ICS 03.060
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

XX/T XXXXX—XXXX
代替

证券期货业信息系统密码技术应用指引

Guildlines for the application of cryptography technology in

information systems of 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 3
引言 4
1 范围 5
2 规范性引用文件 5
3 术语和定义 5
4 概述 7
4.1 标准内容 7
4.2 运用原则 7
5 密码技术、密码产品、密码服务 7
5.1 密码技术 7
5.2 密码产品 8
5.3 密码服务 8
6 密码安全功能和密码技术的关系 8
7 密码技术应用要求相应的密码产品指引 9
7.1 密码产品指引通则 9
7.2 物理和环境安全 10
7.3 网络和通信安全 10
7.4 设备和计算安全 12
7.5 应用和数据安全 13
8 适用的证券期货业数据安全要求 16
8.1 密码技术应用要求和行业数据安全要求的关系 16
8.2 相关证券期货业数据安全要求 16
附录 A（资料性） 堡垒机系统商密应用方案示例 17
A.1 技术方案 17
A.1.1 采用认证的 VPN 网关 17
A.1.2 采用认证的动态口令认证系统 17
A.1.3 采用认证的商密浏览器 17
A.2 商密应用的设备部署 17
A.2.1 部署方式 17
A.3 商密应用工作流程 17
附录 B（资料性） 身份鉴别参考实现 19
B.1 身份鉴别参考实现 19
B.1.1 背景和问题 19
B.1.2 基于对称密码算法的数据存储参考实现 19
B.1.3 基于公钥密码算法的数据存储参考实现 19
B.1.4 基于客户端签名和数字信封的鉴别信息传输参考实现 20

B.1.5 基于客户端签名和服务端公钥加密的鉴别信息传输参考实现.....20
附录 C（资料性） 数据分级对比.....21
C.1 《证券期货业数据分类分级指引》和《金融数据安全 数据安全分级指南》数据分级对比.....21
参考文献.....23

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范》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：中国证监会科技监管局、上海证券交易所、深圳证券交易所、中证机构间报价系统股份有限公司、上交所技术有限责任公司、中国银河证券股份有限公司、国泰君安证券股份有限公司、中国信息通信研究院、公安部第三研究所、北京国家金融科技认证中心有限公司、深圳市纽创信安科技开发有限公司、北京信安世纪科技股份有限公司、北京江南天安科技有限公司、信雅达科技股份有限公司、深圳市财富趋势科技股份有限公司、浙江同花顺智能科技有限公司、三未信安科技股份有限公司、深圳市金证科技股份有限公司、北京天融信网络安全技术有限公司。

本文件主要起草人：姚前、刘铁斌、蒋东兴、周云晖、陈炜、朱立、居红伟、王亚军、沙明、梅养真、徐庆、马聪、徐秀、黎水林、孙国栋、高强裔、杨慈航、郭望、李万召、周骞、邹超、刘硕、戴凌峰、钟才斌、徐金双、方立斌、吴锦超、朱家雄、王冬冬、刘晓东、张玉涛、周贤谦、李雪莹。

引　　言

随着GB/T 39786《信息安全技术 信息系统密码密码应用基本要求》的正式生效，以及随着各类数据日益成为机构的重要资产，证券期货行业在信息系统中加强密码技术应用，力求满足合规性要求、更好保护自身数据资产的需求日益迫切，行业也因此亟需一份易于对标GB/T 39786要求开展信息系统密码应用改造工作的指引。

为帮助证券期货业各类行业核心机构、行业经营机构开展信息系统密码应用工作，便于监管机构对各类行业机构的密码应用工作进行评判，特编制本指南。

证券期货业信息系统密码技术应用指引

1 范围

本文件规定了证券期货业（简称行业）各类行业机构在遵照GB/T 39786 《信息安全技术 信息系统密码应用基本要求》要求开展信息系统密码技术应用时，针对该国标在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全方面的各项要求，在设计方案时可供考虑的技术手段和产品列表，本文件也针对行业机构如何将金融业数据安全方面的若干现存标准和上述国标相结合进行了说明。

本文件适用于证券期货业各类行业机构在开展信息系统密码技术应用时的参考，也适用于监管机构对行业机构的密码技术应用方案进行评估。

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 25069 信息安全技术 术语

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 17964 信息安全技术分组 密码算法的工作模式

GB/T 32922 信息安全技术 IPSec VPN安全接入基本要求与实施指南

GB/T 15843.3 信息技术 安全技术 实体鉴别 第3部分： 采用数字签名技术的机制

GB/T 15852.1 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

GB/T 15852.2 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 19714 信息技术 安全技术 公钥基础设施 证书管理协议

GM/T 0024 SSL VPN技术规范

GM/T 0026 安全认证网关产品规范

JR/T 0223 金融数据安全数据生命周期安全规范

JR/T 0171 个人金融信息保护技术规范

JR/T 0197 金融数据安全数据安全分级指南

JR/T 0158 证券期货业数据分类分级指引

3 术语和定义

下列术语和定义适用于本文件。

3.1

机密性 confidentiality

保证信息不被泄露给非授权实体的性质。

[来源：GB/T 39786-2021，3.1]

3.2

数据完整性 data integrity

数据没有遭受以非授权方式所作的改变的性质。

[来源：GB/T 39786-2021，3.2]

3.3

真实性 authenticity

一个实体是其所声称实体的这种特性。真实性适用于用户、进程、系统和信息之类的实体。

[来源：GB/T 39786-2021，3.3]

3.4

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

[来源：GB/T 39786-2021，3.4]

3.5

消息鉴别码 message authentication code(MAC)

利用对称密码技术或密码杂凑技术，在秘密密钥参与下，由消息所导出的数据项。任何持有这一秘密密钥的实体，可利用消息鉴别码检查消息的完整性和始发者身份。

[来源：GB/T 39786-2021，3.9]

3.6

动态口令 one-time password

基于时间、事件等方式动态生成的一次性口令。

[来源：GB/T 39786-2021，3.11]

3.7

分组密码算法工作模式 block cipher operation mode

分组密码算法的使用方式，主要包括电码本工作模式、密文分组链接工作模式、密文反馈工作模式、输出反馈工作模式、计数器工作模式、带密文挪用的XEX可调分组密码工作模式、带泛杂凑函数的计数器工作模式、分组链接工作模式、带非线性函数的输出反馈工作模式等。

[来源：GB/T 17964-2021，3.1]

3.8

公钥证书 public key certificate

用户的公钥连同其他信息，并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

[来源：GB/T 19714-2005，3.2]

3.9

签名及数字信封数据类型 signedAndEnvelopedData

签名及数字信封数据类型由任意类型的加密数据、至少一个接收者的数据加密密钥和至少一个签名者的签名组成。

[来源：GB/T 35275-2017，10]

3.10

个人金融信息 personal financial information

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

注 1： 本标准中的个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息

及其他反应特定个人某些情况的信息。

[来源：JR/T 0171-2020，3.2]

4 概述

4.1 标准内容

证券期货业信息系统密码技术的应用应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，这些要求中包括了GB/T 39786。证券期货业的典型业务具有高吞吐量、低延时的技术需求。正因为行业机构长期以来对这些技术需求的强调，和金融行业其他领域相比，证券期货业的密码技术应用案例和应用经验相对较少。为帮助行业机构落实密码技术应用相关要求，特结合行业实际编撰本指南。

GB/T 39786定义了信息系统密码应用技术框架，从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出密码应用技术要求，用以保障信息系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性。机密性、完整性、真实性、不可否认性被称为密码安全功能的四个维度。除了上述技术要求，该标准还从信息系统的管理制度、人员管理、建设运行和应急处置四个方面提出了密码应用管理要求。

作为信息系统密码技术应用指南，本标准不再重复GB/T 39786中的密码应用管理要求及其附录B中的密钥生存周期管理要求。

4.2 运用原则

行业在GB/T 39786指引下，参考本标准开展信息系统密码应用改造时，应本着“总体安全”的原则。

密码应用技术要求内部的四个层面并非互相割裂，密码应用技术要求和密码应用管理要求也不应独立看待。虽然某层面的技术安全措施并不能等效替代另一层面的技术安全措施，密码应用管理要求和密码应用技术要求也不能彼此等效替代，但确实存在互相补位、缓解风险的空间。

行业机构应在综合评估本单位信息系统的风险程度、风险概率、业务需求的基础上形成安全风险应对策略，再基于安全风险应对策略形成具体的密码应用方案。

5 密码技术、密码产品、密码服务

5.1 密码技术

行业信息系统所使用的密码技术，其基础是公钥密码算法、密码杂凑算法、对称密码算法等密码算法。针对所有级别的信息系统，行业使用的密码算法都应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，如SM2（包括基于SM2的协同签名算法）、SM3、SM4等密码算法。不得使用MD5、DES、SHA-1、RSA-1024等被证明存在安全风险或安全强度不足的密码算法，也不得采用安全性未知的密码算法，如自行设计的密码算法、经认证的密码产品中未经安全性论证的密码算法等。

行业信息系统所使用的密码技术通常是基于上述密码算法组合而成的密码套件。针对所有级别的信息系统，此类密码套件应当基于上述合规的密码算法，且应遵循密码相关国家标准和行业标准，如遵循相关标准的实体鉴别技术、消息鉴别码技术、SSL VPN技术、IPSec VPN技术等。不得采用存在缺陷或有安全问题警示的密码技术，如SSH1.0、SSL 2.0、SSL 3.0、TLS 1.0等，不得采用安全性未知的密码技术，如未经安全性论证的自行设计的密码通信协议、经认证的密码产品中未经安全性论证的密码通信协议等。

5.2 密码产品

行业信息系统在实施时应当采用经国家密码主管部门核准的密码产品，且产品应符合GB/T 39786中规定的与信息系统级别相适应的安全要求。不得采用自实现且未提供安全性证据的密码产品，不得采用存在高危安全漏洞的密码产品（如OpenSSL产品）、不得在不满足其安全运行前提条件时使用密码产品。

行业机构在使用密码产品时，应对随机数来源、初始化向量、分组密码算法工作模式、密钥管理、密钥保护等方面的合规性予以特别关注。

在证券期货业信息系统密码应用中，常用密码产品包括：软件密码模块（包括协同签名客户端、协同签名服务端、SSL客户端模块等）、智能密码钥匙、PCI-E/PCI密码卡、IPSec VPN安全网关/IPSec VPN、SSL VPN安全网关/SSL VPN、安全认证网关、服务器密码机、签名验签服务器、门禁卡/安全门禁系统、动态令牌/动态令牌认证系统、证书认证系统/证书认证密钥管理系统、对称密钥管理产品、安全芯片等。

金融数据密码机是符合金融磁条卡、IC卡业务特点的密码设备，多用于银行业。因其同样具备消息鉴别码生成和校验、数据加解密、签名验签、密钥管理等功能，故凡可使用服务器密码机、签名验签服务器、对称密钥管理产品之处，若无关成本则也可用其充任。因其在证券期货业中较少使用，故下文不将其单独列出。

5.3 密码服务

行业机构使用的密码服务目前以电子认证服务为主。行业机构使用的密码服务应符合法律法规的相关要求，选用的密码服务提供商应具备相应资质。

6 密码安全功能和密码技术的关系

机密性、完整性、真实性、不可否认性四个密码安全功能维度可以分别通过不同的密码技术来实现，彼此存在内在对应关系，行业机构在选择密码应用方案以及密码产品时可参照该对应关系辅助决策。密码安全功能和密码技术之间的关系，其内容见表1。

表 1 密码安全功能、密码技术的关系

密码安全功能	密码技术	备注
机密性	对称密码算法、公钥密码算法	密码杂凑算法可能被用于生成待隐藏信息的杂凑值，从而避免直接存储待隐藏信息。此时应将生成的杂凑值再进行对称或非对称加密以提供更好的机密性。 应用和数据层面可采用 SM4 算法解决数据传输和存储的机密性，建议采用 CBC 模式。 SSL VPN、IPSec VPN 底层使用了对称密码算法、公钥密码算法，故可以提供网络和通信安全层面、设备和计算安全层面的传输机密性

表 1　密码安全功能、密码技术的关系（续）

密码安全功能	密码技术	备注
完整性	公钥密码算法数字签名、消息鉴别码	单纯使用密码杂凑（如 SM3）不足以实现完整性，因为攻击者可以在修改原像的同时重新生成杂凑值。不应使用普通校验码（如 CRC）来实现完整性。 应用和数据层面可采用 SM2 算法做数字签名解决数据传输的完整性（此方法性能较低），也可考虑采用 HMAC（SM3/SM4）解决数据传输或存储的完整性。 SSL VPN、IPSec VPN 底层使公钥密码算法数字签名、消息鉴别码，故可以提供网络和通信安全层面、设备和计算安全层面的传输完整性
真实性	公钥密码算法数字签名、消息鉴别码、动态口令	应用和数据层面可采用基于数字证书的 SM2 数字签名、HMAC(SM3/SM4)或动态口令，来解决真实性。 SSL VPN、IPSec VPN 底层使公钥密码算法数字签名、消息鉴别码，故可提供网络和通信安全层面、设备和计算安全层面的真实性。
不可否认性	公钥密码算法数字签名	交易不可否认性,可考虑应用和数据层面采用基于数字签名技术对交易数据做 SM2 算法签名来解决不可否认。

7　密码技术应用要求相应的密码产品指引

7.1　密码产品指引通则

针对密码技术应用要求的四个层面，下文将分别给出相应的密码产品指引，用以指导行业机构通过选用合适的密码产品满足密码技术应用要求。指引原则上只给到产品类别，不涉及具体供应商和产品型号。

在所给的密码产品指引中，默认已包含证书认证系统/证书认证密钥管理系统、对称密钥管理产品等起到基础支撑作用的密码产品，故不在每一处重复。软件密码模块因其具有最大的灵活性，除少数特例如协同签名客户端/服务器、签名控件等，不在每一处重复，但使用时应注意其能达到的GB/T 37902安全要求等级是否符合要求。

GB/T 39786中，针对不同级别的信息系统在密码技术应用要求中附带了不同的约束词（可、宜、应等），针对不同级别的信息系统规定了密码技术应用的最低要求。本密码产品指引旨在回答如下问题：当行业机构决定采取措施以满足此项密码技术应用要求时，可供考虑的密码产品列表有哪些。为此，本指引将忽略密码技术应用要求文本中的约束词，直接给出可选密码产品类别列表。

不同密码产品所能达到的GB/T 37092安全要求存在差异。仅靠软件密码模块通常只能达到GB/T 37092一级安全要求，但行业中常用的协同签名客户端/服务器（在硬件密码设备的帮助下）可以提供公钥密码算法数字签名技术的产品实现，且可达到GB/T 37092二级安全要求。对于实现公钥密码算法的密码产品，公钥证书可以公开，私钥管理若仅借助软件密码模块实现，则不应使用于需要达到GB/T 37092二级或以上级别安全要求的场合。

为降低行业机构自行研发密码产品带来的风险，指引中的密码产品列表首选现成产品。

在使用本指引确定可选密码产品列表时，应结合信息系统级别相应的密码产品安全要求进行筛选。

7.2 物理和环境安全

为满足物理和环境安全层面的各项系统密码应用要求，可供考虑的密码产品列表，其内容见表2。

表 2 物理和环境安全：密码产品列表

要求编号	系统密码应用要求	指标要求	优先考虑的密码产品列表
（1）	采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性	真实性	门禁卡/安全门禁系统等。
（2）	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	完整性	门禁卡/安全门禁系统等。
（3）	采用密码技术保证视频监控音像记录数据的存储完整性	完整性	智能密码钥匙、 PCI-E/PCI 密码卡、 服务器密码机、 签名验签服务器等。

7.2.1 重要说明

针对上述系统密码应用要求7.2节表2（1），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：未采用动态口令、消息鉴别码、公钥密码算法的数字签名等技术对重要区域进入人员身份进行身份鉴别；针对人员身份真实性的密码技术实现机制不正确或无效。

——可能的缓解措施有：基于生物识别技术（如指纹等）对进入人员进行身份鉴别；重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控等。

7.3 网络和通信安全

GB/T 39786规定的信息系统在网络和通信安全层面的密码应用技术要求，其相关测评对象主要是针对跨网络访问的通信信道，且此处说的“跨网络访问”主要是指从不受保护的网络区域访问被测系统。

可以从网络类型和通信主体两个方面的同时结合来确定网络和通信安全层面的测评对象：

——网络类型：这里主要依据网络之间是否相对独立进行分类，如互联网、企业专网等。除 7.3.1 节规定的不适用情形，“基于专线”不能作为不适用 GB/T 39786 各项密码应用技术要求的理由。

——通信主体；指的是参与通信的各方，典型的如客户端与服务端，例如 PC 机上运行的浏览器与服务器上运行的 web 服务系统，移动智能终端上运行的 APP 与服务器上运行的应用系统；也可以是服务端与服务端，例如服务端不同系统间的 IPSec VPN。

为满足网络和通信安全层面的各项系统密码应用要求，可供考虑的密码产品列表，其内容见表3。

表 3　网络和通信安全：密码产品列表

要求编号	系统密码应用要求	指标要求	优先考虑的密码产品列表
（1）	采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性	真实性	协同签名客户端/服务器、IPSec VPN 安全网关/IPSec VPN、SSL VPN 安全网关/SSL VPN、安全认证网关、智能密码钥匙、动态令牌/动态令牌认证系统等。
（2）	采用密码技术保证通信过程中数据的完整性	完整性	IPSec VPN 安全网关/IPSec VPN、SSL VPN 安全网关/SSL VPN、安全认证网关等。
（3）	采用密码技术保证通信过程中重要数据的机密性	机密性	IPSec VPN 安全网关/IPSec VPN、SSL VPN 安全网关/SSL VPN、安全认证网关等。
（4）	采用密码技术保证网络边界访问控制信息的完整性	完整性	安全认证网关等。
（5）	采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性	真实性	IPSec VPN 安全网关/IPSec VPN、SSL VPN 安全网关/SSL VPN、安全认证网关等。

7.3.1　重要说明

针对上述系统密码应用要求7.3节表3（1）至表3（5），有下列不适用情形：

——如果双活机房之间的通信链路是纯物理传输的裸光纤而非运营商专线（需要被测方提供证明材料进行裸光纤判定），在对光纤物理防护上有严格的安全保护措施，能够完全保证物理线路安全，不存在安全隐患，则该通道无需作为网络和通信安全层面的测评对象。

针对上述系统密码应用要求7.3节表3（1），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：信息系统与网络边界外建立网络通信信道时，未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）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（第二级和第三级）/双向身份鉴别（第四级）；通信实体身份真实性实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施有：无。

针对上述系统密码应用要求 7.3 节表 3（3），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：信息系统与网络边界外的通信实体建立网络通信信道时，未采用密码技术的加解密功能对通信过程中重要数据进行机密性保护；敏感信息或通信报文机密性实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施有：在“应用和数据安全”层面针对重要数据传输采用符合要求的密码技术进行机密性保护。需注意的是即使提供了此种高风险缓解措施，在商用密码应用安全性评估过程中仍然不因此影响“网络和通信安全”层面的独立计分。

针对上述系统密码应用要求7.3节表3（5），对于行业中的第四级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）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；安全接入认证的实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施：无

7.4 设备和计算安全

为满足设备和计算安全层面的各项系统密码应用要求，可供考虑的密码产品列表，其内容见表4。附录A给出了一个为现有堡垒机设备增加信息传输通道机密性、完整性及设备登录用户身份鉴别机制的参考实现。

表 4 设备和计算安全：密码产品列表

要求编号	系统密码应用要求	指标要求	优先考虑的密码产品列表
（1）	采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性	真实性	协同签名客户端/服务器、IPSec VPN 安全网关/IPSec VPN、SSL VPN 安全网关/SSL VPN、安全认证网关、智能密码钥匙、动态令牌/动态令牌认证系统等。
（2）	远程管理设备时，采用密码技术建立安全的信息传输通道	机密性 完整性	IPSec VPN 安全网关/IPSec VPN、SSL VPN 安全网关/SSL VPN、安全认证网关等。
（3）	采用密码技术保证系统资源访问控制信息的完整性	完整性	安全认证网关、通过开发和能提供公钥密码算法数字签名或消息鉴别码的密码产品进行对接，如对接智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器等。
（4）	采用密码技术保证设备中的重要信息资源安全标记的完整性	完整性	通过开发和能提供公钥密码算法数字签名或消息鉴别码的密码产品进行对接，如对接智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器等。

表 4 设备和计算安全：密码产品列表（续）

要求编号	系统密码应用要求	指标要求	优先考虑的密码产品列表
（5）	采用密码技术保证日志记录的完整性	完整性	通过开发和能提供公钥密码算法数字签名或消息鉴别码的密码产品进行对接，如对接智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器等。
（6）	采用密码技术对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	完整性 真实性	通过开发和能提供公钥密码算法数字签名的密码产品进行对接，如对接智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器等。

7.4.1 重要说明

针对上述系统密码应用要求7.4节表4（1），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对登录设备的用户进行身份鉴别；用户身份真实性的密码技术实现机制不正确或无效。

——可能的缓解措施有：基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性。

针对上述系统密码应用要求 7.4 节表 4（2），对于第三级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：远程管理设备时，未采用密码技术建立安全的信息传输通道；信息传输通道所采用密码技术实现机制不正确或无效；通过不可控网络环境进行远程管理，且鉴别数据以明文形式传输。

——可能的缓解措施有：搭建了与业务网络隔离的管理网络进行远程管理；在“网络和通信安全”层面使用 SSL VPN 网关/IPSec VPN 网关等建立集中管理通道，且使用的密码技术符合要求。

7.5 应用和数据安全

为满足设备和计算安全层面的各项系统密码应用要求，可供考虑的密码产品列表，其内容见表5。附录B针对应用和数据安全层面的身份鉴别信息传输和存储给出了一个参考实现。

表 5　应用和数据安全：密码产品列表

要求编号	系统密码应用要求	指标要求	优先考虑的密码产品列表
（1）	采用密码技术对登录用户进行身份鉴别保证应用系统用户身份的真实性	真实性	协同签名客户端/服务器、 签名控件、 智能密码钥匙、 动态令牌/动态令牌认证系统、 安全芯片等。
（2）	采用密码技术保证信息系统应用的访问控制信息的完整性	完整性	通过开发和能提供公钥密码算法数字签名或消息鉴别码的密码产品进行对接，如对接协同签名客户端/服务器、签名控件、智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器、安全芯片等。
（3）	采用密码技术保证信息系统应用的重要信息资源安全标记的完整性	完整性	通过开发和能提供公钥密码算法数字签名或消息鉴别码的密码产品进行对接，如对接协同签名客户端/服务器、签名控件、智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器、安全芯片等。
（4）	采用密码技术保证信息系统应用的重要数据在传输过程中的机密性	机密性	通过开发对接能提供公钥密码算法数字信封技术、对称密码算法的密码产品，如对接智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器、安全芯片等。
（5）	采用密码技术保证信息系统应用的重要数据在存储过程中的机密性	机密性	通过开发对接能提供公钥密码算法数字信封技术、对称密码算法的密码产品，如对接智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器、安全芯片等。
（6）	采用密码技术保证信息系统应用的重要数据在传输过程中的完整性	完整性	通过开发和能提供公钥密码算法数字签名或消息鉴别码的密码产品进行对接，如对接协同签名客户端/服务器、签名控件、智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器、安全芯片等。

表 5　应用和数据安全：密码产品列表（续）

要求编号	系统密码应用要求	指标要求	优先考虑的密码产品列表
（7）	采用密码技术保证信息系统应用的重要数据在存储过程中的完整性	完整性	通过开发和能提供公钥密码算法数字签名或消息鉴别码的密码产品进行对接，如对接 PCI-E/PCI 密码卡、服务器密码机、签名验签服务器、安全芯片等。
（8）	在可能涉及法律责任认定的应用中宜采用密码技术提供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	不可否认性	通过开发和能提供公钥密码算法数字签名的密码产品进行对接，如对接协同签名客户端/服务器、签名控件、智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、签名验签服务器、安全芯片等。

7.5.1　重要说明

针对上述系统密码应用要求7.5节表5（1），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对登录用户进行身份鉴别；用户身份真实性的密码技术实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施有：基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性

针对上述系统密码应用要求 7.5 节表 5（4），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：未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；重要数据传输机密性实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施有：“网络和通信安全”层面采用符合要求的密码技保证重要数据在传输过程中的机密性。

针对上述系统密码应用要求 7.5 节表 5（5），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：未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；重要数据存储机密性实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施有：无

针对上述系统密码应用要求 7.5 节表 5（7），对于第二级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：未采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对重要数据在存储过程中进行完整性保护；重要数据存储完整性实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施有：应用系统具有符合要求的身份鉴别措施，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份。

针对上述系统密码应用要求 7.5 节表 5（8），对于第三级及以上级别信息系统，有如下重点关注项：

——需关注的安全问题有：在可能涉及法律责任认定的应用中，未采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为和接收行为实现不可否认性；不可否认性的密码技术实现机制不正确或无效；采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

——可能的缓解措施有：无

8 适用的证券期货业数据安全要求

8.1 密码技术应用要求和行业数据安全要求的关系

在GB/T 39786规定的各项密码技术应用要求中，除了提及“电子门禁系统进出记录数据”等具体数据类型之外，还一般性地多处提及“重要数据”。GB/T 39786本身并不针对不同行业进行重要数据分类分级，也不针对不同行业的数据在传输、存储等环节中的数据安全规范作出规定。各行业通过制定本行业的数据安全要求对上述内容作出规定。

在开展商用密码应用安全性评估过程中，通过GB/T 39786的密码技术应用要求和行业数据安全要求的彼此结合形成评估依据。

8.2 相关证券期货业数据安全要求

证券期货业落实GB/T 39786所需的数据安全要求，适用《证券期货业数据分类分级指引》、《金融数据安全 数据生命周期安全规范》、《个人金融信息保护技术规范》各项规定。

《金融数据安全 数据生命周期安全规范》直接引用的《金融数据安全 数据安全分级指南》，根据安全性遭到破坏后的影响范围和影响程度，将金融数据安全级别由高到底划分为5级、4级、3级、2级、1级，且明确将个人金融信息C3、C2、C1三个级别分别映射到4级、3级和2级。《证券期货业数据分类分级指引》则根据数据安全属性遭到破坏时的影响对象、影响范围、影响程度将行业数据等级从高到低划分为4级、3级、2级、1级，且未对个人金融信息进行定级。附录C给出了二者的对比。

为便于落实《金融数据安全 数据生命周期安全规范》各项规定，证券期货业机构应先根据《证券期货业数据分类分级指引》确定行业数据等级，再参照表6将其映射到《金融数据安全 数据安全分级指南》中规定的金融数据安全级别。个人金融信息的金融数据安全级别遵照《金融数据安全 数据安全分级指南》、《个人金融信息保护技术规范》执行。最后，基于金融数据安全级别遵照《金融数据安全 数据生命周期安全规范》各项规定开展工作。

表 6 从行业数据等级到金融数据安全级别的映射

行业数据等级	金融数据安全级别
4 级	4 级
3 级	3 级
2 级	2 级
1 级	1 级

附 录 A
（资料性）
堡垒机系统商密应用方案示例

A.1 技术方案

A.1.1 采用认证的VPN网关

在数据中心运维管理区域中，部署VPN网关产品，用于建立运维终端与服务端VPN之间的安全信息传输通道。

A.1.2 采用认证的动态口令认证系统

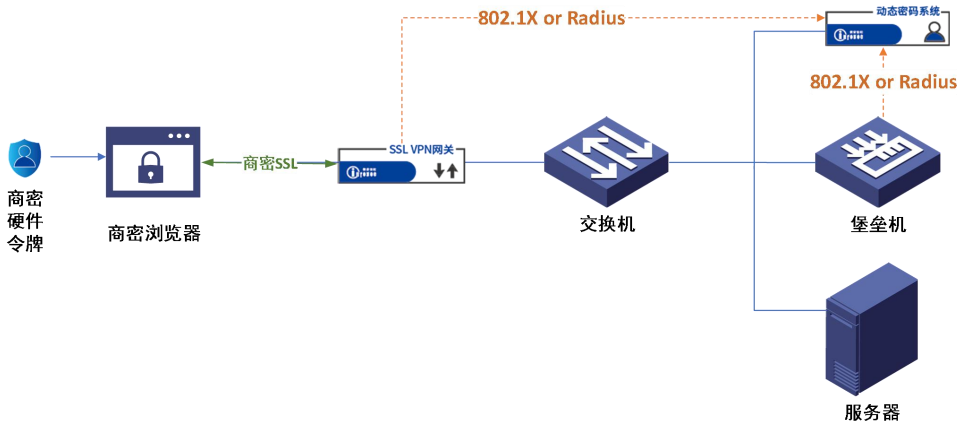
在数据中心运维管理区域中，部署动态口令认证系统，同时为系统管理员配发动态令牌，管理员用户在登录堡垒机系统和VPN系统时，采用用户名、口令及基于商密算法的动态口令认证。动态口令系统采用802.1x协议或Radius协议，为VPN系统和堡垒机系统提供认证功能。

A.1.3 采用认证的商密浏览器

在管理终端部署符合商密标准的浏览器，用于建立运维终端与服务端VPN之间的安全信息传输通道。

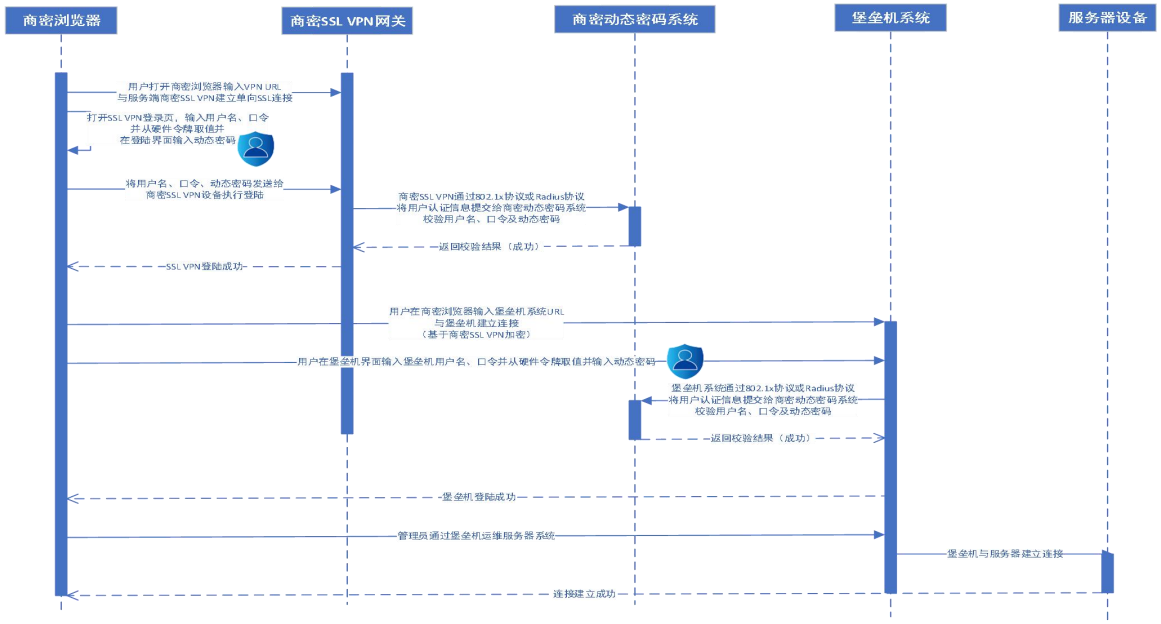
A.2 商密应用的设备部署

A.2.1 部署方式



图A.1 部署方式

A.3 商密应用工作流程



图A.2 改造后密码工作流程

步骤一，运维用户通过商密浏览器登录SSL VPN网关：

a) 运维用户通过商密浏览器打开 SSL VPN 登录页，输入 SSL VPN 网关的用户名、口令及动态密码（从硬件令牌获取）；

b) SSL VPN 网关通过 802.1x 协议或 Radius 协议，将 SSL VPN 网关用户认证信息提交给商密动态密码系统，校验用户名、口令及动态密码，并将结果返回 SSL VPN 网关；

c) 运维用户登录 SSL VPN 网关成功，建立起商密浏览器与 SSL VPN 网关的安全连接。

步骤二，运维用户通过商密浏览器登录堡垒机：

a) 运维用户通过商密浏览器打开堡垒机登录页（连接建立于 SSL VPN 加密通道之上），输入堡垒机的用户名、口令及动态密码（从硬件令牌获取）；

b) 堡垒机通过 802.1x 协议或 Radius 协议，将堡垒机用户认证信息提交给商密动态密码系统，校验用户名、口令及动态密码，并将结果返回堡垒机；

c) 运维用户登录堡垒机成功，建立起商密浏览器与堡垒机的安全连接；

步骤三，堡垒机与服务器建立连接，运维用户通过堡垒机运维服务器系统。

附 录 B
（资料性）
身份鉴别参考实现

B.1 身份鉴别参考实现

B.1.1 背景和问题

GB/T 39786针对第三级信息系统在应用和数据安全层面作出了若干规定，其中包括信息系统应用的重要数据在存储过程中的机密性和完整性。对于证券期货业的各类机构，第三级信息系统应用的身份鉴别信息属于重要数据，应当符合上述两项要求。

为令证券期货业机构在利用密码技术解决上述问题的过程中有所借鉴，针对一个假想的第三级信息系统，本资料性附录给出了两种符合GB/T 39786重要数据存储过程要求的身份鉴别信息存储参考实现，也给出了两种符合GB/T 39786重要数据传输过程要求的身份鉴别消息参考实现。

作为参考实现，本附录并不限制行业机构采用其他技术手段满足同样的要求。

本附录假想的第三级信息系统隶属于某核心机构，该信息系统包括两部分：部署在经营机构侧通过专线访问系统的客户端，及部署在核心机构侧的服务端。经营机构客户端在登录时需提供应用层的用户名/口令信息，同时需要提供利用核心机构预先分发给经营机构、且与用户名绑定的智能密码钥匙进行的签名，经营机构服务端对客户端进行单向身份鉴别。该智能密码钥匙使用SM2公钥签名算法和SM3密码杂凑算法。服务端在数据库中保存的单条身份鉴别信息至少包括用户名、口令、用户签名证书三者，本附录中分别记作user、pwd、sigCert。为简化起见，在本附录假设的场景下，客户端和服务端都有符合要求的真随机数生成设备。

为符合GB/T 39786的相关要求，服务端保持的身份鉴别信息应当在数据存储过程中满足机密性和完整性。本附录的A.1.2给出了一种基于对称密码算法的参考实现，A.1.3给出了一种基于公钥密码算法的参考实现。

为符合GB/T 39786的相关要求，身份鉴别信息应当在数据传输过程中满足机密性和完整性。本附录的A.1.4给出了一种基于签名及数字信封的参考实现，A.1.5给出了一种纯粹基于公钥密码算法的参考实现。

B.1.2 基于对称密码算法的数据存储参考实现

在本参考实现中，为了提供身份鉴别信息在数据存储过程中的机密性和完整性，服务端拥有两个独立的对称密钥Ke和Km，且Ke和Km被保存在服务器密码机（或加密卡等其他满足GB/T 37092二级以上安全要求的设备中）中，且服务端所需的真随机数由服务器密码机（或上述其他设备）提供。

Ke是供SM4算法使用的对称密钥，且服务端在使用SM4算法时使用CBC分组密码工作模式，算法所需的初始化向量值IV每次都使用独立采集的真随机数。Km是供基于密码杂凑算法的消息鉴别码使用的对称密钥，且消息鉴别码使用的密码杂凑算法是SM3。

服务端保存身份鉴别信息时，首先采集IV，并生成口令的密文cypher := SM4(Ke, IV, pwd).

最后保存在数据库的身份鉴别信息记录是：

(user, sigCert, IV, cypher, HMAC(Km, user||sigCert||IV||cypher))

B.1.3 基于公钥密码算法的数据存储参考实现

在本参考实现中，为了提供身份鉴别信息在数据存储过程中的机密性和完整性，服务端拥有两个独立的SM2私钥Ke和Ks，且Ke和Ks被保存在签名验签服务器（或加密卡等其他满足GB/T 37092二级以上安全要求的设备中）中，且服务端所需的真随机数由签名验签服务器（或上述其他设备）提供。

Ke供SM2解密算法使用，Ks供SM2签名算法使用。Ke和Ks对应的公钥证书记作Ce和Cs。

服务端保存身份鉴别信息时，首先生成口令的密文cypher := SM2_Enc(Ce,pwd).

最后保存在数据库的身份鉴别信息记录是：

(user, sigCert, cypher, SM2_Sig(Ks, user||sigCert||cypher))

B.1.4 基于客户端签名和数字信封的鉴别信息传输参考实现

在本参考实现中，为了对应用系统客户端实现单向身份鉴别，需要遵循GB/T 15843.3《信息技术 安全技术 实体鉴别 第3部分： 采用数字签名技术的机制》5.2.2节的规定，基于一次传递单向鉴别来准备原始的身份鉴别信息。

rawInfo := certA || Na || B || user || pwd || sSa(Na || B|| user || pwd)

其中，certA是客户端签名证书，Na是客户端维护的作为时变参数的序号（用以防止重放攻击），B是服务端标识。sSa()函数表示使用客户端签名证书对应的私钥进行SM2签名。

为确保身份鉴别信息在信息传输过程中的机密性和完整性，本参考实现进一步基于SM2/SM3/SM4算法，遵循GB/T 35275《信息安全技术 SM2 密码算法加密签名消息语法规范》10节中的规定，使用签名及数字信封技术对上述rawInfo进行处理后得到signedEnvolope，再发送处理signedEnvolope。

B.1.5 基于客户端签名和服务端公钥加密的鉴别信息传输参考实现

在本参考实现中，为了对应用系统客户端实现单向身份鉴别，需要遵循GB/T 15843.3《信息技术 安全技术 实体鉴别 第3部分： 采用数字签名技术的机制》5.2.2节的规定，基于一次传递单向鉴别来准备原始的身份鉴别信息。

rawInfo := certA || Na || B || user || pwd || sSa(Na || B || user || pwd)

其中，certA是客户端签名证书，Na是客户端维护的作为时变参数的序号（用以防止重放攻击），B是服务端标识。sSa()函数表示使用客户端签名证书对应的私钥进行SM2签名。

为确保身份鉴别信息在信息传输过程中的机密性和完整性，本参考实现中，客户端使用服务器加密公钥对rawInfo进行SM2加密后得到encRawInfo，然后在网络上发送encRawInfo。由于SM2加密算法内部会使用SM3密码杂凑算法，故能结合rawInfo中的Na防止篡改和重放。

附 录 C
（资料性）
数据分级对比

C.1 《证券期货业数据分类分级指引》和《金融数据安全 数据安全分级指南》数据分级对比

《证券期货业数据分类分级指引》根据数据安全属性遭到破坏时的影响对象、影响范围、影响程度将行业数据等级从高到低划分为4级、3级、2级、1级。人行发布的《金融数据安全 数据安全分级指南》根据安全性遭到破坏后的影响范围和影响程度，将金融数据安全级别由高到底划分为5级、4级、3级、2级、1级。

表C.1将这两个标准的数据分级准则进行了对比。

表 C.1 数据分级对比

《证券期货业数据分类分级指引》		《金融数据安全 数据安全分级指南》	
数据级别标识	数据特征	数据安全级别	数据特征
未定义5级	不适用	5	1、重要数据，通常主要用于金融业大型或特大型机、金融交易过程中重要枝心节点类机构的关键业务使用，一般针对特定人员公月， 且仅为必须知悉的对象访问或使用。 2、 数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。
4	1、数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围大（跨行业或跨机构），影响程度一般是“严重”。 2、一般特征：数据主要用于行业内大型或特大型机构中的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。	4	1、数据通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的重要业务使用. 一般针对特定人员公开， 且仅为必须知悉的对象访问或使用。 2、个人金融信息中的C3 类伯息。 3、数据安全性遭到破坏后，对公众权益造成一般影响， 或对个人隐私或企业合法权益造成严重影响，但不影响因家安全。
3	1、数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围中等（一般局限在本机构），影响程度一般是“严重”。 2、一般特征：数据用于重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。	3	1、数据用于金融业机构关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 2、个人金融信息中的C2类信息。 3、数据的安全性遭到破坏后，对公众权益造成轻微彰响，或对个人隐私或企业合法权益造成一般影晌. 但不影响国家安全。

表 C.1　　数据分级对比(续)

《证券期货业数据分类分级指引》		《金融数据安全 数据安全分级指南》	
2	1、数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围较小（一般局限在本机构），影响程度一般是“中等”或“轻微”。 2、一般特征：数据用于一般业务使用，一般针对受限对象公开；一般指内部管理且不宜广泛公开的数据。	2	1、数据用于金融业机构关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 2、个人金融信息中的C2类信息。 3、数据的安全性遭到破坏后，对公众权益造成轻微彰响，或对个人隐私或企业合法权益造成一般影响．但不影响国家安全。
1	1、数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围较小（一般局限在本机构），影响程度一般是“轻微”或“无”。 2、一般特征：数据可被公开或可被公众获知、使用。	1	1、数据一般可被公开或可被公众获知、使用． 2、个人金融信息主体主动公开的信息。 3、数据的安全性遭到破坏后，可能对个人隐私或企业合法权益不造成影响.或仅造成微弱影响但不影响国家安全、公众权益。

参 考 文 献

[1] 商用密码产品认证目录（第一批）
[2] 信息系统密码应用高风险判定指引