ICS 03.060
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0256—2022

金融行业信息系统商用密码应用 测评要求

Information system commercial cryptography application of financial industry—Testing and evaluation 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、深圳证券交易所、中国期货业协会。

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、屈龑浩、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、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、居红伟、艾青。

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》。

金融行业信息系统商用密码应用　测评要求

1　范围

本文件规定了金融行业信息系统不同等级密码应用的测评要求，从密码算法合规性、密码技术合规性、密码产品合规性、密码服务合规性和密钥管理安全性方面，提出了第一级到第五级的密码应用通用测评要求；从金融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密码应用技术的测评要求；从管理制度、人员管理、建设运行和应急处置4个管理方面提出了第一级到第四级密码应用管理的测评要求。同时规定了整体测评、风险分析和评价、测评结论等测评环节的要求。

本文件适用于指导、规范金融行业信息系统在规划、建设、运行环节的商用密码应用安全性评估工作。

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 15843.2　信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制
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 15843.4　信息技术　安全技术　实体鉴别　第4部分：采用密码校验函数的机制
GB/T 20518　信息安全技术　公钥基础设施　数字证书格式
GB/T 36968　信息安全技术　IPSec　VPN技术规范
GB/T 37092　信息安全技术　密码模块安全要求
GB/T 38540　信息安全技术　安全电子签章密码技术规范
GB/T 38556　信息安全技术　动态口令密码应用技术规范
GB/T 39786　信息安全技术　信息系统密码应用基本要求
GM/T 0024　SSL　VPN技术规范
GM/T 0027　智能密码钥匙技术规范
GM/T 0037　证书认证系统检测规范
GM/T 0038　证书认证密钥管理系统检测规范
GM/T 0115　信息系统密码应用测评要求
JR/T 0255　金融行业信息系统商用密码应用　基本要求
GM/Z 4001　密码术语

3　术语和定义

JR/T 0255《金融行业信息系统商用密码应用　基本要求》和GM/Z 4001《密码术语》中界定的以及下列术语和定义适用于本文件。

3.1

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

商用密码应用安全性评估机构中从事商用密码应用安全性评估的人员（以下简称密评人员）。

[来源：GM/T 0115，3.1，有修改]

3.2

核查 examine

密评人员对测评对象进行观察、查验和分析，以理解、澄清或取得证据的过程。
[来源：GM/T 0115，3.2，有修改]

3.3

SM2 算法 SM2 algorithm

1 种椭圆曲线公钥密码算法。
注：该算法密钥长度为 256 比特。
[来源：GM/Z 4001，2.118，有修改]

3.4

SM3 算法 SM3 algorithm

1 种密码杂凑算法。
注：该算法输出为 256 比特。
[来源：GM/Z 4001，2.119，有修改]

3.5

SM4 算法 SM4 algorithm

1 种分组密码算法。
注：该算法分组长度为 128 比特，密钥长度为 128 比特。
[来源：GM/Z 4001，2.120，有修改]

4 缩略语

下列缩略语适用于本文件。
APDU：应用协议数据单元（Application Protocol Data Unit）
ECC：椭圆曲线密码算法（Elliptic Curve Cryptography Algorithm）
IBC：标识密码算法（Identity—Based Cryptography）
IC：集成电路（Integrated Circuit）
IPSec：互联网安全协议（Internet Protocol Security）
MAC：消息验证码（Message Authentication Code）
PIN：个人识别号（Personal Identification Number）
SSL：安全套接层（Secure Sockets Layer）
TCP：传输控制协议（Transmission Control Protocol）
UDP：用户数据报协议（User Datagram Protocol）
VPN：虚拟专用网络（Virtual Private Network）

5 概述

本文件根据JR/T 0255，将金融行业信息系统密码应用测评要求分为通用测评要求和密码应用测评要求。第6章通用测评要求不单独实施，也不单独体现在密评报告的单元测评结果和整体测评结果中，仅供第7章密码应用测评要求在测评实施时使用。密评人员在对金融行业信息系统中密码产品或密码应用功能进行测评实施时，可参考附录A典型密码产品应用测评技术及附录B典型密码功能测评技术。

本文件中测评单元由测评指标、测评对象、测评实施和结果判定组成，具体内容如下。

a) 测评指标：来源于 JR/T 0255 各要求项，括号中文字注明了指标适用的密码应用安全等级。
b) 测评对象：信息系统密码应用测评的具体对象。
c) 测评实施：针对某个测评指标，描述了信息系统密码应用的测评要点。
d) 结果判定：根据测评实施获取的证据，判定信息系统的密码应用是否满足某个测评指标要求的方法和原则。

若测评单元涉及2个及以上测评对象，则每个测评对象需要分别进行测评实施和结果判定。测评单元的结果由该单元涉及的所有测评对象的测评实施结果汇总得出。

对于JR/T 0255中“可”“宜”“应”的条款，按照如下方法确定是否将其纳入测评范围。

a) 对于“可”的条款，由金融行业信息系统责任单位自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第7章相应的测评要求进行测评和结果判定。否则，该测评指标为“不适用”。

b) 对于“宜”的条款，密评人员应根据金融行业信息系统的密码应用方案和方案评估意见决定是否纳入标准符合性测评范围。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“宜”的条款应纳入标准符合性测评范围。

——若纳入测评范围，则密评人员应按照第7章相应的测评要求进行测评和结果判定。

——若未纳入标准符合性测评范围，密评人员应核查风险控制措施的使用条件和落实情况，若均符合密码应用方案和方案评估意见，则该测评指标判定为“不适用”，并在密码应用安全性评估报告中体现核实的过程和结果。若不满足使用条件，则应按照第7章相应的测评要求进行测评和结果判定。

c) 对于“应”的条款，密评人员应按照第7章相应的测评指标要求进行测评和结果判定。若根据金融行业信息系统的密码应用方案和方案评审意见，信息系统不存在与某项测评指标或某些测评指标相关的密码应用需求，则相应测评指标判定为“不适用”。

针对某项测评指标，若密码应用方案要求高于信息系统相应等级密码应用要求，则应按照密码应用方案要求进行测评，例如安全保护等级为第三级的信息系统，选取了第四级密码应用基本要求的相关指标，上述特殊情况的测评实施应体现在密评报告中。

金融行业信息系统密码应用测评的最终输出是密评报告，在报告中应给出各个测评单元的测评结果、整体测评结果以及在进行风险分析和评价后得出的测评结论。其中，整体测评结果是以测评单元的判定结果为基础，经过单元间、层面间测评相互弥补后得出的结果。风险分析和评价是针对整体测评结果中的不符合项和部分符合项，分析和判断安全问题被威胁利用后对信息系统造成影响的程度。测评结论取决于综合得分以及风险分析和评价，表明了信息系统密码应用与相应等级密码应用基本要求的符合程度。

6 通用测评要求

6.1 密码算法合规性

密码算法合规性的具体测评单元如下。

a) 测评指标：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规定。

b) 测评对象：金融行业信息系统中的密码产品、密码服务以及密码算法实现。

c) 测评实施：了解系统使用的密码算法的名称、用途、执行设备及其实现方式（软件、硬件或固件）等，核查密码算法是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意使用的证明文件。

d) 结果判定：本单元测评指标不单独判定符合性。

6.2 密码技术合规性

密码技术合规性的具体测评单元如下。

a) 测评指标：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规定。

b) 测评对象：金融行业信息系统中的密码产品、密码服务以及密码技术实现。

c) 测评实施：核查系统所使用的密码技术是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意使用的证明文件。

d) 结果判定：同6.1d)。

6.3 密码产品合规性

密码产品合规性的具体测评单元如下。

a) 测评指标：金融行业信息系统中使用的密码产品应符合 GB/T 39786 通用要求中关于密码产品的规定。若采用的密码产品遵循密码模块相关标准，则应满足以下要求。
——第二级应达到 GB/T 37092 规定的一级及以上级别安全要求。
——第三级应达到 GB/T 37092 规定的二级及以上级别安全要求。
——第四级应达到 GB/T 37092 规定的三级及以上级别安全要求。
b) 测评对象：金融行业信息系统中的密码产品。
c) 测评实施：了解信息系统中密码产品的型号和版本等配置信息，核查密码产品是否具备合规性证明文件，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。
d) 结果判定：同 6.1d)。

6.4 密码服务合规性

密码服务合规性的具体测评单元如下。
a) 测评指标：金融行业信息系统中使用的密码服务应符合 GB/T 39786 通用要求中关于密码服务的规定。
b) 测评对象：金融行业信息系统中的密码服务。
c) 测评实施：核查信息系统中密码服务是否具备合规性证明文件或取得国家密码管理部门同意使用的证明文件。
d) 结果判定：同 6.1d)。

6.5 密钥管理安全性

密钥管理安全性的具体测评单元如下。
a) 测评指标：
——金融行业信息系统的密钥管理采用的密码产品、密码服务应符合 GB/T 39786 通用要求中关于密码产品、密码服务的规定。
——金融行业信息系统的密钥管理应符合 JR/T 0255 附录 E 中关于密钥管理的要求。
b) 测评对象：密钥管理采用的密码产品、密码服务，信息系统密钥管理实现。
c) 测评实施：
——核查密钥管理使用的密码产品、密码服务是否满足第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”的要求。
——核查信息系统中密钥管理实现机制是否正确有效，密钥生存周期管理检查要点见附录 C。
d) 结果判定：同 6.1d)。

7 密码应用测评要求

7.1 物理和环境安全

7.1.1 身份鉴别

身份鉴别的具体测评单元如下。
a) 测评指标：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) 测评对象：金融行业信息系统主机房、灾备机房、运维管理区、重要设备存放区等重要区域及其电子门禁系统。
c) 测评实施：
——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。
——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查电子门禁系统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区域进入人员进行身份鉴别，并验证人员身份真实性的实现机制是否正确和有效。

d) 结果判定：

——针对单个测评对象，如果均符合以上测评实施内容，则该测评对象符合本单元的测评指标要求。如果测评实施第3项为否，则不符合本单元的测评指标要求。否则，该测评对象部分符合本单元的测评指标要求。

——针对本测评单元，对该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。

7.1.2 电子门禁记录数据存储完整性

电子门禁记录数据存储完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行业信息系统主机房、灾备机房、运维管理区、重要设备存放区等重要区域及其电子门禁系统。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的MAC机制、基于公钥密码算法的数字签名机制等密码技术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。

d) 结果判定：同7.1.1d)。

7.1.3 视频监控记录数据存储完整性

视频监控记录数据存储完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行业信息系统主机房、灾备机房、运维管理区、重要设备存放区等重要区域及其视频监控系统。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的MAC机制、基于公钥密码算法的数字签名机制等密码技术对视频监控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。

d) 结果判定：同7.1.1d)。

7.2 网络和通信安全

7.2.1 身份鉴别

身份鉴别的具体测评单元如下。

a) 测评指标：

——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) 测评对象：金融业信息系统与客户端程序、受理终端、外部系统等网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的 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，并验证通信实体身份真实性的实现机制是否正确和有效。

d) 结果判定：同 7.1.1d)。

7.2.2 通信数据完整性

通信数据完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融业信息系统与客户端程序、受理终端、外部系统等网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的 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。

d) 结果判定：同 7.1.1d)。

7.2.3 通信过程敏感数据的机密性

通信过程敏感数据的机密性具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融业信息系统与客户端程序、受理终端、外部系统等网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——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。

d) 结果判定：同 7.1.1d)。

7.2.4 网络边界访问控制信息的完整性

网络边界访问控制信息的完整性具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融业信息系统与客户端程序、受理终端、外部系统等网络边界外建立的网络通信信道，以及提供网络边界访问控制功能的设备或组件、密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的MAC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。

d) 结果判定：同7.1.1d)。

7.2.5 安全接入认证

安全接入认证的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行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。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的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，并验证安全接入认证机制是否正确和有效。

d) 结果判定：同7.1.1d)。

7.3 设备和计算安全

7.3.1 身份鉴别

身份鉴别的具体测评单元如下。

a) 测评指标：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) 测评对象：通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供身份鉴别功能和加解密功能的密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——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MAC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的实现机制是否正确和有效。

d) 结果判定：同7.1.1d)。

7.3.2 远程管理通道安全

远程管理通道安全的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供安全的信息传输通道的密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——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密码技术实现机制是否正确和有效。

d) 结果判定：同 7.1.1d)。

7.3.3 身份鉴别信息机密性

身份鉴别信息机密性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供机密性保护功能的密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用密码技术的加解密功能对传输和存储的用户身份鉴别信息进行机密性保护，并验证用户身份鉴别信息机密性保护机制是否正确和有效。

d) 结果判定：同 7.1.1d)。

7.3.4 系统资源访问控制信息完整性

系统资源访问控制信息完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的 MAC 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。

d) 结果判定：同 7.1.1d)。

7.3.5 重要信息资源安全标记完整性

重要信息资源安全标记完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的MAC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。

d) 结果判定：同7.1.1d)。

7.3.6 日志记录完整性

日志记录完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的MAC机制、基于公钥密码算法的数字签名机制等密码技术对涉及身份鉴别、远程管理和操作、审计管理等设备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。

d) 结果判定：同7.1.1d)。

7.3.7 不可否认性

不可否认性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供不可否认性功能的密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统设备运维管理中是否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，并验证不可否认性实现机制是否正确和有效。

d) 结果判定：同7.1.1d)。

7.3.8 重要可执行程序完整性和来源真实性

重要可执行程序完整性和来源真实性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护和来源真实性保护功能的密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的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可执行程序进行完整性保护，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对重要可执行程序来源真实性进行验证，并验证重要可执行程序的完整性保护机制及其来源真实性实现机制是否正确和有效。

d) 结果判定：同7.1.1d)。

7.4 应用和数据安全

7.4.1 身份鉴别

身份鉴别的具体测评单元如下。

a) 测评指标：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) 测评对象：金融行业信息系统业务应用，以及提供身份鉴别功能的密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用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，并验证身份真实性的实现机制是否正确和有效。

d) 结果判定：同7.1.1d)。

7.4.2 客户端程序完整性和来源真实性

客户端程序完整性和来源真实性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行业信息系统客户端程序，以及提供完整性保护和来源真实性功能的密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查是否采用基于对称密码算法或密码杂凑算法的MAC机制、基于公钥密码算法的数字签名机制等密码技术对金融行业信息系统客户端程序进行完整性保护，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对重要可执行程序来源真实性进行验证，并验证客户端程序的完整性保护机制及其来源真实性实现机制是否正确和有效。

d) 结果判定：同7.1.1d)。

7.4.3 访问控制信息完整性

访问控制信息完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行业信息系统业务应用，以及提供完整性保护功能的密码产品。

c) 测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用是否采用基于对称密码算法或密码杂凑算法的MAC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。

d）结果判定：同7.1.1d)。

7.4.4 重要信息资源安全标记完整性

重要信息资源安全标记完整性的具体测评单元如下。

a）测评指标：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。

b）测评对象：金融行业信息系统业务应用，以及提供完整性保护功能的密码产品。

c）测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用是否采用基于对称密码算法或密码杂凑算法的MAC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。

d）结果判定：同7.1.1d)。

7.4.5 敏感数据传输机密性

敏感数据传输机密性的具体测评单元如下。

a）测评指标：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。

b）测评对象：金融行业信息系统业务应用，以及提供机密性保护功能的密码产品。

c）测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用是否采用密码技术的加解密功能对敏感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。

d）结果判定：同7.1.1d)。

7.4.6 敏感数据存储机密性

敏感数据存储机密性的具体测评单元如下。

a）测评指标：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。

b）测评对象：金融行业信息系统业务应用，以及提供机密性保护功能的密码产品。

c）测评实施：

——核查是否符合第6章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第6章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用是否采用密码技术的加解密功能对敏感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。

d）结果判定：同7.1.1d)。

7.4.7 敏感数据传输完整性

敏感数据传输完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行业信息系统业务应用，以及提供完整性保护功能的密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用是否采用基于对称密码算法或密码杂凑算法的 MAC 机制、基于公钥密码算法的数字签名机制等密码技术对敏感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。

d) 结果判定：同 7.1.1d)。

7.4.8 敏感数据存储完整性

敏感数据存储完整性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行业信息系统业务应用，以及提供完整性保护功能的密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用是否采用基于对称密码算法或密码杂凑算法的 MAC 机制、基于公钥密码算法的数字签名机制等密码技术对敏感数据在存储过程进行完整性保护，并验证存储数据完整性保护机制是否正确和有效。

d) 结果判定：同 7.1.1d)。

7.4.9 不可否认性

不可否认性的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：金融行业信息系统业务应用，以及提供不可否认性功能的密码产品。

c) 测评实施：

——核查是否符合第 6 章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求。

——核查是否符合第 6 章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求。

——核查信息系统业务应用是否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，并验证不可否认性实现机制是否正确和有效。

d) 结果判定：同 7.1.1d)。

7.5 管理制度

7.5.1 具备密码应用安全管理制度

具备密码应用安全管理制度的具体测评单元如下。

a) 测评指标：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) 测评对象：安全管理制度类文档。

c）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。

d）结果判定：

——针对单个测评对象，如果均符合以上测评实施内容，则该测评对象符合本单元的测评指标要求。如果不符合测评实施中的核查内容，则该测评对象不符合本单元的测评指标要求。否则，该测评对象部分符合本单元的测评指标要求。

——针对本测评单元，对该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。

7.5.2 建立密钥管理规则

建立密钥管理规则的具体测评单元如下。

a）测评指标：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。

b）测评对象：密码应用方案、密钥管理制度及策略类文档。

c）测评实施：核查是否具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。

d）结果判定：同 7.5.1d）。

7.5.3 建立操作规程

建立操作规程的具体测评单元如下。

a）测评指标：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。

b）测评对象：操作规程类文档。

c）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。

d）结果判定：同 7.5.1d）。

7.5.4 定期修订安全管理制度

定期修订安全管理制度的具体测评单元如下。

a）测评指标：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。

b）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。

c）测评实施：核查是否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以及修订后文档。

d）结果判定：同 7.5.1d）。

7.5.5 明确管理制度发布流程

明确管理制度发布流程的具体测评单元如下。

a）测评指标：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。

b）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。

c）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，是否具有发布流程、格式要求及版本编号等相关内容。

d）结果判定：同 7.5.1d）。

7.5.6 制度执行过程记录留存

制度执行过程记录留存的具体测评单元如下。

a) 测评指标：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。
b) 测评对象：安全管理制度类文档和记录表单类文档。
c) 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。
d) 结果判定：同 7.5.1d)。

7.6 人员管理

7.6.1 了解并遵守密码相关法律法规和密码应用安全管理制度

了解并遵守密码相关法律法规和密码管理制度的具体测评单元如下。

a) 测评指标：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) 测评对象：系统相关人员（包括系统负责人、安全主管人员、密钥管理员、密码审计员、密码操作员等）。
c) 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。
d) 结果判定：同 7.5.1d)。

7.6.2 建立密码应用岗位责任制度

建立密码应用岗位责任制度的具体测评单元如下。

a) 测评指标：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。
b) 测评对象：安全管理制度类文档、系统相关人员（包括系统负责人、安全主管人员、密钥管理员、密码审计员、密码操作员等）。
c) 测评实施：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是否不兼任密钥管理员、密码操作员岗位。核查相关设备与系统的管理和使用账号、动态令牌、个人数字证书是否有多人共用情况。核查密钥管理员和密码操作员是否由本机构的正式人员担任，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。
d) 结果判定：同 7.5.1d)。

7.6.3 建立上岗人员培训制度

建立上岗人员培训制度的具体测评单元如下。

a) 测评指标：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。
b) 测评对象：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、安全主管人员、密钥管理员、密码审计员、密码操作员等）。
c) 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。

d) 结果判定：同 7.5.1d)。

7.6.4 定期进行安全岗位人员考核

定期进行安全岗位人员考核的具体测评单元如下。

a) 测评指标：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。
b) 测评对象：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、安全主管人员、密钥管理员、密码审计员、密码操作员等）。
c) 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是否定期进行岗位人员考核，是否具有近期的考核记录。
d) 结果判定：同 7.5.1d)。

7.6.5 建立关键岗位人员保密制度和调离制度

建立关键岗位人员保密制度和调离制度的具体测评单元如下。

a) 测评指标：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。
b) 测评对象：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、安全主管人员、密钥管理员、密码审计员、密码操作员等）。
c) 测评实施：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，是否具有保密合同和人员调离记录，是否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，是否收回离岗人员的智能密码钥匙、动态令牌等密码设备，是否保存并及时更新资产台账信息。
d) 结果判定：同 7.5.1d)。

7.7 建设运行

7.7.1 制定密码应用方案

制定密码应用方案的具体测评单元如下。

a) 测评指标：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 JR/T 0255 附录 D。
b) 测评对象：密码应用方案。
c) 测评实施：核查在信息系统规划阶段，是否依据密码相关标准和信息系统密码应用需求，制定密码应用方案，并核查方案是否通过评估。
d) 结果判定：同 7.5.1d)。

7.7.2 制定密钥安全管理策略

制定密钥安全管理策略的具体测评单元如下。

a) 测评指标：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 JR/T 0255 附录 E。
b) 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。
c) 测评实施：
——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涉及的密钥种类、体系及其生存周期环节，是否与密码应用方案一致。若信息系统没有相应的密码应用方案，则核查是否根据 JR/T 0255 附录 E 制定密钥管理制度及策略类文档。
——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。
d) 结果判定：同 7.5.1d)。

7.7.3 制定实施方案

制定实施方案的具体测评单元如下。

a) 测评指标：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。
b) 测评对象：密码实施方案。
c) 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。
d) 结果判定：同 7.5.1d)。

7.7.4 投入运行前进行密码应用安全性评估

投入运行前进行密码应用安全性评估的具体测评单元如下。

a) 测评指标：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。
b) 测评对象：密码应用安全性评估报告和系统负责人。
c) 测评实施：
——第一级到第二级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商用密码应用安全性评估报告。
——第三级到第四级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商用密码应用安全性评估报告且系统通过评估。
d) 结果判定：同 7.5.1d)。

7.7.5 定期开展密码应用安全性评估及攻防对抗演习

定期开展密码应用安全性评估及攻防对抗演习的具体测评单元如下。

a) 测评指标：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。
b) 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、攻防对抗演习报告和整改方案。
c) 测评实施：核查信息系统投入运行后，责任单位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，并按照整改方案进行整改。
d) 结果判定：同 7.5.1d)。

7.8 应急处置

7.8.1 应急策略

应急策略的具体测评单元如下。

a) 测评指标：
——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) 测评对象：密码应用应急处置方案和应急处置记录类文档。
c) 测评实施：
——第一级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。
——第二级到第四级核查是否根据密码应用安全事件等级制定了相应的应急处置方案，方案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。若发生过密码应用安全事件，核查是否立即启动应急处置方案并具有相应的处置记录。
d) 结果判定：同 7.5.1d)。

7.8.2 应急策略培训与演练

应急策略培训与演练的具体测评单元如下。

a) 测评指标：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。

b) 测评对象：密码应用应急策略的培训记录和演练记录、系统负责人。
c) 测评实施：核查是否定期组织系统相关人员进行密码应用应急策略培训和演练，是否具有培训记录或演练记录，培训记录是否明确培训对象、培训内容、培训结果等，演练记录是否记录演练时间、主要内容、演练结果等。
d) 结果判定：同 7.5.1d)。

7.8.3 事件处置

事件处置的具体测评单元如下。
a) 测评指标：事件发生后，第二级、第三级、第四级应及时向本行业主管部门及归属的密码管理部门进行报告。
b) 测评对象：密码应用应急处置方案和安全事件报告。
c) 测评实施：核查密码应用安全事件发生后，是否及时向本行业主管部门及归属的密码管理部门进行报告。
d) 结果判定：同 7.5.1d)。

7.8.4 向有关主管部门上报处置情况

向有关主管部门上报处置情况的具体测评单元如下。
a) 测评指标：事件处置完成后，第二级、第三级、第四级应及时向本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。
b) 测评对象：密码应用应急处置方案、安全事件发生情况及处置情况报告。
c) 测评实施：核查密码应用安全事件处置完成后，是否及时向本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，例如事件处置完成后，向相关部门提交安全事件发生情况及处置情况报告。
d) 结果判定：同 7.5.1d)。

7.8.5 应急策略修订与完善

应急策略修订与完善具体测评单元如下。
a) 测评指标：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。
b) 测评对象：密码应用应急策略修订和完善记录和系统负责人。
c) 测评实施：核查是否结合密码应用安全事件处置情况，定期组织对密码应用应急策略进行修订和完善，是否具有密码应用应急策略修订和完善记录。
d) 结果判定：同 7.5.1d)。

8 整体测评要求

8.1 概述

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安全层面内的2个或者2个以上不同测评单元间的关联性进行测评分析，以确定这些关联性对信息系统整体密码应用防护能力的影响。层面间测评是指对不同安全层面之间的2个或者2个以上不同测评单元间的关联性进行测评分析，以确定这些关联性对信息系统整体密码应用防护能力的影响。

8.2 单元间测评

在单元测评完成后，如果信息系统的某个测评单元的结果判定存在不符合或部分符合的情况，应进行单元间测评，重点分析信息系统中是否存在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信息系统密码应用防护能力是否缺失，如果经过综合分析单元测评的不符合项或部分符合项未造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

8.3 层面间测评

在单元测评完成后，如果信息系统的某个测评单元的结果判定存在不符合或部分符合的情况，应进行层面间测评，重点分析信息系统中是否存在层面间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的信息系统密码应用防护能力是否缺失，如果经过综合分析单元测评的不符合项或部分符合项未造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

9 风险分析和评价

风险分析和评价是采用风险分析的方法，针对单元测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断信息系统密码应用在合规性、正确性和有效性方面的不符合所产生的安全问题被威胁利用后对信息系统造成影响的程度，以及受到威胁利用的资产自身价值，综合评价这些不符合项或部分符合项对信息系统造成的安全风险。对于信息系统密码应用中可能出现的高风险项，应结合具体业务场景，并参照信息系统密码应用高风险判定有关规范进行综合判定。

10 测评结论

测评结论是确认信息系统达到相应等级密码应用基本要求的程度，测评结论由单元间测评、层面间测评、量化评估、风险分析和评价后综合判定，其中，量化评估主要依据商用密码应用安全性评估有关量化规则执行。测评结论主要包括以下方面。

a) 符合：信息系统中未发现安全问题，测评结果中所有单元测评结果没有不符合项和部分符合项，综合得分为 100 分。

b) 基本符合：信息系统中存在安全问题，所有单元测评结果中存在不符合项和部分符合项，但存在的安全问题不会导致被测信息系统面临高等级安全风险，且综合得分不低于阈值。

c) 不符合：信息系统中存在安全问题，所有单元测评结果中存在不符合项和部分符合项，而且存在的安全问题会导致被测信息系统面临高等级安全风险，或综合得分低于阈值。

附 录 A
（资料性）
典型密码产品应用测评技术

典型密码产品应用测评技术如表A所示。

表 A 典型密码产品应用测评技术

产品类型	测评实施	预期结果
智能IC卡、智能密码钥匙	测评实施主要包括以下内容。 a) 进行错误尝试试验，验证在智能 IC 卡或智能密码钥匙未使用或错误使用时，相关密码应用过程不能正常工作。 b) 条件允许情况下，在模拟的主机或抽选的主机上安装监控软件，用于对智能 IC 卡、智能密码钥匙的 APDU 指令进行抓取和分析，确认调用指令格式和内容符合预期（例如口令和密钥是加密传输的）。 c) 如果智能 IC 卡或智能密码钥匙存储有数字证书，密评人员可以将数字证书导出后，对证书合规性进行检测，具体检测内容见对证书认证系统应用的测评。 d) 验证智能密码钥匙的口令长度和错误口令登录验证次数是否符合 GM/T 0027 的要求。例如，在 GM/T 0027 中要求，智能密码钥匙的口令长度不小于 6 个字符，错误口令登录验证次数不大于 10 次。	预期结果包括以下内容。 a) 智能 IC 卡或智能密码钥匙未使用或错误使用时，相关密码应用能够检测出非正常使用。 b) 智能 IC 卡、智能密码钥匙调用指令格式和内容符合预期。 c) 数字证书的格式和使用符合证书认证系统应用的有关要求。 d) 智能密码钥匙的口令长度和错误口令登录验证次数符合 GM/T 0027 的要求。
金融数据密码机、服务器密码机	测评实施主要包括以下内容。 a) 利用协议分析工具，抓取应用系统调用金融数据密码机或服务器密码机的指令报文，验证其是否符合预期（例如调用频率是否正常、调用指令是否正确）。 b) 管理员登录金融数据密码机或服务器密码机查看相关配置，检查内部存储的密钥是否对应合规的密码算法，密码计算时是否使用合规的密码算法等。 c) 管理员登录金融数据密码机或服务器密码机查看与密钥管理、密码计算相关的日志文件，检查是否使用合规的密码算法等。	预期结果包括以下内容。 a) 应用系统调用金融数据密码机或服务器密码机指令、次数等符合预期。 b) 金融数据密码机或服务器密码机内部存储的密钥对应合规的密码算法，使用合规的密码算法进行密码计算。 c) 相关的日志记录显示使用合规的密码算法。
IPSec VPN产品、SSL VPN产品	测评实施主要包括以下内容。 a) 利用端口扫描工具，探测 IPSec VPN 产品、SSL VPN 产品所对应的端口服务是否开启，例如 IPSec VPN 产品服务对应的 UDP 500、4500 端口，SSL VPN 产品服务常用的 TCP 443 端口。 b) 利用通信协议分析工具，抓取 IPSec 协议密钥交换阶段、协议握手阶段的数据报文，解析密码算法或密码套件标识是否属于已发布为标准的商用密码算法。例如，GB/T 36968 要求 IPSec 协议 SM4 算法标识为 129（在部分早期 IPSec VPN 产品中该值可能为 127），SM3 算法标识为 20，SM2 算法标识为 2。GM/T 0024 要求 SSL 协议中 ECC_SM4 _SM3 套件标识为{0xe0，0x13}，IBC_SM4_SM3 套件标识为{0xe0，0x17}等。 c) 利用协议分析工具，抓取并解析 IPSec 协议密钥交换阶段、协议握手阶段传输的证书内容，判断证书是否合规，具体检测内容见对证书认证系统应用的测评。	预期结果包括以下内容。 a) 端口扫描显示 IPSec VPN 产品、SSL VPN 产品所对应的端口服务已经开启。 b) 通过通信协议分析工具分析，确认使用的密码算法和密码套件标识属于已发布为标准的商用密码算法。 c) 证书的格式和使用符合证书认证系统应用的有关要求。
安全电子签章系统	测评实施主要包括以下内容。 a) 检查电子印章的验证是否符合 GB/T 38540 的要求，其中部分检测内容可以复用产品检测的结果。 b) 检查电子签章的生成和验证是否符合 GB/T 38540 要求，其中部分检测内容可以复用产品检测的结果。	预期结果包括以下内容。 a) 电子印章的验证符合 GB/T 38540 中相应要求。 b) 电子签章的生成和验证符合 GB/T 38540 相应要求。

表 A　典型密码产品应用测评技术（续）

产品类型	测评实施	预期结果
动态令牌、动态令牌认证系统	测评实施主要包括以下内容。 a) 判断动态令牌的 PIN 码保护机制是否满足 GB/T 38556 的要求。例如，在 GB/T 38556 中要求，PIN 码长度不少于 6 位数字。若 PIN 码输入错误次数超过 5 次，则需至少等待 1 小时才可继续尝试。若 PIN 码输入超过最大尝试次数的情况超过 5 次，则动态令牌将被锁定，不可再使用。 b) 尝试对动态口令进行重放，确认重放后的口令无法通过认证系统的验证。 c) 核查种子密钥是否以密文形式导入动态令牌和认证系统中。	预期结果包括以下内容。 a) 动态令牌的 PIN 码保护机制满足要求。 b) 对动态口令进行重放，重放后的口令无法通过认证系统的验证。 c) 种子密钥是以密文形式导入至动态令牌和认证系统中。
安全门禁系统	测评实施主要包括以下内容。 a) 尝试发一些错误的门禁卡，验证这些卡无法打开门禁。 b) 利用安全门禁系统分发不同权限的门禁卡，验证非授权卡无法打开门禁。	预期结果包括以下内容。 a) 错误的门禁卡无法打开门禁。 b) 不同权限的门禁卡仅能打开授权的门禁，非授权的卡无法打开门禁。
证书认证系统	测评实施主要包括以下内容。 a) 对信息系统内部署证书认证系统，密评人员可参考 GM/T 0037 和 GM/T 0038 的要求进行测评。 b) 通过查看证书扩展项字段，确定证书类型（签名证书或加密证书），并验证证书及其相关私钥是否正确使用。 c) 通过数字证书格式合规性检测工具，验证生成或使用的证书格式是否符合 GB/T 20518 的有关要求。	预期结果包括以下内容。 a) 证书认证系统符合 GM/T 0037 和 GM/T 0038 的要求。 b) 证书及其私钥使用正确。 c) 生成和使用的证书格式符合 GB/T 20518 有关要求。

附 录 B
（资料性）
典型密码功能测评技术

典型密码功能测评技术如表B所示。

表 B 典型密码功能测评技术

密码功能	测评实施	预期结果
传输机密性	测评实施主要包括以下内容。 a) 利用协议分析工具，分析传输的敏感数据是否为密文，数据格式（例如分组长度等）是否符合预期。 b) 如果信息系统以外接密码产品的形式实现传输机密性，例如VPN、密码机等，参考对这些密码产品应用的测评方法。	预期结果包括以下内容。 a) 传输的敏感数据均为密文，数据格式（例如分组长度等）符合预期。 b) 实现传输机密性的外接密码产品符合相应密码产品应用的要求。
存储机密性	测评实施主要包括以下内容。 a) 通过读取存储的敏感数据，判断存储的敏感数据是否为密文，数据格式是否符合预期。 b) 如果信息系统以外接密码产品的形式实现存储机密性，例如密码机、加密存储系统、安全数据库等，参考对这些密码产品应用的测评方法。	预期结果包括以下内容。 a) 存储的敏感数据均为密文，数据格式符合预期。 b) 实现存储机密性的外接密码产品符合相应密码产品应用的要求。
传输完整性	测评实施主要包括以下内容。 a) 利用协议分析工具，分析进行完整性保护的数据在传输时的数据格式（例如签名长度、MAC 长度）是否符合预期。 b) 如果使用数字签名技术实现完整性保护，密评人员可以使用公钥对抓取的签名结果进行验证。 c) 如果信息系统以外接密码产品的形式实现传输完整性，例如VPN、密码机等，参考对这些密码产品应用的测评方法。	预期结果包括以下内容。 a) 完整性保护数据的格式（例如签名长度、MAC 长度）符合预期。 b) 通过数字签名技术实现完整性保护的情况下，使用公钥对签名结果验证通过。 c) 实现传输完整性的外接密码产品符合相应密码产品应用的要求。
存储完整性	测评实施主要包括以下内容。 a) 通过读取存储的敏感数据，分析进行完整性保护的数据在存储时的数据格式（例如签名长度、MAC 长度）是否符合预期。 b) 如果使用数字签名技术实现完整性保护，密评人员可使用公钥对存储的签名结果进行验证。 c) 条件允许的情况下，密评人员可尝试对存储数据进行篡改（例如修改 MAC 或数字签名），验证完整性保护措施是否有效。 d) 如果信息系统以外接密码产品的形式实现存储完整性保护，例如密码机、智能密码钥匙等，参考对这些密码产品应用的测评方法。	预期结果包括以下内容。 a) 受完整性保护的数据在存储时的数据格式（例如签名长度、MAC 长度）符合预期。 b) 通过数字签名技术实现完整性保护的情况下，使用公钥对存储的签名结果验证通过。 c) 对存储数据进行篡改，完整性保护措施能够检测出存储数据的完整性受到破坏。 d) 实现存储完整性的外接密码产品符合相应密码产品应用的要求。
真实性	测评实施主要包括以下内容。 a) 如果信息系统以外接密码产品的形式实现对用户、设备的真实性保护，参考对这些密码产品应用的测评方法。 b) 不能复用密码产品检测结果的情况下，还要查看实体鉴别协议是否符合 GB/T 15843.2、GB/T 15843.3、GB/T 15843.4 等标准要求，特别是对于“挑战—响应”方式的鉴别协议，可以通过协议抓包分析，验证每次挑战值是否不同。 c) 对于基于静态口令的鉴别过程，抓取鉴别过程的数据包，确认鉴别信息不以明文形式传输。对于采用数字签名的鉴别过程，抓取鉴别过程的挑战值和签名结果，使用对应公钥验证签名结果的有效性。 d) 如果鉴别过程使用了数字证书，参考对证书认证系统应用的测评方法。如果未使用证书，则要验证公钥与实体的绑定方	预期结果包括以下内容。 a) 实现真实性保护的外接密码产品符合该密码产品应用的相关要求。 b) 实体鉴别协议符合 GB/T 15843.2、GB/T 15843.3、GB/T 15843.4 等相关要求。 c) 静态口令的鉴别信息以非明文形式传输，对于使用数字签名进行鉴别，公钥验证签名结果通过，并且符合证书认证系统应用的相关要求。 d) 公钥与实体的绑定方式可靠，部署过程安全。

表 B　典型密码功能测评技术（续）

密码功能	测评实施	预期结果
	式是否可靠，实际部署过程是否安全。	
不可否认性	测评实施主要包括以下内容。 a) 如果使用第三方电子认证服务，则应对密码服务进行核查。如果信息系统中部署了证书认证系统，参考对证书认证系统密码应用的测评方法。 b) 使用相应公钥对作为不可否认证据的签名结果进行验证。 c) 如果使用电子签章系统，参考对电子签章系统应用的测评方法。	预期结果包括以下内容。 a) 使用的第三方电子认证密码服务或系统中部署的证书认证系统符合相关要求。 b) 使用相应公钥对不可否认性证据的签名结果的验证结果为通过。 c) 使用的电子签章系统符合电子签章系统应用的相关标准规范要求。

附 录 C
（资料性）
密钥生存周期管理检查要点

C.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。信息系统的应用与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。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检查要点建议，检查结果可用于密码应用测评结果的评判参考。

C.2 密钥产生

密钥产生检查要点具体如下。

a) 检查目的：密钥产生所使用的随机数发生器是否具备合规性证明文件，密钥协商算法是否符合密码相关国家标准或行业标准的要求。
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) 检查要点包括以下内容。
——确认密钥是否在经商用密码认证机构认证合格的密码产品中产生。
——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。
——核实密钥产生功能的正确性和有效性，例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。

C.3 密钥分发

密钥分发检查要点具体如下。

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) 检查要点包括以下内容。
——确认系统内部采用何种密钥分发方式，密钥分发主要有离线分发、在线分发、混合分发几种方式。
——确认密钥传递过程中信息系统使用了哪些密码技术对密钥进行处理以保护其机密性、完整性与真实性，并核实保护措施使用的正确性和有效性。

C.4 密钥存储

密钥存储检查要点具体如下。

a) 检查目的：密钥（除公钥外）存储过程是否保证了不被非授权的访问或篡改，公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) 检查要点包括以下内容。

——确认系统内部所有密钥（除公钥外）是否均以密文形式进行存储，或者位于受保护的安全区域。
——确认密钥（除公钥外）存储过程中信息系统使用了哪些密码技术对密钥进行保护，以确保其机密性、完整性，并核实保护措施的正确性和有效性。
——确认公钥存储过程中信息系统使用了哪些密码技术对公钥进行处理以保护其完整性，并核实保护措施使用的正确性和有效性。

C.5 密钥使用

密钥使用检查要点具体如下。
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和管理。
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) 检查要点包括以下内容。
——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。
——确认信息系统是否具有公钥认证机制，以鉴别公钥的真实性与完整性，公钥密码算法是否符合法律、法规的规定和与密码相关国家标准、行业标准的有关要求。
——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，是否使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漏时，系统是否具备应急处理和响应措施。
——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。

C.6 密钥更新

密钥更新检查要点具体如下。
a) 检查目的：密钥是否会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：确认信息系统内部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，是否会根据相应的更新策略进行密钥更新。

C.7 密钥归档

密钥归档检查要点具体如下。
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) 检查要点包括以下内容。
——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。
——核实归档密钥是否仅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。
——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。

C.8 密钥撤销

密钥撤销检查要点具体如下。
a) 检查目的：公钥证书是否具备撤销机制。

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）检查要点包括以下内容。
——若信息系统内部使用公钥证书，则确认是否有公钥证书撤销机制和撤销机制的触发条件，并确认是否有效执行。
——核实撤销后的密钥是否已不具备使用效力。

C.9 密钥备份

密钥备份检查要点具体如下。
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）检查要点包括以下内容。
——若信息系统内部存在需要归档的密钥，则确认是否具有密钥备份机制并有效执行。
——确认密钥备份过程中系统使用了哪些密码技术对密钥进行处理以保护其机密性、完整性。
——确认密钥备份的审计信息是否包括备份的主体、时间等信息。

C.10 密钥恢复

密钥恢复检查要点具体如下。
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）检查要点包括以下内容。
——确认系统内部是否具有密钥的恢复机制并有效执行。
——确认密钥恢复的审计信息是否包括恢复的主体、时间等信息。

C.11 密钥销毁

密钥销毁检查要点具体如下。
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）检查要点包括以下内容。
——确认系统内部是否具有密钥的销毁机制并有效执行。
——核实密钥销毁过程和销毁方式，确认密钥销毁后是否无法被恢复。

参 考 文 献

[1]《信息系统密码应用高风险判定指引》(中国密码学会密评联委会发布).2021-12
[2]《商用密码应用安全性评估量化评估规则》(中国密码学会密评联委会发布).2021-12
[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第23号).2020-05-09