业相关监管要求。

8.1.3.4 结果判定

如果8.1.3.3测评实施内容均为是，则本单元的测评结果为符合；如果8.1.3.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.1.4 安全管理制度

8.1.4.1 测评指标

应定期对密码应用安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订（第三级到第四级）。

8.1.4.2 测评对象

安全管理制度类文档、操作规程类文档、记录表单类文档。

8.1.4.3 测评实施

核查是否定期对密码应用安全管理制度的合理性和适用性进行论证和审定；对经论证和审定后存在不足或需要改进的密码应用安全管理制度和操作规程，核查是否具有修订记录。

8.1.4.4 结果判定

如果8.1.4.3测评实施内容均为是，则本单元的测评结果为符合；如果8.1.4.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.1.5 管理制度发布流程

8.1.5.1 测评指标

应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制(适用于第三级到第四级)。

8.1.5.2 测评对象

安全管理制度类文档、操作规程类文档、记录表单类文档。

8.1.5.3 测评实施

核查相关密码应用安全管理制度和操作规程是否具有相应明确的发布流程和版本控制。

8.1.5.4 结果判定

如果8.1.5.3测评实施内容均为是,则本单元的测评结果为符合;如果8.1.5.3测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

8.1.6 制度执行过程记录

8.1.6.1 测评指标

应具有密码应用操作规程的相关执行记录并妥善保存(第三级到第四级)。

8.1.6.2 测评对象

安全管理制度类文档、记录表单类文档。

8.1.6.3 测评实施

核查是否具有密码应用操作规程执行过程中留存的相关执行记录文件。

8.1.6.4 结果判定

如果8.1.6.3测评实施内容均为是,则本单元的测评结果为符合;如果8.1.6.3测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

8.2 人员管理

8.2.1 密码相关法律法规和密码管理制度

8.2.1.1 测评指标

相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度以及证券期货业相关监管规定(适用于第一级到第四级)。

8.2.1.2 测评对象

系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

8.2.1.3 测评实施

核查系统相关人员是否了解并遵守密码相关法律法规和密码应用安全管理制度以及证券期货业相关监管规定。

8.2.1.4 结果判定

如果8.2.1.3测评实施内容均为是,则本单元的测评结果为符合;如果8.2.1.3测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

8.2.2 密码应用岗位责任制度

8.2.2.1 测评指标

- a) 建立密码应用岗位责任制度,明确各岗位在安全系统中的职责和权限(第二级)。
- b) 建立密码应用岗位责任制度,明确各岗位在安全系统中的职责和权限(第三级):
 - 1) 根据密码应用的实际情况,设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位;
 - 2) 对关键岗位建立多人共管机制;
 - 3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督,其中密码安全审计员岗位不应与密钥管理员、密码操作员兼任;
 - 4) 相关设备与系统的管理和使用账号不应多人共用。
- c) 应建立密码应用岗位责任制度,明确各岗位在安全系统中的职责和权限(第四级):
 - 1) 根据密码应用的实际情况,设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位;
 - 2) 对关键岗位建立多人共管机制;
 - 3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督,其中密码安全审计员岗位不应与密钥管理员、密码操作员兼任;
 - 4) 相关设备与系统的管理和使用账号不应多人共用;
 - 5) 密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任,并应在任前对其进行背景调查。

8.2.2.2 测评对象

密码应用安全管理制度类文档、系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

8.2.2.3 测评实施

本单元测评实施如下:

- a) 对于第二级的信息系统,核查是否建立了密码应用岗位责任制度,安全管理制度中是否明确了各岗位在安全系统中的职责和权限。
- b) 对于第三级的信息系统,核查安全管理制度类文档是否根据密码应用的实际情况,设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位并定义岗位职责;核查是否对关键岗位建立多人共管机制,并确认密码安全审计员岗位人员是否不兼任密钥管理员、密码操作员等关键安全岗位;核查相关设备与系统的管理和使用账号是否有多人共用情况;离职人员及时删除其账号;在密码应用岗位人员发生岗位调动时,应重新评估和修改其访问权限和职责;在密码应用岗位人员离职时,应及时终止其所有密码应用相关的访问权限、操作权限,收回相应的密码产品,并根据密钥管理策略处理相关密钥数据。
- c) 对于第四级的信息系统,核查安全管理制度类文档是否根据密码应用的实际情况,设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位并定义岗位职责;核查是否对关键岗位建立多人共管机制,并确认密码安全审计员岗位人员是否不兼任密钥管理员、密码操作员等关键安全岗位;核查相关设备与系统的管理和使用账号是否有多人共用情况;离职人员及时删除其账号;核查密钥管理员、密码安全审计员和密码操作员是否由本机构的内部员工担任,是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录等;在密码应用岗位人员发生岗位调动时,应重新评估和修改其访问权限和职责;在密码应用岗位人员离职时,应及时终

止其所有密码应用相关的访问权限、操作权限，收回相应的密码产品，并根据密钥管理策略处理相关密钥数据。

8.2.2.4 结果判定

如果8.2.2.3测评实施内容均为是，则本单元的测评结果为符合；如果8.2.2.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.2.3 上岗人员培训制度

8.2.3.1 测评指标

应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能（第二级到第四级）。

8.2.3.2 测评对象

密码应用安全管理制度类文档和记录表单类文档、系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

8.2.3.3 测评实施

核查安全教育和培训计划文档是否具有针对涉及密码的操作和管理的人员的培训计划；核查安全教育和培训记录是否有密码培训人员、密码培训内容、密码培训结果等的描述。

8.2.3.4 结果判定

如果8.2.3.3测评实施内容均为是，则本单元的测评结果为符合；如果8.2.3.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.2.4 安全岗位考核

8.2.4.1 测评指标

应定期对密码应用安全岗位人员进行考核（第三级到第四级）。

8.2.4.2 测评对象

密码应用安全管理制度类文档和记录表单类文档、系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

8.2.4.3 测评实施

核查安全管理制度文档是否包含具体的人员考核制度和惩戒措施；核查人员考核记录内容是否包括安全意识、密码操作管理技能及相关法律法规；核查记录表单类文档确认是否定期进行岗位人员考核。

8.2.4.4 结果判定

如果8.2.4.3测评实施内容均为是，则本单元的测评结果为符合；如果8.2.4.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.2.5 关键岗位人员保密制度

8.2.5.1 测评指标

本单元测评指标如下：

- 应及时终止离岗人员的所有密码应用相关的访问权限、操作权限(适用于第一级)；
- 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务(适用于第二级到第四级)。

8.2.5.2 测评对象

密码应用安全管理制度类文档和记录表单类文档、系统相关人员(包括系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等)。

8.2.5.3 测评实施

本单元测评实施如下：

- a) 对于第一级的信息系统，核查人员离岗时是否具有及时终止其所有密码应用相关的访问权限、操作权限、身份认证设备的记录；
- b) 对于第二级到第四级的信息系统，核查人员离岗的管理文档是否规定了关键岗位人员保密制度和调离制度等；核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容。

8.2.5.4 结果判定

如果8.2.5.3测评实施内容均为是，则本单元的测评结果为符合；如果8.2.5.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.3 建设运行

8.3.1 密码应用方案

8.3.1.1 测评指标

应根据证券期货业信息系统密码应用需求，依据密码相关标准，并结合证券期货业特性制定密码应用方案(适用于第一级到第四级)。

8.3.1.2 测评对象

密码应用方案。

8.3.1.3 测评实施

核查在信息系统规划阶段，是否依据信息系统密码应用需求和密码相关标准以及证券期货业相关监管要求，制定密码应用方案，并核查方案是否通过评估。

8.3.1.4 结果判定

如果8.3.1.3测评实施内容均为是，则本单元的测评结果为符合；如果8.3.1.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.3.2 密钥安全管理策略

8.3.2.1 测评指标

应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理检查要点参照附录A(适用于第一级到第四级)。

8.3.2.2 测评对象

密码应用方案、密钥管理制度及策略类文档、密钥管理过程记录。

8.3.2.3 测评实施

本单元测评实施如下：

- a) 核查是否有通过评估的密码应用方案；核查密钥管理制度及策略类文档是否确定系统设计的密钥种类、体系及其生存周期环节，是否与密码应用方案一致；如信息系统没有相应的密码应用方案，参照附录A核查密钥管理制度及策略类文档。
- b) 核查相关密钥管理过程记录，核查是否按照密钥管理制度及策略类文档完成密钥管理。

8.3.2.4 结果判定

如果8.3.2.3测评实施内容均为是，则本单元的测评结果为符合；如果8.3.2.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.3.3 实施方案

8.3.3.1 测评指标

应按照应用方案实施建设（第一级到第四级）。

8.3.3.2 测评对象

密码实施方案。

8.3.3.3 测评实施

核查是否有通过评估的密码应用方案，并核查是否按照密码应用方案，制定密码实施方案。

8.3.3.4 结果判定

如果8.3.3.3测评实施内容均为是，则本单元的测评结果为符合；如果8.3.3.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.3.4 投入运行前的密码应用安全性评估

8.3.4.1 测评指标

本单元测评指标如下：

- 投入运行前可进行密码应用安全性评估(适用于第一级)；
- 投入运行前宜进行密码应用安全性评估(适用于第二级)；
- 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行(适用于第三级到第四级)。

8.3.4.2 测评对象

密码应用安全性评估报告。

8.3.4.3 测评实施

本单元测评实施如下：

- a) 对于第一级到第二级的信息系统，核查信息系统投入运行前，是否组织进行密码应用安全性评估；核查是否具有系统投入运行前编制的密码应用安全性评估报告。
- b) 对于第三级到第四级的信息系统，核查信息系统投入运行前，是否组织进行密码应用安全性评估；核查是否具有系统投入运行前编制的密码应用安全性评估报告且系统通过评估。

8.3.4.4 结果判定

如果8.3.4.3测评实施内容均为是，则本单元的测评结果为符合；如果8.3.4.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.3.5 投入运行后的密码应用安全性评估

8.3.5.1 测评指标

在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改(适用于第三级到第四级)。

8.3.5.2 测评对象

密码应用安全管理制度、密码应用安全性评估报告、攻防对抗演习报告、整改文档。

8.3.5.3 测评实施

核查信息系统投入运行后，信息系统责任方是否严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并具有相应的密码应用安全性评估报告及攻防对抗演习报告；核查是否根据评估结果制定整改方案，并进行相应整改。

8.3.5.4 结果判定

如果8.3.5.3测评实施内容均为是，则本单元的测评结果为符合；如果8.3.5.3测评实施内容均为否，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

8.4 应急处置

8.4.1 应急策略

8.4.1.1 测评指标

本单元测评指标如下：

- 可根据密码产品提供的安全策略，由用户自主处置密码应用安全事件(适用于第一级)；
- 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，按照应急处置措施结合实际情况及时处置(适用于第二级)；
- 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置(适用于第三级到第四级)。

8.4.1.2 测评对象

密码应用应急策略、应急处置记录类文档。

8.4.1.3 测评实施

本单元测评实施如下：

- a) 对于第一级的信息系统，核查用户是否根据密码产品提供的安全策略处置密码应用安全事件。

b) 对于第二级的信息系统, 核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审, 应急策略中是否明确了密码应用安全事件发生时的应急处理流程及其他管理措施, 并遵照执行; 如发生过密码应用安全事件, 核查是否具有相应的处置记录。

c) 对于第三级到第四级的信息系统, 核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审, 应急策略中是否明确了密码应用安全事件发生时的应急处理流程及其他管理措施, 并遵照执行; 如发生过密码应用安全事件, 核查是否立即启动应急处置措施并具有相应的处置记录。

8.4.1.4 结果判定

如果8.4.1.3测评实施内容均为是, 则本单元的测评结果为符合; 如果8.4.1.3测评实施内容均为否, 则本单元的测评结果为不符合; 否则, 本单元的测评结果为部分符合。

8.4.2 事件处置

8.4.2.1 测评指标

本单元测评指标如下:

——事件发生后, 应及时向信息系统主管部门进行报告(适用于第三级);

——事件发生后, 应及时向信息系统主管部门及归属的密码管理部门进行报告(适用于第四级)。

8.4.2.2 测评对象

a) 密码应用应急策略类文档、安全事件报告。

8.4.2.3 测评实施

本单元测评实施如下:

a) 对于第三级的信息系统, 核查密码应用安全事件发生后, 是否及时向信息系统主管部门进行报告, 并按照《证券期货业网络安全事件报告与调查处理办法》进行处置。

b) 对于第四级的信息系统, 核查密码应用安全事件发生后, 是否及时向信息系统主管部门及归属的密码管理部门进行报告, 并按照《证券期货业网络安全事件报告与调查处理办法》进行处置。

8.4.2.4 结果判定

如果8.4.2.3测评实施内容均为是, 则本单元的测评结果为符合; 如果8.4.2.3测评实施内容均为否, 则本单元的测评结果为不符合; 否则, 本单元的测评结果为部分符合。

8.4.3 处置情况上报

8.4.3.1 测评指标

事件处置完成后, 应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况(适用于第三级到第四级)。

8.4.3.2 测评对象

密码应用应急策略类文档、安全事件发生情况及处置情况报告。

8.4.3.3 测评实施

核查密码应用安全事件处置完成后,是否及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况,如事件处置完成后,向相关部门提交安全事件发生情况及处置情况报告。

8.4.3.4 结果判定

如果8.4.3.3测评实施内容均为是,则本单元的测评结果为符合;如果8.4.3.3测评实施内容均为否,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

9 特殊测评要求

9.1 适用范围

证券期货业信息系统具有高并发、高可用、低时延等行业属性,为保障商用密码改造后系统运行安全,本标准增设适配行业场景的系统压力与可用性专项测评要求,测评指标涵盖系统吞吐量、交易响应时延、设备故障切换能力等关键内容。对证券交易所交易系统、证券登记结算机构结算系统、证券经营机构交易及结算系统、期货交易所交易及结算系统、期货经营机构交易及结算系统、期货市场监管中心开户系统开展密码应用安全性评估时,评估人员应当查验评估对象提交的系统压力测试、可用性测试报告。

9.2 系统可用性

9.2.1 测评指标

本单元测评指标如下:

证券期货业信息系统密码应用应遵循行业系统对于可用性的要求,保证系统业务的连续性(适用于证券交易所交易系统、证券登记结算公司结算系统、证券经营机构交易系统、证券经营机构结算系统、期货交易所交易系统、期货交易所结算系统、期货经营机构交易系统、期货经营机构结算系统、期货市场监管中心开户系统)。

9.2.2 测评对象

证券期货业信息系统。

9.2.3 测评实施

开展本单元测评工作时,应核查测试报告是否包含下列内容:

- a) 证券期货业信息系统部署情况,密码设备、服务节点、密钥存储及运算单元是否具备主备或多活等冗余机制;
- b) 系统冗余机制是否满足 6.1、6.2、6.3、6.4 和 6.5 的要求;
- c) 发生密码设备硬件或网络故障时密码应用是否具备有效的切换或逃生能力,使系统业务连续性可控。

9.2.4 结果判定

本单元可能涉及多个测评对象。

对于单个测评对象,如果9.1.3测评结果均为是,则该测评对象符合本单元的测评指标要求;如果9.1.3 c)测评结果为否,则不符合本单元的测评指标要求;否则,部分符合本单元的测评指标要求。

本单元如只涉及单个测评对象,单个测评对象的测评结果即为本单元的测评结果。本单元如涉及多个测评对象,对本单元涉及的所有测评对象的判定结果进行汇总。如果判定结果均为符合,则本单元的测评结果为符合;如果判定结果均为不符合,则本单元的测评结果为不符合;否则,本单元的测评结果为部分符合。

9.3 系统压力

9.3.1 证券交易所交易系统峰值压力下的订单发送速率

9.3.1.1 测评指标

在短时间内以多倍生产峰值瞬时压力历史最大值报入订单，系统能够处理的订单请求数量应能达到行业要求。（适用于证券交易所交易系统）

9.3.1.2 测评对象

以负责交易数据接收与反馈的网关或前置组件为起点，交易请求经承载交易风控、订单撮合、成交确认等核心业务的组件处理后，最终流转至负责交易结果反馈的网关或前置组件为终点，该链路中的全部组件集合。

9.3.1.3 测评实施

开展本单元测评工作时，应核查测试报告是否包含以下内容：

1. 集合竞价阶段的有效订单率；2. 连续交易阶段峰值时刻的订单峰值发送速率；3. 连续交易阶段的订单处理时延99%分位值；4. 报入过程中最小响应速率；5. 报入过程中交易单元/网关断连情况；6. 订单丢失率；7. 订单正确率；8. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.1.4 结果判定

以下结果均符合，则本单元的测评结果为符合；否则，本单元的测评结果为不符合：

1. 集合竞价阶段的有效订单率不低于97%；2. 连续交易阶段峰值时刻的订单峰值发送速率可以达到峰值订单速率历史最大值的压力倍数要求；3. 连续交易阶段的订单处理时延99%分位值不超过(T+15)秒；4. 报入过程中最小响应速率大于0；5. 报入过程中无交易单元/网关断连；6. 订单丢失率为0%；7. 订单正确率为100%；8. 与业务处理相关模块的内存峰值占用率均需低于90%，磁盘空间峰值占用率均需低于80%。

9.3.2 证券经营机构交易系统峰值压力下的订单及查询吞吐率

9.3.2.1 测评指标

在短时间内以多倍生产峰值瞬时压力历史最大值报入业务，系统每秒能够处理的业务请求数量应能达到行业要求。（适用于证券经营机构交易系统）

9.3.2.2 测试对象

以经营机构自行运营的中继后台服务组件为起点，其中交易请求经承载交易指令校验、订单生成、合规审核等核心业务的组件处理后，发送至交易所并接收其返回结果，查询请求经承载查询指令校验、数据调取等核心业务组件处理后返回结果，最终流转至该中继后台服务组件为终点，该链路中机构侧的全部组件集合。

9.3.2.3 测试实施

开展本单元测评工作时，应核查测试报告是否包含以下内容：

1. 有效订单及查询率；2. 订单峰值吞吐率及并发查询处理能力之和；3. 订单处理时延99%分位值；4. 报入过程中最小响应速率；5. 订单丢失率；6. 订单正确率；7. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.2.4 结果判定

以下结果均符合,则本单元的测评结果为符合;否则,本单元的测评结果为不符合:

1. 有效订单及查询率不低于97%; 2. 订单峰值吞吐率及并发查询处理能力之和可以达到峰值订单及查询速率历史最大值的压力倍数要求; 3. 订单处理时延99%分位值不超过1秒; 4. 报入过程中最小响应速率大于0; 5. 订单丢失率为0%; 6. 订单正确率为100%; 7. 与业务处理相关模块的内存、磁盘空间峰值占用率均需低于80%。

9.3.3 证券经营机构交易系统峰值压力下的登录吞吐率

9.3.3.1 测评指标

短时间内以多倍生产峰值瞬时压力历史最大值持续登录,系统每秒能够处理的登录请求数量应能达到行业要求。(适用于证券经营机构交易系统)

9.3.3.2 测评对象

以经营机构自行运营的中继后台服务组件为起点,其中交易请求经承载交易指令校验、订单生成、合规审核等核心业务的组件处理后,发送至交易所并接收其返回结果,查询请求经承载查询指令校验、数据调取等核心业务组件处理后返回结果,最终流转至该中继后台服务组件为终点,该链路中机构侧的全部组件集合。

9.3.3.3 测评实施

开展本单元测评工作时,应核查测试报告是否包含下列内容:

1. 有效登录率; 2. 并发登录处理能力; 3. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.3.4 结果判定

以下结果均符合,则本单元的测评结果为符合;否则,本单元的测评结果为不符合:

1. 有效登录率不低于97%; 2. 并发登录处理能力可以达到峰值登录速率历史最大值的压力倍数要求; 3. 与业务处理相关模块的内存峰值占用率均需低于90%,磁盘空间峰值占用率均需低于80%。

9.3.4 证券经营机构交易系统结算耗时

9.3.4.1 测评指标

以多倍于生产总成交笔数和总持仓条数历史最大值进行结算,系统结算耗时应能达到行业要求。(适用于证券经营机构结算系统)

9.3.4.2 测评对象

以负责交易数据接收或交易所结算文件处理的核心组件为起点,通过承载持仓结算、资金结算等核心业务的组件完成交易数据的结算处理后,最终流转至负责结算结果反馈的组件为终点,该链路中的全部组件集合。

9.3.4.3 测评实施

开展本单元测评工作时,应核查测试报告是否包含下列内容:

1. 结算耗时; 2. 结算耗时升高比例; 3. 日成交处理容量; 4. 日结算处理容量; 5. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.4.4 结果判定

以下结果均符合,则本单元的测评结果为符合;否则,本单元的测评结果为不符合:

1. 结算耗时不超过5小时; 2. 结算耗时升高比例不超过20%(若首次测试,则建立基线); 3. 日成交处理容量可以达到总成交笔数历史最大值的容量倍数要求; 4. 日结算处理容量可以达到总成交笔数和总持仓条数历史最大值之和的容量倍数要求; 5. 与业务处理相关模块的内存峰值占用率均需低于90%、磁盘空间峰值占用率均需低于80%。

9.3.5 证券登记结算公司结算系统日间结算耗时

9.3.5.1 测评指标

以多倍于日结算量历史最大值进行结算,系统日间结算耗时应能达到行业要求。(适用于证券登记结算公司结算系统)

9.3.5.2 测评对象

以负责交易数据接收的核心组件为起点,通过承载持仓结算、资金结算等核心业务的组件完成交易数据的结算处理后,最终流转至负责结算文件生成与结算结果反馈的组件为终点,该链路中的全部组件集合。

9.3.5.3 测评实施

开展本单元测评工作时,应核查测试报告是否包含下列内容:

1. 日间的结算耗时; 2. 日间的结算耗时升高比例; 3. 日结算处理容量; 4. 与业务处理相关模块的磁盘空间峰值占用率。

9.3.5.4 结果判定

以下结果均符合,则本单元的测评结果为符合;否则,本单元的测评结果为不符合:

1. 日间的结算耗时不超过7小时; 2. 日间的结算耗时升高比例不超过50%(若首次测试,则仅建立基线); 3. 日结算处理容量可以达到日结算量历史最大值的容量倍数要求; 4. 与业务处理相关模块的磁盘空间峰值占用率均需低于80%。

9.3.6 期货交易所交易系统峰值压力下的订单发送速率

9.3.6.1 测评指标

在短时间内以多倍生产峰值瞬时压力历史最大值报入订单,系统能够处理的订单请求数量应能达到行业要求。(适用于期货交易所交易系统)

9.3.6.2 测评对象

以负责交易数据接收与反馈的网关或前置组件为起点,交易请求经承载交易风控、订单撮合、成交确认等核心业务的组件处理后,最终流转至负责交易结果反馈的网关或前置组件为终点,该链路中的全部组件集合。

9.3.6.3 测评实施

开展本单元测评工作时,应核查测试报告是否包含下列内容:

1. 集合竞价阶段的有效订单率; 2. 连续交易阶段的有效订单率; 3. 连续交易阶段峰值时刻的订单峰值发送速率; 4. 连续交易阶段的订单处理时延99%分位值; 5. 报入过程中最小响应速率; 6. 报入过程中交易席位断连情况; 7. 订单丢失率; 8. 订单正确率; 9. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.6.4 结果判定

以下结果均符合,则本单元的测评结果为符合;否则,本单元的测评结果为不符合:

1. 集合竞价阶段的有效订单率不低于97%; 2. 连续交易阶段的有效订单率不低于97%; 3. 连续交易阶段峰值时刻的订单峰值发送速率可以达到峰值订单速率历史最大值的压力倍数要求; 4. 连续交易阶段的订单处理时延99%分位值不超过(T+3)秒; 5. 报入过程中最小响应速率大于0; 6. 报入过程中无交易席位断连; 7. 订单丢失率为0%; 8. 订单正确率为100%; 9. 与业务处理相关模块的内存峰值占用率均需低于90%, 磁盘空间峰值占用率均需低于80%。

9.3.7 期货交易所结算系统结算耗时

9.3.7.1 测评指标

以多倍于生产总成交笔数和总持仓数历史最大值进行结算,系统结算耗时应能达到行业要求。(适用于期货交易所结算系统)

9.3.7.2 测评对象

以负责交易数据接收的核心组件为起点,通过承载持仓结算、资金结算等核心业务的组件完成交易数据的结算处理后,最终流转至负责结算文件生成与结算结果反馈的组件为终点,该链路中的全部组件集合。

9.3.7.3 测评实施

开展本单元测评工作时,应核查测试报告是否包含下列内容:

1. 结算耗时; 2. 结算耗时升高比例; 3. 日成交处理容量; 4. 日结算处理容量; 5. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.7.4 结果判定

以下结果均符合,则本单元的测评结果为符合;否则,本单元的测评结果为不符合:

1. 结算耗时不超过2.5小时; 2. 结算耗时升高比例不超过50%(若首次测试,则建立基线); 3. 日成交处理容量可以达到总成交笔数历史最大值的容量倍数要求; 4. 日结算处理容量可以达到总成交笔数和总持仓条数历史最大值之和的容量倍数要求; 5. 与业务处理相关模块的内存峰值占用率均需低于90%, 磁盘空间峰值占用率均需低于80%。

9.3.8 期货经营机构交易系统峰值压力下的订单及查询吞吐率

9.3.8.1 测评指标

在短时间内以多倍生产峰值瞬时压力历史最大值报入业务,系统每秒能够处理的业务请求数量应能达到行业要求。(适用于期货经营机构交易系统)

9.3.8.2 测评对象

以经营机构自行运营的中继后台服务组件为起点,其中交易请求经承载交易指令校验、订单生成、合规审核等核心业务的组件处理后,发送至交易所并接收其返回结果,查询请求经承载查询指令校验、数据调取等核心业务组件处理后返回结果,最终流转至该中继后台服务组件为终点,该链路中机构侧的全部组件集合。

9.3.8.3 测评实施

开展本单元测评工作时,应核查测试报告是否包含下列内容:

1. 有效订单及查询率；2. 订单峰值吞吐率及并发查询处理能力之和；3. 订单处理时延99%分位值；4. 报入过程中最小响应速率；5. 订单丢失率；6. 订单正确率；7. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.8.4 结果判定

以下结果均符合,则本单元的测评结果为符合；否则,本单元的测评结果为不符合：

1. 有效订单及查询率不低于97%；2. 订单峰值吞吐率及并发查询处理能力之和可以达到峰值订单及查询速率历史最大值的压力倍数要求；3. 订单处理时延99%分位值不超过1秒；4. 报入过程中最小响应速率大于0；5. 订单丢失率为0%；6. 订单正确率为100%；7. 与业务处理相关模块的内存峰值占用率均需低于90%，磁盘空间峰值占用率均需低于80%。

9.3.9 期货经营机构交易系统结算耗时

9.3.9.1 测评指标

以多倍于生产总成交笔数和总持仓条数历史最大值进行结算，系统结算耗时应能达到行业要求。（适用于期货经营机构结算系统）

9.3.9.2 测评对象

以负责交易数据接收或交易所结算文件处理的核心组件为起点，通过承载持仓结算、资金结算等核心业务的组件完成交易数据的结算处理后，最终流转至负责结算结果反馈的组件为终点，该链路中的全部组件集合。

9.3.9.3 测评实施

开展本单元测评工作时，应核查测试报告是否包含下列内容：

1. 结算耗时；2. 结算耗时升高比例；3. 日成交处理容量；4. 日结算处理容量；5. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.9.4 结果判定

以下结果均符合,则本单元的测评结果为符合；否则,本单元的测评结果为不符合：

1. 结算耗时不超过2.5小时；2. 结算耗时升高比例不超过50%（若首次测试，则建立基线）；3. 日成交处理容量可以达到总成交笔数历史最大值的容量倍数要求；4. 日结算处理容量可以达到总成交笔数和总持仓条数历史最大值之和的容量倍数要求；5. 与业务处理相关模块的内存峰值占用率均需低于90%，磁盘空间峰值占用率均需低于80%。

9.3.10 期货市场监控中心开户系统开户业务处理耗时

9.3.10.1 测评指标

以多倍于日开户量历史最大值进行处理，系统开户业务处理耗时应能达到行业要求。（适用于期货市场监控中心开户系统）

9.3.10.2 测评对象

以负责开户原始数据接收的核心组件为起点，经承载数据检查、开户规则校验等核心业务的组件完成开户数据的处理后，以最终流转至交易所的网关或前置为终点，该链路中的全部组件集合。

9.3.10.3 测评实施

开展本单元测评工作时，应核查测试报告是否包含下列内容：

1. 开户业务处理耗时；2. 开户业务处理耗时升高比例；3. 日开户处理容量；4. 与业务处理相关模块的内存、磁盘空间峰值占用率。

9.3.10.4 结果判定

以下结果均符合，则本单元的测评结果为符合；否则，本单元的测评结果为不符合：

1. 开户业务处理耗时不超过5小时；2. 开户业务处理耗时升高比例不超过20%（若首次测试，则仅建立基线）；3. 日开户处理容量可以达到日开户量历史峰值的容量倍数要求；4. 与业务处理相关模块的内存峰值占用率均需低于90%，磁盘空间峰值占用率均需低于80%。

10 整体测评要求

10.1 概述

整体测评从单元间、层面间等方面进行测评和综合安全分析。整体测评包括单元间测评和层面间测评。

单元间测评是指对同一技术层面或管理方面（不包含特殊测评要求）内的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全防护能力的影响。

层面间测评是指对不同技术层面或管理方面（不包含特殊测评要求）之间的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全防护能力的影响。

10.2 单元间测评

在单元测评完成后，应对单元测评结果中存在的不符合项和部分符合项进行单元间测评，重点分析信息系统中是否存在同一层面单元间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的密码安全防护能力是否缺失，如果经过综合分析单元测评中的不符合项和部分符合项未导致信息系统整体安全防护能力的缺失，则对该测评单元的测评结果予以调整。

10.3 层面间测评

在单元测评完成后，应对单元测评结果中存在的不符合项和部分符合项进行层面间测评，重点分析信息系统中是否存在不同层面单元间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的密码安全防护能力是否缺失，如果经过综合分析单元测评中的不符合项和部分符合项未导致信息系统整体安全防护能力的缺失，则对该测评单元的测评结果予以调整。

10.4 特殊测评要求

特殊测评要求的测评结果不参与整体测评和量化评估，但参与整体风险分析与评价。系统建设方可自行或委托专业机构开展相关测评，其实施过程应符合本标准相关要求。若最近一次特殊测评要求评估后，系统未发生较大技术架构的变更，能够真实反映当前系统状态，密评机构可复用最近一次测试结果。若自最近一次特殊指标评估后，系统发生了较大技术架构变更（包括但不限于密码算法替换、密钥管理体系调整、密码产品更换或密码服务部署结构变化等），则原有特殊测评结果不得复用，应依据本标准重新开展特殊指标测评。

11 风险分析和评价

密码应用安全性评估报告应对整体测评之后单元测评结果中的不符合项和部分符合项进行风险分析和评价。

对单元测评结果中存在的不符合项和部分符合项，采用风险分析方法分析密码应用在合规性、正确性和有效性方面对应的安全问题被威胁利用的可能性和对信息系统造成的影响，综合评价这些不符合项和部分符合项对信息系统带来的不同程度的安全风险。

不符合项和部分符合项是否会给信息系统带来高安全风险的判定依据可参考其他相关标准或文件。对未满足密码应用的合规性、正确性、有效性且存在明显安全风险的情形，例如使用的密码技术不符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，应结合具体业务场景做出高安全风险判定。关于行业特殊业务场景风险评价的判定请参考附录C。

12 测评结论

信息系统密码应用测评的最终输出是密码应用安全性评估报告，在报告中应描述以下环节的测评情况：各个测评单元的测评结果、整体测评结果、风险分析和评价结果，以及测评结论等。其中，测评结论基于整体测评结果和风险分析结果综合给出，分为如下三种。

- a) 符合：信息系统所有单元（包含特殊测评要求）测评结果不存在不符合项和部分符合项。
- b) 基本符合：信息系统单元（不包含特殊测评要求）测评结果中存在不符合项和部分符合项，与测评指标存在一定差距，但存在的不符合项和部分符合项（包含特殊测评要求）未导致信息系统高安全风险。
- c) 不符合：信息系统单元（不包含特殊测评要求）测评结果中存在不符合项和部分符合项，与测评指标存在较大差距，或存在的不符合项和部分符合项（包含特殊测评要求）导致信息系统高安全风险。

附录 A

(资料性)

密钥生存周期管理检查要点

A.1 概述

密钥管理对于保证密钥全生存周期的安全性至关重要，可以保证密钥(除公开密钥外)不被非授权的访问、使用、泄露、修改和替换，可以保证公开密钥不被非授权的修改和替换。在信息系统密码应用方案中，需明确信息系统的密钥生存周期管理。密钥管理包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。

A.2 密钥产生

密钥产生测评内容如下。

a) 检查目的

密钥是否在经商用密码认证机构认证的密码产品中产生，密钥协商算法是否经国家密码管理部门核准。

b) 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

- 1) 确认密钥产生所使用的随机数发生器是否具有商用密码认证机构颁发的认证证书；
- 2) 确认密钥协商算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；
- 3) 核实密钥产生功能的正确性和有效性，如随机数发生器的运行状态、所产生密钥的关联信息，密钥关联信息包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等。

A.3 密钥分发

密钥分发测评内容如下。

a) 检查目的

密钥分发过程是否保证了密钥的机密性、完整性以及分发者、接收者身份的真实性等。

b) 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

- 1) 确认信息系统内部采用何种密钥分发方式(离线分发方式、在线分发方式、混合分发方式)；
- 2) 确认密钥传递过程中信息系统使用了何种密码技术保证密钥的机密性、完整性与真实性，并核实采用密码技术的合规性、正确性和有效性。

A.4 密钥存储

密钥存储测评内容如下。

a) 检查目的

密钥(除公开密钥)存储过程是否保证了不被非授权的访问或篡改,公开密钥存储过程是否保证了不被非授权的篡改。

b) 检查对象

密钥、密钥管理制度及策略类文档,以及密钥存储涉及的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

1) 确认信息系统内部所有密钥(除公开密钥)是否均以密文形式进行存储,或者位于受保护的安全区域;

2) 确认密钥(除公开密钥)存储过程中信息系统使用了何种密码技术保证密钥的机密性(除公开密钥)、完整性,并核实采用密码技术的合规性、正确性和有效性;

3) 确认公开密钥存储过程中信息系统使用了何种密码技术保证公开密钥的完整性,并核实采用密码技术的合规性、正确性和有效性。

A.5 密钥使用

密钥使用测评内容如下。

a) 检查目的

所有密钥是否都有明确的用途且各类密钥是否均被正确地使用、管理。

b) 检查对象

密钥、密钥管理制度及策略类文档,以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

1) 确认信息系统内部是否具有严格的密钥使用管理机制,以及所有密钥是否有明确的用途并按用途被正确使用;

2) 确认信息系统是否具有鉴别公开密钥的真实性与完整性的认证机制,采用的公钥密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求;

3) 确认信息系统采用了何种安全措施来防止密钥泄露或替换,是否采用了密码算法以及算法是否符合相关法规和标准的要求,并核实当发生密钥泄露时,信息系统是否具备应急处理和响应措施;

4) 确认信息系统是否定期更换密钥,并核实密钥更换处理流程中是否采取有效措施保证密钥更换时的安全性。

A.6 密钥更新

密钥更新测评内容如下。

a) 检查目的

密钥是否根据相应的更新策略进行更新。

b) 检查对象

密钥、密钥管理制度及策略类文档,以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

确认信息系统是否具有密钥的更新策略,并核实当密钥超过使用期限、已泄露或存在泄露风险时,是否根据相应的更新策略进行密钥更新。

A.7 密钥归档

密钥归档测评内容如下。

a) 检查目的

密钥归档过程是否保证了密钥的安全性和正确性，并生成了审计信息。

b) 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

- 1) 确认信息系统内部密钥归档时是否采取有效的安全措施，以保证归档密钥的安全性和正确性；
- 2) 核实归档密钥是否仅用于解密被加密的历史信息或验证被签名的历史信息；
- 3) 确认密钥归档的审计信息是否包括归档的密钥、归档的时间等信息。

A.8 密钥撤销

密钥撤销测评内容如下。

a) 检查目的

公钥证书、对称密钥是否具备撤销机制。

b) 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

- 1) 如信息系统内部使用公钥证书、对称密钥，则确认是否有公钥证书、对称密钥撤销机制和撤销机制的触发条件，并确认是否有效执行；
- 2) 核实撤销后的密钥是否已不具备使用效力。

A.9 密钥备份

密钥备份测评内容如下。

a) 检查目的

密钥备份过程是否保证了密钥的机密性和完整性，并生成了审计信息。

b) 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

- 1) 如信息系统内部存在需要备份的密钥，则确认是否具有密钥备份机制并有效执行；
- 2) 确认密钥备份过程中，信息系统使用了何种密码技术保证备份密钥的机密性、完整性；
- 3) 确认是否包括备份主体、备份时间等密钥备份的审计信息。

A.10 密钥恢复

密钥恢复测评内容如下。

a) 检查目的

密钥是否具备恢复机制，并生成审计信息。

b) 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

- 1) 确认信息系统内部是否具有密钥的恢复机制并有效执行；
- 2) 确认是否包括恢复主体、恢复时间等密钥恢复的审计信息。

A.11 密钥销毁

密钥销毁测评内容如下。

a) 检查目的

密钥是否具备销毁机制，销毁过程是否具备不可逆性。

b) 检查对象

密钥、密钥管理制度及策略类文档，以及信息系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 检查要点

- 1) 确认信息系统内部是否具有密钥的销毁机制并有效执行；
- 2) 核实密钥销毁过程和销毁方式，确认是否密钥销毁后无法被恢复。

附录 B
(资料性)
典型商用密码应用场景案例

B.1 证券公司网上交易接入系统

证券网上交易接入系统主要由客户端、通讯网络和服务器端组成。在进行商用密码安全加固设计过程中，引入密码技术、密码产品和密码服务提升证券网上交易接入系统整体安全。服务器端由SSL接入网关、协同签名服务端模块、硬件加密设备、密钥管理系统（KMS）和SM2数字证书系统组成。客户端由SSL组件和协同签名客户端模块组成，其组成如图B.1所示。

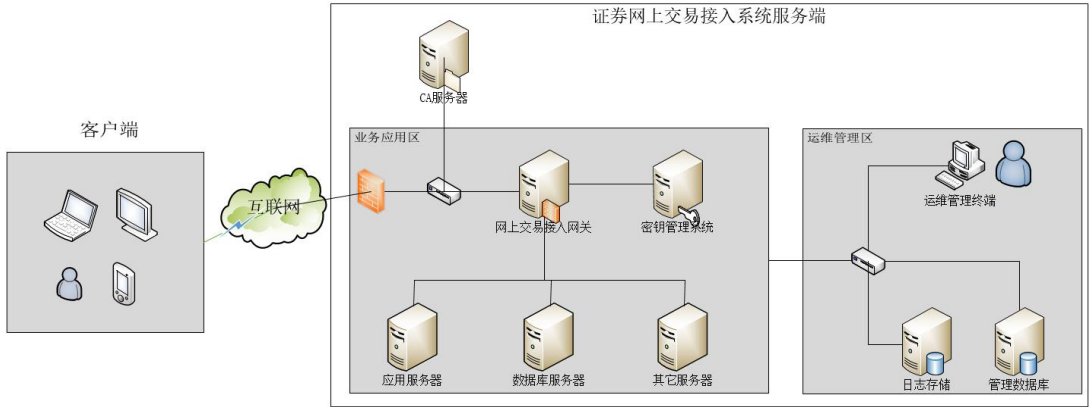


图 B.1 证券网上交易接入系统示意图

根据证券网上交易接入系统的业务特点，其密码应用需求如表B.1所示：

表 B.1 证券网上交易接入系统密码应用需求表

序号	安全区域	密码功能点	密码应用描述
1	客户端与网上交易接入网关	通信链路保护	客户端与SSL接入网关建立安全通道，交互信息使用对称算法SM4加密传输。
		身份认证	使用SM2数字证书和协同签名模块实现身份认证。
		数据传输机密性和完整性	SSL安全通道使用SM4加密传输，使用SM3算法的MAC技术保证完整性。
2	网上交易接入网关和密钥管理系统	身份认证	内部网络信息交互，产品符合GB/T 37092标准并取得产品资质证书。
		数据传输机密性和完整性	
3	客户端	数据存储机密性和完整性保护	对客户端存储的重要数据采用SM4对称加密算法、SM2非对称加密算法或SM3算法的MAC技术实现机密性和

			完整性保护，防止数据被窃取或篡改。
4	网上交易接入网关	数据存储机密性和完整性保护	对服务端存储的重要数据采用硬件加密设备进行机密性和完整性保护，防止数据被窃取或篡改。

根据以上密码应用需求分析，采用密码技术实现系统密码应用相应功能点，其密码应用总体部署如图 B. 2所示。

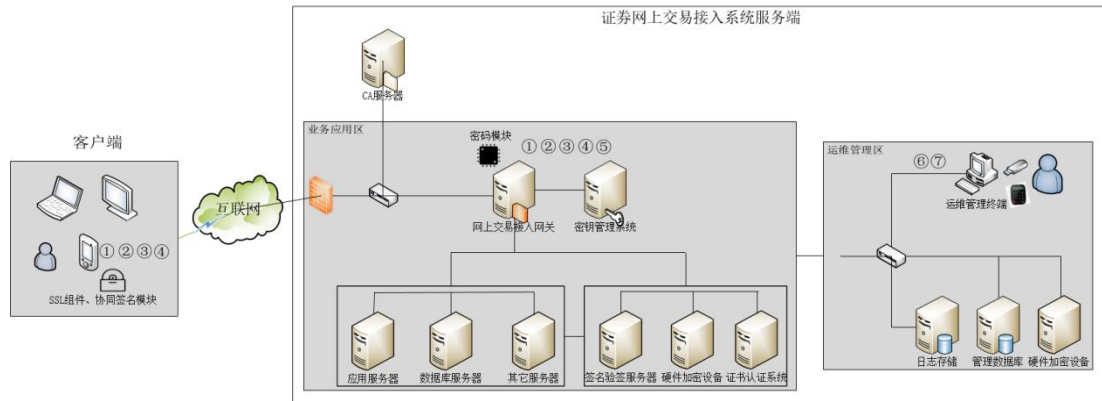


图 B. 2 证券网上交易接入系统密码应用总体部署图

具体密码应用环节说明如下：

- a) 客户端集成 SSL 组件和协同签名客户端模块等，服务端网络边界部署 SSL 接入网关和硬件加密设备，双方基于密码协议建立安全通信链路，实现网络通信实体的身份鉴别，以及网络通信数据的机密性和完整性保护；
- b) 客户端使用 SSL 组件和协同签名客户端模块等，服务端部署签名验签服务器等，通过数字签名技术实现客户端的身份标识和鉴别，确保用户身份的真实性；
- c) 客户端使用 SSL 组件和协同签名客户端模块等，服务端部署硬件加密设备等，通过数据加解密、计算 MAC（或数字签名），实现通信过程中用户数据、证券交易数据、证券查询信息等数据的机密性保护或完整性保护；
- d) 客户端使用 SSL 组件和协同签名客户端模块等，服务端部署协同签名服务端模块和硬件加密设备等，通过协同签名客户端模块保证客户端存储的机密性，协同签名客户端模块和协同签名服务端模块共同完成客户端身份的认证；
- e) 证券网上交易接入系统服务端部署硬件加密设备，通过对服务端存储的证券网上交易接入系统重要数据进行加解密或计算 MAC（或数字签名），实现数据的机密性保护或完整性保护；
- f) 证券网上交易接入系统服务端使用智能密码钥匙、动态令牌等对登录运维管理终端的用户进行身份鉴别，确保登录用户身份的真实性；
- g) 证券网上交易接入系统服务端通过智能密码钥匙、硬件加密设备等密码设备对运维管理终端与系统相关服务器之间传输的重要数据进行加解密或计算 MAC（或数字签名），实现运维管理中重要数据的机密性或完整性保护。

附录 C

(资料性)

风险评价

C.1 证券期货业信息系统风险评价

本附录旨在对“风险分析和评价”相关条款在证券期货业的落地实施提供补充性指引，为密评人员开展具体测评工作提供判定参考，密评人员可参照本附录的判定思路进行综合研判得出最终结论。需要特别说明的是，本附录所列缓解措施并非唯一可行技术路径或任意场景下均适用，实际应用中，系统责任方可结合自身系统现状、业务需求及风险承受能力，选择等效或更为适宜的方案。

- a) 行业信息系统与非中国大陆地区机构建立的网络通信信道确需遵循外部机构接入规范的，在检查通道具备有效补偿性安全措施（如专用加密隧道、专线、实时审计等）的前提下，可酌情降低网络和通信安全层面相关指标风险等级；
- b) 用户登录经营机构交易系统时，如系统已具备有效密码技术进行身份鉴别，但未关闭手机验证码登录方式的，可酌情降低应用和数据安全层面身份鉴别指标风险等级；
- c) 对于仅能在与系统处于同一物理管控区域的运维管理区通过与业务网络物理隔离的内网环境进行设备运维，且网络传输不涉及中间不可控和公共交换设备，设备计算安全层面远程管理通道安全指标可视为采取了风险缓解措施；
- d) 对于在运维管理区通过堡垒机统一进行设备运维的情况，如果堡垒机身份鉴别指标测评结论为“符合”或“部分符合”，没有高风险，且仅能通过堡垒机进行集中运维的设备，设备计算安全层面身份鉴别指标可视为采取了风险缓解措施。
- e) 对于异地机房间网络通道经过了不可控的公共交换设备，如果在连接该不可控链路的网络设备之间启用了动态路由协议认证，可酌情降低网络和通信安全层面身份鉴别指标风险等级；
- f) 对于涉及行业业务实时性要求限制的改造对象以技术可行性能满足行业业务需求为前提，在具备成熟的密码产品或密码服务能够稳定、持续地支撑业务系统生产量级数据对实时性、吞吐量及可用性的要求时进行完全改造。若现有密码产品或密码服务不能满足行业场景要求，未采用密码技术进行保护，系统建设方在已通过评估的密码应用方案或相关设计文档中，应充分论证当前无可行的密码技术或产品可满足需求，内容包括业务场景、实时性量化指标、数据量级、现有密码产品性能瓶颈分析等。在查验系统实际情况与密码应用方案的一致性后，可酌情降低应用和数据安全层面重要数据传输、存储过程中机密性、完整性的风险等级；
- g) 本标准中的特殊测评要求涉及高风险，原则上应严格遵循指标要求进行判定，若实际测评中存在客观条件限制，被测方需提供充分的证明材料，对限制因素及其对指标的影响程度予以清晰阐述，经密评机构审核确认后，可酌情降低特殊测评要求的风险等级。客观条件限制的情形包括但不限于：（1）系统处于未上线或试运行阶段，测试环境无法完全模拟生产配置；（2）第三方基础设施或外部系统存在依赖瓶颈（如外部 CA 系统、时间源、数据源等非被测方可控因素），密评时需基于被测方提交的证明材料，结合上述情形的实际影响范围、系统部署及具体业务场景，综合评定密码改造后系统对于特殊测评要求相关指标的最终风险等级。

C.2 系统可用性保障措施的风险评价说明

为保障业务连续性，系统应具备可用性应急保障机制（如切换备用设备、非国密通道或非密码技术身份鉴别方式等）。在系统发生失效或故障、确影响业务连续运行的紧急情况下，系统可临时切换至应急措施，以确保业务不中断。

应急措施应满足以下管理要求：

- a) 应急措施仅允许在密码设备、服务故障或不可用期间开启，系统正常运行状态下应保持关闭；
- b) 应急措施应具备明确的开启条件判定与触发机制，防止误用或滥用；
- c) 应急措施开启期间应有日志记录；
- d) 密码设备或服务恢复正常后，应及时关闭应急措施，恢复至合规运行状态。

在系统正常运行时处于关闭状态的应急措施，不纳入系统密评过程中各层面的测评范围；若系统正常运行状态下应急措施处于开启状态，则应将其纳入密评过程中各层面的测评范围，并依据本标准相关条款判定其风险及合规性。

参 考 文 献

- [1] JR/T 0145—2016 资本市场交易结算系统核心技术指标
 - [2] JR/T 0255—2022 金融行业信息系统商用密码应用基本要求
 - [3] JR/T 0256—2022 金融行业信息系统商用密码应用测评要求
 - [4] JR/T 0257—2022 金融行业信息系统商用密码应用测评过程指南
 - [5] JR/T 0292—2023 证券公司核心交易系统技术指标
 - [6] 商用密码应用安全性评估测评实施指引（2024-11）
-