ICS 03.060
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0255—2022

金融行业信息系统商用密码应用 基本要求

Information system commercial cryptography application of financial industry—Basic requirements

2022-11-25 发布　　2022-11-25 实施

中国人民银行　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专利的责任。

本文件由中国人民银行科技司提出。

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：中国人民银行科技司、中国证券监督管理委员会科技监管局、北京国家金融科技认证中心有限公司、中国金融电子化集团有限公司、中国银联股份有限公司、北京银联金卡科技有限公司、中金金融认证中心有限公司、中互金认证有限公司、中国工商银行股份有限公司、中国建设银行股份有限公司、中国民生银行股份有限公司、蚂蚁科技集团股份有限公司、中证信息技术服务有限责任公司、国家信息技术安全研究中心、中国银河证券股份有限公司、格尔软件股份有限公司、北京海泰方圆科技股份有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司。

本文件主要起草人：李伟、姚前、陈立吾、刘铁斌、潘润红、车珍、沈筱彦、陈炜、夏磊、王涛、咎新、曹正阳、段越、侯漫丽、郭师嘉、张海燕、唐辉、李振、李凡、高强裔、孙国栋、刘文娟、陈雪峰、马成龙、李禹泽、王大地、王炤宇、张璐、李博文、汤洋、郑峥、张光巧、李增局、赵旭、靳芸生、刘书洪、姜志辉、安辉耀、周桉、于博洋、范佳奇、林青、魏自恩、梅养真、陈红梅、王学进、王翊心、候宇。

引　言

金融行业是国民经济的重要领域，金融行业网络安全是国家网络安全的重要组成部分，密码技术作为保障网络安全的核心技术，是金融信息保护和网络信任体系建设的基础。随着国家商用密码应用相关标准的发布，需要一系列适用于金融行业信息系统商用密码应用的标准作为支撑，以规范和指导金融行业信息系统商用密码应用和商用密码应用安全性评估工作的实施，从而保障金融行业商用密码应用的合规、正确、有效，有力提升金融行业网络安全防护水平。

本文件是金融行业信息系统商用密码应用系列标准之一，金融行业信息系统商用密码应用系列标准包括以下标准。

——《金融行业信息系统商用密码应用　基本要求》。

——《金融行业信息系统商用密码应用　测评要求》。

——《金融行业信息系统商用密码应用　测评过程指南》。

本文件根据GB/T 22239《信息安全技术　网络安全等级保护基本要求》的等级保护对象应具备的基本安全保护能力要求，结合金融行业业务特点及安全保护需求，在GB/T 39786《信息安全技术　信息系统密码应用基本要求》的基础上，提出金融行业密码应用自低向高的5个等级，分别为第一级、第二级、第三级、第四级和第五级。

本文件中，对于“可”的条款，金融行业信息系统责任单位自行决定是否纳入密码应用范围。对于“宜”的条款，金融行业信息系统责任单位根据信息系统密码应用方案和方案评审意见决定是否纳入密码应用范围，若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则应将该条款纳入信息系统密码应用范围。对于“应”的条款，金融行业信息系统责任单位应将其纳入信息系统密码应用范围，若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与该条款相关的密码应用需求，则不将该条款纳入信息系统密码应用范围。

金融行业信息系统商用密码应用　基本要求

1　范围

本文件规定了金融行业信息系统不同等级的密码应用基本要求，从密码算法合规性、密码技术合规性、密码产品和密码服务合规性方面提出了密码应用通用要求，从金融行业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4个技术层面提出了第一级到第四级的密码应用技术要求，从管理制度、人员管理、建设运行和应急处置4个方面提出了第一级到第四级的密码应用管理要求。结合金融行业尚无第五级密码应用的实际，本文件对第五级密码应用技术要求和管理要求暂不做具体描述。

本文件适用于指导金融机构、商用密码应用安全性评估机构和金融行业主管部门实施信息系统商用密码应用的规划、建设、运行、测评及监督管理。

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 22239　信息安全技术　网络安全等级保护基本要求
GB/T 22240　信息安全技术　网络安全等级保护定级指南
GB/T 37092　信息安全技术　密码模块安全要求
GB/T 39786　信息安全技术　信息系统密码应用基本要求
GM/T 0054　信息系统密码应用基本要求
JR/T 0068　网上银行系统信息安全通用规范
JR/T 0071.2　金融行业网络安全等级保护实施指引　第2部分：基本要求
JR/T 0158　证券期货业数据分类分级指引
JR/T 0185　商业银行应用程序接口安全管理规范
JR/T 0197　金融数据安全　数据安全分级指南

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 39786，3.1]

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 39786，3.2]

3.3

真实性　authenticity

1 个实体是其所声称实体的特性。

注：真实性适用于用户、进程、系统和信息之类的实体。

[来源：GB/T 39786，3.3，有修改]

3.4

不可否认性 non-repudiation

证明1个已经发生的操作行为无法否认的性质。

[来源：GB/T 39786，3.4]

3.5

加密 encipherment；encryption

对数据进行密码变换以产生密文的过程。

[来源：GB/T 39786，3.5]

3.6

解密 decipherment；decryption

加密过程对应的逆过程。

[来源：GM/T 0054，3.5]

3.7

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

[来源：GM/T 0054，3.6]

3.8

密钥 key

控制密码算法运算的关键信息或参数。

[来源：GB/T 39786，3.6]

3.9

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。

[来源：GB/T 39786，3.7]

3.10

身份鉴别 identity authentication

证明 1 个实体所声称身份的过程。

[来源：GB/T 39786，3.8]

3.11

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果。

注：该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的不可否认性。

[来源：GM/T 0054，3.10，有修改]

3.12

消息鉴别码 message authentication code；MAC

利用对称密码技术或密码杂凑技术，在密钥参与下，由消息所导出的数据项。

注：任何持有这一密钥的实体，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 39786，3.9，有修改]

3.13

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 39786，3.10]

3.14

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1种机制。

[来源：GB/T 39786，3.11]

3.15

密码模块 cryptographic module

实现了密码安全功能的硬件、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。

[来源：GB/T 37092，3.5，有修改]

3.16

商用密码应用安全性评估 security evaluation of commercial cryptographic application

按照国家商用密码应用法律法规和标准规范要求，对采用商用密码技术、产品和服务的网络和信息系统密码应用的合规性、正确性和有效性进行评估的活动。

3.17

客户端程序 client program

为金融行业信息系统用户提供人机交互功能的程序，以及提供必需功能的组件。

注：客户端程序包括运行于移动终端上的应用软件，不包括通用浏览器。

[来源：JR/T 0068，3.6，有修改]

3.18

应用程序接口 application programming interface；API

1组预先定义好的功能，开发者可通过该功能（或功能的组合）便捷地访问相关服务，而无需关注服务的设计与实现。

[来源：JR/T 0185，3.1]

3.19

敏感数据 sensitive data

金融行业信息系统中一旦泄露或误用可能产生潜在有害影响的数据。

注：证券期货业敏感数据参照 JR/T 0158 规定的交易业务类型中的成交信息、委托信息、交易日志信息、账户信息、银期转账、银证转账、操作员日志记录、登录信息和客户基本信息等。非证券期货业敏感数据参照 JR/T 0197 规定的 4 级数据和 3 级数据，JR/T 0197 中重要数据的保护参照国家及行业有关规定执行。

4 缩略语

下列缩略语适用于本文件。

APP：应用程序（Application）

ATM：自动柜员机（Automatic Teller Machine）

IC：集成电路（Integrated Circuit）

IPSec：互联网安全协议（Internet Protocol Security）

POS：销售点终端（Point of Sale）

PCI：外设部件互连（Peripheral Component Interconnect）
PCI-E：外设部件互连的改进版（Peripheral Component Interconnect Express）
SSL：安全套接层（Secure Sockets Layer）
VPN：虚拟专用网络（Virtual Private Network）

5 概述

5.1 金融行业信息系统密码应用技术框架

5.1.1 框架概述

本文件从金融行业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4个层面提出密码应用技术要求，保障金融行业信息系统的实体身份真实性、敏感数据的机密性和完整性、操作行为的不可否认性。同时，从金融行业信息系统的管理制度、人员管理、建设运行和应急处置4个方面提出密码应用管理要求，为金融行业信息系统提供管理方面的密码应用安全保障。

5.1.2 密码应用技术要求维度

密码应用技术要求主要由机密性、完整性、真实性、不可否认性4个密码安全功能维度构成，具体保护对象或应用场景描述如下。

a) 使用密码技术的加密功能和解密功能实现机密性，信息系统中使用密码技术实现机密性保护的对象如下。
——身份鉴别信息。
——密钥数据。
——传输的敏感数据。
——信息系统应用中所有存储的敏感数据。

b) 使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实现完整性，信息系统中使用密码技术实现完整性保护的对象如下。
——身份鉴别信息。
——密钥数据。
——日志记录。
——访问控制信息。
——重要信息资源安全标记。
——重要可执行程序。
——视频监控音像记录。
——电子门禁系统进出记录。
——传输的敏感数据。
——信息系统应用中所有存储的敏感数据。

c) 使用动态口令机制、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实现真实性，信息系统中使用密码技术实现真实性的应用场景如下。
——进入重要物理区域人员的身份鉴别。
——通信双方的身份鉴别。
——网络设备接入时的身份鉴别。
——重要可执行程序的来源真实性保证。
——登录操作系统和数据库系统的用户身份鉴别。
——应用系统的用户身份鉴别。

d) 使用基于公钥密码算法的数字签名机制等密码技术来保证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。

金融行业信息系统责任单位应根据系统业务情况和安全风险，确定系统具体密码应用需求，从而进行系统密码应用安全设计，金融行业重要信息系统密码应用设计示例见附录A。

5.1.3 密码应用管理要求维度

管理要求由管理制度、人员管理、建设运行、应急处置4个密码应用管理维度构成，具体如下。

a) 密码应用安全管理相关流程制度的制定、发布、修订的规范性要求。
b) 密码相关安全人员的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的培养，人员工作流程要求等。
c) 建设运行过程中密码应用安全要求及方案落地执行的一致性和有效性要求。
d) 处理密码应用安全相关的应急突发事件的能力要求。

5.2 密码应用基本要求等级

本文件中第一级、第二级、第三级、第四级密码应用基本要求描述如下。

a) 第一级是金融行业信息系统密码应用安全要求等级的最低等级，要求信息系统符合通用要求和最低限度的管理要求，并鼓励使用密码保障信息系统安全。
b) 第二级在第一级要求的基础上，增加操作规程、人员上岗培训与考核、应急预案等管理要求，并要求优先选择使用密码保障信息系统安全。
c) 第三级在第二级要求的基础上，增加对真实性、机密性的技术要求以及全部的管理要求。
d) 第四级在第三级要求的基础上，增加对完整性、不可否认性的技术要求。

本文件所要求的不同级别密码应用基本要求汇总见附录B。

信息系统密码应用基本要求等级一般由其网络安全等级保护的级别确定，金融行业信息系统根据GB/T 22240确定网络安全等级保护级别后，同步确定密码应用基本要求等级。金融行业信息系统根据其密码应用基本要求等级选择相应的密码保障技术能力及管理能力，并进行密码应用的设计与实现。金融行业信息系统密码应用设计应与网络安全等级保护安全技术设计相结合，避免重复设计。JR/T 0071.2中关于密码应用要求与本文件的对应关系见附录C。

6 通用要求

金融行业信息系统密码应用应符合以下通用要求。

a) 金融行业信息系统中使用的密码算法应符合 GB/T 39786 通用要求中关于密码算法的要求。
b) 金融行业信息系统中使用的密码技术应符合 GB/T 39786 通用要求中关于密码技术的要求。
c) 金融行业信息系统中使用的密码产品、密码服务应符合 GB/T 39786 通用要求中关于密码产品、密码服务的要求。

7 密码应用基本要求

7.1 物理和环境安全

物理和环境安全密码应用基本要求包括以下内容。

a) 身份鉴别：第一级可/第二级、第三级宜/第四级应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，重要区域包括但不限于金融行业信息系统主机房、灾备机房、运维管理区、重要设备存放区等。
b) 电子门禁记录数据存储完整性：第一级可/第二级、第三级宜/第四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。
c) 视频监控记录数据存储完整性：第二级可/第三级宜/第四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。
d) 密码服务：以上如采用密码服务，第一级、第二级、第三级、第四级应符合 GB/T 39786 中关于密码服务的要求。
e) 密码产品：
——以上采用的密码产品，第二级应达到 GB/T 37092 规定的一级及以上级别安全要求。
——以上采用的密码产品，第三级应达到 GB/T 37092 规定的二级及以上级别安全要求。
——以上采用的密码产品，第四级应达到 GB/T 37092 规定的三级及以上级别安全要求。

7.2 网络和通信安全

网络和通信安全密码应用基本要求包括以下内容。

a) 身份鉴别：
——第一级可/第二级宜/第三级应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，通信双方包括但不限于金融行业信息系统与客户端程序、金融行业信息系统与受理终端、金融行业信息系统与外部系统等。
——第四级应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性，通信双方包括但不限于金融行业信息系统与客户端程序、金融行业信息系统与受理终端、金融行业信息系统与外部系统等。

b) 通信数据完整性：第一级、第二级可/第三级宜/第四级应采用密码技术保证通信过程中数据的完整性。

c) 通信过程敏感数据的机密性：第一级可/第二级宜/第三级、第四级应采用密码技术保证通信过程敏感数据的机密性。

d) 网络边界访问控制信息的完整性：第一级、第二级可/第三级宜/第四级应采用密码技术保证网络边界访问控制信息的完整性，网络边界访问控制信息包括但不限于访问控制列表。

e) 安全接入认证：第三级可/第四级宜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，确保接入设备身份的真实性。

f) 密码服务：以上如采用密码服务，第一级、第二级、第三级、第四级应符合 GB/T 39786 中关于密码服务的要求。

g) 密码产品：
——以上采用的密码产品，第二级应达到 GB/T 37092 规定的一级及以上级别安全要求。
——以上采用的密码产品，第三级应达到 GB/T 37092 规定的二级及以上级别安全要求。
——以上采用的密码产品，第四级应达到 GB/T 37092 规定的三级及以上级别安全要求。

7.3 设备和计算安全

设备和计算安全密码应用基本要求包括以下内容。

a) 身份鉴别：第一级可/第二级宜/第三级、第四级应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。

b) 远程管理通道安全：第一级可/第二级宜/第三级、第四级应采用密码技术建立安全的远程管理信息传输通道。

c) 身份鉴别信息机密性：第一级可/第二级宜/第三级、第四级应采用密码技术保证用户身份鉴别信息的机密性。

d) 系统资源访问控制信息完整性：第一级、第二级可/第三级宜/第四级应采用密码技术保证系统资源访问控制信息的完整性。

e) 重要信息资源安全标记完整性：第三级宜/第四级应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。

f) 日志记录完整性：第一级、第二级可/第三级宜/第四级应采用密码技术保证涉及身份鉴别、远程管理和操作、审计管理等日志记录的完整性。

g) 不可否认性：第二级可/第三级宜/第四级应采用密码技术提供数据原发证据和数据接收证据，实现运维管理中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。

h) 重要可执行程序完整性和来源真实性：第三级宜/第四级应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。

i) 密码服务：以上如采用密码服务，第一级、第二级、第三级、第四级应符合 GB/T 39786 中关于密码服务的要求。

j) 密码产品：
——以上采用的密码产品，第二级应达到 GB/T 37092 规定的一级及以上级别安全要求。
——以上采用的密码产品，第三级应达到 GB/T 37092 规定的二级及以上级别安全要求。

——以上采用的密码产品，第四级应达到GB/T 37092规定的三级及以上级别安全要求。

7.4 应用和数据安全

应用和数据安全密码应用基本要求包括以下内容。

a) 身份鉴别：第一级可/第二级宜/第三级、第四级应采用密码技术对通过客户端程序、浏览器、受理终端、应用程序接口等方式登录或访问应用系统的用户和执行关键交易的用户进行身份鉴别，保证应用系统用户身份的真实性。
b) 客户端程序完整性和来源真实性：第二级可/第三级宜/第四级应采用密码技术保证客户端程序的完整性，并对其来源进行真实性验证。
c) 访问控制信息完整性：第一级、第二级可/第三级宜/第四级应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。
d) 重要信息资源安全标记完整性：第三级宜/第四级应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。
e) 敏感数据传输机密性：第一级可/第二级宜/第三级、第四级应采用密码技术保证信息系统应用的敏感数据在传输过程中的机密性。
f) 敏感数据存储机密性：第一级可/第二级宜/第三级、第四级应采用密码技术保证信息系统应用的敏感数据在存储过程中的机密性。
g) 敏感数据传输完整性：第一级可/第二级、第三级宜/第四级应采用密码技术保证信息系统应用的敏感数据在传输过程中的完整性。
h) 敏感数据存储完整性：第一级可/第二级、第三级宜/第四级应采用密码技术保证信息系统应用的敏感数据在存储过程中的完整性。
i) 不可否认性：在可能涉及法律责任认定的应用中，第三级宜/第四级应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。
j) 密码服务：以上如采用密码服务，第一级、第二级、第三级、第四级应符合GB/T 39786中关于密码服务的要求。
k) 密码产品：
——以上采用的密码产品，第二级应达到GB/T 37092规定的一级及以上级别安全要求。
——以上采用的密码产品，第三级应达到GB/T 37092规定的二级及以上级别安全要求。
——以上采用的密码产品，第四级应达到GB/T 37092规定的三级及以上级别安全要求。

7.5 管理制度

使用密码技术的金融行业信息系统应符合以下管理制度要求。

a) 具备密码应用安全管理制度：第一级、第二级、第三级、第四级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。
b) 密钥管理规则：第一级、第二级、第三级、第四级应根据密码应用方案建立相应根密钥、对称密钥、非对称密钥等密钥管理规则。
c) 建立操作规程：第一级、第二级、第三级、第四级应对密钥管理人员或密码设备操作人员执行的日常管理操作建立操作规程。
d) 定期修订安全管理制度：第三级、第四级应定期对密码应用安全管理制度和操作规程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，保存论证记录、审定记录、修订记录以及修订后文档。
e) 明确管理制度发布流程：第三级、第四级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、格式要求及文档编号，并进行版本控制。
f) 制度执行过程记录留存：第二级、第三级、第四级应具有密码应用操作规程的相关执行记录并妥善保存，针对密钥管理制定密钥各个生存周期管理的记录表单。

7.6 人员管理

使用密码技术的金融行业信息系统应符合以下人员管理要求。

a) 了解并遵守密码相关法律法规和密码应用安全管理制度：第一级、第二级、第三级、第四级相关人员应了解并遵守密码相关法律法规和密码应用安全管理制度。
b) 建立密码应用岗位责任制度：第二级、第三级、第四级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。
——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，密钥管理员主要负责信息系统密钥的管理，密码操作员主要负责密码设备的相关操作，密码安全审计员主要负责密钥管理和密码设备操作相关的审计。
——对关键岗位建立多人共管机制。
——密钥管理员、密码安全审计员、密码操作员职责互相制约互相监督，其中密码安全审计员不可兼任密钥管理员、密码操作员。
——相关设备与系统的管理和使用账号、动态令牌、个人数字证书不得多人共用。
——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。
c) 建立上岗人员培训制度：第二级、第三级、第四级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，对培训效果进行考核，确保其具备岗位所需专业技能，并保存培训和考核记录。
d) 定期进行安全岗位人员考核：第三级、第四级应建立关键人员考核制度，定期对密码应用安全岗位人员进行考核，并保存考核记录。
e) 建立关键岗位人员保密制度和调离制度：第一级、第二级、第三级、第四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，保存保密合同和人员调离记录，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，收回相应的密码产品或设备，例如智能密码钥匙、动态令牌等，保存并及时更新资产台账。

7.7 建设运行

使用密码技术的金融行业信息系统应符合以下建设运行管理要求。
a) 制定密码应用方案：第一级、第二级、第三级、第四级应依据密码相关标准和密码应用需求，制定密码应用方案，密码应用方案模板见附录 D。
b) 制定密钥安全管理策略：第一级、第二级、第三级、第四级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，各环节密钥生存周期管理见附录 E。
c) 制定实施方案：第一级、第二级、第三级、第四级应按照密码应用方案制定密码应用实施方案，依据密码应用实施方案实施建设。
d) 投入运行前进行密码应用安全性评估：投入运行前，第一级可/第二级宜/第三级、第四级应进行商用密码应用安全性评估。
e) 定期开展密码应用安全性评估及攻防对抗演习：第三级、第四级在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展商用密码应用安全性评估及攻防对抗演习，并根据评估结果制定整改方案进行整改。

7.8 应急处置

使用密码技术的金融行业信息系统应符合以下应急处置管理要求。
a) 应急策略：
——第一级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。
——第二级、第三级、第四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。
b) 应急策略培训与演练：第二级、第三级、第四级应定期对系统相关人员进行密码应用应急策略培训，并进行密码应用应急策略的演练。
c) 事件处置：事件发生后，第二级、第三级、第四级应及时向行业主管部门及归属的密码管理部门进行报告。
d) 向有关主管部门上报处置情况：事件处置完成后，第二级、第三级、第四级应及时向行业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。

e）应急策略修订与完善：第二级、第三级、第四级应结合密码应用安全事件处置情况，定期对密码应用应急策略进行修订和完善。

附 录 A
（资料性）
金融行业重要信息系统密码应用设计示例

A.1 概述

金融行业重要信息系统包含银行业、证券期货业、保险业等重要信息系统，例如，银行业重要信息系统包含网上银行系统、综合前置系统、银行核心系统、银企直连系统、中间业务系统等业务系统，以及银行清算系统、国库系统、法定数字货币系统等金融信息基础设施，网上银行系统通过浏览器、移动终端客户端程序等线上渠道开展银行业务，综合前置系统通过柜面、ATM终端、POS机具、自助终端等线下渠道开展银行业务，银企直连系统实现银行与外部企业等机构之间的银行业务处理，中间业务系统与外部证券公司、基金公司、保险公司等外部机构系统交互实现代销基金、代理保险等业务处理。银行业重要信息系统示意如图A.1所示。

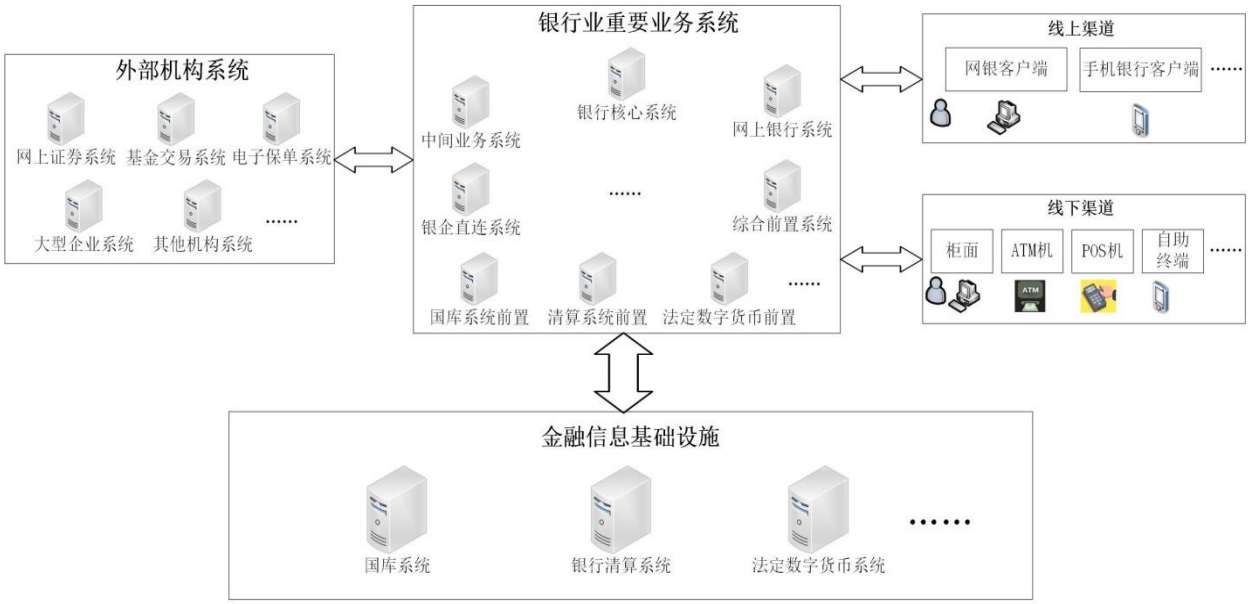

图 A.1 银行业重要信息系统示意图

金融业重要信息系统具有交易流程复杂、业务连续性要求高、安全要求强等特点，其密码应用也呈现出复杂性、多样性和高安全性等特点。下面围绕信息系统网络和通信安全、设备和计算安全、应用和数据安全层面主要密码应用功能点，介绍网上银行系统密码应用设计示例。

注：金融行业其他重要信息系统密码应用设计示例详见全国金融标准化技术委员会官方网站（https://www.cfstc.org/）下载专区“金融行业信息系统密码应用设计示例”。

A.2 网上银行系统密码应用设计示例

网上银行系统是银行业金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供网上金融服务的系统。网上银行系统主要由客户端、通信网络和服务端组成，并可通过不同类型的通信网络连接到外部其他行业机构系统，开展各类合作业务。在银行业金融机构内部，网上银行系统与银行核心系统等内部系统进行交互完成业务处理。本示例网上银行系统参照JR/T 0068，但不包括银企直连系统。网上银行系统关键密码应用需求如表A.1所示。

表 A.1　网上银行系统关键密码应用需求

序号	安全区域	密码应用功能点	密码应用需求分析
1	网上银行系统客户端与服务端之间	客户端用户的身份鉴别	对通过浏览器、客户端程序等方式登录或访问网上银行系统的用户进行身份标识和鉴别，并对执行关键交易操作的用户进行身份鉴别，防止非法人员假冒用户身份。
2		敏感数据传输机密性	对客户端与服务端之间传输的敏感数据进行机密性保护，防止数据被非法窃取。
3		敏感数据传输完整性	对客户端与服务端之间传输的敏感数据进行完整性保护，防止数据被非法篡改。
4		用户关键交易不可否认	实现用户在客户端关键交易操作的不可否认，防止用户事后否认交易行为。
5		通信实体身份鉴别	对客户端与服务端之间通信链路进行保护，实现网络通信实体的身份鉴别、通信过程敏感数据的机密性保护和通信数据的完整性保护。
6		通信过程敏感数据机密性	
7		通信数据完整性	
8	网上银行系统与外部系统之间	系统之间身份鉴别	对访问网上银行系统的外部系统进行身份鉴别，确保外部系统身份的真实性，同时，网上银行系统也需要向外部系统证明其身份的真实性。
9		敏感数据传输机密性	对网上银行系统与外部系统之间传输的敏感数据进行机密性保护，防止数据被非法窃取。
10		敏感数据传输完整性	对网上银行系统与外部系统之间传输的敏感数据进行完整性保护，防止数据被非法篡改。
11		系统关键交易不可否认	实现网上银行系统与外部系统之间关键交易的不可否认，防止事后否认交易行为。
12		通信实体身份鉴别	对网上银行系统与外部系统之间通信链路进行保护，实现网络通信实体的身份鉴别、通信过程敏感数据的机密性保护和通信数据的完整性保护。
13		通信过程敏感数据机密性	
14		通信数据完整性	
15	运维管理终端与设备之间	登录设备用户的身份鉴别	对通过运维管理终端登录设备进行管理的用户进行身份鉴别，确保用户身份的真实性。
16		运维管理通道安全	对运维管理终端与系统设备之间的管理通道进行保护，实现管理通道中敏感数据传输的机密性和完整性，防止数据被非法窃取或篡改。
17		关键运维操作不可否认	实现系统运维管理中关键操作的不可否认，防止运维人员事后否认操作行为。
18	网上银行系统客户端	敏感数据存储机密性	对网上银行系统客户端存储的敏感数据进行机密性保护，防止数据被非法窃取。
19		敏感数据存储完整性	对网上银行系统客户端存储的敏感数据进行完整性保护，防止数据被非法篡改。
20	网上银行系统服务端	敏感数据存储机密性	对网上银行系统服务端存储的敏感数据进行机密性保护，防止数据被非法窃取。
21		敏感数据存储完整性	对网上银行系统服务端存储的敏感数据进行完整性保护，防止数据被非法篡改。

根据网上银行系统关键密码应用需求分析，采用密码技术实现系统相应密码应用功能点，网上银行系统密码应用部署示例如图A.2所示。

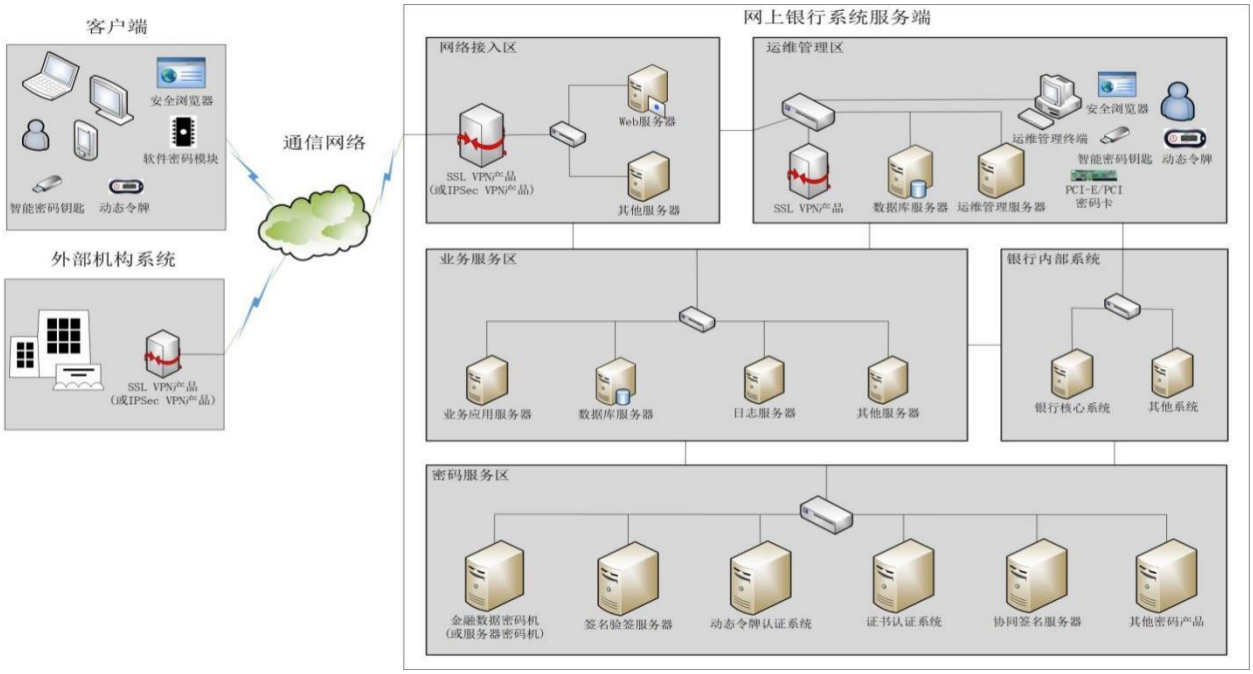

图 A.2　网上银行系统密码应用部署示例

根据网上银行系统密码应用部署示例，网上银行系统密码应用设计如表A.2所示。

表 A.2　网上银行系统密码应用设计

序号	安全区域	密码应用功能点	密码应用设计说明
1	网上银行系统客户端与服务端之间	客户端用户的身份鉴别	具体密码应用设计可使用如下 2 种方式之一。 a) 为用户配备智能密码钥匙（内置用户数字证书），或在客户端程序内置协同签名客户端密码模块（内置用户数字证书）等，服务端使用签名验签服务器、协同签名服务器等，通过基于公钥密码算法的数字签名技术对用户登录数据和关键交易数据进行签名和签名的验证（以下简称验签），实现用户登录和关键交易的身份鉴别。 b) 为客户端用户配备动态令牌，服务端部署动态令牌认证系统，通过基于商用密码算法的动态口令机制，实现用户登录和用户关键交易的身份鉴别。
2		敏感数据传输机密性	客户端通过智能密码钥匙或密码加密类密码模块等，服务端使用金融数据密码机或服务器密码机等，通过对称密码算法或公钥密码算法加密和解密技术，实现客户端和服务端之间传输敏感数据的机密性保护。
3		敏感数据传输完整性	客户端使用智能密码钥匙或密码加密类密码模块等，服务端使用金融数据密码机、服务器密码机或签名验签服务器等，通过基于对称密码算法或密码杂凑算法的MAC技术、基于公钥密码算法的数字签名技术等，实现客户端和服务端之间传输敏感数据的完整性保护。
4		用户关键交易不可否认	客户端用户使用智能密码钥匙（内置用户数字证书），或在客户端程序内置协同签名客户端密码模块（内置用户数字证书）等，服务端使用签名验签服务器、协同签名服务器等，通过基于公钥密码算法的数字签名技术对用户关键交易数据进行签名和验签，实现用户关键交易不可否认。
5		通信实体身份鉴别	客户端部署安全浏览器密码模块或内置密码协议类密码模块等，服务端网络边界部署SSL VPN产品等，双方基于密码协议建立安全通信链路，实现通信实体的身份鉴别、通信过程敏感数据的机密性保护和通信数据完整性保护。
6		通信过程敏感数据机密性	
7		通信数据完整性	
8			

表 A.2　网上银行系统密码应用设计（续）

序号	安全区域	密码应用功能点	密码应用设计示例
9	网上银行系统与外部系统之间	系统之间身份鉴别	网上银行系统使用签名验签服务器（内置系统数字证书）等，通过基于公钥密码算法的数字签名技术对通信报文进行签名和验签，实现系统之间身份鉴别。
10		敏感数据传输机密性	网上银行系统使用金融数据密码机或服务器密码机等，通过对称密码算法或公钥密码算法加密和解密技术，实现网上银行系统和外部系统之间传输敏感数据的机密性保护。
11		敏感数据传输完整性	网上银行系统使用金融数据密码机、服务器密码机或签名验签服务器等，通过基于对称密码算法或密码杂凑算法的MAC技术、基于公钥密码算法的数字签名技术等，实现系统之间传输敏感数据的完整性保护。
12		系统关键交易不可否认	网上银行系统使用签名验签服务器（内置系统数字证书）等，通过基于公钥密码算法的数字签名技术对系统关键交易数据进行签名和验签，实现系统之间关键交易的不可否认。
13		通信实体身份鉴别	网上银行系统网络边界部署SSL VPN产品（或IPSec VPN产品）等，外部系统网络边界部署SSL VPN产品（或IPSec VPN产品）等，双方基于密码协议建立安全通信链路，实现系统之间网络通信实体的身份鉴别、通信过程敏感数据的机密性保护和通信数据的完整性保护。
14		通信过程敏感数据机密性	
15		通信数据完整性	
16	运维管理终端与设备之间	登录设备用户的身份鉴别	具体密码应用设计可使用如下 2 种方式之一。 a) 为登录设备的用户配备智能密码钥匙(内置用户数字证书）等，运维管理服务端部署签名验签服务器等，通过基于公钥密码算法的数字签名技术对用户登录数据进行签名和验签，实现用户身份鉴别。 b) 为登录设备的用户配备动态令牌,运维管理服务端部署动态令牌认证系统,通过基于商用密码算法的动态口令技术，实现登录设备用户的身份鉴别。
17		运维管理通道安全	在运维管理终端部署安全浏览器密码模块等，运维管理服务端部署SSL VPN产品、PCI-E密码卡或PCI密码卡等，双方基于密码协议建立运维管理安全通道，实现管理通道中敏感数据传输的机密性保护和完整性保护。
18		关键运维操作不可否认	为登录设备的用户配备智能密码钥匙（内置用户数字证书）等，运维管理服务端使用签名验签服务器、PCI-E密码卡或PCI密码卡等，通过基于公钥密码算法的数字签名技术对用户关键运维操作数据进行签名和验签，实现运维管理中用户关键操作的不可否认。
19	网上银行系统客户端	敏感数据存储机密性	客户端使用智能密码钥匙或在客户端程序内置密码加密类密码模块等，通过对称密码算法或公钥密码算法加密和解密技术，实现网上银行系统客户端存储敏感数据的机密性保护。
20		敏感数据存储完整性	客户端使用智能密码钥匙或在客户端程序内置密码加密类密码模块等，通过基于对称密码算法或密码杂凑算法的MAC技术、基于公钥密码算法的数字签名技术等，实现网上银行系统客户端存储敏感数据的完整性保护。
21	网上银行系统服务端	敏感数据存储机密性	服务端使用金融数据密码机或服务器密码机等，通过对称密码算法或公钥密码算法加密和解密技术，实现网上银行系统服务端存储敏感数据的机密性保护。
22		敏感数据存储完整性	服务端使用金融数据密码机、服务器密码机或签名验签服务器等，通过基于对称密码算法或密码杂凑算法的MAC技术、基于公钥密码算法的数字签名技术等，实现网上银行系统服务端存储敏感数据的完整性保护。

附 录 B
（资料性）
不同级别密码应用基本要求汇总

第一级至第四级密码应用基本要求见表B。

表 B 第一级至第四级密码应用基本要求汇总

指标体系			第一级	第二级	第三级	第四级
技术要求	物理和环境安全	身份鉴别	可	宜	宜	应
		电子门禁记录数据存储完整性	可	宜	宜	应
		视频监控记录数据存储完整性	—	可	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	网络和通信安全	身份鉴别	可	宜	应	应
		通信数据完整性	可	可	宜	应
		通信过程敏感数据的机密性	可	宜	应	应
		网络边界访问控制信息的完整性	可	可	宜	应
		安全接入认证	—	—	可	宜
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	设备和计算安全	身份鉴别	可	宜	应	应
		远程管理通道安全	可	宜	应	应
		身份鉴别信息机密性	可	宜	应	应
		系统资源访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		日志记录完整性	可	可	宜	应
		不可否认性	—	可	宜	应
		重要可执行程序完整性和来源真实性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	应用和数据安全	身份鉴别	可	宜	应	应
		客户端程序完整性和来源真实性	—	可	宜	应
		访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		敏感数据传输机密性	可	宜	应	应
		敏感数据存储机密性	可	宜	应	应
		敏感数据传输完整性	可	宜	宜	应
		敏感数据存储完整性	可	宜	宜	应
		不可否认性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
管理要求	管理制度	具备密码应用安全管理制度	应	应	应	应
		密钥管理规则	应	应	应	应
		建立操作规程	应	应	应	应
		定期修订安全管理制度	—	—	应	应
		明确管理制度发布流程	—	—	应	应
		制度执行过程记录留存	—	应	应	应
	人员管理	了解并遵守密码相关法律法规和密码应用安全管理制度	应	应	应	应

表 B　第一级至第四级密码应用基本要求汇总列表（续）

指标体系			第一级	第二级	第三级	第四级
		建立密码应用岗位责任制度	—	应	应	应
		建立上岗人员培训制度	—	应	应	应
		定期进行安全岗位人员考核	—	—	应	应
		建立关键岗位人员保密制度和调离制度	应	应	应	应
	建设运行	制定密码应用方案	应	应	应	应
		制定密钥安全管理策略	应	应	应	应
		制定实施方案	应	应	应	应
		投入运行前进行密码应用安全性评估	可	宜	应	应
		定期开展密码应用安全性评估及攻防对抗演习	—	—	应	应
	应急处置	应急策略	可	应	应	应
		应急策略培训与演练	—	应	应	应
		事件处置	—	应	应	应
		向有关主管部门上报处置情况	—	应	应	应
		应急策略修订与完善	—	应	应	应

附 录 C
（资料性）
JR/T 0071.2 中关于密码应用要求与本文件的对应关系

为指导金融行业信息系统责任单位在网络安全等级保护工作中同步开展商用密码应用安全设计，同时也为有效衔接金融行业网络安全等级测评工作与商用密码应用安全性评估测评工作，避免重复评估和测评，下面以网络安全等级保护四级系统为例，将JR/T 0071.2中关于密码应用要求与本文件的对应关系摘录如表C所示，以下内容仅适用于基于JR/T 0071.2开展测评时参考使用。

表 C JR/T 0071.2 中关于密码应用要求与本文件的对应关系

序号	JR/T 0071.2 中关于密码应用要求内容	本文件对应要求
1	9.1.2.2 a）应采用校验技术或密码技术保证通信过程中数据的完整性，并按照国家密码管理部门与行业有关要求使用密码算法。	6 通用要求 a）、b）、c）。 7.2 b）第四级应采用密码技术保证通信过程中数据的完整性。
2	9.1.2.2 b）应采用密码技术保证通信过程中数据的保密性，并按照国家密码管理部门与行业有关要求使用密码算法。	6 通用要求 a）、b）、c）。 7.2 c）第四级应采用密码技术保证通信过程敏感数据的机密性。
3	9.1.2.2 c）应在通信前基于密码技术对通信的双方进行验证或认证。	6 通用要求 a）、b）、c）。 7.2 a）第四级应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性，通信双方包括但不限于金融行业信息系统与客户端程序、金融行业信息系统与受理终端、金融行业信息系统与外部系统等。
4	9.1.2.2 d）应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。	7.2 f）以上如采用密码服务，第四级应符合GB/T 39786中关于密码服务的要求。 g)以上采用的密码产品，第四级应达到GB/T 37092规定的三级及以上级别安全要求。
5	9.1.4.1 d）当进行远程管理时，应对终端进行身份标识和鉴别，采用密码技术防止鉴别信息在网络传输过程中被窃听。	6 通用要求 a）、b）、c）。 7.3 b）第四级应采用密码技术建立安全的远程管理信息传输通道。
6	9.1.4.1 e）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	6 通用要求 a）、b）、c）。 7.4 a）第四级应采用密码技术对通过客户端程序、浏览器、受理终端、应用程序接口等方式登录或访问应用系统的用户和执行关键交易的用户进行身份鉴别，保证应用系统用户身份的真实性。
7	9.1.4.7 a）应采用密码技术保证敏感数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	6 通用要求 a）、b）、c）。 7.4 g）第四级应采用密码技术保证信息系统应用的敏感数据在传输过程中的完整性。
8	9.1.4.7 b）应采用校验技术或密码技术保证敏感数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	6 通用要求 a）、b）、c）。 7.4 h）第四级应采用密码技术保证信息系统应用的敏感数据在存储过程中的完整性。
9	9.1.4.7 c）在可能涉及法律责任认定的应用中，应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抗抵赖和数据接收行为的抗抵赖。证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录	6 通用要求 a）、b）、c）。 7.4 i）在可能涉及法律责任认定的应用中，第四级应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。

表 C　JR/T 0071.2 中关于密码应用要求内容与本文件的对应关系（续）

序号	JR/T 0071.2 中关于密码应用要求内容	本文件对应要求
9	用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户。	
10	9.1.4.8 a）应采用密码技术保证敏感数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	6 通用要求 a）、b）、c）。 7.4 e）第四级应采用密码技术保证信息系统应用的敏感数据在传输过程中的机密性。
11	9.1.4.8 b）应采用密码技术保证敏感数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护其存储过程中的保密性。	6 通用要求 a）、b）、c）。 7.4 f）第四级应采用密码技术保证信息系统应用的敏感数据在存储过程中的机密性。
12	9.1.9.2 b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。	7.7 a）第四级应依据密码相关标准和密码应用需求，制定密码应用方案，密码应用方案模板见附录 D。
13	9.1.9.3 b）应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。	6 通用要求 c）。
14	9.1.9.7 b）应由项目承担单位（部门）或公正的第三方制订安全测试方案，进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容，并将测试报告报科技部门审查。	7.7 d）投入运行前，第四级应进行商用密码应用安全性评估，评估通过后系统方可正式运行。 e）第四级在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展商用密码应用安全性评估及攻防对抗演习，并根据评估结果制定整改方案进行整改。
15	9.1.10.9 a）应遵循密码相关国家标准和行业标准。	6 通用要求 a）、b）。
16	9.1.10.9 b）选用的密码产品和加密算法应符合国家相关密码管理政策规定，应优先使用国产密码算法。	6 通用要求 a）、b）、c）。
17	9.1.10.9 c）应使用国家密码管理主管部门认证核准的密码技术和产品。	6 通用要求 a）、b）、c）。
18	9.1.10.9 d）应采用硬件密码模块实现密码运算和密钥管理。	7.1 e）以上采用的密码产品，第四级应达到 GB/T 37092 规定的三级及以上级别安全要求。 7.2 g）以上采用的密码产品，第四级应达到 GB/T 37092 规定的三级及以上级别安全要求。 7.3 j）以上采用的密码产品，第四级应达到 GB/T 37092 规定的三级及以上级别安全要求。 7.4 k）以上采用的密码产品，第四级应达到 GB/T 37092 规定的三级及以上级别安全要求。
19	9.1.10.9 e）应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。 h）密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责，密钥资料须保存在保险柜内，保险柜钥匙由专人负责，使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。 j）应支持各类环境中密码设备使用、管理权限分离。	7.5 a）第四级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。 b）第四级应根据密码应用方案建立相应根密钥、对称密钥、非对称密钥等密钥管理规则。 c）第四级应对密钥管理人员或密码设备操作人员执行的日常管理操作建立操作规程。 7.6 b）第四级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。

附 录 D
（资料性）
密码应用方案模板

密码应用方案是信息系统密码应用建设和改造的基础和依据，密码应用方案设计应遵循总体性、科学性、完备性、可行性等原则。密码应用方案应包含但不限于项目背景、系统概述、密码应用需求分析、设计目标及原则、技术方案、安全管理方案、实施保障方案等关键要素，各要素主要内容见表D。

表 D 密码应用方案模板

关键要素	主要内容
项目背景	项目背景应包含但不限于以下内容。 a） 项目实施的国家有关法律、法规要求，以及项目实施的必要性。 b） 系统的建设规划情况，以及与规划有关的前期情况。
系统概述	系统概述应包含但不限于以下内容。 a） 系统基本情况。包含系统名称、项目建设单位情况（名称、地址、所属密码管理部门、单位类型等）、系统上线运行时间、网络安全保护定级（或拟定级）情况、等级保护备案时间及编号、系统用户情况（使用单位、使用人员、使用场景等）等。 b） 系统网络拓扑图及描述。描述系统网络体系架构、网络所在机房情况、网络边界划分、设备组成及实现功能、所采取的安全防护措施等。 c） 承载业务情况。描述系统承载的业务应用、业务功能、信息种类、关键数据类型等。 d） 系统软硬件构成。描述系统服务器、用户终端、网络设备、存储、安全防护设备、密码设备等硬件资源和操作系统、数据库、应用中间件等软件设备资源情况。 e） 管理制度。描述系统管理机构、管理人员、管理职责、管理制度、安全策略等。 f） 密码应用现状分析。描述当前信息系统各安全层面（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）密码应用情况（适用于改造类信息系统）。
密码应用需求分析	密码应用需求分析应包含但不限于以下内容。 a） 根据信息系统面临的风险情况，描述信息系统风险控制需求。 b） 根据信息系统风险控制需求以及确定的密码应用基本要求等级，分析信息系统的密码应用需求。 c） 描述密码应用基本要求在信息系统中不适用部分的原因说明及其替代性安全控制措施。
设计目标及原则	设计目标及原则应包含但不限于以下内容。 a） 描述信息系统密码应用总体设计目标或分阶段设计目标。 b） 描述信息系统密码应用总体设计原则，依据的密码相关政策法规、技术标准或规范。
技术方案	技术方案应包含但不限于以下内容。 a） 密码应用技术框架。描述信息系统密码应用技术框架及框架说明，技术框架应包括密码服务支撑、各安全层面（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）密码应用设计架构等。 b） 物理和环境安全。描述该层面密码保护对象和密码保护措施，包含密码子系统组成和功能、密码产品及其遵循的标准、密码服务、密码算法、密码协议、密码应用工作流程、密钥管理体系与实现等。 c） 网络和通信安全。描述该层面密码保护对象和密码保护措施，包含密码子系统组成和功能、密码产品及其遵循的标准、密码服务、密码算法、密码协议、密码应用工作流程、密钥管理体系与实现等。 d） 设备和计算安全。描述该层面密码保护对象和密码保护措施，包含密码子系统组成和功能、密码产品及其遵循的标准、密码服务、密码算法、密码协议、密码应用工作流程、密钥管理体系与实现等。 e） 应用和数据安全。描述该层面密码保护对象和密码保护措施，包含密码子系统组成和功能、密码产品及其遵循的标准、密码服务、密码算法、密码协议、密码应用工作流程、密钥管理体系与实现等。 f） 密钥管理。描述信息系统中各密钥生存周期涉及的密钥管理方案和使用的独立密钥管理

表 D　密码应用方案模板（续）

关键要素	主要内容
	设备或设施（若有）。 g） 密码服务支撑设计。描述密码应用和密码服务功能提供模式、密码设备部署情况、应用系统调用密码设备的方式。密码设备部署设计包含设备选型原则、软硬件设备清单（包括已有的密码产品清单）、部署示意图及说明等。 h） 安全与合规性分析。对政策法规、标准规范的符合程度进行自评价。针对相应等级密码应用基本要求的每一项的符合性进行自评价（符合或不适用），对于不适用项，描述不适用原因（比如环境约束、业务条件约束、经济社会稳定性等），并说明采用了何种替代性风险控制措施来达到等效控制。
安全管理方案	安全管理方案应包含但不限于以下内容。 a） 信息系统密码安全制度方面采取的管理措施。 b） 信息系统密码安全人员方面采取的管理措施。 c） 信息系统密码安全实施方面采取的管理措施。 d） 信息系统密码安全应急方面采取的管理措施。
实施保障方案	实施保障方案应包含但不限于以下内容。 a） 实施内容。描述项目实施对象的边界及密码应用的范围、任务要求等，分析项目实施的重难点问题，描述实施过程中可能存在的风险点及应对措施。实施内容包含采购、软硬件开发或改造、系统集成、综合调试、试运行等。 b） 实施计划。按照施工进度计划确定实施步骤，分阶段描述任务分工、实施主体、项目建设单位、阶段交付物等，实施计划包含实施路线图、进度计划、重要节点等。 c） 保障措施。描述项目实施过程中的组织保障、人员保障、经费保障、质量保障、监督检查等措施。 d） 经费概算。描述密码应用项目建设和产生的相关费用概算，应包含新增的密码产品名称及数量、密码服务类型及数量等。

附 录 E
（资料性）
密钥生存周期管理

E.1 概述

密钥管理对于保证密钥全生存周期的安全性是至关重要的，可以保证密钥（除公钥外）不被非授权的访问、使用、泄露、篡改和替换，可以保证公钥不被非授权的篡改和替换。信息系统的应用和数据层面的密钥体系由业务系统根据密码应用需求在密码应用方案中明确，并在密码应用实施中落实。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。以下给出各个环节的密钥管理建议供参考。

E.2 密钥产生

密钥可以以随机产生、协商产生等不同的方式来产生。密钥在符合GB/T 37092的密码产品中产生是十分必要的，产生的同时可在密码产品中记录密钥关联信息，包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等。

E.3 密钥分发

密钥分发是密钥从一个密码产品传递到另一个密码产品的过程，分发时要注意抗截取、篡改、假冒等攻击，保证密钥的机密性、完整性以及分发者、接收者身份的真实性等。

E.4 密钥存储

密钥不以明文方式存储在密码产品外部是十分必要的，并采取严格的安全防护措施，防止密钥被非授权的访问或篡改。

公钥是例外，可以以明文方式在密码产品外存储、传递和使用，但有必要采取安全防护措施，防止公钥被非授权篡改或替换。

E.5 密钥使用

每个密钥一般只有单一的用途，明确用途并按用途正确使用是十分必要的。密钥使用环节需要注意的安全问题是：使用密钥前获得授权、使用公钥证书前对其进行有效性验证、采用安全措施防止密钥的泄露和替换等。另外，有必要为密钥设定更换周期，并采取有效措施保证密钥更换时的安全性。

E.6 密钥更新

密钥更新发生在密钥超过使用期限、已泄露或存在泄露风险时，根据相应的更新策略进行更新。

E.7 密钥归档

如果信息系统中有密钥归档需求，则根据实际安全需求采取有效的安全措施，保证归档密钥的安全性和正确性。需要注意的是，归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。如果执行密钥归档，则有必要生成审计信息，包括归档的密钥、归档的时间等。

E.8 密钥撤销

密钥撤销一般针对公钥证书所对应的密钥。当证书到期后，密钥自然撤销。也可以按需进行密钥撤销，撤销后的密钥具备使用效力。

E.9 密钥备份

对于需要备份的密钥，采用安全的备份机制对密钥进行备份是必要的，以确保备份密钥的机密性和完整性，这与密钥存储的要求是一致的。密钥备份行为是审计涉及的范围，有必要生成审计信息，包括备份的主体、备份的时间等。

E.10 密钥恢复

可以支持用户密钥恢复和司法密钥恢复。密钥恢复行为是审计涉及的范围，有必要生成审计信息，包括恢复的主体、恢复的时间等。

E.11 密钥销毁

密钥销毁要注意的是销毁过程的不可逆，即无法从销毁结果中恢复原密钥。

参 考 文 献

[1] GM/T 0070 电子保单密码应用技术要求
[2] JR/T 0223 金融数据安全 数据生命周期安全规范
[3]《商用密码产品认证目录（第一批）》(国家市场监督管理总局 国家密码管理局公告2020年第23号公布).2020-05-09
[4]《商用密码产品认证目录（第二批）》(国家市场监督管理总局 国家密码管理局公告2022年第24号公布).2022-07-13