

密码标准应用指南



密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2020 年 8 月

序 言

密码是网络安全的核心技术和基础支撑。针对已颁布的密码算法及相关技术进行标准化和规范化，是密码技术走向大规模商用的必然需求。

自 2012 年以来，国家密码管理局陆续发布了我国商用密码技术标准，截止目前已发布密码行业标准 93 项（计小项），范围涵盖密码算法、密码协议、密码产品、密码应用、密码检测等多个方面，已经初步形成体系，能够满足我国社会各行业在构建信息安全保障体系时的密码应用需求。自 2015 年起，以全国信息安全标准化技术委员会 WG3 工作组为依托，具有通用性的密码行业标准陆续成为推荐性国家标准，截止目前已发布密码国家标准 35 项（计小项）。

为指导国内各行业对密码标准的正确使用，密码行业标准化技术委员会特编制本指南，根据密码标准体系框架对已颁布的密码标准进行分类阐述。行业信息系统用户在信息安全产品研发或信息系统建设中面临密码应用需求时，可根据本指南并结合自身应用特点，查询该领域适用的密码标准，指导研发和建设工作的正确开展。

密码行业标准化技术委员每年将视该年度密码国家标准和行业标准的发布状况，对本指南进行按需更新，以保持指南的时效性；对于密码标准技术体系框架子类中暂时缺失的标准，将逐步丰富和完善。

目 录

一 密码标准体系框架.....	1
二 密码基础类标准	6
(一) 密码术语与标识	6
1. GM/Z 4001 密码术语	6
2. GB/T 33560 信息安全技术 密码应用标识规范.....	6
(二) 密码算法	8
1. 对称密码算法	8
(1) GB/T 33133 信息安全技术 祖冲之序列密码算法	8
(2) GB/T 32907 信息安全技术 SM4 分组密码算法.....	9
2. 公钥密码算法	11
(1) GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法	11
(2) GM/T 0044 SM9 标识密码算法.....	13
3. 密码杂凑算法	15
(1) GB/T 32905 信息安全技术 SM3 密码杂凑算法	15
(三) 算法设计与应用	16
1. GB/T 35276 信息安全技术 SM2 密码算法使用规范.....	16
2. GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范	17
(四) 密码协议	18
1. GB/T 36968 信息安全技术 IPSec VPN 技术规范.....	18
2. GM/T 0024 SSL VPN 技术规范	20
三 基础设施类标准	22
(一) 公钥基础设施	22
1. GM/T 0014 数字证书认证系统密码协议规范.....	22
2. GB/T 20518 信息安全技术 公钥基础设施 数字证书格式规范.....	24
3. GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范	25
四 密码产品类标准	29
(一) 安全性	29
1. 通用要求	29
(1) GB/T 37092 信息安全技术 密码模块安全要求	29
(二) 设备接口	32
1. 应用编程接口	32
(1) GM/T 0012 可信计算 可信密码模块接口规范	32

(2) GB/T 35291 信息安全技术 智能密码钥匙应用接口规范	33
(3) GB/T 36322 信息安全技术 密码设备应用接口规范	34
(4) GM/T 0056 多应用载体密码应用接口规范	37
(5) GM/T 0058 可信计算 TCM 服务模块接口规范	38
2. 数据格式接口	39
(1) GM/T 0017 智能密码钥匙密码应用接口数据格式规范	39
(三) 设备管理	41
1. GM/T 0050 密码设备管理 设备管理技术规范	41
2. GM/T 0051 密码设备管理 对称密钥管理技术规范	42
3. GM/T 0052 密码设备管理 VPN 设备监察管理规范	43
4. GM/T 0053 密码设备管理 远程监控和合规性检验接口数据规范	44
(四) 技术规范	45
1. GM/T 0027 智能密码钥匙技术规范	45
2. GM/T 0029 签名验签服务器技术规范	47
3. GM/T 0030 服务器密码机技术规范	49
4. GM/T 0045 金融数据密码机技术规范	51
(五) 产品规范	53
1. GM/T 0023 IPsec VPN 网关产品规范	53
2. GM/T 0025 SSL VPN 网关产品规范	54
3. GM/T 0026 安全认证网关产品规范	55
五 应用支撑类标准	57
(一) 通用支撑	57
1. GM/T 0019 通用密码服务接口规范	57
2. GM/T 0020 证书应用综合服务接口规范	58
3. GM/T 0032 基于角色的授权管理与访问控制技术规范	60
4. GM/T 0033 时间戳接口规范	62
5. GM/T 0057 基于 IBC 技术的身份鉴别规范	63
6. GM/T 0067 基于数字证书的身份鉴别接口规范	64
7. GM/T 0068 开放的第三方资源授权协议框架	66
8. GM/T 0069 开放的身份鉴别框架	67
(二) 典型支撑	69
1. GB/T 29829 信息安全技术 可信计算密码支撑平台功能与接口规范	69
六 密码应用类标准	70
(一) 应用要求	70
1. GM/T 0054 信息系统密码应用基本要求	70
(二) 典型应用	73

1. GM/T 0021 动态口令密码应用技术规范	73
2. GM/T 0031 安全电子签章密码技术规范	75
3. GB/T 37033 信息安全技术 射频识别系统密码应用技术要求	76
4. GM/T 0036 采用非接触卡的门禁系统密码应用技术指南	79
5. GM/T 0055 电子文件密码应用技术规范	81
6. GM/T 0070 电子保单密码应用技术要求	82
7. GM/T 0071 电子文件密码应用指南	84
8. GM/T 0072 远程移动支付密码应用技术要求	85
9. GM/T 0073 手机银行信息系统密码应用技术要求	86
10. GM/T 0074 网上银行密码应用技术要求	88
11. GM/T 0075 银行信贷信息系统密码应用技术要求	90
12. GM/T 0076 银行卡信息系统密码应用技术要求	91
13. GM/T 0077 银行核心信息系统密码应用技术要求	93
七 密码检测类标准	94
(一) 随机性检测	94
1. GB/T 32915 信息安全技术 二元序列随机性检测方法	94
2. GM/T 0062 密码产品随机数检测要求	96
(二) 算法与协议检测	97
1. GM/T 0042 三元对等密码安全协议测试规范	97
2. GM/T 0043 数字证书互操作检测规范	98
(三) 产品检测	100
1. 功能检测	100
(1) GM/T 0013 可信密码模块接口符合性测试规范	100
(2) GM/T 0037 证书认证系统检测规范	101
(3) GM/T 0038 证书认证密钥管理系统检测规范	102
(4) GM/T 0040 射频识别标签模块密码检测准则	104
(5) GM/T 0041 智能 IC 卡密码检测规范	106
(6) GM/T 0046 金融数据密码机检测规范	107
(7) GM/T 0047 安全电子签章密码检测规范	109
(8) GM/T 0048 智能密码钥匙密码检测规范	110
(9) GM/T 0049 密码键盘密码检测规范	111
(10) GM/T 0059 服务器密码机检测规范	113
(11) GM/T 0060 签名验签服务器检测规范	115
(12) GM/T 0061 动态口令密码应用检测规范	116
(13) GM/T 0063 智能密码钥匙密码应用接口检测规范	117
(14) GM/T 0064 限域通信(RCC)密码检测要求	118

2. 安全检测	120
(1) GM/T 0008 安全芯片密码检测准则.....	120
(2) GM/T 0039 密码模块安全检测要求.....	121
八 密码管理类标准	122
1. GM/T 0065 商用密码产品生产和保障能力建设规范.....	122
2. GM/T 0066 商用密码产品生产和保障能力建设实施指南.....	124
附录 A. 编号索引	127
附录 B. 金融领域国产密码应用推进中的密码标准适用要求	132

一 密码标准体系框架

密码标准体系框架由三个维度组成，如图 1 所示。其中技术维包含密码基础类标准、基础设施类标准、密码产品类标准、应用支撑类标准、密码应用类标准、密码检测类标准和密码管理类标准七大类密码标准，每一大类又细分若干子类；管理维上，目前主要包含密码国家标准、密码行业标准，未来可能会出现密码团体标准；应用维上，则包含不同的应用领域，如金融行业密码应用、交通行业密码应用、云计算密码应用、物联网密码应用等。

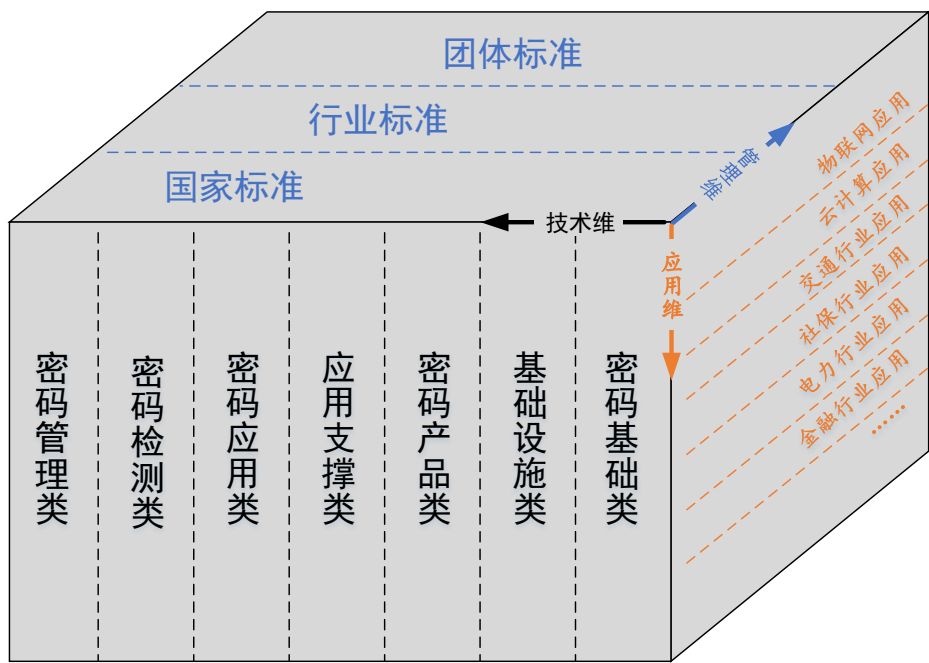


图 1 密码标准体系框架

需要说明的是，如果以应用领域划分，可以形成面向不同应用领域的二维密码应用标准体系，包括技术维和管理维，如金融密码应用标准体系、云计算密码应用标准体系等。所有应用领域的密码应用标准体系在技术维和管理维上是一致的，即任何应用领域的密码应用标

准体系在技术维上都包含七大类，在管理维上也皆可能存在国家标准、行业标准或团体标准。根据具体密码标准在不同应用领域的适用性，一个密码标准可能会重复出现在不同应用领域的密码应用标准体系之中。

在技术维上，七大类密码标准根据具体情况细分为若干子类，从而形成密码标准的技术体系框架，如图 2 所示。

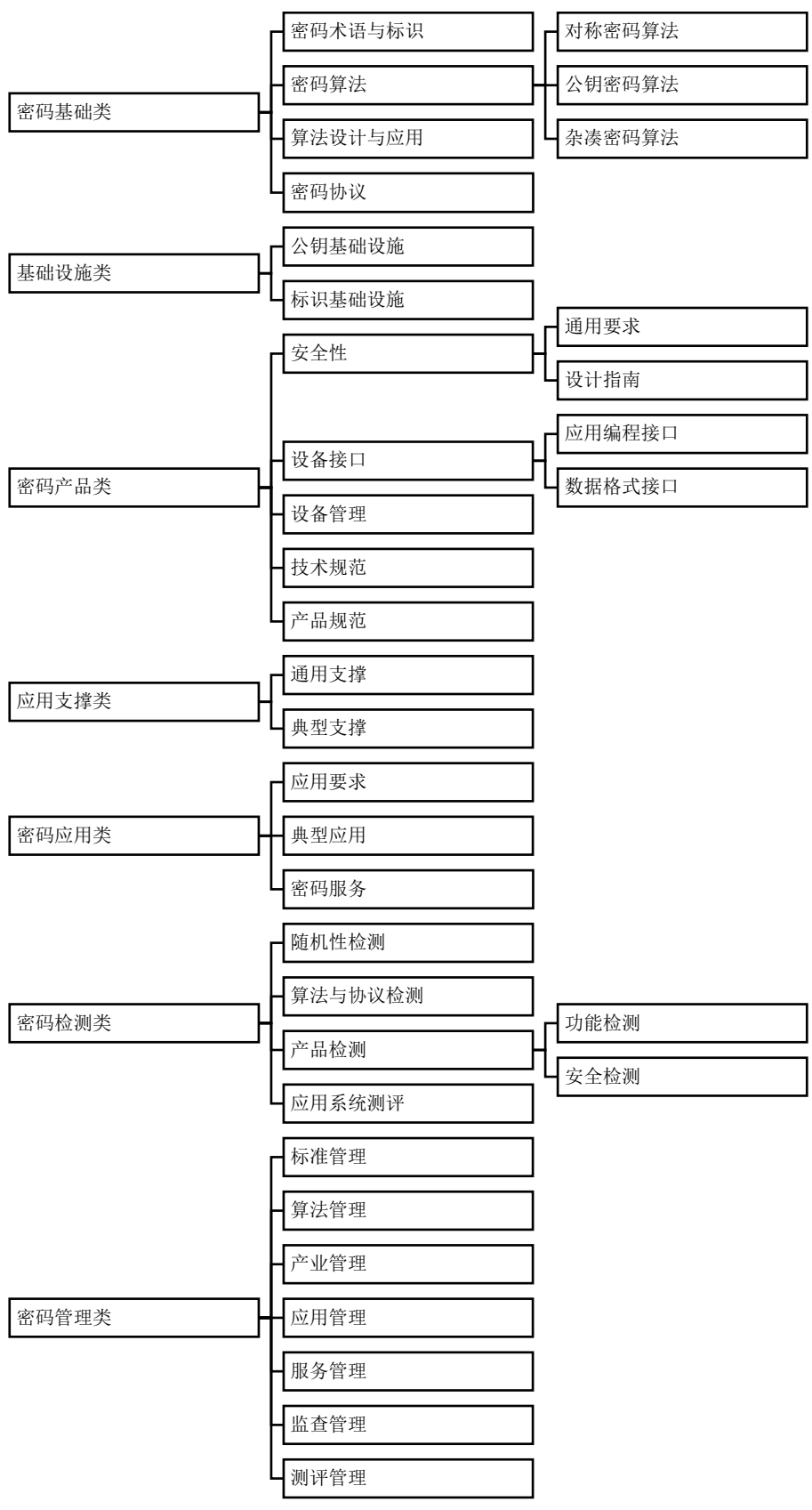


图 2 密码标准技术体系框架

密码基础类标准主要对通用密码技术进行规范，它是体系框架内的基础性规范，主要包括密码术语与标识标准、密码算法标准、密码设计与应用标准、密码协议标准等。

基础设施类标准主要针对密码基础设施进行规范，包括：证书认证系统密码协议、数字证书格式、证书认证系统密码及相关安全技术等，目前已颁布的密码标准只涉及公钥基础设施。

密码产品类标准主要规范各类密码产品的接口、规格以及安全要求。对于智能密码钥匙、VPN、安全认证网关、密码机等密码产品给出设备接口、技术规范和产品规范；对于密码产品的安全性，则不区分产品功能的差异，而以统一的准则给出要求；对于密码产品的配置和技术管理架构，则以 GM/T 0050《密码设备管理 设备管理技术规范》为基础统一制定。

应用支撑类标准针对密码报文、交互流程、调用接口等方面进行规范，包括通用支撑和典型支撑两个层次。通用支撑规范（如 GM/T 0019）通过统一的接口向典型支撑标准和密码应用标准提供加解密、签名验签等通用密码功能，典型支撑类标准是基于密码技术实现的与应用无关的安全机制、安全协议和服务接口，如可信计算可信密码支撑平台接口、证书应用综合服务接口等。

密码应用类标准是对使用密码技术实现某种安全功能的应用系统提出的要求以及规范，包括应用要求、典型应用和密码服务三类。应用要求旨在规范社会各行业信息系统对密码技术的合规使用。典型应用定义了具体的密码应用，如动态口令、安全电子签章等，典型应用类标准也包括其它行业标准机构制定的跟行业密切相关的密码应用类标准，如 JR/T 0025《中国金融集成电路（IC）卡规范》中，对

金融 IC 卡业务过程中的密码技术应用做了详细规范。密码服务类标准用以规范面向公众或特定领域提供的各类密码服务。

密码检测类标准针对标准体系所确定的基础、产品和应用等类型的标准出台对应检测标准，如针对随机数、安全协议、密码产品功能和安全性等方面的检测规范。其中对于密码产品的功能检测，分别针对不同的密码产品定义检测规范；对于密码产品的安全性检测则基于统一的准则执行。

密码管理类标准主要包括国家密码管理部门在密码标准、密码算法、密码产业、密码服务、密码应用、密码监查、密码测评等方面的管理规程和实施指南。

本文后续章节将以密码标准技术体系框架组成为基础，将已经发布的密码国家标准和密码行业标准按照该框架归入到相应章节，并对其逐一展开描述。

二 密码基础类标准

(一) 密码术语与标识

1. GM/Z 4001 密码术语

(1) 版本

GM/Z 4001-2013《密码术语》是当前的最新版本。

(2) 用途与适用范围

该标准对基本或通用的密码术语和定义进行了规范,以达到密码标准簇在术语方面的一致性。

该标准适用于统一信息安全技术领域中对密码基本概念的理解,规范技术交流和研究的表达。

(3) 内容概要

该标准共 4 章:

第 1 章范围,第 2 章术语,第 3 和第 4 章分别列出了中文和英文索引。

(4) 应用说明

——扩展应用领域

非密码技术领域在使用到相关密码术语时可参照该标准。

2. GB/T 33560 信息安全技术 密码应用标识规范

(1) 版本

GB/T 33560-2017《信息安全技术 密码应用标识规范》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0006《密码应用标识规范》,最后版本为 GM/T 0006-2012。

（2）用途与适用范围

该标准定义了密码应用中所使用的标识，用于规范算法标识、密钥标识、设备标识、数据标识、协议标识、角色标识等的表示和使用。

该标准适用于指导密码设备、密码系统的研制和使用过程中，对标识进行规范化的使用，也可用于指导其他相关标准或协议的编制中对标识的使用。

（3）内容概要

该标准共 7 个部分：

第 1 章范围、第 2 章术语和定义、第 3 章符号和缩略语。

第 4 章定义了标识的格式和编码。

第 5 章定义了密码标识，包括密码算法标识、数据标识和协议标识。其中，密码算法标识包括分组算法、公钥算法、杂凑算法以及签名算法的标识；数据标识定义了使用的数据类型、数据常量，并定义了通用的数据对象以及证书解析项的标识；协议标识定义了各类密码接口的标识和证书验证模式的标识。

第 6 章定义了安全管理类标识，包括角色管理标识、密钥管理标识、系统管理标识以及设备管理标识。

附录 A 是规范性附录，给出了商用密码领域中的相关 OID 定义。

（4）应用说明

该标准为基础性标准，其他标准涉及到密码标识的时候均应遵循该标准。如果其他标准中有新增标识需求，应在该标准中扩展。

(二) 密码算法

1. 对称密码算法

(1) GB/T 33133 信息安全技术 祖冲之序列密码算法

a) 版本

该标准对应的密码行业标准是 GM/T 0001《祖冲之序列密码算法》，共分为三个部分：

——GM/T 0001.1-2012《祖冲之序列密码算法第 1 部分：算法描述》是第 1 部分的最后版本；

——GM/T 0001.2-2012《祖冲之序列密码算法第 2 部分：基于祖冲之算法的机密性算法》是第 2 部分的最新版本，尚未推荐国家标准；

——GM/T 0001.3-2012《祖冲之序列密码算法第 3 部分：基于祖冲之算法的完整性算法》是第 3 部分的最新版本，尚未推荐为国家标准。

GB/T 33133.1-2016《信息安全技术 祖冲之序列密码算法第 1 部分：算法描述》系该标准第 1 部分的国家标准最新版本。

2018 年 4 月，《祖冲之序列密码算法》以补篇形式纳入 ISO/IEC 18033-4:2011 Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers 的提案获得立项。

b) 用途与适用范围

该标准描述了祖冲之密码算法（ZUC），以及使用祖冲之算法实现机密性和完整性保护的方法。

该标准适用于使用祖冲之序列密码算法产品的研制、生产和检测。

c) 内容概要

GM/T 0001《祖冲之序列密码算法》共分为三个部分：GM/T 0001.1《祖冲之序列密码算法第1部分：算法描述》描述了祖冲之密码算法的基本原理，该部分已发布为国家标准 GB/T 33133.1；GM/T 0001.2《祖冲之序列密码算法第2部分：基于祖冲之算法的机密性算法》描述了使用祖冲之密码算法加密明文数据流的方法；GM/T 0001.3《祖冲之序列密码算法第3部分：基于祖冲之算法的完整性算法》描述了使用祖冲之密码算法针对明文生成 32 比特 MAC 值的方法。

d) 应用说明

——使用注意事项

使用祖冲之算法进行机密性和完整性保护，应事先共享密钥 CK 或 IK，同时注意 CK、IK 及初始向量 IV 等参数的更新。在不同的加解密和生成 MAC 过程中，应采用互不相同的 (CK、IV) 对或 (IK、IV) 对。

该标准适用于祖冲之序列密码算法的工程实现和理论研究。在密码算法实现及使用过程中，应参照该标准第一部分附录 C 的测试向量保证祖冲之序列密码算法实现及使用的正确性。在非移动通信场景中，可根据实际情况定义 IV，并事先约定。

(2) GB/T 32907 信息安全技术 SM4 分组密码算法

a) 版本

GB/T 32907-2016《信息安全技术 SM4 分组密码算法》系该标准国家标准最新版本。该标准对应的密码行业标准是 GM/T 0002《SM4 分组密码算法》，最后版本为 GM/T 0002-2012。

b) 用途与适用范围

该标准描述了 SM4 分组密码算法，是一种密钥长度 128 比特，分组长度也是 128 比特的密码算法。

该标准适用于使用分组密码算法进行数据保护的场合，实现对明文数据的加密保护，以及以 CBC-MAC 等方式实现的完整性保护。

c) 内容概要

该标准共 8 个部分：

第 1 章范围、第 2 章术语和定义、第 3 章符号和缩略语。

第 4 章定义了 SM4 算法的结构，使用 SM4 的加密和解密计算在结构上完全相同，只是轮密钥的次序相反。

第 5 章描述了 SM4 的 128 比特密钥和 32 个 32 比特轮密钥，以及算法中用到的 FK 和 CK 两个算法参量。

第 6 章描述了每一轮运算的轮函数 F。

第 7 章详细描述了算法的实现，包括加密算法，解密算法以及密钥扩展算法。

附录 A 是资料性附录，给出了运算示例。

d) 应用说明

——直接相关标准

GB/T 17964-2008 信息安全技术 分组密码算法的工作模式

——使用注意事项

该标准在实施过程中需严格按照 SM4 分组密码算法的描述进行实现，测试结果符合标准中的运算示例，以保证算法实现的正确性。同时，分组密码只能处理一个分组长度的数据，无法处理任意长度的数据，因此在实际应用中应根据安全需求选择合适的分组密码工作模式和填充方法，以实现相应的安全功能。

当该算法用于保护数据的机密性时,应选取合适的工作模式,例如 CBC、CFB、OFB、CTR、BC、OFB/NL 等工作模式,见 GB/T 17964-2008 《信息安全技术 分组密码算法的工作模式》;当该算法用于鉴别数据的完整性时,应选取合适的工作模式,例如 CBC-MAC 系列的工作模式,见 GB/T 15852.1-2008 《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》;当该算法用于同时保护数据的机密性和完整性时,应选取合适的可鉴别加密工作模式,例如 OCB、CCM、Key Wrap、EAX、GCM 等工作模式,见 GB/T 36624-2018 《信息技术 安全技术 可鉴别的加密机制》。

2. 公钥密码算法

(1) GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

a) 版本

GB/T 32918 《信息安全技术 SM2 椭圆曲线公钥密码算法》共分为 5 个部分:

——GB/T 32918.1-2016 《信息安全技术 SM2 椭圆曲线公钥密码算法第1部分:总则》;

——GB/T 32918.2-2016 《信息安全技术 SM2 椭圆曲线公钥密码算法第2部分:数字签名算法》;

——GB/T 32918.3-2016 《信息安全技术 SM2 椭圆曲线公钥密码算法第3部分:密钥交换协议》;

——GB/T 32918.4-2016 《信息安全技术 SM2 椭圆曲线公钥密码算法第4部分:公钥加密算法》;

——GB/T 32918.5-2017 《信息安全技术 SM2 椭圆曲线公钥密码

算法第 5 部分：参数定义》。

该标准对应的密码行业标准是 GM/T 0003 《SM2 椭圆曲线公钥密码算法》，最后版本为 GM/T 0003-2012。

SM2 算法已经纳入 ISO/IEC 国际标准：ISO/IEC 14888-3:2018 IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms。

b) 用途与适用范围

该标准适用于 SM2 椭圆曲线公钥密码算法相关技术研究、系统和产品的研制及算法正确性验证。

c) 内容概要

该标准共 5 个部分：

第 1 部分描述了 SM2 算法的数学原理，包括椭圆曲线及椭圆曲线上有有限域的概念、椭圆曲线涉及的参数、数据类型及其转换等。

第 2 部分描述了使用 SM2 算法进行数字签名和验签的方法，并给出了一个加密解密的示例。

第 3 部分描述了使用 SM2 算法进行密钥交换的协议和流程，并给出了一个密钥交换的示例。

第 4 部分描述了使用 SM2 算法进行公钥加密和解密的方法，并给出了一个公钥加解密运算的示例。

第 5 部分描述了 SM2 算法的椭圆曲线参数，并给出了基于此参数进行数字签名验签、密钥协商以及公钥加解密的示例。

d) 应用说明

——直接相关标准

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
——使用注意事项

在实施过程中需要重点确保密钥安全性和随机数的安全性，不安全的存储方式直接威胁密码算法的安全性；弱随机数将威胁密码算法甚至密钥的安全性；同时需要注意严格执行检查条件，否则可能导致安全漏洞。

(2) GM/T 0044 SM9 标识密码算法

a) 版本

GM/T 0044-2016《SM9 标识密码算法》是当前的最新版本。

该标准分为 5 个部分：

——GM/T 0044.1-2016《SM9 标识密码算法第 1 部分：总则》；

——GM/T 0044.2-2016《SM9 标识密码算法第 2 部分：数字签名算法》；

——GM/T 0044.3-2016《SM9 标识密码算法第 3 部分：密钥交换协议》；

——GM/T 0044.4-2016《SM9 标识密码算法第 4 部分：密钥封装机制和公钥加密算法》；

——GM/T0044.5-2016《SM9 标识密码算法第 5 部分：参数定义》。

该标准已经纳入到国际标准 ISO/IEC 14888-3:2018 IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms。

b) 用途与适用范围

该标准描述了基于双线性对的标识密码算法。SM9 属于公钥密码算法的一种，可用于数字签名、数据加密、密钥协商等公钥密码算法

的用途。

该标准适用于 SM9 标识密码算法相关技术研究、系统和设备研制，以及算法正确性验证。

c) 内容概要

该标准共 5 个部分：

第 1 部分描述了必要的数学基础知识与相关密码技术，以帮助了解 and 实现该标准其它各部分所规定的密码机制，包括有限域和椭圆曲线，双线性对和安全曲线。本部分还介绍了该标准用到的数据类型及其相互转换方法，以及标识密码算法使用的系统参数。

第 2 部分描述了 SM9 数字签名算法，包括算法参数和辅助函数，签名流程以及验签流程。

第 3 部分描述了 SM9 密钥交换协议，包括算法参数与辅助函数，以及密钥交换协议的流程。

第 4 部分描述了 SM9 密钥封装机制和公钥加密算法，包括算法参数与辅助函数，密钥封装的机制和流程，以及公钥加密的算法和流程。

第 5 部分定义了 SM9 算法的参数，包括椭圆曲线方程及参数、群 G_1 和 G_2 的生成元等，以及扩域元素的表示方法，同时还给出了算法实现示例。

d) 应用说明

由于 SM9 标识密码算法中签名和加密主密钥参与用户密钥的生成过程，在应用中要确保其安全性。

标准使用时需严格执行标准中的检查条件，避免可能产生缺漏导致对密码算法的攻击。

3. 密码杂凑算法

(1) GB/T 32905 信息安全技术 SM3 密码杂凑算法

a) 版本

GB/T 32905-2016《信息安全技术 SM3 密码杂凑算法》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0004《SM3 密码杂凑算法》，最后版本为 GM/T 0004-2012。

SM3 算法已经纳入 ISO/IEC 国际标准：ISO/IEC10118-3:2018《Information technology — Security Techniques — Hash-functions —Part 3: Dedicated hash-functions》。

b) 用途与适用范围

该标准可用于消息摘要的计算、数字签名和验证、消息鉴别码的生成与验证，以及随机数的生成。

该标准适用于 SM3 密码杂凑算法相关技术研究、系统和产品的研制及算法正确性验证。

c) 内容概要

该标准共 6 个部分：

第 1 章范围、第 2 章术语和定义、第 3 章符号。

第 4 章描述了 SM3 算法涉及的初始值 IV 和常量 Tj 的取值，以及用到的布尔函数和置换函数。

第 5 章描述了 SM3 的算法实现及过程，包括填充、迭代压缩和杂凑计算。

附录 A 是资料性附录，给出了 SM3 密码杂凑算法的运算示例。

d) 应用说明

——直接相关标准

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

——使用注意事项

该标准实施时应对照给出的运算示例，保证算法实现及使用的正确性；当应用于构建消息鉴别码时，应保障其密钥的机密性。

(三) 算法设计与应用

1. GB/T 35276 信息安全技术 SM2 密码算法使用规范

(1) 版本

GB/T 35276-2017《信息安全技术 SM2 密码算法使用规范》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0009《SM2 密码算法使用规范》，最后版本为 GM/T 0009-2012。

(2) 用途与适用范围

该标准为使用 SM2 密码算法的产品提供统一算法使用规范，为算法的实现方、使用方和检测方提供依据和指导，为包含 SM2 密码算法的产品开发、使用及检测提供基准。

(3) 内容概要

该标准共 10 章：

第 1 章范围、第 2 章规范性引用文件、第 3 章术语和定义、第 4 章符号和缩略语。

第 5 章描述了 SM2 算法的公钥和私钥的数据结构。

第 6 章数据转换，描述了数据在位串与字符串之间的转换方法和整数和字符串之间的转换方法。

第 7 章数据格式，定义了密钥数据格式、加密数据格式、签名数据格式和密钥对保护数据格式。

第 8 章预处理，描述了 Z 值计算过程和签名运算所需的杂凑计算过程。

第 9 章计算过程，描述了生成密钥、加密、解密、数字签名、签名验证和密钥协商的计算过程。

第 10 章用户身份标识，提供了用户身份标识的默认值。

(4) 应用说明

——直接相关标准

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

——使用注意事项

该标准规定了默认用户身份标识用于通用领域；在专用领域，可自行定义该系统需要的用户身份标识。

2. GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

(1) 版本

GB/T 35275-2017《信息安全技术 SM2 密码算法加密签名消息语法规范》系该标准国家标准最新版本。

该标准对应的密码行业标是 GM/T 0010《SM2 密码算法加密签名消息语法规范》，最后版本为 GM/T 0010-2012。

(2) 用途与适用范围

该标准定义了使用 SM2 密码算法的加密签名消息语法。

该标准适用于使用 SM2 密码算法进行加密和签名操作时对操作结果的标准化封装。

(3) 内容概要

该标准共 13 章：

第 1 章范围、第 2 章规范性引用文件、第 3 章术语和定义、第 4 章符号和缩略语。

第 5 章给出了语法中用到的 OID 的定义。

第 6 章给出了语法中用到的基本类型的定义。

第 7 章至第 12 章分别对数据类型、签名数据类型、数字信封数据类型、签名及数字信封数据类型、加密数据类型和密钥协商类型进行了详细定义。

第 13 章定义了 SM2 密钥格式。

(4) 应用说明

——直接相关标准

GB/T 20518 信息安全技术 公钥基础设施数字证书格式规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

(四) 密码协议

1. GB/T 36968 信息安全技术 IPsec VPN 技术规范

(1) 版本

GB/T 36968-2018《信息安全技术 IPsec VPN 技术规范》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0022《IPsec VPN 技术规范》，最后版本为 GM/T 0022-2014。

(2) 用途与适用范围

该标准规定了 IPsec VPN 的技术协议、产品研制要求以及产品检测要求及判定标准。

该标准适用于 IPSec VPN 产品的研制，也可用于指导 IPSec VPN 产品的检测、管理和使用。

（3）内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和缩略语。

第 4 章描述了 IPSec VPN 的密码算法、密钥种类及定义。该部分规定了 IPSec VPN 网关产品应使用的算法及其使用方式，定义了设备密钥、工作密钥和会话密钥。

第 5 章描述了 IPSec 协议的组成，包括密钥交换协议和安全报文协议。其中，密钥交换协议包括两个阶段：第一阶段用于进行双方的身份鉴别以及协商第二阶段所需的工作密钥；第二阶段用于协商双方数据通信时的共享策略和密钥。密钥交换协议还对密钥交换过程中每次数据交互所需的数据内容、密钥交换报文数据格式、载荷数据格式及载荷各字段的值与含义进行了规定。安全报文协议规定了鉴别头协议与封装安全载荷协议这两种安全报文协议报文头的数据格式。

第 6 章描述了 IPSec VPN 的产品要求，包括功能、性能参数和安全管理要求。

第 7 章描述了 IPSec VPN 产品的检测要求，包括功能、性能和安全检测要求，与第 6 章产品要求相对应。

第 8 章描述了 IPSec VPN 产品检测判定标准。

附录 A 是资料性附录，介绍了 IPSec VPN 的基础架构、基本概念和基本内容。

（4）应用说明

——直接相关标准

GB/T 20518 信息安全技术 公钥基础设施数字证书格式规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0023 IPsec VPN 网关产品规范

GM/T 0026 安全认证网关产品规范

——扩展应用领域

该标准可用于指导具备 IPsec VPN 功能的其他产品的研制、使用及检测，如加密防火墙、加密路由器、安全接入设备等，还可用于使用 IPsec 协议的其他产品。

2. GM/T 0024 SSL VPN 技术规范

(1) 版本

GM/T 0024-2014《SSL VPN 技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了 SSL VPN 的技术协议、产品研制要求以及产品检测要求及判定标准。其中，产品研制要求包括功能要求、性能要求和安全管理要求；产品检测要求包括功能检测要求、性能检测要求和安全管理检测要求，分别与产品研制要求相关内容对应。

该标准 2014 版的制定参考了 RFC4346 (TLS1.1)，按照我国相关密码政策和法规，结合我国实际应用需求及产品生产厂商的实践经验，在 TLS1.1 的握手协议中增加了 ECC、IBC 的认证模式和密钥交换模式，取消了 DH 密钥交换方式，修改了密码套件的定义。

该标准适用于 SSL VPN 产品的研制，也可用于指导 SSL VPN 产品的检测、管理和使用。

(3) 内容概要

该标准共 9 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章符号和缩略语。

第 5 章描述了 SSL 协议中采用的密码算法类别、密钥种类及相互关系。密码算法包括非对称密码算法、分组密码算法、密码杂凑算法、数据扩展函数 P_hash、伪随机函数 PRF 等，并给出了 P_hash 和 PRF 函数的定义；密钥种类包括服务端密钥、客户端密钥、预主密钥、主密钥、工作密钥等。

第 6 章描述了 SSL 协议使用的数据类型、记录层协议、握手协议族、密钥计算方法和网关到网关协议。其中，记录层协议主要规定了连接状态以及数据的分段、压缩、校验和加密的方法和数据结构；握手协议族主要规定了该协议族由密钥规格变更协议、报警协议和握手协议三类协议组成，用于进行双方身份验证并协商出供记录层使用的安全参数以及向对方报告错误等，定义了握手消息交互流程及重用握手消息交互流程，定义了各类消息结构及错误报警表；密钥计算方法主要规定了主密钥和工作密钥的计算方法；网关到网关协议主要规定了 SSL VPN 之间建立网关到网关的传输层隧道对 IP 数据报文进行安全传输时所采用的报文格式、控制报文交换过程以及数据报文封装过程，明确网关到网关协议与握手协议处于同一层次，使用 80 作为协议类型编号。

第 7 章描述了 SSL VPN 产品的功能要求、性能要求及安全管理要求。产品功能要求明确 SSL VPN 产品必须支持客户端—服务端工作模式，网关—网关工作模式为可选；生成的随机数必须符合 GM/T 0005 标准；必须通过协商生成工作密钥；应具备身份鉴别功能；支持细粒度访问控制；工作密钥有效期在客户端—服务端工作模式下不超过 8

小时，在网关—网关工作模式下不超过 1 小时；应具备客户端主机安全检查功能。性能要求明确了 SSL VPN 产品的四个性能参数，分别为最大并发用户数、最大并发连接数、每秒新建连接数和吞吐率。安全管理要求包括技术要求和安全管理要求两部分。

第 8 章描述了 SSL VPN 产品的检测要求，包括功能检测要求、性能检测要求和安全管理检测要求，与第 7 章产品要求相对应。

第 9 章描述了 SSL VPN 产品检测判定标准。

(4) 应用说明

——直接相关标准

GM/T 0025 SSL VPN 网关产品规范

GM/T 0026 安全认证网关产品规范

——扩展应用领域

该标准也可用于指导具备 SSL VPN 功能的加密防火墙、加密路由器、安全接入设备等产品的研制、使用及检测，还可用于使用 SSL/TLS 的其他产品。

三 基础设施类标准

(一) 公钥基础设施

1. GM/T 0014 数字证书认证系统密码协议规范

(1) 版本

GM/T 0014-2012《数字证书认证系统密码协议规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了数字证书认证系统中各部分的关系、安全协议流程

和数据格式定义等内容，以保障数字证书认证系统在使用、运行中的真实性、机密性、完整性，实现可认证和不可否认等安全需求。

该标准适用于电子政务、电子商务中数字证书认证系统的设计、研发、建设、检测和运营。

（3）内容概要

该标准共 10 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章规定了数字证书认证系统中涉及到密码技术的相关安全协议，给出了具体流程和数据参数定义。主要包括：用户端同 RA 之间的安全协议；RA 同 CA 之间的安全协议；CA 同 KM 之间的安全协议；CA 同 LDAP 服务之间的安全协议；CA 同 OCSP 服务之间的安全协议；用户同 LDAP 服务之间的安全协议；用户同 OCSP 服务之间的安全协议。

第 6 章描述了第 5 章定义协议中涉及到的加密数据、摘要数据、数字签名、数字信封的报文语法。

附录 A 是规范性附录，给出了证书模板格式、CRL 格式、加密值、消息状态码和故障信息、证书识别、带外根 CA 公钥、存档选项、发布信息的语法说明。

附录 B 和附录 C 是资料性附录，分别给出了 RA 与 CA 间相关协议和协议报文的实例。

附录 D 是规范性附录，给出了非实时发布证书协议的流程。

（4）应用说明

——直接相关标准

GB/T 19713 信息技术 安全技术 公钥基础设施在线证书状态协

议

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

2. GB/T 20518 信息安全技术 公钥基础设施 数字证书格式规范

(1) 版本

GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式规范》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0015《基于 SM2 密码算法的数字证书格式规范》，最后版本为 GM/T 0015-2012。

(2) 用途与适用范围

该标准是 GB/T 20518-2006 标准的替代，增加了与 SM2、SM3 密码算法相关的部分，并且撤销了不安全的密码算法支持。

该标准规定了数字证书和证书撤销列表的具体结构定义，并对数字证书和证书撤销列表中的各数据项内容进行了详细描述。

该标准适用于数字证书认证系统相关产品的研发和基于数字证书的各种应用。

(3) 内容概要

该标准共 11 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章定义了基于 ASN.1 编码的 SM2 密码算法数字证书详细格式和证书吊销列表 CRL 的详细格式。

第 6 章明确了应优先使用国家标准的密码算法。

附录 A 是规范性附录，给出了证书结构的简明表述。

附录 B 是规范性附录，分别给出了用户证书、服务器证书的结构实例。

附录 C 是规范性附录，定义了证书的内容表。

附录 D 是资料性附录，给出了基于 SM2 算法的证书编码实例。

附录 E 是资料性附录，明确了用 SM3 算法替换了其他密码杂凑算法，并明确与 SM2 密码算法结合使用。

(4) 应用说明

——直接相关标准

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

——使用注意事项

该标准中存在使用 RSA 和相关算法的描述。实施时数字证书应该采用双数字证书机制，使用加密证书进行加密保护，使用签名证书进行鉴别认证。数字证书使用的密码算法应采用 SM2/SM3 算法。

在该标准附录 D 的 SM2 示例最后签名值的 DER 编码有个笔误。

“ 02 20 B5 70 08 46 76 7B 6F 27 43 6C BE D7 45 98 C4 5B 98 5C CB C8 1A 14 0E 2A 3B 03 55 CA BE F1 72 F2”。

应为：“ 02 **21 00** B5 70 08 46 76 7B 6F 27 43 6C BE D7 45 98 C4 5B 98 5C CB C8 1A 14 0E 2A 3B 03 55 CA BE F1 72 F2”。

3. GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

(1) 版本

GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0034《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》，最后版本为 GM/T 0034-2014。

（2）用途与适用范围

该标准规定了数字证书认证系统的设计、建设、检测、运行及管理规范，以及数字证书认证系统的密码及相关安全的技术要求。

该标准适用于指导第三方认证机构的数字证书认证系统的建设和检测评估，规范数字证书认证系统中密码及相关安全技术的应用。非第三方认证机构数字证书认证系统的建设、运行及管理也可参照该标准。

（3）内容概要

该标准共 13 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语，第 4 章缩略语。

第 5 章证书认证系统，规定了证书认证系统必须采用双证书、双中心机制，包括功能要求、系统设计、数字证书和证书撤销列表。其中，功能要求部分规定了证书认证系统中各子系统应当具备的主要功能；系统设计部分规定了各子系统的逻辑结构及各组成部分应当具备的主要功能；数字证书和证书撤销列表部分明确了数字证书和证书撤销列表的结构和格式应当遵循的标准，并规定了颁发者名称和主体名称的顺序以及密码算法要求。

第 6 章密钥管理系统，描述了密钥管理中心逻辑结构、功能描述、

系统设计、KMC 与 CA 的安全通信协议。其中，功能描述部分规定了密钥管理中心在密钥生命周期各个阶段应当满足的功能要求；系统设计部分给出了密钥管理中心的模块划分及各个模块应当具备的主要功能；KMC 与 CA 的安全通信协议部分定义了 CA 与 KMC 应当采用基于双向身份鉴别的安全通信协议。

第 7 章密码算法、密码设备及接口。其中，密码算法部分规定了证书认证系统使用的算法类别、用途和要求；密码设备部分规定了系统使用的密码设备类别、应当具备的功能和安全要求；密码服务接口部分规定了系统使用的密码设备应当符合的接口标准。

第 8 章证书认证中心，规定了系统、安全、数据备份、可靠性、物理安全、人事管理制度等建设要求。

第 9 章密钥管理中心，规定了系统、安全、数据备份、可靠性、物理安全、人事管理制度等建设要求。

第 10 章证书认证中心运行管理要求，规定了人员管理、业务运行管理、密钥分管、安全管理、安全审计、文档配备等管理要求。

第 11 章密钥管理中心运行管理要求，规定了人员管理、业务运行管理、密钥分管、安全管理、安全审计、文档配备等管理要求。

第 12 章证书操作流程，描述了证书申请、更新、吊销、挂起、解除挂起和用户密钥恢复的操作流程，以及司法密钥恢复流程。

附录 A 是资料性附录，给出了证书认证系统的网络结构图。

（4）应用说明

——直接相关标准

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0018 密码设备应用接口规范

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 0043 数字证书互操作检测规范

——使用注意事项

基于数字证书的身份认证系统可基于该结构进行适度裁剪。

四 密码产品类标准

(一) 安全性

1. 通用要求

(1) GB/T 37092 信息安全技术 密码模块安全要求

a) 版本

GB/T 37092-2018《信息安全技术 密码模块安全要求》系该标准国家标准最新版本。

该标准对应的密码行业标是 GM/T 0028《密码模块安全技术要求》，最后版本为 GM/T 0028-2014。

b) 用途与适用范围

该标准规定对密码模块采用分级管理，明确密码模块分为四个递增的、定性的安全等级，针对不同安全等级明确相应的安全要求以满足密码模块在不同应用和工作环境中的要求。

密码模块是密码应用的核心部件，自身的安全性直接影响到基于它构建的密码系统的安全性与可靠性。密码模块可以是软件、硬件或软硬混合，可以是独立产品如密码芯片、密码机等，也可以是某应用产品中实现密码功能的部分，如具备密码功能的 CPU 等。

该标准规定了密码模块在安全设计、实现、运行与废弃等环节的安全要求，不涉及密码模块的正确应用和安全部署。

该标准适用于密码模块的设计、生产、使用和检测。密码模块厂商可参照该标准进行产品设计，以确保产品满足该标准指定等级的安全要求；商用密码检测机构依据该标准进行检测，以确认送检产品是否达到了声称的安全级别；密码使用机构可根据其应用的安全需求及

所处环境的安全现状参照该标准选取合适的安全等级的密码模块产品对其应用进行保护。

c) 内容概要

该标准共 13 个部分：

第 1 章范围、第 2 章规范性引用文件、第 3 章术语和定义、第 4 章缩略语。

第 5 章描述了四个安全级别的含义。安全一级是最低等级安全要求，没有对物理安全机制提出要求，适用于模块外部已配置物理安全、网络安全及安全管理手段的情况；安全二级在安全一级的基础上，增加了对拆卸证据的要求和基于角色访问控制的要求；安全三级增加了物理安全要求，规定了基于身份的鉴别机制的使用，并增加了对非入侵式攻击缓解的要求；安全四级增加了外层完整封套保护、多因素鉴别、更高的非入侵式攻击缓解要求。对于软件密码模块，可符合的级别在安全二级及以下。

第 6 章描述了密码模块功能性安全目标。

第 7 章描述了所有的安全要求，共有 12 个条款：通用要求，密码模块规格，密码模块接口，角色、服务和鉴别，软件/固件安全，运行环境，物理安全，非入侵式安全，敏感安全参数管理，自测试，生命周期保障，以及对其他攻击的缓解。在这所有的要求中，凡没有阐明特定级别的，则表示所有密码模块均需遵循；特定级别需要遵循的不同要求，则在文中明确进行了分级表述。

附录 A 是规范性附录，规定了对各个条款的文档要求。

附录 B 是规范性附录，规定了对各个条款安全策略表述的要求。

附录 C 是规范性附录，给出了适用于该标准的核准的安全功能列

表，包括分组密码、流密码、非对称密钥、消息鉴别码、杂凑函数、实体鉴别、密钥建立和随机数生成器。

附录 D 是规范性附录，给出了适用于该标准的敏感安全参数生成和建立方法列表。

附录 E 是规范性附录，给出了适用于该标准的核准的鉴别机制列表。

附录 F 是规范性附录，给出了适用于该标准的非入侵式攻击及常用的缓解方法。

d) 应用说明

——直接相关标准

GM/T 0039 密码模块安全检测要求

GM/T 0054 信息系统密码应用基本要求

——使用注意事项

根据国家密码管理局 2018 年发布的第 419 号公告，除安全芯片和密码系统外的所有密码产品类型都须按照该标准进行分级检测。该标准是密码产品的通用安全标准，密码设备厂商在进行设备研制时，应注意除须遵循相应的技术规范、产品规范外，还须遵循该标准进行设备安全性设计；密码检测机构在进行密码产品分级检测时，应结合 GM/T 0039 配套使用；密码使用方在基于 GM/T 0054 标准进行应用系统密码应用方案设计、建设时，应参考该标准确定其应用场景下应选择何种安全等级的密码模块产品进行安全防护。

(二) 设备接口

1. 应用编程接口

(1) GM/T 0012 可信计算 可信密码模块接口规范

a) 版本

GM/T 0012-2012《可信计算可信密码模块接口规范》是当前的最新版本。

b) 用途与适用范围

该标准定义了可信密码模块的接口、管理功能，可为可信计算密码支撑平台提供身份标识与认证、数据保护、完整性度量与报告功能及接口。

该标准适用于可信密码模块相关产品的研制、生产、测评和应用开发。

c) 内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语、定义和缩略语。

第 4 章说明了可信密码模块的硬件和固件构成，以及主体功能。

第 5 章可信密码模块管理功能，定义了启动、状态保存、自检、使用过程中的所有者管理、属性管理、升级与维护、授权值管理、非易失性存储管理、运行环境管理、审计、时钟、计数器等内容。

第 6 章定义了可信密码模块提供的、用于标识自身及所在计算平台的功能和接口，以及身份标识密钥的管理和认证方法。

第 7 章定义了可信密码模块提供的用于保护可信计算密码支撑平台数据所需的功能和接口，包括：保护可信密码模块内部资源（如

密钥)的访问控制方法;保护平台内可信密码模块以外的数据的密码学操作;管理可信密码模块密钥的方法。

第 8 章定义了可信密码模块用于存储和引证平台完整性度量值的功能和接口。

附录 A 是规范性附录,定义了第 5 章至第 8 章所述接口使用的数据结构。

d) 应用说明

——直接相关标准

GB/T 29829 信息安全技术 可信计算可信密码支撑平台功能与接口规范

GM/T 0013 可信密码模块接口符合性测试规范

GM/T 0058 可信计算 TCM 服务模块接口规范

(2) GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

a) 版本

GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0016《智能密码钥匙密码应用接口规范》,最后版本为 GM/T 0016-2012。

b) 用途与适用范围

该标准用于规范智能密码钥匙的应用接口。智能密码钥匙中间件通过实现该标准,向应用提供统一的、与具体产品无关的调用接口。

该标准定义了基于 PKI 密码体制的智能密码钥匙应用接口,描述了密码应用接口的函数、数据类型、参数结构和设备安全要求。该标准适用于智能密码钥匙产品的研制、使用和检测。

c) 内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章结构模型，明确了该标准提出的接口在智能密码钥匙应用层次关系中的位置，以及设备的应用结构。

第 6 章数据类型，定义了该标准接口中使用的算法标识、基本数据类型、常量和复合数据类型。

第 7 章接口函数，定义了具体的接口函数形式，包括函数原型、功能描述、输入输出参数、返回值，分为设备管理、访问控制、应用管理、文件管理、容器管理和密码服务类。

第 8 章设备的安全要求，从设备使用阶段、权限管理、密钥安全、设备抗攻击要求方面规定了设备的安全要求。

附录 A 是规范性附录，定义了接口的返回值及其含义。

d) 应用说明

——直接相关标准

GB/T 35276 信息安全技术 SM2 密码算法使用规范

——使用注意事项

“外来私钥签名”、“外来私钥运算”、“明文导入会话密钥”、“生成外部密钥对”相关接口仅用于调试和检测，不可用于实际业务。

(3) GB/T 36322 信息安全技术 密码设备应用接口规范

a) 版本

GB/T 36322-2018《信息安全技术 密码设备应用接口规范》系该标准国家标准最新版本。

该标准对应的密码行业标准是 GM/T 0018 《密码设备应用接口规范》，最后版本为 GM/T 0018-2012。

b) 用途与适用范围

该标准是服务端密码设备的接口规范，通过该接口调用密码设备，向上层多用户、多应用提供统一的基本密码服务。该标准可为服务器密码机、PCI/PCI-E 密码卡等密码设备的开发、使用及检测提供标准依据和指导，有利于提高该类密码设备的产品化、标准化和系列化水平。

该标准只规范服务接口，不涉及管理接口及网络通信协议；密码设备需要提供管理界面，通过管理界面对设备进行配置管理。该标准遵循密钥的默认使用原理，按指令功能选用密钥；该标准规范非对称密钥应采用加密密钥和签名密钥的双密钥体制，设置设备密钥，仅用于设备的管理；设置用户密钥，用于用户数据保护。

c) 内容概要

该标准共 6 章，第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章描述了算法标识、密钥分类和相关数据结构定义。标准规定算法标识应遵循 GM/T 0006-2012 标准，定义了设备信息定义、密钥分类及存储定义、RSA 密钥数据结构定义、ECC 密钥数据结构定义、ECC 加密数据结构定义、ECC 签名数据结构定义、ECC 加密密钥对保护结构定义等。

第 6 章描述了标准在公钥密码基础设施应用技术体系结构中的位置以及一系列设备接口函数定义。设备接口函数划分为设备管理类函数、密钥管理类函数、非对称算法运算类函数、对称算法运算类函

数、杂凑运算类函数、用户文件操作类等六类函数。

附录 A 是规范性附录，描述了函数调用返回代码的定义。

d) 应用说明

——直接相关标准

GM/T 0006-2012 密码应用标识规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

——扩展应用领域

使用其他计算机语言可以参考该标准开发相应接口。

——使用注意事项

使用该标准进行应用开发时，应注意以下事项：

该标准中定义的：产生 ECC 密钥对并输出、导入明文会话密钥、产生 RSA 密钥对并输出、外部私钥 RSA 运算、外部密钥 ECC 签名、外部密钥 ECC 私钥解密 6 个接口仅用于正确性验证使用，不可为应用系统提供密码服务。

该标准设备管理类函数定义了设备打开与关闭、会话创建与关闭、设备信息获取、随机数产生、私钥权限获取与释放等接口。调用密码设备使用具体的密码服务之前应首先调用设备打开和会话创建两个接口，完成密码设备使用环境初始化。调用密码设备结束后，应注意依次调用会话关闭和设备关闭两个接口，完成密码设备使用环境释放，避免造成内存泄露。使用密码设备执行非对称密钥私钥运算之前，必须首先调用私钥权限获取接口，并在执行完非对称密钥私钥运算之后调用私钥权限释放接口完成私钥使用权限释放，避免造成非对称密钥私钥的非授权使用。

该标准规定密钥分类包括设备密钥、用户密钥、密钥加密密钥和

会话密钥。其中，设备密钥占用非对称密钥的 0 号索引号，该密钥仅限于进行对密码设备进行管理，禁止使用该密钥对用户数据进行操作。

密码设备的主要功能是提供密钥管理、密码运算等服务，该标准中定义的用户文件操作类函数主要供密码设备使用方在密码设备中存储部分敏感文件，建议密码设备使用方避免在密码设备中存储不涉及敏感信息的文件。

该标准中规定的 RSA 相关算法接口不作为实现的必须要求。

(4) GM/T 0056 多应用载体密码应用接口规范

a) 版本

GM/T 0056-2018《多应用载体密码应用接口规范》是当前的最新版本。

b) 用途与适用范围

该标准中的多应用载体是指具备独立、开放的片上操作系统、提供多应用运行环境、能够实现载体上多个应用的下载、安装、重用、共存的安全载体，通常由硬件、驱动、COS 和应用构成。典型的多应用载体如智能 IC 卡。

该标准规定了多应用载体中 SM2、SM3、SM4 系列算法的密码应用接口。

该标准适用于各种多应用载体的研制、应用和检测。

c) 内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符合和缩略语。

第 5 章对多应用载体的系统框架进行了描述。多应用载体内部系

统由硬件层、驱动层、OS 层、应用层组成。

第 6 章描述了多应用载体密码应用接口的调用流程，以及密码算法能力标识和密码应用接口规格的约束。

第 7 章定义了 Java 技术方案中密码应用接口、密码算法能力标识、密码应用包、应用接口和应用类信息。

附录 A 是资料性附录，描述了多应用载体中多应用安全管理的密码应用要求。

附录 B 是资料性附录，规定了多应用安全管理中的证书格式。

d) 应用说明

——直接相关标准

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

——使用注意事项

在多应用管理实现中，应实现应用之间的隔离，如敏感数据和密钥信息。

(5) GM/T 0058 可信计算 TCM 服务模块接口规范

a) 版本

GM/T 0058-2018《可信计算 TCM 服务模块接口规范》是当前的最新版本。

b) 用途与适用范围

该标准定义了 TCM 服务模块组成和接口规范，适用于基于 TCM 的应用开发、使用及检测。

c) 内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章给出了 TCM 服务模块软件架构。

第 6 章定义了 TCM 应用服务的操作命令与函数接口规范。

第 7 章定义了 TCM 核心服务的操作命令与函数接口规范。

第 8 章定义了可信设备驱动库。

附录 A 是规范性附录，描述了可信密码模块功能命令与函数接口涉及的数据结构、授权数据的处理及接口返回码定义。

d) 应用说明

——直接相关标准

GB/T 29829 信息安全技术 可信计算密码支撑平台功能与接口规范

GM/T 0012 可信计算 可信密码模块接口规范

GM/T 0013 可信密码模块接口符合性测试规范

2. 数据格式接口

(1) GM/T 0017 智能密码钥匙密码应用接口数据格式规范

a) 版本

GM/T 0017-2012《智能密码钥匙密码应用接口数据格式规范》是当前的最新版本。

b) 用途与适用范围

该标准规范了智能密码钥匙应用数据接口的 APDU 报文、接口函数的编码和设备协议等内容，适用于智能密码钥匙的研制和检测。

c) 内容概要

该标准共 13 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章定义了该标准中使用的记号。

第 6 章给出了智能密码钥匙的结构模型，明确了该标准在模型中所处的层次关系。

第 7 章 APDU 报文结构，定义了命令和响应报文的数据结构。对 APDU 指令编码按照用途进行了分类，包括：设备管理、访问控制、应用管理、文件管理、容器管理和密码服务。

第 8 章给出了命令头、数据字段和响应字段的编码约定。

第 9 章给出了 APDU 指令和响应编码。

第 10 章给出了支持的设备协议。

附录 A 是规范性附录，给出了设备返回码的定义和说明。

附录 B 是规范性附录，给出了安全报文计算方法和要求。

附录 C 是资料性附录，给出了编程范例。

d) 应用说明

——直接相关标准

GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0048 智能密码钥匙密码检测规范

——扩展应用领域

该标准允许使用第 10 章规定的 CCID、MassStorage 和 HID 通信协议之外的蓝牙、红外、键盘等其他通信协议。

(三) 设备管理

1. GM/T 0050 密码设备管理 设备管理技术规范

(1) 版本

GM/T 0050-2016《密码设备管理设备管理技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了密码设备管理的体系结构、管理流程、安全通道协议、管理信息结构、应用接口和标准管理消息格式。

该标准适用于密码设备管理系统、密码设备管理应用、密码机等密码设备的研制、开发和检测。

(3) 内容概要

该标准共 11 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章描述了密码设备管理体系框架，包括密码设备层、管理平台层和管理应用层，规定了各层间通过安全通道进行通信。

第 6 章定义了管理总中心、分中心、被管设备间的安全通道协议，包括安全通道协议框架、安全通道消息的数据项和数据格式、安全通道建立的时机和安全通道的使用。

第 7 章定义了被管设备的对象属性，包括基本信息、接口信息和管理实体信息。

第 8 章定义了总中心与分中心以及中心与被管设备间通过安全通道传递的管理消息，包括消息名称、功能和具体消息格式。

第 9 章规定了设备管理平台对管理应用提供的接口。

附录 A 是规范性附录，定义了错误代码。

附录 B 是规范性附录，定义了安全通道协议框架。

(4) 应用说明

该标准重点定义的是设备管理中心、被管设备以及管理应用之间的通信协议和消息格式，并没有明确规定设备管理中心的权限和访问控制、身份认证等安全机制，在实际开发和使用时应参照其他标准。

2. GM/T 0051 密码设备管理 对称密钥管理技术规范

(1) 版本

GM/T 0051-2016《密码设备管理 对称密钥管理技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准为密码设备制定了对称密钥管理及相关安全技术要求，包括对称密钥管理安全要求、系统体系结构及功能要求、密钥管理安全协议及接口设计要求、管理中心建设、运行及管理要求等。

该标准适用于对称密钥管理系统的研制、建设、运行及管理，也可用于密码设备的研制。

(3) 内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语，第 4 章缩略语。

第 5 章描述了对称密钥管理的安全要求，包括系统安全要求和功能安全要求。其中功能安全要求部分规定了密钥生成、存储和备份、分发和加载、使用、更新、归档、销毁、恢复等整个密钥生命周期的安全要求。

第 6 章描述了密钥管理应用系统在密码基础设施体系结构中的位置、管理范围、系统技术框架、系统功能结构、功能描述和功能设计要求。

第 7 章描述了对称密钥管理应用指令及管理接口。

附录 A 是规范性附录，定义了错误码。

附录 B 是规范性附录，定义了密钥格式配置文件。

(4) 应用说明

——直接相关标准

GM/T 0050 密码设备管理 设备管理技术规范

——扩展应用领域

该标准适用于密码服务平台或密码应用等系统中涉及对密码设备的对称密钥管理的功能，可为其提供对称密钥管理的安全要求和接口规范参考。

3. GM/T 0052 密码设备管理 VPN 设备监察管理规范

(1) 版本

GM/T 0052-2016《密码设备管理 VPN 设备监察管理规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了重要信息系统与网络中的 VPN 设备的监察管理，以发现和定位网络中的非法 VPN 设备，并检测合法设备在使用过程中的违规操作。

该标准适用于 VPN 设备监察管理系统及监察设备的研发与应用，也可用于指导检测该类监察设备。

(3) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章描述了 VPN 设备的监察管理体系结构和监察管理流程。

第 6 章描述了管理应用层向监察设备下发数据包的过滤规则、基于 IPSec VPN 协议的检测规则、基于 SSL VPN 协议的检测规则。

第 7 章定义了 VPN 设备管理应用层和监察设备之间的网络通信消息，包括 VPN 设备的监察设备配置消息、过滤规则消息、告警消息的消息格式。

附录 A 是资料性附录，给出了 XML 格式的通信报文示例。

（4）应用说明

——直接相关标准

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0053 密码设备管理 远程监控与合规性检验接口数据规范

——扩展应用领域

该标准可用于专用 VPN 设备和 VPN 管理平台，也可以用于带有 VPN 功能的安全设备或应用服务器等。商用密码应用安全性评估开展时可以依据该标准对支持相关接口的、已部署的 VPN 设备进行检测。

4. GM/T 0053 密码设备管理 远程监控和合规性检验接口数据规范

（1）版本

GM/T 0053-2016《密码设备管理远程监控和合规性检验接口数据规范》是当前的最新版本。

（2）用途与适用范围

该标准规定了对密码设备进行远程监控、设备合规性检验等管理

应用的接口数据，定义了管理应用与密码设备间的消息传递格式。

该标准适用于密码设备中的管理代理的研发与应用，也可以指导该类密码设备管理代理的检测。

(3) 内容概要

该标准共 6 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章描述了密码设备管理应用体系结构，规定了密码设备、管理代理和安全通信的基本要求。

第 6 章定义了密码设备远程监控与合规性检验的接口数据格式，包括远程监控、设备合规性检验等管理应用的详细消息格式。

(4) 应用说明

——直接相关标准

GM/T 0050 密码设备管理 设备管理技术规范

(四) 技术规范

1. GM/T 0027 智能密码钥匙技术规范

(1) 版本

GM/T 0027-2014 《智能密码钥匙技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准定义了智能密码钥匙的相关术语，描述了智能密码钥匙的功能要求、硬件要求、软件要求、性能要求、安全要求、环境适应性要求和可靠性要求等有关内容。

该标准适用于智能密码钥匙的研制、使用和检测。

(3) 内容概要

该标准共 12 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章描述了智能密码钥匙的功能要求，包括应具备的出厂初始化要求、对密码算法的支持要求、密钥管理要求、设备管理要求、自检要求等。

第 6 章描述了智能密码钥匙的硬件要求，包括了接口、芯片和线路传输要求。

第 7 章描述了智能密码钥匙 APDU 的要求。

第 8 章给出了智能密码钥匙的性能要求。

第 9 章给出了智能密码钥匙的安全要求，包括算法配用、密钥安全、多应用隔离、传输安全、软件防护。

第 10 章给出了智能密码钥匙的环境适应性要求，包括温湿度、机械性能等。

第 11 章给出了智能密码钥匙的可靠性要求，包括平均无故障时间、文件写入次数、掉电保护。

附录 A 是规范性附录，给出了智能密码钥匙应达到的具体性能指标。

（4）应用说明

——直接相关标准

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

——使用注意事项

智能密码钥匙的硬件接口可为 USB、SD、Dock、Lightning、

Bluetooth、NFC、音码、WiFi、ISO7816、ISO14443 或其它接口，使用这些通信接口时应保证通信的安全性。

2. GM/T 0029 签名验签服务器技术规范

(1) 版本

GM/T 0029-2014《签名验签服务器技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了签名验签服务器在研发、生产、使用过程中，必须遵循的技术要求，规定了签名验签服务器需提供的功能、安全服务接口和消息协议语法、密码算法和密钥管理等方面的技术要求。

该标准适用于签名验签服务器的研制设计、应用开发、管理和使用，也可用于指导签名验签服务器的检测。

(3) 内容概要

该标准主要包括 11 部分内容：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章签名验签服务器的功能要求，主要阐述了签名验签服务器的初始化功能、与 CA 基础设施的连接功能、应用管理功能、证书管理和验证功能、数字签名功能、访问控制功能、日志管理功能、系统自检功能、NTP 时间源同步功能。其中，与 CA 基础设施的连接功能包括 CRL 连接配置和 OCSP 连接配置；应用管理功能主要包括应用实体的注册、配置密钥、设置私钥授权码等，以及安全存储要求；证书管理和验证功能包括实体证书和用户证书及根证书或证书链的导入、存储、验证、使用以及备份和恢复等功能；数字签名功能规定了算法和强度要求及数据格式要求；访问控制功能包含身份鉴别机制和实现

方式；日志管理功能包括日志记录内容、查看、审计和导出功能要求；系统自检功能包括密码功能、算法正确性、随机数检查及存储数据完整性检查等；NTP 时间源同步功能要求具有可配置时间源服务器及自动同步时间功能。

第 6 章签名验签服务器的安全要求，包括密码设备、系统要求、使用要求、管理要求、设备物理安全防护、网络部署要求、应用编程接口 API、环境适应性及可靠性。其中，管理要求包含管理角色要求、设备初始化、设备自检等；网络部署要求对网络环境、服务方式做出要求，并列举了常见的 4 种网络部署方式；应用编程接口定义了签名验签服务器应遵循两种接口规范中的一种。

第 7 章签名验签服务器检测要求，包括外观和结构的检查、提交文档的检查、功能检查、性能检查、环境适应性检查等，定义了针对第 5 章、第 6 章中要求的各检测项的检测内容、检测方法、判定条件等。

第 8 章给出了合格判定的标准，定义了第 7 章中必须检测通过的项目。

附录 A、B、C 均为资料性附录。其中附录 A 给出了签名验签服务器的消息协议语法规则，是签名验签服务器遵循的两种接口规范之一；附录 B 给出了基于 HTTP 的签名消息协议语法规则，是附录 A 的一种扩展实现；附录 C 给出了签名验签服务器应用编程接口的响应码定义和说明。

（4）应用说明

——直接相关标准

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 19713 信息技术 安全技术 公钥基础设施 在线证书状态协议

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 20518 信息安全技术 公钥基础设施数字证书格式规范

GM/T 0020 证书应用综合服务接口规范

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0060 签名验签服务器检测规范

——扩展应用领域

以签名验签服务器为安全支撑的密码产品或密码系统，如电子签章系统，应依据该标准执行。

——使用注意事项

签名验签服务器的安全性设计除满足该标准要求外，还应遵循 GB/T 37092 《信息安全技术 密码模块安全要求》。签名验签服务器的产品检测按照 GM/T 0060 《签名验签服务器检测规范》和 GM/T 0039 《密码模块安全检测要求》执行。该标准没有定义密码服务通道的安全要求，如有需要则应遵循 GM/T 0024 《SSL VPN 技术规范》。签名验签服务器接受密码设备管理中心管理时应遵循 GM/T 0050 《密码设备管理 设备管理技术规范》。

3. GM/T 0030 服务器密码机技术规范

(1) 版本

GM/T 0030-2014 《服务器密码机技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了服务器密码机需提供的功能、服务接口、密码算法和密钥管理等方面的要求；同时也定义了服务器密码机必须提供的物

理安全防护措施，以及用户在服务器密码机的使用和管理上必须满足的要求。

该标准适用于服务器密码机的研制、使用和检测，保证服务器密码机基本技术规格的一致性。

（3）内容概要

该标准共 10 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章服务器密码机功能要求，包括密码机的初始化、密码运算、密钥管理、随机数生成和检验、访问控制、设备管理、日志审计、设备自检的要求。其中，密码运算部分提出了服务器密码机应至少支持的密码算法和运算模式；密钥管理部分定义了密钥安全结构及产生、安装、存储、使用、销毁以及备份和恢复等整个密钥生命周期中的安全要求。

第 6 章服务器密码机硬件要求，包括密码机对外接口、随机数发生器、环境适应性以及可靠性。其中，对外接口要求服务接口和管理接口分离；随机数发生器要求至少使用两个独立的物理噪声源芯片实现，并要求支持出厂检测、上电检测、使用检测。

第 7 章服务器密码机软件要求，包括基本要求、应用编程接口和管理工具。其中，应用编程接口实现应遵循 GM/T 0018《密码设备应用接口规范》；管理工具可以是内部管理程序也可以是外部管理中心。

第 8 章服务器密码机安全要求，包括密码算法、密钥管理、系统要求、使用要求、管理要求、设备物理安全防护、设备状态、过程保护。其中，密钥管理进一步对管理密钥和内部存储的密钥提出安全要

求；管理要求定义了远程管理的内容、管理员安全管理、设备初始化、设备检查等安全事项。

第 9 章服务器密码机检测要求，包括外观和结构的检查、提交文档的检查、功能检查、性能检查、环境适应性检查等，定义了针对第 5 章、第 6 章、第 7 章、第 8 章中要求的各检测项的检测内容、检测方法、判定条件等。

第 10 章是合格判定，定义了第 9 章中必须检测通过的项目。

(4) 应用说明

——直接相关标准

GM/T 0018 密码设备应用接口规范

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0059 服务器密码机检测规范

——扩展应用领域

以服务器密码机为基础进行功能扩展的密码产品可依据该标准执行。以服务器密码机为安全支撑的密码产品或密码系统，如证书认证系统、密钥管理系统、电子签章系统等，应依据该标准执行。

——使用注意事项

服务器密码机的产品检测按照 GM/T 0059《服务器密码机检测规范》和 GM/T 0039《密码模块安全检测要求》执行。该标准没有定义服务通道的安全要求，如有需要则应遵循 GM/T 0024《SSL VPN 技术规范》。服务器密码机接受密码设备管理中心管理时应遵循 GM/T 0050《密码设备管理 设备管理技术规范》。

4. GM/T 0045 金融数据密码机技术规范

(1) 版本

GM/T 0045-2016《金融数据密码机技术规范》是当前的最新版本。

（2）用途与适用范围

该标准规定了金融数据密码机的功能要求、硬件要求、业务要求、安全性要求和检测要求，可用于指导金融数据密码机的研制、检测、使用和管理。

（3）内容概要

该标准共 10 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章功能要求，从密码算法、密钥管理、随机数、访问控制、设备管理、设备初始化、设备自检等方面规定了金融数据密码机应当具备的功能。

第 6 章硬件要求，规定了金融数据密码机应当具备的物理接口、状态指示器、随机数发生器等部件，并明确了环境适应性和可靠性的具体指标。

第 7 章安全业务要求，规定了金融数据密码机的算法工作模式和初始向量、数据报文接口格式，并针对磁条卡应用、IC 卡应用和基础密码运算服务，明确了应当支持的业务功能和输入输出数据格式，同时还规定了通用错误码。

第 8 章安全性要求，规定了金融数据密码机的安全性应当符合 GM/T 0028《密码模块安全技术要求》的要求。

第 9 章检测要求，规定了金融数据密码机的具体检测项目，分为功能检测、性能检测、环境适应性检测和安全性检测。

第 10 章合格判定，规定了除“性能检测”外，第 9 章规定的所

有检测项目必须检测通过方为合格。

(4) 应用说明

——直接相关标准

GM/T 0046 金融数据密码机检测规范

——扩展应用领域

该产品可用于金融相关业务系统开发参考，金融交易相关密码产品（如密码键盘）在研发过程中也可以参照该标准。

(五) 产品规范

1. GM/T 0023 IPsec VPN 网关产品规范

(1) 版本

GM/T 0023-2014《IPsec VPN 网关产品规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了 IPsec VPN 网关产品研制要求和检测要求，可用于指导 IPsec VPN 网关产品的研制、检测、使用和管理。

(3) 内容概要

该标准共 7 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和缩略语。

第 4 章描述了 IPsec VPN 的密码算法、密钥种类及定义。该部分规定了 IPsec VPN 网关产品应使用的算法及其使用方式，定义了设备密钥、工作密钥和会话密钥。

第 5 章描述了 IPsec VPN 的产品要求，包括功能、性能参数和安全管理要求。

第 6 章描述了 IPsec VPN 的产品检测要求，与第 5 章内容相对应。

第 7 章规定了 IPsec VPN 网关产品检测判定标准。

(4) 应用说明

——直接相关标准

GB/T 36968 信息安全技术 IPSec VPN 技术规范

2. GM/T 0025 SSL VPN 网关产品规范

(1) 版本

GM/T 0025-2014《SSL VPN 网关产品规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了 SSL VPN 网关产品的功能、性能、安全性、管理等要求以及产品检测方法，适用于 SSL VPN 网关产品研制、检测、使用和管理。

(3) 内容概要

该标准共 7 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和缩略语。

第 4 章描述了 SSL VPN 网关产品采用的算法和使用方式。

第 5 章以 GM/T 0024《SSL VPN 技术规范》第 7 章内容为基础进行扩充。其中，产品功能要求明确了产品应采用多路硬件噪声源产生随机数，补充了信息审计和信息传递要求；将 GM/T 0024 标准的安全管理要求拆分为安全性要求和管理要求，明确了会话密钥安全保护要求，对日志格式和设备自检内容进行详细描述，补充了针对 SSL VPN 网关产品的硬件要求、过程保护要求和参数可配置能力要求。

第 6 章以 GM/T 0024《SSL VPN 技术规范》第 8 章内容为基础进行扩充。对最大并发用户数和最大并发连接数的涵义进行了详细描述，并针对该标准第 5 章的扩充内容明确相应的检测要求。

第 7 章描述了 SSL VPN 产品检测判定标准。

(4) 应用说明

——直接相关标准

GM/T 0024 SSL VPN 技术规范

3. GM/T 0026 安全认证网关产品规范

(1) 版本

GM/T 0026-2014《安全认证网关产品规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了安全认证网关产品的密码算法和密钥种类、功能要求、硬件要求、软件要求、安全性要求、管理要求和检测要求，适用于安全认证网关产品的研制、检测、使用和管理。

(3) 内容概要

该标准共 9 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章符号和缩略语。

第 5 章描述了安全认证网关产品的功能、部署模式以及与一般安全网关产品的区别。该部分规定了安全认证网关基于数字证书向应用系统提供用户管理、身份鉴别、单点登录、传输加密、访问控制和安全审计等功能，规定了网关产品必须支持物理串联部署模式，可选支持物理并联部署模式。

第 6 章描述了安全认证网关的密码算法、密钥分类及定义。该部分规定了安全认证网关产品应采用的密码算法和使用方式；定义了设备密钥、工作密钥和会话密钥。

第 7 章描述了安全认证网关产品的功能要求、性能参数、安全性要求、管理要求、硬件要求和过程保护。

产品功能要求规定：应支持对访问用户和需要保护的应用进行管理，并支持单点登录、NAT 穿越、抗重放攻击等功能；应基于数字证书实现用户身份鉴别，并规定了代理模式和调用模式下基于 IPSec 协议和 SSL 协议实现身份鉴别的要求；可基于用户管理和应用管理信息制定访问控制策略；应根据其实现协议，分别遵循 GM/T 0022《IPSec VPN 技术规范》和 GM/T 0024《SSL VPN 技术规范》标准。

安全性要求规定了密钥安全、密钥配置安全等要求。

管理安全规定了安全认证网关的远程管理、日志管理、设备初始化、设备注册及监管、设备自检和管理员权限及口令限制等要求。

硬件要求规定了安全认证网关的接口、加密部件、随机数发生器、环境适应性及电磁兼容等要求。

过程保护规定了安全认证网关在安装、运输过程中软硬件功能不被恶意篡改等要求。

第 8 章描述了安全认证网关产品的检测要求，包括功能检测要求、性能检测要求、安全管理检测要求。

第 9 章描述了安全认证网关产品检测判定标准。

（4）应用说明

——直接相关标准

GM/T 0024 SSL VPN 技术规范

GM/T 0022 IPSec VPN 技术规范

五 应用支撑类标准

(一) 通用支撑

1. GM/T 0019 通用密码服务接口规范

(1) 版本

GM/T 0019-2012《通用密码服务接口规范》是当前的最新版本。

(2) 用途与适用范围

该标准主要为典型密码服务层和应用层规定了统一的、与密码协议无关、与密钥管理无关、与密码设备管理无关的通用密码服务接口。

该标准规定的是使用公钥密码算法、使用双数字证书机制的密码服务。

该标准适用于通用密码服务相关产品的研制、检测和使用。

(3) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章算法标识和数据结构，定义了数字证书内容和对应的密钥容器结构。

第 6 章密码服务接口，将通用密码服务接口分为环境类函数、证书类函数、密码运算类函数和消息类函数四类。环境类函数用于创建和管理程序空间、创建和管理所需的各种资源、创建与密码设备的安全连接和管理用户与密钥的对应访问令牌；证书类函数用于实现数字证书的获取、解析与验证。数字证书为使用 SM2/SM3 算法的双数字证书；密码运算类函数用于随机数生成、对称算法计算、非对称算法计

算和数据编解码；消息类函数用于对数据进行进一步封装，封装成符合 GB/T 35275 《信息安全技术 SM2 密码算法加密签名消息语法规则》要求的消息数据。

第 7 章密码服务接口函数定义，分别对环境类函数、证书类函数、密码运算类函数、消息类函数进行了定义和说明。

附录 A 是规范性附录，定义了密码服务接口调用后可能返回的错误代码。

（4）应用说明

——直接相关标准

GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

GB/T 36322 信息安全技术 密码设备应用接口规范

——使用注意事项

该标准类似于 CSP 和 PKCS#11，都是提供底层密码服务，但该标准和 CSP、PKCS#11 在标准协同性、数据格式、接口定义存在诸多不同。依据该标准提供的密码服务接口和 CSP、PKCS#11 接口不能简单替换。依据 CSP、PKCS#11 接口开发的应用系统需要根据该标准重新设计开发。

2. GM/T 0020 证书应用综合服务接口规范

（1）版本

GM/T 0020-2012 《证书应用综合服务接口规范》是当前的最新版本。

（2）用途与适用范围

该标准定义了证书应用综合服务接口，分为客户端接口和服务端接口两类。证书应用综合服务接口位于应用系统和典型密码服务接

口之间，向应用层直接提供证书信息解析、基于数字证书身份认证和信息的机密性、完整性、不可否认性等高级密码服务。

该标准规定了与密码协议、密钥管理、密码设备管理无关的面向证书应用的统一服务接口，为密码系统中间件提供规范依据。

该标准适用于基于数字证书的密码服务相关产品的研制、检测与使用。

（3）内容概要

该标准共 10 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章给出了该标准所采用的标识和数据结构要求。

第 6 章证书应用综合服务接口概述，主要对客户端服务接口、服务器端服务接口进行了简要说明。其中，服务器端服务接口采用 COM 组件形式和 Java 形式两类，适用于服务器端程序调用，接口的形态包括 COM 组件、JAR 包、WebService 等形态；客户端服务接口采用客户端控件方式形态包括 DLL 动态库、ActiveX 控件、Applet 插件等。

第 7 章证书应用综合服务接口函数定义，分别对客户端的 31 个控件接口函数、服务端的 35 个 COM 组件接口函数和 36 个 JAVA 组件接口函数进行了定义和说明。

附录 A 是规范性附录，定义了证书应用综合服务接口的错误代码。

附录 B 是资料性附录，给出了一个证书应用综合服务接口的典型部署模型。

附录 C 是资料性附录，给出了一个证书应用综合服务接口的集成示例。

(4) 应用说明

——直接相关标准

GM/T 0019 通用密码服务接口规范

——扩展应用领域

除标准中规定的服务接口形态，还允许使用 HTTP、RPC、Socket 等其他服务接口形态。

——使用注意事项

当以网络通信接口形态提供服务接口时，应确保通信信道的安全性。

3. GM/T 0032 基于角色的授权管理与访问控制技术规范

(1) 版本

GM/T 0032-2014《基于角色的授权管理与访问控制技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了基于角色的授权与访问控制框架结构及框架内各组成部分的逻辑关系；定义了各组成部分的功能、操作流程及操作协议；定义了访问控制策略描述语言、授权策略描述语言的统一格式和访问控制协议的标准接口。

该标准适用于公钥密码基础设施应用技术体系下基于角色的授权与访问控制系统的研制，并可指导对该类系统的检测及相关应用的开发。

(3) 内容概要

该标准共 10 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4

章缩略语。

第 5 章授权与访问控制框架，描述了保障授权信息、访问控制策略的安全性、完整性和有效性的方法，及与具体应用无关的访问控制的机制。

第 6 章访问控制策略描述语言，定义了角色、资源、操作权限间的逻辑关系。

第 7 章授权策略描述语言，定义了主体与角色间的分配关系。

第 8 章访问控制协议，定义了应用系统与访问控制系统间的接口。

第 9 章定义了应用系统必须满足的基本要求。

附录 A 是规范性附录，定义了访问控制判定状态代码。

（4）应用说明

——直接相关标准

GM/T 0019 通用密码服务接口规范

——使用注意事项

应用开发商、用户单位权限主管部门和访问控制产品开发商按照上述描述实现访问控制策略、授权策略和访问控制协议后，访问控制产品和应用系统就可以互联。

在标准的使用中，应该注意以下几个方面的问题：

访问控制执行部件可以是由独立的服务实现，也可直接由应用系统实现。

应用系统开发商应按访问控制策略描述语言的要求来描述应用的访问控制策略，绑定角色与资源。通常，应用功能被确定后，角色表达应相对稳定。

用户的权限管理部门按照应用的角色表达，将角色分配给用户，

或修改用户与角色的对应关系。

访问控制系统应在访问控制判定前完成身份鉴别，该标准不对身份鉴别过程进行规范。

4. GM/T 0033 时间戳接口规范

(1) 版本

GM/T 0033-2014《时间戳接口规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了时间戳服务的标准接口，用以实现和具体时间戳系统无关以及和证书认证系统无关的时间认证服务，保证时间戳服务对用户、对应用的透明性和无关性。应用系统一般不直接访问时间戳基础设施，而是通过该标准的接口中间件访问基础设施。

该标准规定了面向应用系统和时间戳系统的时间戳服务接口，包括时间戳请求和响应消息的格式、传输方式和时间戳服务接口函数。

该标准适用于指导基于公钥密码基础设施应用技术体系框架内的时间戳服务相关产品的研制、使用与检测。

(3) 内容概要

该标准共 11 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章定义了标识、密码服务接口以及时间戳服务接口常量。

第 6 章描述了时间戳服务在公钥基础设施技术体系架构中的位置以及接口的逻辑结构。

第 7 章定义了时间戳服务请求格式和响应格式。

第 8 章定义了时间戳服务与时间戳服务机构的 5 种通讯方式，包

括电子邮件方式、文件方式、Socket 方式、HTTP 方式和 SOAP 方式，并规定了消息传输格式。

第 9 章描述了 7 个与时间戳服务有关的函数，涵盖了获取时间戳服务的全部功能，包括环境函数和时间戳服务函数两大类。

附录 A 是规范性附录，定义了时间戳接口错误代码。

附录 B 是资料性附录，给出了时间戳接口应用的一个示例。

(4) 应用说明

——直接相关标准

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式规范

GM/T 0019 通用密码服务接口规范

GM/T 0018 密码设备应用接口规范

——扩展应用领域

时间戳服务接口可以以多种形式提供，该标准提供了一个 C 语言接口，开发者可以根据不同的开发语言和开发平台提供相应的接口。

5. GM/T 0057 基于 IBC 技术的身份鉴别规范

(1) 版本

GM/T 0057-2018《基于 IBC 技术的身份鉴别规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了基于 SM9 密码算法的身份鉴别协议，给出了标识具体定义、鉴别过程中的参数定义和具体流程。

该标准适用于基于 SM9 标识密码算法的身份鉴别系统和产品的研发、应用和检测。

(3) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章定义了标识的数据结构。

第 6 章定义了用户身份鉴别协议，包括两种单向身份鉴别要求（接收者鉴别发起者身份、发起者鉴别接收者身份）和一种双向身份鉴别协议。该标准描述了三种协议的具体流程，定义了其参数数据格式。

附录 A 是规范性附录，定义了公共参数查询相关协议。

附录 B 是规范性附录，定义了 SM9 密码算法密钥数据结构和签名加密数据结构。

（4）应用说明

——直接相关标准

GM/T 0044 SM9 标识密码算法

6. GM/T 0067 基于数字证书的身份鉴别接口规范

（1）版本

GM/T 0067-2019《基于数字证书的身份鉴别接口规范》是当前的最新版本。

（2）用途与适用范围

该标准规定了公钥密码基础设施体系上层应用中基于数字证书的身份鉴别接口。

该标准适用于公钥密码基础设施体系上层应用中身份鉴别服务的开发，证书应用支撑平台身份鉴别系统的研制及检测，也可用于指导应用系统规范化地使用证书进行身份鉴别。

(3) 内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章缩略语。

第 5 章描述了身份鉴别代理鉴别和调用模式两种实现方式。

第 6 章定义了算法标识与数据结构。其中，算法标识定义包含数据类型、常量和全局参数。

第 7 章定义了基于数字证书的身份鉴别接口及函数，包括身份鉴别接口在公钥密码基础设施应用技术体系框架中的位置、逻辑结构、消息定义和接口函数。

附录 A 是规范性附录，定义了错误代码。

附录 B 是资料性附录，给出了身份鉴别应用流程示例。

(4) 应用说明

——直接相关标准

GB/T 15843.1 信息技术 安全技术 实体鉴别 第 1 部分：概述

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

——使用注意事项

该标准针对的身份鉴别框架是在 GB/T 15843.3 中规定的采用数字签名技术的鉴别机制，采用其他鉴别机制的身份鉴别接口不适用该标准。

7. GM/T 0068 开放的第三方资源授权协议框架

(1) 版本

GM/T 0068-2019《开放的第三方资源授权协议框架》是当前的最新版本。

(2) 用途与适用范围

该标准规定了第三方资源授权协议的流程、不同类型的授权许可、协议各端点的功能要求以及系统实体之间传递消息的格式和参数要求等。

该标准适用于在互联网跨安全域应用场景中，身份鉴别与授权服务的开发、测试、评估和采购。

(3) 内容概要

该标准共 10 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章缩略语。

第 5 章描述了协议流程、协议通道要求、协议端点。其中，协议端点包含授权端点、令牌端点和重定向端点。

第 6 章提出了第三方应用程序及安全要求，规定了第三方应用程序的类型、标识符、注册要求、身份鉴别方案和安全要求。

第 7 章描述了授权码许可流程、隐藏式许可流程、资源拥有者口令凭据许可流程、第三方应用程序身份凭据许可流程 4 种授权许可流程，并对每种授权许可流程从协议流程、授权请求和响应、访问令牌请求和响应等方面提出了具体的要求。

第 8 章描述了访问令牌和刷新令牌两种令牌类型，规定了访问令牌的发放流程以及刷新令牌的发放和验证机制。

第 9 章描述了受保护资源访问流程。

附录 A 是资料性附录，描述了 OAuth 的协议参数和错误码。

(4) 应用说明

——直接相关的标准

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

GM/T 0069 开放的身份鉴别框架

8. GM/T 0069 开放的身份鉴别框架

(1) 版本

GM/T 0069-2019《开放的身份鉴别框架》是当前的最新版本。

(2) 用途与适用范围

该标准规定了依赖方（网络应用或服务）使用身份服务提供方提供的鉴别功能、对终端用户进行身份鉴别的协议框架，定义了协议参与实体的要求、鉴别协议流程、用户信息的访问要求、以及协议消息的加密和签名要求等。

该标准适用于终端用户访问网络应用的场景中，用户身份鉴别服务的开发、测试、评估和采购。

(3) 内容概要

该标准共 13 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章缩略语。

第 5 章描述了身份鉴别协议框架，包括 3 类参与实体及相关协议。其中，3 类参与实体分别为依赖方、身份服务提供方和终端用户；协议包括鉴别请求、鉴别与授权、鉴别响应、用户信息请求、用户信息

响应等。

第6章提出了对身份服务提供方和依赖方2类实体的要求。其中，对身份服务提供方提出了安全管理用户信息要求、安全配置协议要求、安全传输和处理协议要求、鉴别与授权要求；对依赖方是否具有保密能力，从注册和协议配置、身份鉴别等方面提出了要求。

第7章描述了鉴别流程，包括授权码鉴别流程、隐式鉴别流程、混合鉴别流程。其中，授权码鉴别流程适用于可以安全保存密钥的依赖方；隐式鉴别流程主要用于在浏览器中使用脚本语言实现的依赖方或本机应用程序类型的依赖方；混合鉴别流程适用于没有安全保存机密信息能力的依赖方。

第8章提出了令牌类型、JSON令牌和令牌安全保护要求。其中，令牌类型包括ID令牌、访问令牌和刷新令牌；JSON令牌包括签名JSON令牌、加密JSON令牌、嵌套JSON令牌、JSON令牌密钥、JSON令牌算法；规定了访问令牌、刷新令牌和ID令牌等令牌的安全保护要求。

第9章提出了用户信息访问的要求，包括对声明的类型、语言和文字声明、用户信息端点、用户信息请求声明、声明的稳定性和唯一性等的要求。

第10章提出了签名和加密要求。其中，签名算法包括非对称签名算法和对称签名算法；加密算法包括非对称加密算法和对称加密算法。

（4）应用说明

——直接相关的标准

GM/T 0068 开放的第三方资源授权协议框架

(二) 典型支撑

1. GB/T 29829 信息安全技术 可信计算密码支撑平台功能与接口规范

(1) 版本

GB/T 29829-2013《信息安全技术 可信计算密码支撑平台功能与接口规范》系该标准国家标准最新版本。

该标准对应的密码行业标是 GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》，最后版本为 GM/T 0011-2012。

(2) 用途与适用范围

该标准描述了可信计算密码支撑平台功能原理与要求，定义了可信计算密码支撑平台的密码算法、密钥管理、证书管理、密码协议、密码服务等应用接口规范。

该标准适用于可信计算密码支撑平台相关产品的研制、生产、测评与应用开发。

(3) 内容概要

该标准共 7 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语、定义和缩略语。

第 4 章可信计算密码支撑平台功能原理，描述了平台体系结构、密码算法要求和功能原理，核心内容是平台构成、TCM（可信密码模块）和 TSM（TCM 服务模块）三者之间的关系，以及平台完整性、平台身份可信和平台数据安全保护三方面的功能原理。

第 5 章可信计算密码支撑平台功能接口，描述了上下文管理、策略管理、可信密码模块管理、密钥管理、数据加密与解密、PCR（平

台配置寄存器)管理、杂凑操作和密钥协商八个模块的功能接口、参数以及与其他接口的关系。

附录 A、B 均为规范性附录，附录 A 定义了数字证书格式；附录 B 定义了相关接口的数据结构。

(4) 应用说明

——直接相关标准

GM/T 0012 可信计算 可信密码模块接口规范

GM/T 0013 可信密码模块接口符合性测试规范

GM/T 0058 可信计算 TCM 服务模块接口规范

六 密码应用类标准

(一) 应用要求

1. GM/T 0054 信息系统密码应用基本要求

a) 版本

GM/T 0054-2018《信息系统密码应用基本要求》是当前的最新版本。

b) 用途与适用范围

该标准规定了信息系统密码应用的基本要求。

该标准适用于指导和规范关键信息基础设施、网络安全等级保护对象、以及其他重要领域网络与信息系统中的密码应用。

该标准是信息系统密码应用的总体性标准，提出了密码算法、密码技术、密钥管理、安全管理、密码产品和密码服务等方面的密码应用要求，是保障密码应用安全的重要指导。信息系统的责任单位可以依据该标准开展密码应用系统的规划和建设，并按照《密码法》等法

法律法规和相关标准规范的要求开展商用密码应用安全性评估。

c) 内容概要

该标准共 11 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章规定了密码算法、密码技术、密码产品、密码服务总体要求。

第 6 章规定了信息系统的机密性、完整性、真实性和不可否认性等密码功能要求。

第 7 章分四个安全等级规定了信息系统中的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等密码应用要求。

物理和环境安全主要包括物理访问控制及访问控制记录、监控信息等敏感信息数据完整性的安全保护要求。其中，第一级对密码使用不做要求；第二级推荐使用密码技术进行安全保护，并推荐使用二级及以上密码模块；第三级要求使用密码技术实现安全保护，并推荐使用三级及以上密码模块；第四级在第三级安全要求基础上，要求使用三级及以上密码模块。

网络和通信安全主要包括网络设备认证、通信双方身份认证、数据通信、访问控制信息、安全设备管理的安全保护要求。其中，第一级对密码使用不做要求；第二级推荐使用密码技术实现鉴别信息机密性、网络设备实体身份鉴别、访问控制信息完整性、数据通信完整性、敏感信息数据机密性的安全保护，并推荐使用二级及以上密码模块；第三级要求使用密码技术实现第二级的安全要求，增加了使用密码技术实现设备管理安全通道的安全保护，并推荐使用三级及以上密码模

块；第四级在第三级安全要求基础上，要求使用三级及以上密码模块。

设备和计算安全主要包括用户登录身份鉴别、访问控制信息、重要信息资源敏感标记、重要程序和文件、日志记录的安全保护要求。其中，第一级对密码使用不做要求；第二级推荐使用密码技术实现用户身份标准和鉴别、远程登录鉴别信息机密性、访问控制信息完整性、重要信息资源敏感标记完整性、日志记录完整性的安全保护，并推荐使用二级及以上密码模块；第三级要求使用密码技术实现第二级的安全要求，并推荐使用三级及以上密码模块；第四级在第三级安全要求基础上，要求使用三级及以上密码模块。

应用和数据安全主要包括用户身份鉴别、访问控制信息、重要信息资源敏感标记、重要数据传输、重要数据存储、重要程序、实体行为、日志记录的安全保护要求。其中，第一级对密码使用不做要求；第二级推荐使用密码技术实现用户身份鉴别、访问控制信息完整性、重要信息资源敏感标记完整性、重要数据传输机密性和完整性、重要数据存储机密性和完整性、日志记录完整性的安全保护，并推荐使用二级及以上密码模块；第三级要求使用密码技术实现第二级的安全要求，增加了使用密码技术实现应用程序加载和卸载的安全保护，并推荐使用三级及以上密码模块；第四级在第三级安全要求基础上，增加了应采用密码技术实现对数据原发行为和数据接收行为的不可否认性要求，并要求使用三级及以上密码模块。

第8章规定了四个安全等级的密钥全生命周期的安全要求，包括密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节。

第9章规定了四个安全等级的安全管理要求，包括制度、人员、

实施和应急等方面。

附录 A 是资料性附录，给出了不同安全保护等级信息系统中的密码技术应用要求，汇总了要求的各个条款和不同等级的推荐强度。

附录 B 是资料性附录，给出了截至 2017 年年底已经发布的密码行业标准列表。

d) 应用说明

——直接相关标准

GM/T 0028 密码模块安全技术要求

——使用注意事项

该标准是开展商用密码应用安全性评估工作的基础性标准，但该标准并没有规定商用密码应用安全性评估的开展过程，《信息系统密码应用测评要求》和《商用密码应用安全性测评过程指南》等详细规范测评活动的密码行业标准目前还在制定发布过程中。

(二) 典型应用

1. GM/T 0021 动态口令密码应用技术规范

(1) 版本

GM/T 0021-2012《动态口令密码应用技术规范》是当前最新版本。

(2) 用途与适用范围

动态口令是一种一次性口令机制。用户无需记忆口令，也无需手工更改口令，口令通过用户持有的客户端器件生成，并基于一定的算法与服务端形成同步，从而作为证明用户身份的依据。动态口令机制可广泛用于身份鉴别场合。

该标准规定了动态口令应用相关的动态口令系统、动态口令生成方式、动态令牌特性、认证系统、密钥管理系统等内容，适用于动

态令牌、动态口令认证系统的研制、生产及检测。

(3) 内容概要

该标准共 13 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号。

第 5 章定义了动态口令系统的框架和认证原理。

第 6 章描述了动态口令的生成方式，该标准给出了基于 SM3 密码杂凑算法和基于 SM4 分组密码算法的口令生成方式。

第 7 章描述了动态令牌的特性，包括物理特性和安全特性，为动态令牌的产品设计提出了要求。

第 8 章描述了认证系统，即动态令牌应用的服务端系统的构成及功能要求。

第 9 章描述了动态口令系统所依赖的密钥管理系统的构成和功能要求，包括系统架构、功能要求、安全性设计和硬件接口要求。

附录 A 是资料性附录，给出了动态口令生成算法的 C 语言示例。

附录 B 是资料性附录，给出了动态口令生成算法的计算示例。

附录 C 是资料性附录，给出了动态口令计算参数说明及示例。

附录 D 是资料性附录，给出了一个认证系统的接口示例。

(4) 应用说明

——直接相关标准

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

——使用注意事项

依据该标准开发的动态令牌和动态口令认证系统，只用于用户身

份鉴别。动态口令认证系统向应用系统提供的接口应确保安全。

2. GM/T 0031 安全电子签章密码技术规范

(1) 版本

GM/T 0031-2014《安全电子签章密码应用技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了电子印章和电子签章数据结构格式，给出了验证流程。

该标准适用于电子签章产品的研发、应用和检测，有利于相关应用的标准化和互联互通。

(3) 内容概要

该标准共 6 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章描述了电子签章应用的安全机制，简要概述了电子签章采用的密码技术体系、安全性保障机制和应用呈现效果。

第 6 章定义了电子签章密码应用协议，包括电子印章的数据结构格式和验证流程，电子签章的数据结构格式，以及电子签章的生成与验证流程。

(4) 应用说明

——直接相关标准

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0047 安全电子签章密码检测规范

——使用注意事项

该标准中存在使用 RSA 和相关算法的描述。在实际使用中，应使用 SM2、SM3 密码算法。

3. GB/T 37033 信息安全技术 射频识别系统密码应用技术要求

(1) 版本

GB/T 37033-2018《信息安全技术 射频识别系统密码应用技术要求》系该标准国家标准最新版本。共分为 3 个部分：

GB/T 37033.1-2018《信息安全技术 射频识别系统密码应用技术要求 第 1 部分 密码安全保护框架及安全级别》

GB/T 37033.2-2018《信息安全技术 射频识别系统密码应用技术要求 第 2 部分 电子标签与读写器及其通信密码应用技术要求》

GB/T 37033.3-2018《信息安全技术 射频识别系统密码应用技术要求 第 3 部分 密钥管理技术要求》

该标准对应的密码行业标准是 GM/T 0035《射频识别系统密码应用技术要求》（5 个部分），最后版本为 GM/T 0035-2014。

(2) 用途和适用范围

该标准第 1 部分定义了射频识别系统密码保护安全框架，描述了该标准适用的场景，规定了射频识别系统密码安全级别及对各级别的要求。该部分适用于射频识别系统密码安全的设计、实现与应用。

该标准第 2 部分规定了采用密码技术的电子标签芯片、读写器及其通信的密码安全要素和密码安全技术要求。该部分适用于采用密码安全技术的电子标签芯片和读写器的设计开发、生产制造和应用。

该标准第 3 部分规定了射频识别系统在采用密码机制时电子标

签、读写器及其通信相关的密钥管理要求。该部分适用于射频识别系统中密钥管理系统的设计、实现与应用。

(3) 内容概要

该标准分为 3 个部分，描述了统一框架下对射频识别系统的电子标签芯片、读写器、通信和密钥管理的要求。

该标准第 1 部分共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章规定了射频识别系统密码安全保护框架，包括电子标签、电子标签和读写器间的通信、读写器、读写器与中间件通信、中间件、中间件与信息处理系统通信、信息处理系统和密钥管理系统。

第 6 章规定了安全级别及划分标准。共分为 4 级，每个级别在身份鉴别、访问控制、机密性、完整性、抗抵赖和审计等安全机制方面具有不同的安全技术要求。

第 7 章规定了采用的密码算法种类及其用途。

本部分附录 A 是资料性附录，给出了电子标签防伪应用密码安全解决方案。

该标准第 2 部分共 12 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章给出了电子标签和读写器及其通信密码安全示意图。

第 6 章规定了电子标签、读写器及二者通信的安全要素。

第 7 章根据该标准第 1 部分规定了不同的系统安全级别对电子标签、读写器及通信的密码安全技术要求。

第 8 章规定了传输信息的保密性、完整性和身份鉴别的实现方式。其中，机密性部分规定了传输密钥的产生模式和信息加密的实现方法；完整性部分描述了采用 CBC-MAC 和 HMAC 两种方式进行完整性校验的实现过程；身份鉴别部分描述了唯一标识符鉴别、单向身份鉴别和双向身份鉴别的具体过程。

本部分附录 A 是资料性附录，给出了电子标签芯片设计实例。

本部分附录 B 是资料性附录，给出读写器密码应用安全实例。

本部分附录 C 是资料性附录，描述了采用对称分组密码算法的双向身份鉴别与流加密应用过程。

本部分附录 D 是资料性附录，描述了采用非对称密码算法的双向身份鉴别和密钥协商过程。

该标准第 3 部分共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章描述了射频识别系统密钥管理的安全要素和密码体制。

第 6 章规定了密钥管理模型，包含了密钥生命周期中的密钥生成、分发、使用和销毁等过程。

第 7 章规定了密钥管理的通用要求，包括生成、传输/分发、存储和使用要求。

第 8 章规定了密钥管理应用要求，包括对称密钥的身份鉴别、访问控制、机密性和完整性，以及非对称密钥的鉴别、机密性和完整性。

该部分附录 A 是资料性附录，给出了射频识别系统的密钥管理示例。

(4) 应用说明

——直接相关标准

GM/T 0008 安全芯片密码检测准则

GM/T 0036 采用非接触卡的门禁系统密码应用技术指南

GM/T 0040 射频识别标签模块密码检测准则

——扩展应用领域

可用于采用 135KHz、13.56MHz、433MHz、800/900MHz、2.45GHz 的短距离射频识别系统，如防伪溯源、电子票证、小额支付等应用。

可用于采用 NB-IoT 协议和 LoRa 协议窄带通信的长距离射频识别系统，如智能表计、智能门锁、智能路灯、智能烟感、物品跟踪等应用。

——使用注意事项

标准中规定的安全等级指的是射频识别系统的安全等级，不同的系统安全等级对电子标签芯片、读写器和通信协议提出了不同的安全要素要求。

电子标签芯片应符合《GM/T 0008 安全芯片密码检测准则》或《GM/T 0040 射频识别标签模块密码检测准则》；读写器应符合《GB/T 37092-2018 信息安全技术 密码模块安全要求》和《GM/T 0039 密码模块安全检测要求》。

该标准只规定了电子标签安全、电子标签与读写器通信安全、读写器安全和密钥管理，其它部分属于信息系统范畴，该标准未作规定。

4. GM/T 0036 采用非接触卡的门禁系统密码应用技术指南

(1) 版本

GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》是当前的最新版本。

（2）用途和适用范围

该标准规定了采用非接触式 IC 卡的门禁系统中使用的密码算法、密码设备、密码协议和密钥管理等技术要求。

该标准适用于采用非接触式 IC 卡的门禁系统，包括新建重要门禁系统的设计和实现、已建重要门禁系统中密码系统的改造。

（3）内容概要

该标准共 10 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章描述了系统构成，包括应用系统、密钥管理及发卡系统。应用系统由门禁卡、门禁卡读卡器和后台管理系统构成，通过密码模块提供密码安全保护；密钥管理及发卡系统分为密钥管理子系统和发卡子系统，密钥管理子系统实现生成密钥、初始化密钥模块、向密码模块注入密钥等功能，发卡子系统实现门禁卡初始化、注入密钥和写入应用信息等功能。

第 6 章规定了密码应用、密码设备、密码算法、密码协议和密钥管理等安全技术要求。

第 7 章描述了基于 SM7 密码算法的非接触逻辑加密卡方案和基于 SM1/SM4 密码算法的非接触 CPU 卡方案。

第 8 章描述了密码应用安全要求之外的其它应考虑的安全因素，包括后台管理系统的管理要求、读卡器与后台管理系统的安全保障、其他与密码安全机制无关的管理及技术措施。

附录 A 是资料性附录，给出了基于 SM7 密码算法的非接触式逻辑加密卡方案。

附录 B 是资料性附录，给出了基于 SM1/SM4 算法的非接触式 IC 卡方案。

(4) 应用说明

a) 直接相关标准

GM/T 0008 安全芯片密码检测准则

GB/T 37033 信息安全技术 射频识别系统密码应用技术要求

b) 扩展应用领域

贵重物品防伪溯源密码方案的制定可参考该标准。

c) 使用注意事项

采用非接触式 IC 卡的门禁系统应符合 GB/T 37033 《信息安全技术 射频识别系统密码应用技术要求》规定的三级及以上安全要求。

采用的非接触式 IC 卡芯片应符合 GM/T 0008 《安全芯片密码检测准则》规定的二级及以上安全要求。

5. GM/T 0055 电子文件密码应用技术规范

(1) 版本

GM/T 0055-2018 《电子文件密码应用技术规范》是当前的最新版本。

(2) 用途与适用范围

该标准描述了电子文件保护所涉及的密码技术，不限制具体的文件类型，也不规定特定的应用系统。

该标准适用于安全电子文件密码服务中间件的开发和检测，也可用于指导使用该中间件的应用系统的开发。

(3) 内容概要

该标准共 11 个部分：

第1章为范围,第2章为规范性引用文件,第3章为术语和定义,第4章为符号和缩略语。

第5章标签机制,包括基于标签的安全电子文件系统架构、基于标签的安全机制、中间件对安全电子文件的处理过程、安全电子文件的存储方式和标签与文件的绑定机制等内容。

第6章密码算法与密码服务,描述了安全电子文件系统中使用的密码体制、密码算法、基础密码服务、个性密码服务和密钥对象。

第7章标签,定义了标签结构和标签属性。其中,标签的逻辑结构由标签头和标签体组成,标签头定义了标签的基本信息,标签体定义了文件的签名、权限、内容、日志、扩展等属性。

第8章基础密码操作,描述了中间件对标签和文件实施的7个共性密码操作。

第9章安全电子文件密码服务接口,定义了常量、结构和接口函数。其中接口函数由初始化操作函数、标签和文件操作函数、属性操作函数、密码操作函数等4类82个函数组成。

附录A、B均为资料性附录,分别描述了数字水印和指纹识别的原理和操作过程。

(4) 应用说明

——直接相关标准

GM/T 0031 安全电子签章密码技术规范

GM/T 0071 电子文件密码应用指南

6. GM/T 0070 电子保单密码应用技术要求

(1) 版本

GM/T 0070-2019《电子保单密码应用技术要求》是当前的最新版

本。

（2）用途与适用范围

该标准描述了保险行业电子保单业务的密码应用需求，针对投保、签发、存储、验证、递送等主要环节提出了密码应用技术要求。

该标准适用于电子保单系统的开发和使用。

（3）内容概要

该标准共 8 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章描述了电子保单的业务流程和安全需求。

第 6 章描述了电子保单密码应用技术框架，包括业务支撑层、密码功能层和基础设施层。其中，业务支撑层包括电子保单的投保、签发、验证、存储、递送、失效等环节，通过调用密码功能层实现安全的电子保单管理；密码功能层提供加解密、签名验证、密钥管理、身份认证、电子签章、时间戳等密码基本功能，为业务支撑层提供相关的密码服务功能；基础设施层提供第三方电子认证服务。

第 7 章规定了电子保单的投保、签发、存储、递送、验证和失效五个主要业务环节的密码应用要求。其中，投保环节要求采用数字签名、时间戳、签名验证等密码技术实现投保申请的电子签名，并根据业务需求对个人敏感信息采用加密保护技术；保单签发环节要求保险公司采用安全电子签章技术完成保单签署；保单存储环节要求采用密码技术实现数据机密性、完整性、身份鉴别和访问控制等安全功能；保单递送环节要求在投保人签署电子回执的电子递送、以及 Web 下载等方式中采用相应密码技术；保单验证环节要求对电子保单中的数字

签名及时间戳进行验证；保单失效环节要求对电子保单失效名单进行数字签名。

第8章规定了密码算法、密码设备、密钥生命周期管理、证书管理、证书格式、签名数据安全等方面的密码技术要求。

（4）应用说明

——直接相关标准

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 20520 信息安全技术 公钥基础设施时间戳规范

GM/T 0031 安全电子签章密码技术规范

——扩展应用领域

该标准描述了保险行业电子保单业务的密码应用需求，其他行业单据类业务系统的密码应用也可参考该标准。

——使用注意事项

该标准在实施过程中应按照国家有关法规实施，并遵循密码相关国家标准和行业标准。

7. GM/T 0071 电子文件密码应用指南

（1）版本

GM/T 0071-2019《电子文件密码应用指南》是当前的最新版本。

（2）用途与适用范围

该标准提出了电子文件的密码应用技术框架和安全目标，描述了对电子文件进行密码操作的方法和电子文件应用系统使用密码技术的方法。

该标准适用于电子文件应用系统的开发和使用。

（3）内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章符号和缩略语。

第 5 章描述了密码应用技术框架，包括密码算法与密码服务、用户、应用系统、电子文件和安全目标。

第 6 章描述了电子文件在应用系统的不同业务场景下采用密码技术保证其安全目标的实现。

第 7 章描述了实际业务场景中采用密码技术实现身份鉴别、权限控制、存储安全、安全交换、审计跟踪的应用方法。

第 8 章描述了文书类电子文件采用密码技术的技术路线。

附录 A 是资料性附录，给出了文书类电子文件采用密码技术的示例。

（4）应用说明

——直接相关标准

GM/T 0055 电子文件密码应用技术规范

8. GM/T 0072 远程移动支付密码应用技术要求

（1）版本

GM/T 0072-2019《远程移动支付密码应用技术要求》是当前的最新版本。

（2）用途与适用范围

该标准描述了基于密码模块的远程移动支付密码应用架构，规定了远程移动支付的密码安全要素以及密码应用的技术要求。

该标准适用于由移动智能终端发起并通过密码模块提供密码服务的远程支付方式，对远程移动支付中密码应用需要考虑的密码安全

要素以及遵循的技术要求提供指导。

(3) 内容概要

该标准共 7 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章符号和缩略语。

第 5 章描述了远程移动支付系统构成，包括移动终端侧、平台侧两部分。其中，移动终端侧包括客户端应用和密码模块；平台侧包括远程支付系统、账户管理系统和密码平台。

第 6 章描述了远程移动支付密码应用安全需求，包括远程移动支付过程中数据的机密性、完整性、身份鉴别以及抗抵赖性等。

第 7 章提出了密码算法使用、终端侧安全、平台侧安全、通信安全等方面的密码安全技术要求。

(4) 应用说明

——直接相关标准

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式规范

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GM/T 0024 SSL VPN 技术规范

——扩展应用领域

其它基于密码模块的移动密码应用系统的建设可参考该标准。

9. GM/T 0073 手机银行信息系统密码应用技术要求

(1) 版本

GM/T 0073-2019《手机银行信息系统密码应用技术要求》是当前的最新版本。

(2) 用途与适用范围

该标准基于 GM/T 0054《信息系统密码应用基本要求》和 JR/T 0071《金融行业信息系统信息安全等级保护实施指引》等标准的基础上，结合手机银行信息系统的特点，及该类信息系统等级保护安全建设工作中密码技术的应用需要，从密码安全技术要求、密钥安全与管理要求、安全管理要求三方面，针对手机银行等级保护二级、三级信息系统中涉及的密码技术提出了具体要求。

该标准适用于指导、规范、评估手机银行信息系统的商用密码应用。

（3）内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章缩略语。

第 5 章对典型的手机银行信息系统提出了模型结构，包括手机银行移动客户端和手机银行服务端。

第 6 章给出了需遵循 GM/T0054-2018 标准中第 5 章、第 6 章规定的原则性要求。

第 7 章规定了手机银行信息系统密码技术安全保护二级要求的各项指标定义和技术要求，包括基本技术要求、密码技术安全要求、密钥安全与管理要求、安全管理要求。其中，密码技术安全要求部分包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密码配用策略等要求；密钥安全与管理要求部分包括密钥的导入导出、存储与保管、使用与更换、备份与恢复等要求；安全管理要求部分包括安全管理制度、人员管理要求、密码设备的安全管理等要求。

第 8 章在安全保护二级要求的基础上，增加了三级要求。

附录 A 是资料性附录，给出了二、三级安全要求的对照表。

(4) 应用说明

——直接相关标准

GM/T 0054 信息系统密码应用基本要求

——使用注意事项

在实际应用中要与 GM/T 0054 配套使用。

10. GM/T 0074 网上银行密码应用技术要求

(1) 版本

GM/T 0074-2019《网上银行密码应用技术要求》是当前的最新版本。

(2) 用途与适用范围

该标准规定了密码技术在网上银行业务中应用的相关要求，包括密码算法、密钥管理、证书管理、安全通道、密码设备及数字签名六个方面。

该标准适用于指导网上银行业务中密码技术相关安全功能的设计、实现和使用，对于网上银行系统中密码子系统的测试、管理可参照使用。手机银行等系统中相关部分内容也可以参照该标准。

(3) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章符号和缩略语。

第 5 章描述了网上银行系统架构和网上银行业密码应用技术体系，分析了网上银行业务系统安全需求。利用密码技术支撑真实性、

机密性、完整性和抗抵赖等特性，形成对网上银行系统与业务的安全支撑，以保护其应用安全及运行安全。

第 6 章对网上银行的查询业务、资金变动业务及签约等各项业务进行分类，对不同业务的安全性要求进行了归纳总结。

第 7 章从密码功能、密钥管理、证书管理、通道安全、密码设备及数字签名 6 个方面分别阐述了网上银行业务相关要求。其中，密码功能要求包括电子银行业务中的身份鉴别、数据机密性、数据完整性以及交易的抗抵赖性对应的密码算法应满足的相关标准；密钥管理是网上银行系统运行管理的基础，密钥管理要求从密钥的生成、存储、使用、备份和恢复以及撤销与存档全生命周期的管理，结合 GM/T 0054 以及特定场景的密钥管理应遵循相关标准作出了明确要求；证书管理从系统建设、证书格式、证书生命周期三个方面明确了相关的标准及具体要求，生命周期管理涵盖了证书的申请、下载、更新、吊销四个方面；通道安全明确了使用场景及使用具体协议时应当符合的标准；密码设备明确了密码功能的定义、服务接口要求、以及签名验签服务器、服务器密码机、智能密码钥匙、动态口令终端等密码设备应符合的技术标准。在电子银行业务中的数字签名，明确了格式标准及相关的时戳标准。

附录 A 是资料性附录，结合 GM/T 0054 和该标准的规定，以等级保护第三级网上银行系统为例给出了等级保护第三级网上银行系统建设示例。

（4）应用说明

——直接相关标准

GM/T 0054 信息系统密码应用基本要求

——使用注意事项

在实际应用中要与 GM/T 0054 配套使用。

11. GM/T 0075 银行信贷信息系统密码应用技术要求

(1) 版本

GM/T 0075-2019《银行信贷信息系统密码应用技术要求》是当前的最新版本。

(2) 用途与适用范围

该标准基于 GM/T 0054《信息系统密码应用基本要求》、JR/T 0071《金融行业信息系统信息安全等级保护实施指引》等标准的基础上，结合银行业银行信贷信息系统的特点及该类信息系统等级保护安全建设工作中密码技术的应用需要，从密码安全技术要求、密钥安全与管理要求、安全管理要求等三方面，对不同安全保护等级的信贷信息系统中的密码应用提出具体要求。

该标准适用于指导、规范和评估信贷信息系统的商用密码应用。

(3) 内容概要

该标准共 9 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章缩略语。

第 5 章提出了典型的银行信贷信息系统模型结构，包括信贷系统操作终端和信贷业务处理服务端两部分。

第 6 章给出了密码应用原则性要求和密码应用功能要求。

第 7 章规定了信贷信息系统密码技术安全保护二级要求的各项指标定义和技术要求，包括基本技术要求、密码技术安全要求、密钥安全与管理要求、安全管理要求。其中，密码技术安全要求部分包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安

全、密码配用策略等要求；密钥安全与管理要求部分包括密钥的导入导出、存储与保管、使用与更换、备份与恢复等要求；安全管理要求部分包括安全管理制度、人员管理要求、密码设备的安全管理等要求。

第 8 章在安全保护二级要求的基础上，增加了三级要求。

附录 A 是资料性附录，给出了二、三级安全要求的对照表。

（4）应用说明

——直接相关标准

GM/T 0054 信息系统密码应用基本要求

——使用注意事项

在实际应用中要与 GM/T 0054 配套使用。

12. GM/T 0076 银行卡信息系统密码应用技术要求

（1）版本

GM/T 0076-2019《银行卡信息系统密码应用技术要求》是当前的最新版本。

（2）用途与适用范围

该标准在 GM/T 0054-2018《信息系统密码应用基本要求》、JR/T 007-2012《金融行业信息系统信息安全等级保护实施指引》等标准基础上，结合银行业金融机构银行卡系统的特点及该类信息系统等级保护安全建设工作中密码技术的应用需要，从密码安全技术要求、密钥安全与管理要求、安全管理要求等三方面，对不同安全保护等级的银行卡系统中密码技术的应用提出具体的安全要求。

该标准适用于指导、规范和评估银行卡信息系统中的商用密码应用。

（3）内容概要

该标准共 10 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章缩略语。

第 5 章描述了典型的银行卡信息系统模型，包括银行卡操作终端和银行卡信息处理服务端。

第 6 章规定了银行卡信息系统密码应用基本要求和密码应用功能要求。

第 7 章规定了银行卡信息系统密码技术安全保护二级要求的各项指标定义和技术要求，包括基本技术要求、密码技术安全要求、密钥安全与管理要求、安全管理要求。其中，密码技术安全要求部分包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密码配用策略等要求；密钥安全与管理要求部分包括密钥的导入导出、存储与保管、使用与更换、备份与恢复等要求；安全管理要求部分包括安全管理制度、人员管理要求、密码设备的安全管理等要求。

第 8 章和第 9 章在安全保护二级要求的基础上，增加了三、四级要求。

附录 A 是规范性附录，给出了第二、三、四级的安全要求对照表。

应用说明

——直接相关标准

GM/T 0054 信息系统密码应用基本要求

——扩展应用领域

该标准可用于以银行卡为载体的交通、社保、健康、电子身份认证（eID）、电子证件等信息系统的密码系统设计、检测与实施。

——使用注意事项

在实际应用中应与 GM/T 0054 配套使用。

安全保护等级的选用应由银行业金融机构自行确定。

在银行卡系统密码技术的安全建设、安全使用和监督管理过程中，宜在成本可接受的情况下尽可能地提高安全强度，选用更高级别的安全系统和产品。

13. GM/T 0077 银行核心信息系统密码应用技术要求

(1) 版本

GM/T 0077-2019《银行核心信息系统密码应用技术要求》是当前的最新版本。

(2) 用途与适用范围

该标准在 GM/T 0054-2018《信息系统密码应用基本要求》、JR/T 007-2012《金融行业信息系统信息安全等级保护实施指引》等标准基础上，结合银行业金融机构银行核心信息系统的特点及该类信息系统等级保护安全建设工作中密码技术的应用需要，从密码安全技术要求、密钥安全与管理要求、安全管理要求等三方面，对不同安全保护等级的银行核心信息系统中密码技术的应用提出具体的要求。

该标准适用于指导、规范和评估银行核心信息系统中的商用密码应用。

(3) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义，第 4 章缩略语。

第 5 章定义了典型的银行核心信息系统模型，包括物理云、业务

云和用户应用系统。

第 6 章描述了银行核心信息系统密码技术安全保护三级要求，包括基本技术要求、密码技术安全要求、密钥安全与管理要求、安全管理要求。其中，密码技术安全要求部分包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密码配用策略等要求；密钥安全与管理要求部分包括密钥的导入导出、存储与保管、使用与更换、备份与恢复等要求；安全管理要求部分包括安全管理制度、人员管理要求、密码设备的安全管理等要求。

第 7 章在第 6 章的基础上，增加了四级要求的指标和定义。

附录 A 是规范性附录，给出了第三、四级的安全要求对照表。

(4) 应用说明

——直接相关标准

GM/T 0054 信息系统密码应用基本要求

——使用注意事项

在实际应用中要与 GM/T 0054 配套使用。

七 密码检测类标准

(一) 随机性检测

1. GB/T 32915 信息安全技术 二元序列随机性检测方法

(1) 版本

GB/T 32915-2016《信息安全技术 二元序列随机性检测方法》系该标准国家标准最新版本。

该标准对应的密码行业标是 GM/T 0005《随机性检测规范》，最后版本为 GM/T 0005-2012。

（2）用途与适用范围

该标准规定了商用密码应用中的随机性检测指标和检测方法，对随机数发生器所产生二元序列的随机性进行检测。

该标准适用于数字物理噪声源等专用随机数芯片进行统计检测，也可对其他密码产品的随机数质量检测提供参考。

（3）内容概要

该标准共 7 个部分：

第 1 章范围，第 2 章术语和定义，第 3 章符号和缩略语。

第 4 章描述了针对二元序列的 15 项检测方法，包括：单比特频数检测、块内频数检测、扑克检测、重叠子序列检测、游程总数检测、游程分布检测、块内最大"1"游程检测、二元推导检测、自相关检测、矩阵秩检测、累加和检测、近似性检测、线性复杂度检测、Maurer 通用统计检测、离散傅立叶检测。

第 5 章描述了对随机数发生器的检测过程，包括采样、存储、检测和判定。

附录 A 是资料性附录，描述了 15 项随机性检测方法的原理。

附录 B 是资料性附录，给出了随机性检测参数设置表。

（4）应用说明

——使用注意事项

该标准广泛用于对密码产品检测过程中随机数质量的检测，并给出通过与否的结论。使用时应当按照实际要求的参数进行设置，但分组长度应不低于 10^6 比特，分组数量应不少于 1000 组。

该标准的检测对象是随机序列，并不涉及对随机数发生器设计原理和随机数产生机制的合理性和安全性评价。关于对密码产品中随机

数的其他检测要求,还应满足 GM/T 0062《密码产品随机数检测要求》。

2. GM/T 0062 密码产品随机数检测要求

(1) 版本

GM/T 0062-2018《密码产品随机数检测要求》是当前的最新版本。

(2) 用途与适用范围

该标准规定了密码产品应用中,硬件实现随机数发生器产生随机数的随机性检测指标和检测要求。

该标准适用于随机数发生器的检测,亦可指导随机数发生器的研制。

(3) 内容概要

该标准共 9 章:

第 1 章范围,第 2 章规范性引用文件,第 3 章术语、定义和符号。

第 4 章随机数检测说明,将产品形态划分为 A 类、B 类、C 类、D 类、E 类 5 种产品类别,以及对应用阶段划分为送样、出厂、上电和使用四个不同阶段检测,同时对检测数据格式、检测项目、显著性水平、参数设置进行了说明。

第 5、6、7、8、9 章分别规定了 A、B、C、D、E 类产品的随机数检测要求。从送样、出厂、上电、使用等阶段规定了具体的检测要求。检测要求包括检测量、检测项目、检测判断标准。

(4) 应用说明

——直接相关标准

GB/T 32915 信息安全技术 二元序列随机性检测方法

——使用注意事项

该标准使用了 GB/T 32915 定义的检测项,但部分项目在参数上

有所调整，以适应不同类型产品和不同检测场景的需要。

送样检测和出厂检测一般是外部检测，即检测过程在密码产品外部执行，检测功能由外部检测平台实现；上电检测和使用检测一般是内部检测，即检测过程在密码产品内部执行，检测功能由密码产品实现。

(二) 算法与协议检测

1. GM/T 0042 三元对等密码安全协议测试规范

(1) 版本

GM/T 0042-2015《三元对等密码安全协议测试规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了三元对等密码安全协议对相关密码算法与安全协议应满足的基本技术要求和对应的测试方法。

该标准适用于符合国际标准 ISO/IEC 9798-3:1998/Amd. 1:2010 和国家标准 GB/T 15843.3、GB/T 28455—2012 的设备，用于检测其密码算法和协议实现是否符合上述标准的要求。

(3) 内容概要

该标准共 13 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章基本技术要求，规定了密码算法实现的正确性和一致性、协议实现的符合性和互操作性等要求。

第 6 章测试环境要求，描述了请求者 REQ、鉴别访问控制器 AAC 和鉴别服务器 AS 三种被测设备的不同测试环境网络拓扑。

第 7 章三元对等密码安全协议测试统一封装,定义了封装数据结构和数据元素封装格式。

第 8 章算法实现的正确性和一致性测试方法,规定了对称密码算法、数字签名算法、密钥交换协议、公钥加密算法、数字证书格式、密码杂凑算法、随机数的测试方法和参考标准。

第 9 章协议实现一致性和互操作性测试方法,规定了端口控制、TAEP 协议封装、TAEPoL 协议封装、TCP/UDP 端口等测试方法。

附录 A、B、C、D 均为资料性附录,附录 A 给出了 TAEP 协议封装 Request 和 Response 分组格式中 Type 字段的定义;附录 B 给出了三元对等密码安全协议测试统一封装数据元素;附录 C 给出了证书中的设备命名规则;附录 D 给出了测试向量。

(4) 应用说明

——直接相关标准

GB/T 28455 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

GM/T 0039 密码模块安全检测要求

2. GM/T 0043 数字证书互操作检测规范

(1) 版本

GM/T 0043-2015《数字证书互操作检测规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了数字证书的格式和互操作检测要求。

该标准适用于证书认证系统签发的数字证书的检测。

(3) 内容概要

该标准共 9 个部分:

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章规定了送检单位应当提交的文档资料内容。

第 6 章规定了具体检测内容，包括入根检测、数字证书和 CRL 格式符合性检测以及数字证书互操作检测。其中，入根检测部分规定了 CA 系统应具备申请 CA 证书的能力和申请文件的格式；数字证书和 CRL 格式符合性检测部分规定了证书基本项、扩展项和 CRL 格式的检测要求；数字证书互操作检测部分规定了证书信任链、签名证书和加密证书的检测要求。

第 7 章规定了入根检测、数字证书和 CRL 格式符合性检测、数字证书互操作检测的检测方法。

第 8 章规定了合格判定要求。

附录 A 是资料性附录，给出了 CA 证书申请文件的编码格式。

（4）应用说明

——直接相关标准

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GM/T 0014 数字证书认证系统密码协议规范

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

——扩展应用领域

该标准除作为检测使用外，在相关产品研发和系统建设时，也可作为依据。另外，在独立的两个 CA 系统之间需要互相认证时，也可

以参照本规范。

(三) 产品检测

1. 功能检测

(1) GM/T 0013 可信密码模块接口符合性测试规范

a) 版本

GM/T 0013-2012《可信密码模块接口符合性测试规范》是当前的最新版本。

b) 用途与适用范围

该标准定义了可信密码模块的命令测试向量，提供了有效的测试方法与灵活的测试脚本。

该标准适用于可信密码模块的符合性测试，不能取代其安全性检查。可信密码模块的安全性检测需要按照其它相关规范来进行。

c) 内容概要

该标准共 7 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义。

第 4 章可信密码模块接口符合性测试，描述了对可信密码模块实现规范符合性测试时采用的策略和方法。

第 5 章命令依赖关系，描述了调用可信密码模块命令实现测试时，各命令之间的相互依赖关系。

第 6 章向量命令，规定了适用于多数可信密码模块的向量命令测试方法。

第 7 章脚本向量，规定了部分命令所需的较为复杂的测试方法。

d) 应用说明

——直接相关标准

GB/T 29829 信息安全技术 可信计算密码支撑平台功能与接口规范

GM/T 0012 可信计算 可信密码模块接口规范

GM/T 0058 可信计算 TCM 服务模块接口规范

——使用注意事项

对于需要执行一个命令序列才能测试的命令，需要根据所涉及命令的测试向量组成测试脚本来进行符合性测试。

(2) GM/T 0037 证书认证系统检测规范

a) 版本

GM/T 0037-2014《证书认证系统检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规定了证书认证系统的检测内容与检测方法。该标准适用于按照 GB/T 25056 研制或建设的证书认证运营系统的检测，也可为其它证书认证系统的检测提供参考。

c) 内容概要

该标准共 13 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章定义了产品和项目两种检测对象。其中，产品指由 CA 服务器、RA 服务器、OCSP 服务器、LDAP 服务器、密码机、证书与私钥存储介质，以及相关软件等组成的证书认证系统；项目指采用证书认证系统产品并按照 GM/T 0034 要求建设的证书认证服务运营系统。

第 6 章规定了测试大纲编制的原则。

第 7 章定义了产品和项目的检测环境。

第 8 章规定了场地、网络、岗位及权限管理、安全管理、系统初始化、系统功能、性能、数据备份和恢复、第三方安全产品、入根、证书格式、证书链、算法等检测内容及其适用范围。

第 9 章规定了第 8 章各项检测内容的具体检测方法。

第 10 章规定了判定产品和项目合格的条件。

附录 A 是资料性附录，给出了可供参考的测试大纲的示例。

附录 B 是资料性附录，给出了证书认证系统网络结构示例。

附录 C 是资料性附录，给出了证书认证系统机房布局及设备位置摆放的示例。

d) 应用说明

——直接相关标准

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0038 证书认证密钥管理系统检测规范

GM/T 0043 数字证书互操作检测规范

GB/T 20518 信息安全技术 公钥基础设施数字证书格式规范

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

——使用注意事项

项目检测时，应对 RA、CA 和 KM 等数据的一致性要进行实际使用场景逐一核查。

(3) GM/T 0038 证书认证密钥管理系统检测规范

a) 版本

GM/T 0038-2014《证书认证密钥管理系统检测规范》是当前的最

新版本。

b) 用途与适用范围

该标准规定了证书认证密钥管理系统的检测内容与检测方法。该标准适用于按照 GB/T 25056 《信息安全技术 证书认证系统密码及其相关安全技术规范》研制或建设的证书认证密钥管理系统的检测，也可为其证书认证密钥管理系统的检测提供参考。

c) 内容概要

该标准共 12 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义。

第 4 章定义了产品和项目两种检测对象。其中，产品指由密钥管理服务器、密钥管理数据库服务器、密码机、KM 管理终端、KM 审计终端以及相关软件等组成的证书认证密钥管理系统；项目指采用证书认证密钥管理产品并按照 GB/T 25056 第 9 章要求建设的证书认证密钥管理系统。

第 5 章规定了测试大纲编制的原则。

第 6 章定义了产品和项目的检测环境。

第 7 章规定了场地、网络、岗位及权限管理、安全管理、系统初始化、系统功能、性能、数据备份和恢复、第三方安全产品等检测内容及适用范围。

第 8 章规定了第 7 章检测内容的具体检测方法。

第 9 章规定了判定产品和项目合格的条件。

附录 A 是资料性附录，给出了可供参考的测试大纲的示例。

附录 B 是资料性附录，给出了密钥管理系统网络结构示例。

附录 C 是资料性附录，给出了密钥管理系统机房布局及设备位置

摆放的示例。

d) 应用说明

——直接相关标准

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0037 证书认证系统检测规范

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

——使用注意事项

项目检测时，应对 CA 和 KM 等数据的一致性进行实际使用场景逐一核查。

(4) GM/T 0040 射频识别标签模块密码检测准则

a) 版本

GM/T 0040-2015《射频识别标签模块密码检测准则》是当前的最新版本。

b) 用途和适用范围

该标准规定了采用密码技术的射频识别标签模块产品密码检测的检测内容和要求，适用于射频识别标签模块的密码及安全功能检测。也可用于符合 GB/T 28925-2012 和 GB/T 29768-2013 射频识别空中接口协议产品的密码检测。

c) 内容概要

该标准共 7 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章规定了射频识别标签模块根据是否具备与读写器双向鉴

别的能力而分为 I 类和 II 类。具备双向鉴别能力的 II 类又根据是否支持传输的机密性和完整性分为 II-A 类和 II-B 类。

第 6 章规定了一般要求、密码算法、密码服务、密码性能、敏感信息保护、抗抵赖、生命周期安全、审计、密钥管理、开发环境保障等方面的检测要求。其中，密码算法部分规定了密码算法和随机数的检测要求；密码服务部分规定了数据传输和数据存储的机密性和完整性的检测要求；密码性能部分规定了鉴别性能和数据交互性能的检测要求；敏感信息保护部分规定了口令保护和敏感信息保护的检测要求；抗抵赖部分规定了抗原发抵赖的检测要求；生命周期安全部分规定了标签模块灭活、防非法指令、防初始使用权欺骗和防生命周期越界的检测要求；审计部分规定了标签模块唯一标识的检测要求；密钥管理部分规定了密钥生成、存储、使用、更新、导入和清除的检测要求；开发环境保障部分规定了文档管理、开发环境安全、隐蔽通道声明、人员管理和源文件管理等要求。

附录 A 为规范性附录，给出了“射频识别标签模块密码检测项”表格。

d) 应用说明

——直接相关标准

GB/T 37033 信息安全技术 射频识别系统密码应用技术要求

——扩展应用领域

可用于采用 SM1 或 SM4 密码算法的射频识别标签模块密码检测；也可用于采用 NB-IoT 或 LoRa 通信协议的射频识别标签模块密码检测。

——使用注意事项

该标准应用于轻量级安全防护的射频识别系统中射频识别标签

模块的密码检测。通常受限于标签计算能力限制，射频识别标签无法采用 GM/T 0008 《安全芯片密码检测准则》要求进行更强的安全防护措施。在计算能力有保障的前提下，应提高随机数的随机性要求，进而符合 GM/T 0005 《随机性检测规范》。

(5) GM/T 0041 智能 IC 卡密码检测规范

a) 版本

GM/T 0041-2015 《智能 IC 卡密码检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规定了智能 IC 卡产品的检测项目及检测方法。

该标准适用于智能 IC 卡产品的密码检测，也可用于指导智能 IC 卡产品的研发。智能 IC 卡产品包括但不限于金融 IC 卡、公交 IC 卡、社保 IC 卡、SIM 卡等。

c) 内容概要

该标准共 7 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章检测项目，描述了智能 IC 卡的具体检测项目，包括 COS 安全管理功能、COS 安全机制、密钥的素性、随机数质量、密码算法正确性、密码算法性能、设备安全性等 7 个类别。其中，COS 安全管理功能检测包括内外部认证、PIN 管理、应用锁定解锁、非对称密钥导入导出以及密码信封的产生和打开等；COS 安全机制检测包括报文安全传送、密钥安全传送、安全状态和访问权限以及应用防火墙；密钥素性检测明确了 RSA 密钥的素性要求；随机数质量检测项明确了应当遵循 GM/T 0005 的相关要求；密码算法正确性和性能检测明确了检

测的算法类别；设备安全性部分明确了应当遵循 GM/T 0039 的相关要求。

第 6 章检测方法，规定了第 5 章检测项目的检测方法，包括正常情况和异常情况的检测步骤。

第 7 章合格性判断准则，明确了送检产品必须满足的检测项和可选满足的检测项。

d) 应用说明

——直接相关标准

GM/T 0039 密码模块安全检测要求

——使用注意事项

该标准是针对智能 IC 卡的通用性安全要求，在实际使用中，行业主管部门和用户应当加强对加载于智能 IC 卡内的行业应用的安全性审查。

(6) GM/T 0046 金融数据密码机检测规范

a) 版本

GM/T 0046-2016《金融数据密码机检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规范了金融数据密码机的检测环境、检测仪器和软件、硬件检测内容和环境适应性检测要求，规定了检测项目、检测方法和判定标准。

该标准适用于金融数据密码机的研发、应用和检测。

c) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4

章缩略语。

第 5 章检测环境要求，描述了检测环境的组成、网络拓扑和各组成部分的主要用途。

第 6 章检测内容和检测方法，规定了金融数据密码机的检测项目，包括外观和结构检查、功能检测、性能检测及其他检测等。其中，外观和结构检查部分规定了具体的外观和结构检查项目，明确了接口和部件；功能检查部分规定了初始化、密码运算、密钥管理、随机数、访问控制、设备管理、日志审计、设备自检、报文接口等检测项；性能检测规定了密码服务、业务功能检测项和性能指标的计算方法；其他检测部分规定了设备安全性测试、环境适应性测试、可靠性测试需要遵循的标准。

第 7 章送检技术文档要求，规定了产品送检时应当提交的文档内容。

第 8 章定义了合格判定条件。

附录 A 是规范性附录，给出了测试项目列表。

d) 应用说明

——直接相关标准

GM/T 0045 金融数据密码机技术规范

GM/T 0039 密码模块安全检测要求

——使用注意事项

该标准没有对产品的具体密钥容量等非安全性功能进行检测，用户可根据实际需求自行选择。

对于用户根据自身需求提出的扩展业务功能要求，由需求方自行评估安全性。

(7) GM/T 0047 安全电子签章密码检测规范

a) 版本

GM/T 0047-2016《安全电子签章密码检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规范了安全电子签章产品的密码检测内容、检测方法、送检要求，以及合格判定准则。

该标准适用于按照 GM/T 0031 研制的电子签章系统的密码技术检测。

c) 内容概要

该标准共 8 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章规定了检测内容，包括检测对象，以及数字签名算法、电子印章数据、电子印章验证、电子签章数据、电子签章验证五个方面的检测要求。

第 6 章规定了检测方法，围绕数字签名算法、电子印章数据、电子印章验证、电子签章数据、电子签章验证五个方面，给出了检测方法与步骤。

第 7 章规定了送检技术文档要求。

第 8 章明确了检测结果的合格判定条件。

d) 应用说明

——直接相关标准

GM/T 0031 安全电子签章密码技术规范

(8) GM/T 0048 智能密码钥匙密码检测规范

a) 版本

GM/T 0048-2016《智能密码钥匙密码检测规范》是当前的最新版本。

b) 用途与适用范围

该标准定义了智能密码钥匙的相关术语,描述了智能密码钥匙的检测环境、检测内容和检测方法等内容。

该标准适用于智能密码钥匙产品检测,也可用于指导智能密码钥匙产品的研制和使用。

c) 内容概要

该标准共 7 章:

第 1 章范围,第 2 章规范性引用文件,第 3 章术语和定义,第 4 章缩略语。

第 5 章检测环境,描述了检测环境的网络拓扑、检测仪器和软件及其用途。

第 6 章检测内容,规定了智能密码钥匙的检测功能检测、性能检测 and 安全性检测项目。

第 7 章检测方法,规定了具体的检测项目及其检测目的、检测条件、检测过程和通过标准。其中,功能检测部分规定了设备管理、访问控制、应用管理、文件管理、容器管理、密码服务等检测项目和检测方法;性能测试部分规定了文件读写、对称算法、非对称算法和杂凑算法等性能测试项;安全性测试部分明确了按照 GM/T 0039 的要求进行检测。

d) 应用说明

——直接相关标准

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0039 密码模块安全检测要求

GM/T 0063 智能密码钥匙密码应用接口检测规范

(9) GM/T 0049 密码键盘密码检测规范

a) 版本

GM/T 0049-2016《密码键盘密码检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规定了密码键盘产品的安全等级划分、检测内容及检测方法、合格判定规则，适用于密码键盘产品的密码检测、检验及分级。

c) 内容概要

该标准共 10 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章规定了密码键盘分为 4 个安全等级。

第 6 章规定了检测内容及检测方法，包括安全管理功能检测、密码算法检测、密钥素性检测、环境失效保护检测、密码算法稳定性检测、算法性能测试、设备安全性检测、设备安全要求检测和送检技术文档要求。其中，安全管理功能检测部分包括外部认证、自检、PIN 数据块检测；密码算法检测部分包括对称算法加解密、MAC 算法、非对称算法、杂凑算法检测；随机数质量检测部分规定了随机数检测方法；环境失效保护检测部分规定了安全 3 级产品和安全 4 级产品的安

全机制，以及环境失效时的处理方法；密码算法稳定性检测部分规定了对称、非对称和杂凑算法的检测项目和检测步骤；算法性能测试部分规定了算法的数据采样数量、检测步骤和结果计算方法；设备安全性检测部分明确了遵循 GM/T 0039 的要求；设备安全要求检测部分规定了每个安全等级的检测步骤；送检技术文档要求部分明确了送检时应当提交的文档内容。

第 7 章规定了产品合格判定条件。

附录 A 是资料性附录，给出了检测中用到的 PIN 数据块填充格式。

附录 B 是资料性附录，给出了 CBC-MAC 计算方法。

附录 C 是资料性附录，给出了蒙特卡洛检测方法。

d) 应用说明

——直接相关标准

GM/T 0039 密码模块安全检测要求

——扩展应用领域

该标准也可用于包含密码键盘的其他产品检测。

——使用注意事项

该标准规定了密码键盘的密码功能和密码相关安全性的检测要求，密码键盘还应当符合的其他行业关于该类产品的业务功能规范和安全要求不在该标准范围内。

(10) GM/T 0059 服务器密码机检测规范

a) 版本

GM/T 0059-2018《服务器密码机检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规定服务器密码机的检测环境要求、检测要求及送检文档要求等有关内容。

该标准适用于服务器密码机类密码设备的检测，以及该类密码设备的研制，也可用于指导基于该类密码设备的应用开发。

c) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章规定了服务器密码机的检测环境，包括常规检测环境和跨网段检测环境，在两种检测环境中均能对服务器密码机一对一、一对多等服务方式进行检测。

第 6 章规定了服务器密码机的检测内容和检测方法，共有 20 个检测项，包括设备外观及结构、设备管理功能、设备状态、设备自检、设备配置管理、设备密钥管理、设备 SM1/SM2/SM3/SM4 算法运算、设备随机数质量、设备应用接口、设备管理接口、设备访问控制、设备日志记录以及设备性能、安全性、网络适应性。其中，设备外观及结构检查定义了服务器密码机产品的主要部件和接口等检查项；设备管理功能检查包含端口分离要求、远程管理安全通道要求以及管理工具管理功能等检测项；设备状态检测定义了设备状态及状态转换等检测

项；设备自检检测定义了自检功能项及检测结果报告等检测项；设备配置管理检测定义了权限配置、网络配置以及访问控制配置等管理功能等方面的检测项；设备密钥管理检测定义了密钥结构及密钥在生存周期的各个环节的安全性检测项；设备密码算法正确性与一致性检测定义了对称密码算法、非对称密码算法、密码杂凑算法等检测项；设备随机数质量检测定义了随机数发生器数量及随机性检测等检测项；设备应用接口检测定义了密码服务接口的检测项；设备远程管理接口检测定义了远程管理相关的检测项；设备访问控制检测定义了鉴别机制、密钥访问控制码等检测项；设备日志记录检测定义了日志记录内容、查看、导出等检测项；设备性能检测定义了性能指标的计算方法；设备网络适应性检测包括适用性、扩展性等检测项；设备安全性检测按照 GM/T 0039 检测；设备环境适应性检测按照 GB/T 9813 要求检测；设备可靠性检测规定了设备平均无故障时间检测项。

第 7 章对服务器密码机的送检文档提出了要求，规定了设备送交检测时应提交的基本文档要求，说明了送检文档应该包含的主要内容。

附录 A 是资料性附录，列举了常用的检测项。

d) 应用说明

——直接相关标准

GM/T 0030 服务器密码机技术规范

GM/T 0018 密码设备应用接口规范

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0039 密码模块安全检测要求

GM/T 0062 密码产品随机数检测要求

——扩展应用领域

该标准可用于包含服务器密码机功能的密码产品检测，也可用于以服务器密码机为安全支撑的密码产品或密码系统的检测。

(11) GM/T 0060 签名验签服务器检测规范

a) 版本

GM/T 0060-2018《签名验签服务器检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规定了签名验签服务器设备的检测内容、检测方法及检测要求等。

该标准适用于签名验签服务器设备的检测，以及该类密码设备的研制，也可用于指导基于该类密码设备的应用开发。

c) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章检测环境要求，描述了签名验签服务器主要检测环境，主要分为常规检测环境和跨网段检测环境两种。

第 6 章检测内容及检测方法，规定了外观和结构检测、功能检测、性能检测、其他检测等方面的签名验签服务器检测项目。其中，外观和结构检测是对签名验签服务器的外观、尺寸、内部部件、密码运算部件、管理员身份验证设备及附件进行检查；功能检测是对签名验签服务器功能项的检测，包括初始化、与公钥基础设施的连接、应用管理、证书管理和验证、数字签名、访问控制、日志管理、系统自检、NTP 时间源同步、服务接口、管理工具、管理员管理、随机数、密钥管理、算法正确性与一致性等检测内容；性能检测包括数字签名、算

法、并发等检测内容及性能指标的计算方法；其他检测包括设备网络适应性、设备安全性、设备环境适应性、设备可靠性等检测项。

第7章送检技术文档要求，规定了提交检测时需要提交的技术文档内容。

附录A是规范性附录，给出了测试项目列表。

d) 应用说明

——直接相关标准

GM/T 0029 签名验签服务器技术规范

GM/T 0039 密码模块安全检测要求

GM/T 0062 密码产品随机数检测要求

——扩展应用领域

该标准可用于包含签名验签服务器功能的产品检测，也可用于以签名验签服务器为安全支撑的密码产品或密码系统的检测。

(12) GM/T 0061 动态口令密码应用检测规范

a) 版本

GM/T 0061-2018《动态口令密码应用检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规定了动态口令系统的口令算法、动态令牌、认证系统和密钥管理系统等相关的检测内容，适用于动态口令相关密码产品的密码和安全功能检测。

c) 内容概要

该标准共6章：

第1章范围，第2章规范性引用文件，第3章术语和定义，第4

章符号和缩略语。

第 5 章检测内容和检测方法，规定了动态口令生成算法、动态令牌、动态令牌认证、密钥管理 4 个方面的检测内容和检测方法。

第 6 章送检技术文档要求，规定了需要提交的技术工作总结报告、安全性设计报告、用户手册及密码检测材料等相关文档要求。

d) 应用说明

——直接相关标准

GM/T 0021 动态口令密码应用技术规范

(13) GM/T 0063 智能密码钥匙密码应用接口检测规范

a) 版本

GM/T 0063-2018《智能密码钥匙密码应用接口检测规范》是当前的最新版本。

b) 用途与适用范围

该标准规定了智能密码钥匙密码应用接口检测环境、检测内容和检测方法以及产品送检材料等有关内容，便于智能密码钥匙产品应用接口的检测和认证。

该标准适用于智能密码钥匙密码应用接口检测，也可用于指导智能密码钥匙的研制和使用。

c) 内容概要

该标准共 8 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章送检材料说明，列出了送检时应提交的文档资料。

第 6 章至第 7 章，规定了智能密码钥匙密码应用接口的检测环境

和检测内容，包括应用功能检测、接口功能检测、安全性检测、兼容性检测及互操作性检测。

第 8 章，对智能密码钥匙的功能接口检测过程给出检测方法，包括检测目的、条件、过程和通过标准。

d) 应用说明

——直接相关标准

GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

(14) GM/T 0064 限域通信(RCC)密码检测要求

a) 版本

GM/T 0064-2018《限域通信（RCC）密码检测要求》是当前的最新版本。

b) 用途与适用范围

限域通信（Range Controlled Communication, RCC）是我国自主研发的基于 2.45GHz 射频技术的近距离无线通信技术，可广泛应用于交通、金融、社保、校企等行业。RCC-SIM 卡可适配所有手机，不受手机类型和型号的局限，因此特别适用于手机刷卡类应用场景，给用户带来了极大的便利。RCC 产品之间的无线通信协议采用了密码技术来保证射频通信链路的传输安全性。

该标准针对采用密码技术的 RCC 产品，规定了其密码和安全方面的检测内容及要求，其他功能性检测按照其相应的产品检验规范进行。

该标准适用于限域通信（RCC）产品开发、生产和检测认证等过程中的密码检测。

c) 内容概要

该标准共 8 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章符号和缩略语。

第 5 章对 RCC 产品进行分类，包括 RCC 发起方产品（例如：RCC 读写器模块、支持 RCC 的 POS 终端设备等）和 RCC 响应方产品（例如：RCC-SIM、RCC-SD 等智能卡）。

第 6 章提出了 RCC 产品的检测要求，包括密码算法（随机数、通讯链路加密算法实现正确性）、密码服务（信道传输机密性、数据加解密服务）、数据加解密性能、传输距离、命令交互（有效命令、非法或无效命令）、RCC 产品 UID 等方面。

附录 A 是资料性附录，给出了 RCC 的产品测试系统结构，还给出了 RCC 测试环境参考要求。

附录 B 是资料性附录，给出了基于 RCC 产品的应用密钥管理和安全保障要求。

d) 应用说明

——直接相关标准

GB/T 33736 手机支付 基于 2.45GHz RCC（限域通信）技术的非接触射频接口技术要求

GB/T 33737 手机支付 基于 2.45GHz RCC（限域通信）技术的智能卡测试方法

GB/T 33738 手机支付 基于 2.45GHz RCC（限域通信）技术的智能卡技术要求

GB/T 33740 手机支付 基于 2.45GHz RCC（限域通信）技术的非接触射频接口测试方法

GB/T 33741 手机支付 基于 2.45GHz RCC（限域通信）技术的非

接触式读写器终端技术要求

GB/T 34096 手机支付 基于 2.45GHz RCC（限域通信）技术的非接触式读写器终端测试方法

——使用注意事项

目前并没有针对 RCC 密码技术应用要求的密码行业标准，该标准以检测要求的形式规范了对密码技术应用的要求。

2. 安全检测

(1) GM/T 0008 安全芯片密码检测准则

a) 版本

GM/T 0008-2012《安全芯片密码检测准则》是当前的最新版本。

b) 用途与适用范围

该标准规定了安全芯片的三个安全等级，以及相应的密码检测要求。该标准适用于安全芯片的密码检测，亦可指导安全芯片的研制。

c) 内容概要

该标准共 13 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语、定义和缩略语。

第 4 章规定了安全芯片三个安全等级的划分依据和各安全等级的应用场景。

第 5 章至第 13 章规定了安全芯片应具有的九项安全能力，即密码算法、安全芯片接口、密钥管理、敏感信息保护、安全芯片固件安全、自检、审计、攻击的削弱与防护和生命周期保障。第 5 章规定了随机数的生成、分组密码算法、公钥密码算法、密码杂凑算法和序列

密码算法的检测要求；第 6 章规定了安全芯片物理接口和逻辑接口的检测要求；第 7 章规定了密钥生成、存储、使用、更新、导入、导出和清除等密钥管理相关检测要求；第 8 章规定了密钥等敏感信息的存储、清除、运算和传输等检测要求；第 9 章规定了固件存储、执行与导入等检测要求；第 10 章规定了自检要求；第 11 章规定了安全芯片标识和生命周期标识的审计要求；第 12 章规定了攻击的消弱与防护要求；第 13 章规定了生命周期保证要求。

d) 应用说明

——直接相关标准

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 33133 信息安全技术 祖冲之序列密码算法

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0005 随机性检测规范

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

——扩展应用领域

可用于检测含密码功能的芯片类产品，如 GPU、CPU 等。

(2) GM/T 0039 密码模块安全检测要求

a) 版本

GM/T 0039-2015《密码模块安全检测要求》是当前的最新版本。

b) 用途与适用范围

该标准依据 GM/T 0028-2014 的要求，规定了密码模块的检测规程、检测方法和对应的送检文档要求。

该标准适用于密码模块的检测。

c) 内容概要

该标准共 7 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语。

第 5 章说明了该标准主要条款的描述方法。

第 6 章规定了安全检测要求，包括通用要求、密码模块规格、密码模块接口、角色服务和鉴别、软件/固件安全、运行环境、物理安全、非入侵式安全、敏感安全参数管理、自测试、生命周期保障和对其它攻击的缓解等。

附录 A 是资料性附录，给出了安全等级对应表。

d) 应用说明

——直接相关标准

GB/T 37092 信息安全技术 密码模块安全要求

——使用注意事项

该标准是 GB/T 37092-2018《信息安全技术 密码模块安全要求》的配套性检测要求文档，需与其配合使用。

八 密码管理类标准

1. GM/T 0065 商用密码产品生产和保障能力建设规范

(1) 版本

GM/T 0065-2019《商用密码产品生产和保障能力建设规范》是当

前的最新版本。

（2）用途与适用范围

该标准规定了商用密码产品生产和保障能力的评估要素和评估要求。

该标准适用于对商用密码产品生产单位的生产能力、质量保障能力、安全保障能力和服务保障能力进行能力建设及核查。

（3）内容概要

该标准共包括 7 章：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义。

第 4 章规定了评估要素，包括基本项、声明项和评估项。

第 5 章规定了基本项要求，包括法人资格、主要技术人员、产品研发和行业管理遵从 4 个方面的具体要求。

第 6 章规定了声明项要求，包括关键人员信息、单位性质和数据管理 3 个方面的具体要求。

第 7 章规定了评估项要求，包括生产能力、质量保障能力、安全保障能力和服务保障能力 4 个方面的具体要求。

生产能力包括技术力量、生产管理、生产条件和生产工艺与流程 4 个方面。其中，技术力量对人力资源、主要技术团队、技术积累及优势、技术创新和研发工具和设备 5 个方面提出了具体要求；生产管理对岗位设置、制度保障、管理系统和供应链管理 4 个方面提出了具体要求；生产条件对生产场所、生产设备和生产外协 3 个方面提出了具体要求；生产工艺与流程对生产技术管理、批量生产和检测能力和生产外协 3 个方面提出了具体要求。

质量保障能力包括制度保障、开发过程质量管理、质量问题管理

和持续改进产品质量措施 4 个方面。其中，制度保障对制度建设及落实情况提出了具体要求；开发过程质量管理对开发与测试体系、研发过程管理和版本管理 3 个方面提出了具体要求；质量问题管理对如何管理质量问题提出了具体要求；持续改进产品质量措施对如何持续改进产品质量提出了具体要求。

安全保障能力包括组织保障和安全管理 2 个方面。其中，组织保障从领导力承诺、建立组织机制和人力资源安全 3 个方面提出了具体要求；安全管理从安全生产制度保障、物理和环境安全、计算机和网络安全、访问控制、介质控制、开发和支持过程中的安全、资产管理、日志审计、事故管理和业务持续性管理 10 个方面提出了具体要求。

服务保障能力包括制度保障、应急响应能力和服务响应方式 3 个方面。其中，制度保障对如何从制度上保障提出了具体要求；应急响应能力对如何处理应对突发情况提出了具体要求；服务响应方式从服务网络和受理与反馈 2 个方面提出了具体要求。

（4）应用说明

——直接相关标准

GM/T 0066 商用密码产品生产和保障能力建设实施指南

——扩展应用领域

该标准可用于商用密码产品生产单位自我评估，也可用于第三方机构或应用单位对商用密码产品生产单位进行评估。

2. GM/T 0066 商用密码产品生产和保障能力建设实施指南

（1）版本

GM/T 0066-2019《商用密码产品生产和保障能力建设实施指南》是当前的最新版本。

（2）用途与适用范围

该标准是 GM/T 0065 《商用密码产品生产和保障能力建设规范》的具体实施指南，规定了商用密码产品生产和保障能力评估的方法、程序、报告和要点说明。

该标准适用于对商用密码产品生产单位的生产能力、质量保障能力、安全保障能力和服务保障能力进行建设指导。

（3）内容概要

该标准共包括 13 个部分：

第 1 章范围，第 2 章规范性引用文件，第 3 章术语及定义。

第 4 章为实施概述，阐述了评估内容、评估方式和评估原则。评估内容即为 GM/T 0065 中规定的评估项，包括基本项、声明项和评估项等评估要素；评估方式分为单位自证和专家评分相结合的方式。

第 5 章为实施指南，提出了基本项、声明项和评估项的评估内容及方法的具体要求，针对各评估项进行了细化和举例，以及评估时应提供的证明材料等。

第 6 章为评估程序，包括评估要求、评估流程和实施评估。其中，评估流程分为形式审查和实质审查两部分；实施评估规定了材料审查、前置评估、现场审核、专家评估和评估结果等内容。

第 7 章为评估报告，规范了报告内容、报告形式、报告要求和报告归档的具体要求。

第 8 章为实施要点说明，分别从评估单位、申请单位和使用单位三个角度提出了评估实施的要点和注意事项。

附录A是规范性附录，提供了商用密码产品生产和保障能力评估配套表格，包括指标项、评价标准、评分指南、信息来源等内容。

附录B是规范性附录，提供了商用密码产品生产和保障能力评估报告模板。

附录C是资料性附录，提供了常用的审核方法。

附录D是资料性附录，给出了归档材料清单。

附录E是资料性附录，从使用方角度提出了在重要领域使用商用密码产品的要求和注意事项。

（4）应用说明

——直接相关标准

GM/T 0065 商用密码产品生产和保障能力建设规范

——扩展应用领域

该标准可用于商用密码产品生产单位自我评估，也可用于第三方机构或应用单位对商用密码产品生产单位进行评估。

——使用注意事项

被评估单位应保证所提供信息的真实性和有效性。第三方机构或应用单位依据该标准对商用密码产品生产单位实施评估时应本着公平公正、保密性、独立性和基于证据的基本原则，履行对评估过程中所涉及的商业秘密、知识产权等信息的保密义务。

附录A. 编号索引

本附录给出已发密码国家标准和密码行业标准按照标准号排序的索引列表。

表 A.1 已发密码国家标准编号索引

序号	标准名称	页码
1.	GB/T 20518 信息安全技术 公钥基础设施数字证书格式规范	24
2.	GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范	26
3.	GB/T 29829 信息安全技术 可信计算密码支撑平台功能与接口规范	69
4.	GB/T 32905 信息安全技术 SM3 密码杂凑算法	15
5.	GB/T 32907 信息安全技术 SM4 分组密码算法	9
6.	GB/T 32915 信息安全技术 二元序列随机性检测方法	95
7.	GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法	11
8.	GB/T 33133 信息安全技术 祖冲之序列密码算法	8
9.	GB/T 33560 信息安全技术 密码应用标识规范	6
10.	GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范	17
11.	GB/T 35276 信息安全技术 SM2 密码算法使用规范	16
12.	GB/T 35291 信息安全技术 智能密码钥匙应用接口规范	33
13.	GB/T 36322 信息安全技术 密码设备应用接口规范	34
14.	GB/T 36968 信息安全技术 IPSec VPN 技术规范	18
15.	GB/T 37033 信息安全技术 射频识别系统密码应用技术要求	76
16.	GB/T 37092 信息安全技术 密码模块安全要求	29

表 A.2 已发密码行业标准编号索引

序号	标准名称	页码
1.	GM/T 0001 祖冲之序列密码算法	8
2.	GM/T 0002 SM4 分组密码算法	9
3.	GM/T 0003 SM2 椭圆曲线公钥密码算法	11
4.	GM/T 0004 SM3 密码杂凑算法	15
5.	GM/T 0005 随机性检测规范	95
6.	GM/T 0006 密码应用标识规范	6
7.	GM/T 0008 安全芯片密码检测准则	121
8.	GM/T 0009 SM2 密码算法使用规范	16
9.	GM/T 0010 SM2 密码算法加密签名消息语法规则	17
10.	GM/T 0011 可信计算 可信密码支撑平台功能与接口规范	69
11.	GM/T 0012 可信计算 可信密码模块接口规范	32
12.	GM/T 0013 可信密码模块接口符合性测试规范	101
13.	GM/T 0014 数字证书认证系统密码协议规范	22
14.	GM/T 0015 基于 SM2 密码算法的数字证书格式规范	24
15.	GM/T 0016 智能密码钥匙密码应用接口规范	33
16.	GM/T 0017 智能密码钥匙密码应用接口数据格式规范	39
17.	GM/T 0018 密码设备应用接口规范	34
18.	GM/T 0019 通用密码服务接口规范	57
19.	GM/T 0020 证书应用综合服务接口规范	58
20.	GM/T 0021 动态口令密码应用技术规范	73
21.	GM/T 0022 IPSec VPN 技术规范	18

序号	标准名称	页码
22.	GM/T 0023 IPSec VPN 网关产品规范	53
23.	GM/T 0024 SSL VPN 技术规范	20
24.	GM/T 0025 SSL VPN 网关产品规范	54
25.	GM/T 0026 安全认证网关产品规范	55
26.	GM/T 0027 智能密码钥匙技术规范	45
27.	GM/T 0028 密码模块安全技术要求	29
28.	GM/T 0029 签名验签服务器技术规范	47
29.	GM/T 0030 服务器密码机技术规范	49
30.	GM/T 0031 安全电子签章密码技术规范	75
31.	GM/T 0032 基于角色的授权管理与访问控制技术规范	60
32.	GM/T 0033 时间戳接口规范	62
33.	GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范	26
34.	GM/T 0035 射频识别系统密码应用技术要求	76
35.	GM/T 0036 采用非接触卡的门禁系统密码应用技术指南	79
36.	GM/T 0037 证书认证系统检测规范	102
37.	GM/T 0038 证书认证密钥管理系统检测规范	103
38.	GM/T 0039 密码模块安全检测要求	122
39.	GM/T 0040 射频识别标签模块密码检测准则	105
40.	GM/T 0041 智能 IC 卡密码检测规范	107
41.	GM/T 0042 三元对等密码安全协议测试规范	98
42.	GM/T 0043 数字证书互操作检测规范	99
43.	GM/T 0044 SM9 标识密码算法	13

序号	标准名称	页码
44.	GM/T 0045 金融数据密码机技术规范	51
45.	GM/T 0046 金融数据密码机检测规范	108
46.	GM/T 0047 安全电子签章密码检测规范	110
47.	GM/T 0048 智能密码钥匙密码检测规范	111
48.	GM/T 0049 密码键盘密码检测规范	112
49.	GM/T 0050 密码设备管理 设备管理技术规范	41
50.	GM/T 0051 密码设备管理 对称密钥管理技术规范	42
51.	GM/T 0052 密码设备管理 VPN 设备监察管理规范	43
52.	GM/T 0053 密码设备管理 远程监控和合规性检验接口数据规范	44
53.	GM/T 0054 信息系统密码应用基本要求	70
54.	GM/T 0055 电子文件密码应用技术规范	81
55.	GM/T 0056 多应用载体密码应用接口规范	37
56.	GM/T 0057 基于 IBC 技术的身份鉴别规范	63
57.	GM/T 0058 可信计算 TCM 服务模块接口规范	38
58.	GM/T 0059 服务器密码机检测规范	114
59.	GM/T 0060 签名验签服务器检测规范	116
60.	GM/T 0061 动态口令密码应用检测规范	117
61.	GM/T 0062 密码产品随机数检测要求	97
62.	GM/T 0063 智能密码钥匙密码应用接口检测规范	118
63.	GM/T 0064 限域通信(RCC)密码检测要求	119
64.	GM/T 0065 商用密码产品生产和保障能力建设规范	123
65.	GM/T 0066 商用密码产品生产和保障能力建设实施指南	125

序号	标准名称	页码
66.	GM/T 0067 基于数字证书的身份鉴别接口规范	64
67.	GM/T 0068 开放的第三方资源授权协议框架	66
68.	GM/T 0069 开放的身份鉴别框架	67
69.	GM/T 0070 电子保单密码应用技术要求	82
70.	GM/T 0071 电子文件密码应用指南	84
71.	GM/T 0072 远程移动支付密码应用技术要求	85
72.	GM/T 0073 手机银行信息系统密码应用技术要求	86
73.	GM/T 0074 网上银行密码应用技术要求	88
74.	GM/T 0075 银行信贷信息系统密码应用技术要求	90
75.	GM/T 0076 银行卡信息系统密码应用技术要求	92
76.	GM/T 0077 银行核心信息系统密码应用技术要求	94
77.	GM/Z 4001 密码术语	6

附录B. 金融领域国产密码应用推进中的密码标准适用要求

一、 总体要求

金融领域所有涉及到密码的芯片、设备、部件、软件和系统都应优先支持 SM2/3/4 密码算法。

金融业务标准规范中使用密码的部分，应引用国产密码算法和密码算法使用等密码标准规范。

二、 密码算法

SM2 算法实现应遵循 GB/T 32918《信息安全技术 SM2 椭圆曲线公钥密码算法》。

SM3 算法实现应遵循 GB/T 32905《信息安全技术 SM3 密码杂凑算法》。

SM4 算法实现应遵循 GB/T 32907《信息安全技术 SM4 分组密码算法》。

三、 密码算法使用

SM2 算法使用应遵循 GB/T 35276《信息安全技术 SM2 密码算法使用规范》。

SM4 算法使用应遵循 GB/T 17964《信息安全技术 分组密码算法的工作模式》。

交易报文中的数字信封或数字签名应遵循 GB/T 35275《信息安全技术 SM2 密码算法加密签名消息语法规则》。

四、 金融 IC 卡

金融 IC 卡采用的数字证书公钥格式和签名格式应遵循 GB/T 35276《信息安全技术 SM2 密码算法使用规范》。

五、 网上银行

1. 网上银行采用的智能密码钥匙应遵循 GM/T 0017-2012《智能密码钥匙密码应用接口数据格式规范》，调用智能密码钥匙应遵循 GB/T 35291《信息安全技术 智能密码钥匙应用接口规范》。

2. 网上银行后台处理系统采用的密码机应遵循 GB/T 36322《信息安全技术 密码设备应用接口规范》。

3. SSL 网关应遵循 GM/T 0025-2014《SSL VPN 网关产品规范》。

4. 浏览器应遵循 GM/T 0024-2014《SSL VPN 技术规范》。

5. 应用软件调用客户端安全套件或密码服务中间件应遵循 GM/T 0020-2012《证书应用综合服务接口规范》或 GM/T 0019-2012《通用密码服务接口规范》。

6. 动态口令系统（包括动态令牌和动态令牌认证系统等）应遵循 GM/T 0021-2012《动态口令密码应用技术规范》。

7. 网上银行采用的签名验签服务器应遵循 GM/T 0029-2014《签名验签服务器技术规范》。

六、 移动支付

1. 采用金融 IC 卡方式的移动支付的数字证书公钥格式和签名格式应遵循 GB/T 35276《信息安全技术 SM2 密码算法使用规范》；采用网银方式的移动支付的数字证书格式应遵循 GB/T 20518《信息安全技术 公钥基础设施数字证书格式规范》。

2. 移动支付采用的 SD 卡、智能密码钥匙等终端密码设备应遵循 GM/T 0017-2012《智能密码钥匙密码应用接口数据格式规范》，调用时应遵循 GB/T 35291《信息安全技术 智能密码钥匙应用接口规范》。

3. 移动支付后台处理系统采用的密码机应遵循 GB/T 36322《信

息安全技术 密码设备应用接口规范》。

4. 移动支付采用的签名验签服务器应遵循 GM/T 0029-2014 《签名验签服务器技术规范》。

七、 电子认证

1. 网上银行采用的数字证书格式应遵循 GB/T 20518 《信息安全技术 公钥基础设施数字证书格式规范》。

2. 网上银行中使用的证书均为双证书即签名证书和加密证书。

3. 网上银行的电子认证基础设施的建设和服务应遵循 GB/T 25056 《信息安全技术 证书认证系统密码及其相关安全技术规范》和 GM/T 0014-2012 《数字证书认证系统密码协议规范》，支持基于 SM2 算法的撤销列表下载、OCSP 查询、数字证书的查询和导入导出。

4. 网上银行使用的浏览器应置入国家根证书，作为可信根。

八、 安全芯片

金融领域采用的安全芯片应符合 GM/T 0008-2012 《安全芯片密码检测准则》，其中金融 IC 卡芯片应满足安全等级 2 级及以上要求。