

GM/Y 5001-2019

密码标准应用指南



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

2019 年 5 月

目 录

一 序言	1
二 密码标准体系框架	2
三 密码基础类标准	7
1. 密码术语与标识	7
1.1 GM/Z 4001 密码术语	7
1.2 GB/T 33560 信息安全技术 密码应用标识规范	7
2. 密码算法	9
2.1 对称密码算法	9
2.1.1 GB/T 33133 信息安全技术 祖冲之序列密码算法	9
2.1.2 GB/T 32907 信息安全技术 SM4 分组密码算法	11
2.2 公钥密码算法	12
2.2.1 GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法	12
2.2.2 GM/T 0044 SM9 标识密码算法	13
2.3 杂凑密码算法	15
2.3.1 GB/T 32905 信息安全技术 SM3 密码杂凑算法	15
3. 算法设计与使用	16
3.1 GB/T 35276 信息安全技术 SM2 密码算法使用规范	16
3.2 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 基础设施类标准	18
1. 公钥基础设施	18
1.1 GM/T 0014 数字证书认证系统密码协议规范	18
1.2 GB/T 20518 信息安全技术 公钥基础设施数字证书格式规范	20
1.3 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	21
五 密码产品类标准	23
1. 安全性	23
1.1 通用要求	23
1.1.1 GB/T 37092-2018 信息安全技术 密码模块安全要求	23
2. 设备接口	25
2.1 应用编程接口	25
2.1.1 GM/T 0012 可信密码模块接口规范	25
2.1.2 GB/T 35291 信息安全技术 智能密码钥匙应用接口规范	27
2.1.3 GB/T 36322 信息安全技术 密码设备应用接口规范	28

2.1.4	GM/T 0056 多应用载体密码应用接口规范.....	29
2.1.5	GM/T 0058 可信计算 TCM 服务模块接口规范.....	30
2.2	数据格式接口.....	32
2.2.1	GM/T 0017 智能密码钥匙密码应用接口数据格式规范.....	32
3.	设备管理.....	33
3.1	GM/T 0050 密码设备管理 设备管理技术规范.....	33
3.2	GM/T 0051 密码设备管理 对称密钥管理技术规范.....	34
3.3	GM/T 0052 密码设备管理 VPN 设备监察管理规范.....	35
3.4	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.....	36
4.	技术规范.....	37
4.1	GB/T 36968 信息安全技术 IPSec VPN 技术规范.....	37
4.2	GM/T 0024 SSL VPN 技术规范.....	38
4.3	GM/T 0027 智能密码钥匙技术规范.....	39
4.4	GM/T 0029 签名验签服务器技术规范.....	40
4.5	GM/T 0030 服务器密码机技术规范.....	42
4.6	GM/T 0045 金融数据密码机技术规范.....	43
5.	产品规范.....	44
5.1	GM/T 0023 IPSec VPN 网关产品规范.....	44
5.2	GM/T 0025 SSL VPN 网关产品规范.....	46
5.3	GM/T 0026 安全认证网关产品规范.....	46
六	应用支撑类标准.....	48
1.	通用支撑.....	48
1.1	GM/T 0019 通用密码服务接口规范.....	48
2.	典型支撑.....	49
2.1	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.....	49
2.2	GM/T 0020 证书应用综合服务接口规范.....	51
2.3	GM/T 0032 基于角色的授权管理与访问控制技术规范.....	52
2.4	GM/T 0033 时间戳接口规范.....	54
2.5	GM/T 0057 基于 IBC 技术的身份鉴别规范.....	56
2.6	GB/T 32922 信息安全技术 IPSec VPN 安全接入基本要求与实施指南.....	57
七	密码应用类标准.....	60
1.	应用要求.....	60
1.1	GM/T 0054 信息系统密码应用基本要求.....	60
2.	典型应用.....	61
2.1	GM/T 0021 动态口令密码应用技术规范.....	61

2.2	GM/T 0031 安全电子签章密码技术规范.....	62
2.3	GB/T 37033 信息安全技术 射频识别系统密码应用技术要求.....	63
2.4	GM/T 0036 采用非接触卡的门禁系统密码应用技术指南.....	68
2.5	GM/T 0055 电子文件密码应用技术规范.....	70
八	密码检测类标准.....	72
1.	随机性检测.....	72
1.1	GB/T 32915 信息安全技术 二元序列随机性检测方法.....	72
1.2	GM/T 0062 密码产品随机数检测要求.....	74
2.	算法与协议检测.....	75
2.1	GM/T 0042 三元对等密码安全协议测试规范.....	75
2.2	GM/T 0043 数字证书互操作检测规范.....	77
3.	产品检测.....	78
3.1	功能检测.....	78
3.1.1	GM/T 0013 可信计算可信密码模块接口符合性测试规范.....	78
3.1.2	GM/T 0037 证书认证系统检测规范.....	79
3.1.3	GM/T 0038 证书认证密钥管理系统检测规范.....	81
3.1.4	GM/T 0040 射频识别标签模块密码检测准则.....	82
3.1.5	GM/T 0041 智能 IC 卡密码检测规范.....	84
3.1.6	GM/T 0046 金融数据密码机检测规范.....	85
3.1.7	GM/T 0047 安全电子签章密码检测规范.....	86
3.1.8	GM/T 0048 智能密码钥匙密码检测规范.....	87
3.1.9	GM/T 0049 密码键盘密码检测规范.....	88
3.1.10	GM/T 0059 服务器密码机检测规范.....	89
3.1.11	GM/T 0060 签名验签服务器检测规范.....	90
3.1.12	GM/T 0061 动态口令密码应用检测规范.....	91
3.1.13	GM/T 0063 智能密码钥匙密码应用接口检测规范.....	91
3.1.14	GM/T 0064 限域通信 (RCC) 密码检测要求.....	92
3.2	安全检测.....	94
3.2.1	GM/T 0008 安全芯片密码检测准则.....	94
3.2.2	GM/T 0039 密码模块安全检测要求.....	95
九	密码管理类标准.....	96
附录 A.	编号索引.....	97
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.....	101

一 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 2018 年 12 月，已发布密码行业标准 64 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推荐国家标准，截止 2018 年 12 月已颁布 19 项密码国家标准。

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，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。

二 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。

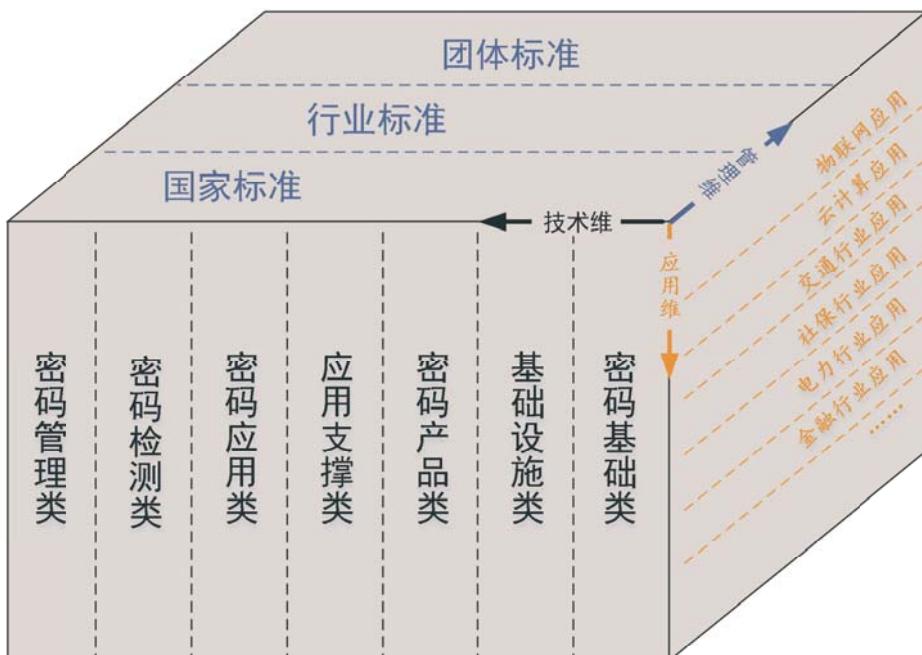


图 1 密码标准体系框架

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。

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。

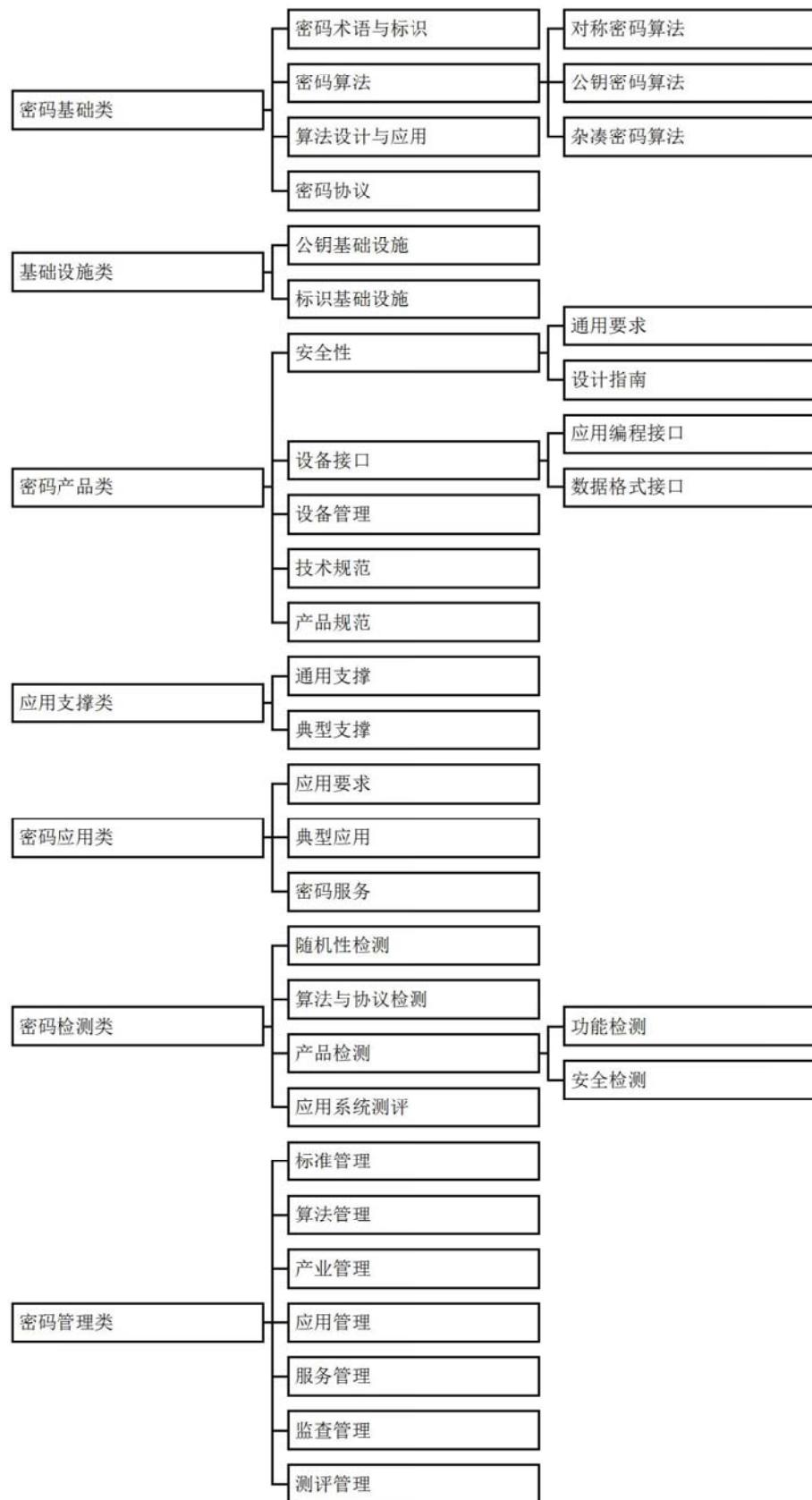


图 2 密码标准技术体系框架

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，对已经颁布的密码国家标准和密码行业标准逐一展开描述。

三 密码基础类标准

1. 密码术语与标识

1.1 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

术语是在技术交流的基础语言。统一规范术语和定义，有助于准确理解和表达技术内容，方便技术交流和研究。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。

该标准适用于为密码有关标准、指导性技术文件的编制提供指导，也可用于指导密码技术和产品的论证、设计、生产、使用、检测和评估等。

(3) 内容概要

该标准包括4章，第1章“范围”划定了该标准的适用范围，第2章“术语”是该标准的核心部分，列举了商用密码领域的主要术语及其解释，第3和第4章分别针对所有定义的术语，使用中文和英文列出索引，以便使用时检索。

1.2 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

在密码应用中，通常使用某一字段或短语来表示所使用的密码算法或数据实体等信息数据，如果不对这些标识的定义进行统一，则很难做到密码协议、密码接口间的互联互通，进而影响密码产品的标准化。

该标准旨在统一密码协议接口、管理等各方面使用的标识，以实现密码应用系统各组成部分间的兼容和统一，可用于指导其他相关标准或协议的编制中对标识的使用，也能够有效地指导、帮助密码设备的研制和协议的实现，以及助力密码管理部门实施有效的管理。

(3) 内容概要

该标准包括 6 章，第 1 章范围、第 2 章术语和定义、第 3 章符号和缩略语。

第 4 章说明了标识的格式和编码，其中所有标识符都为 32 比特无符号整数，跨平台传输时应将标识符按照高位字节在前的网络字节顺序(Big-endian) 进行处理。

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，例如 SGD_KEY_INDEX 表示密钥索引对象，SGD_PRIVATE_KEY_SIGN 表示签名私钥对象，SGD_CERT_SERIAL 表示证书序列号等；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，例如 SGD_PROTOCOL_PKCS11 表示 PKCS#11 接口，SGD_CRL_VERIFY 表示使用 CRL 方式进行证书验证等。

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 给出了商用密码领域中的相关 OID 定义，包括国家密码管理局、密标委以及各类密码算法的 OID 等。

2. 密码算法

2.1 对称密码算法

2.1.1 GB/T 33133 信息安全技术 祖冲之序列密码算法

(1) 版本

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。

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。

(2) 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。祖冲之密码算法是 128 比特密钥的序列密码算法，该标准定义了使用祖冲之算法产生密钥流并加密明文，或

对明文生成 MAC 的方法，其中 MAC 值为 32 比特。

祖冲之密码算法是我国自主设计的序列密码算法，已被 3GPP 组织采纳为 LTE 的标准密码算法之一，该标准的内容也与 3GPP LTE 机密性算法 128-EEA3 和完整性算法 128-EIA3 (ETSI/SAGE TS 35.221) 保持一致。虽然祖冲之算法的初始设计是为移动通信服务，但同样适用于其它采用 128 比特密钥的数据加密和完整性保护场合。

(3) 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，本部分已上升为国家标准 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。

其中，第 1 部分描述了祖冲之算法的整体结构。其逻辑上划分为上中下三层，上层是模 $2^{31}-1$ 的 16 级线性反馈移位寄存器 (LFSR)，中层是比特重组 (BR) 单元，下层是非线性函数 F。算法工作分为两个阶段，首先是初始化阶段，在这一阶段密钥和初始向量 (IV) 被装入线性反馈移位寄存器 (LFSR)，并经过 32 轮的运行，初始化阶段不产生密钥流；之后是工作阶段，这一阶段每运行一个节拍产生 32 比特密钥字，持续运行则可以产生任意长度密钥流。

第 2 部分定义了使用祖冲之算法加密数据的方法。其基本原理就是使用第 1 部分描述的算法，在工作状态时产生密钥流，将密钥流与明文流模二加即可得到密文流。

第 3 部分定义了使用祖冲之算法计算明文 MAC 的方法。其基本原理是使用第 1 部分描述的算法产生大于明文位数的密钥字，然后将明文对应位置为 1 的密钥字逐个模二加，并与最后一个密钥字模二加之和得到 MAC。

2.1.2 GB/T 32907 信息安全技术 SM4 分组密码算法

(1) 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。

(2) 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。

SM4 分组密码算法是我国自主设计的分组密码算法，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。

(3) 内容概要

该标准描述了 SM4 分组密码算法，分为 7 章，第 1 章范围、第 2 章术语和定义、第 3 章符号和缩略语。

第 4 章介绍了 SM4 算法的结构，使用 SM4 的加密和解密计算结构上完全相同，只是轮密钥的次序相反。

第 5 章介绍了 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，其中 FK 为系统参数，CK 为固定参数，这两个参量在算法中都有明确的取值。

第 6 章介绍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。

2.2 公钥密码算法

2.2.1 GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

(1) 版本

GB/T 32918《信息安全技术 SM2 椭圆曲线公钥密码算法》共分为五个部分：

——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》系该标准第 1 部分国家标准最新版本；

——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》系该标准第 2 部分国家标准最新版本；

——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》系该标准第 3 部分国家标准最新版本；

——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》系该标准第 4 部分国家标准最新版本；

——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》系该标准第 5 部分国家标准最新版本。

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。

(2) 用途与适用范围

该标准描述了 SM2 公钥密码算法，可广泛用于 SSL、IPSec 等使用公钥密码算法的安全协议，以及电子支付、通信保护等应用场景，以实现数字签名、密钥协商、公钥加密等安全机制。

(3) 内容概要

GB/T 32907《信息安全技术 SM2 椭圆曲线公钥密码算法》共分为 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 部分定义了使用 SM2 算法进行数字签名和验签的方法，并在附录 A 给出了一个加密解密的示例。

第 3 部分定义了使用 SM2 算法进行密钥交换的协议和流程，并在附录 A 给出了一个密钥交换的示例。

第 4 部分定义了使用 SM2 算法进行公钥加密和解密的方法，并在附录 A 给出了一个公钥加解密运算的示例。

第 5 部分定义了 SM2 算法的椭圆曲线参数，并在附录中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。

2.2.2 GM/T 0044 SM9 标识密码算法

(1) 版本

GM/T 0044-2016《SM9 标识密码算法》是当前的最新版本，共分为五个部分：

——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/T 0044.5-2016《SM9 标识密码算法 第 5 部分：参数定义》。

(2) 用途与适用范围

该标准描述了基于标识的密码算法 SM9。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典型用途。

基于标识的密码算法，其典型特点是公钥是由用户身份标识唯一确定的，因而无需使用“数字证书”来将二者绑定，这使得密钥管理环节得到适当简化。该标准 2016 版对于私钥的管理有其独特的特点，用户标识（公钥）对应的私钥并非由用户自行产生，而是由密钥生成中心（KGC）根据用户的标识计算而得出，这意味着在基于标识的密码体系中，私钥具有内在的可托管性质。

该标准包括 5 个部分，分别描述了 SM9 算法的数学基础、数学原理、数字签名算法、加密算法、密钥协商算法等，适用于任何使用 SM9 算法的应用场合，同时也是对 SM9 密码体系进行检测时，对合规性进行判断的依据。

(3) 内容概要

GM/T 0044《SM9 标识密码算法》共分为 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，以帮助了解和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 部分定义了采用 SM9 的数字签名算法，包括算法参数和辅助函数，数字签名流程以及数字签名验签流程。

第3部分定义了采用SM9的密钥交换协议，包括其算法参数与辅助函数，以及密钥交换协议的流程。

第4部分定义了采用SM9的密钥封装机制和公钥加密算法，包括其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部分给出了SM9算法的参数定义，包括椭圆曲线方程及参数、群 G_1 和 G_2 的生成元等，同时还给出了扩域元素的表示方法。

2.3 杂凑密码算法

2.3.1 GB/T 32905 信息安全技术 SM3 密码杂凑算法

(1) 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。

(2) 用途与适用范围

该标准规定了SM3密码杂凑算法的计算方法和计算步骤。密码杂凑算法是一种将任意长信息转换成固定长杂凑值的数学方法，在实际应用中的用途十分广泛：可用于数字签名机制中，首先使用密码杂凑算法对明文计算杂凑值，然后使用非对称私钥对杂凑值签名；可用于构造明文消息的“消息认证码（MAC）”，以保证其完整性和认证身份；可用于随机数发生器的后处理单元，确保随机数质量；还常被用作口令保护，即对用户键入的口令计算杂凑值，将杂凑值传输或存储。

该标准所描述的SM3密码杂凑算法是一种杂凑长度为256比特的

算法，适用于我国商用密码应用中的数字签名和验证、消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。同时，该标准还可为安全产品生产商提供产品和技术的标准定位以及标准化的参考，提高安全产品的可信性与互操作性。

（3）内容概要

该标准描述了 SM3 密码杂凑算法，共分为 5 章，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 T_j 的取值，以及用到的布尔函数和置换函数。

第 5 章介绍了 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 给出了两个 SM3 密码杂凑算法的计算示例。

3. 算法设计与使用

3.1 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

该标准旨在为使用 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，有利于提高密码产品的标准化和互联互通。

(3) 内容概要

该标准主要包括 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表示。

第 6 章数据转换过程，包括数据在位串与字符串之间的转换方法，整数和字符串之间的转换方法。

第 7 章数据格式，主要内容为密钥数据格式，加密数据格式，签名数据格式，密钥对保护数据格式。对于密文的结构定义中没有采用 GB/T 32918 中的自然顺序，而是使用了方便程序访问的数据元次序。

第 8 章预处理，包括 Z 值计算过程和签名操作所需的杂凑操作。

第 9 章计算过程，包括生成密钥，加密，解密，数字签名，签名验证和密钥协商。

第 10 章用户身份标识，提供了用户身份标识的默认值。

3.2 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准是 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，适用于使用 SM2 算法进行加密和签名操作时对操作结果的标准化封装。

该标准定义的加密签名消息语法可广泛用在密码芯片、密码模块、

密码设备、密码服务、密码应用系统之中，增强不同设备或系统之间的互联互通性，也可为检测提供参考。

(3) 内容概要

该标准包含 12 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 data、签名数据类型 signedData、数字信封数据类型 envelopedData、签名及数字信封数据类型 signedAndEnvelopedData、加密数据类型 encryptedData 和密钥协商类型 keyAgreementInfo 进行了详细定义。

标准附录 A 为规范性附录，定义了 SM2 密钥格式。

四 基础设施类标准

1. 公钥基础设施

1.1 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

该标准描述了证书认证和数字签名中通用的安全协议流程、数据格式和密码函数接口等内容。以密码技术为基础，为网络内的数字证书认证系统提供统一、通用的通联协议服务，以满足网络内的实体对数字证书认证系统的真实性、保密性、完整性、可认证性和不可否认

性等安全需求。

该标准适用于电子政务、电子商务中基于密码技术的数字证书认证系统的设计、建设、检测、运营及管理，规范数字证书认证系统中密码协议的标准化应用，推动数字证书认证系统的互联互通和相互认证。对于组织、机构内部使用的数字证书认证系统密码协议的建设、运营及管理，可参考使用。标准同时还可为安全产品生产商提供产品和技术的准确定位和标准化的参考，提高安全产品的可靠性和互操作性。

(3) 内容概要

该标准分为 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。规范的主体部分包括第 5 章和第 6 章。

第 5 章定义了数字证书认证系统中涉及到密码技术的相关安全协议，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 章定义的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、发布信息等项的语法说明。

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一个实例。

附录 D 是规范性附录，给出了非实时发布证书协议的流程。

1.2 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

该标准规定了数字证书和证书撤销列表的基本结构，并对数字证书和证书撤销列表中的各数据项内容进行了描述。适用于数字证书认证系统的研发、数字证书认证机构的运营以及基于数字证书的安全应用，并可用于指导各 PKI/CA 厂商研发具有统一规范的 SM2 证书应用安全产品，指导应用系统实现基于数字证书的应用集成，方便证书应用开发和项目实施，满足应用系统对数字证书和密码应用的需求，实现证书应用安全标准化和统一性，促进基于数字证书应用的推广，提升应用系统的安全保障能力。

(3) 内容概要

标准分为 5 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 章详细定义了基于 SM2 密码算法的数字证书和 CRL 的格式。

标准附录 A 为规范性附录，列表给出了证书结构的简明表述。

标准附录 B 为规范性附录，列表分别给出了用户证书、服务器证书的结构实例。

标准附录 C 为规范性附录，定义了证书的内容表。

标准附录 D 为资料性附录，定义了 RSA、SM2 证书的编码实例。

1.3 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

该标准规定了为公众服务的数字证书认证系统的设计、建设、检测、运行及管理规范，其目标是为实现数字证书认证系统的互连互通和交叉认证提供统一的依据，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，并有利于相关检测机构对该类产品的规范化检测。标准还规定了基于 SM2 密码算法的数字证书认证系统的密码及相关安全的技术要求，包括证书认证中心，密钥管理中心，密码算法、密码设备及接口等。

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

该标准分为 12 章，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 章介绍了证书认证系统的设计细节，包括系统的总体设计和各子系统设计，并提供了设计原则以及各个子系统的实现方式。

第 6 章描述了密钥管理中心的组成模块，包括密钥生成、密钥管理、密钥库管理、认证管理、安全审计、密钥恢复和密码服务等模块。

第 7 章定义了证书认证系统和密钥管理中心使用的密码算法、密码设备和接口。

第 8 章从系统、安全、数据备份、可靠性、物理安全、人事管理制度等方面规范了证书认证中心的建设。

第 9 章从系统、安全、数据备份、可靠性、物理安全、人事管理制度等方面规范了密钥管理中心的建设。

第 10 章从人员管理、业务运行管理、密钥分管、安全管理、安全审计、文档配备等方面对证书认证中心的运行管理要求进行了规范。

第 11 章从人员管理、业务运行管理、密钥分管、安全管理、安全审计、文档配备等方面对密钥管理中心的运行管理要求进行了规范。

第 12 章定义了证书操作流程。

附录 A 是资料性附录，给出了证书认证系统的网络结构图。

五 密码产品类标准

1. 安全性

1.1 通用要求

1.1.1 GB/T 37092-2018 信息安全技术 密码模块安全要求

(1) 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准是 GM/T 0028《密码模块安全技术要求》，最后版本为 GM/T 0028-2014。

(2) 用途与适用范围

该标准是针对实现密码功能的密码模块的安全技术要求。密码模块是密码应用的核心部件，密码系统的安全性与可靠性直接取决于实现它们的密码模块。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。

该标准规定了四个递增的、定性的安全要求等级，以满足密码模块在不同应用和工作环境中的要求。该标准规定的安全要求涵盖了有关密码模块的安全设计、实现、运行与废弃的安全元素(域)，这些元素(域)包括：密码模块规格，密码模块接口，角色、鉴别和服务，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。

该标准对密码模块提出了安全要求，但不对密码模块的正确应用和安全部署进行规范。密码模块的操作员在应用或部署模块时，有责

任确保模块提供的安全保护是充分的，且对信息所有者而言是可接受的，同时任何残余风险要告知信息所有者。必须选取合适的安全等级的密码模块，使得模块能够满足应用的安全需求并适应所处环境的安全现状。

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本产品进行设计，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。此外，该标准也适用于密码和信息相关的方案咨询、标准编制活动，当其中涉及对密码模块的安全要求时，可引用该标准的相应等级。

（3）内容概要

该标准包含 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 章介绍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。每个条款包含若干项要求，以[xx. yy]的形式表示，例如[01. 01]表示通用要求条款的第1项要求。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为规范性附录，规定了对各个条款的文档要求。

附录B为规范性附录，规定了对各个条款安全策略表述的要求。

附录C为规范性附录，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为规范性附录，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为规范性附录，给出了适用于该标准的核准的鉴别机制列表。

附录F为规范性附录，给出了适用于该标准的非入侵式攻击及常用的缓解方法。

2. 设备接口

2.1 应用编程接口

2.1.1 GM/T 0012 可信计算 可信密码模块接口规范

(1) 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。

(2) 用途与适用范围

该标准描述了可信密码模块的接口规范，用以指导可信密码模块的产品开发和应用。

类似于 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》，该标准在制订时借鉴了国际先进的可信计算技术框架与技术理念，同时依据我国自身的安全需求、产业市场以及信息安全技术的最新发展情况进行了创新，例如采用了我国自主设计的密码算法和证书体系，研发了新型授权协议等。

该标准详细定义了可信密码模块的管理功能，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。

（3）内容概要

该标准分为 8 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 章定义了可信密码模块正常发挥作用所需的一系列管理功能，包括启动过程中的启动模式设定、工作模式设定，自检、关机过程中的状态保存，使用过程中的所有者管理、升级维护、上下文保存与恢复以及时钟和计数器等。

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一系列功能和接口，还定义了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一系列功能和接口，包括三部分内容：一是保护可信

密码模块内部资源（如密钥）的访问控制方法，包括授权协议和传输会话；二是保护平台内可信密码模块以外的数据的密码学操作，包括加解密、数字签名、封装与解封装等；三是管理可信密码模块密钥的方法，包括密钥生成、加载、协商等。

第8章定义了可信密码模块提供的、用于存储和引证平台完整性度量值的功能和接口。

附录A为规范性附录，定义了第5章至第8章所述接口使用的数据结构。

2.1.2 GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

(1) 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。

(2) 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。该标准还可为智能密码钥匙厂商提供产品和技术的标准定位以及标准化的参考，提高智能密码钥匙产品的安全性、易用性与互操作性。

(3) 内容概要

该标准描述了智能密码钥匙的应用接口，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，给出了智能密码钥匙应用接口与智能密码钥匙设备、驱动、应用之间的层次关系，给出了应用接口访问时所需的角色、容器、密钥和文件模型。

第6章数据类型，定义了接口所需的参数和返回值的数据类型和常量。

第7章接口函数，定义了智能密码钥匙对上层提供的功能函数接口。接口函数按照用途分为设备管理、访问控制、应用管理、文件管理、容器管理和密码服务等类别。

第8章安全要求，对设备的生命周期、权限管理、密钥管理和抗攻击性提出了要求。

在该标准中定义了智能密码钥匙在典型PKI应用中的结构模型，该结构支持设备认证密钥和多应用，同时划分了管理员和用户角色。通过对文件、证书和多容器的支持，可以在一个设备上支持多个安全应用。

2.1.3 GB/T 36322 信息安全技术 密码设备应用接口规范

(1) 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。

(2) 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。该标准可为该类密

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，不规范管理接口；密码设备需要提供管理界面，通过管理界面管理设备。该标准遵循密钥的默认使用原理，按指令功能选用密钥；设置了设备密钥，用于设备的管理。

该标准适用于服务器密码机、PCI/PCI-E 密码卡等密码设备的应用接口的定义和规范，可用于服务器密码机、PCI/PCI-E 密码卡等密码设备的研制、使用，以及基于该类密码设备的应用开发，也可用于指导该类密码设备的检测。

(3) 内容概要

该标准主要包括 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 章算法标识和数据结构，规定了算法标识定义、设备信息定义、密钥分类及存储定义等，并规定了 RSA 密钥数据结构、ECC 密钥数据结构、ECC 加密数据结构、ECC 签名数据结构、ECC 加密密钥对保护结构等。

第 6 章设备接口描述，定义了设备管理类函数、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、用户文件操作类函数。

第 7 章安全要求，主要对密钥管理、密码服务、设备状态等提出安全性要求。

附录 A 为规范性附录，给出了函数调用返回代码的定义。

2.1.4 GM/T 0056 多应用载体密码应用接口规范

(1) 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。

(2) 用途与适用范围

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，具体包括SM2/SM3/SM4算法在多应用载体中的标识，SM2/SM3/SM4算法的密码应用接口规格。该标准适用于各种多应用载体的研制，也可用于指导多应用载体的密码应用检测。

本文中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。

该标准规范了SM系列算法在多应用载体中的密码算法能力标识、接口定义，保障用户应用使用密码功能的统一性和完整性。

(3) 内容概要

该标准主要包括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章符合和缩略语。

第5章对多应用载体的系统框架进行了描述。

第6章对多应用载体密码应用接口的调用流程进行了描述。

第7章描述了Java技术方案中密码应用接口的具体定义。定义了Java技术方案下的密码算法能力标识定义、密码应用包定义、SM2/SM3/SM4算法的应用接口定义，以及具体的类实现定义。

附录A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规定了多应用安全管理使用到的证书格式。

2.1.5 GM/T 0058 可信计算 TCM 服务模块接口规范

(1) 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。

(2) 用途与适用范围

该标准规定了 TCM 服务模块的组成和接口标准，包含 TSP、TCS 和 TDDL，是面向 TCM 应用层的接口标准。

该标准描述了可信计算 TCM 服务模块接口规范，目标是制定统一的可信计算 TCM 服务模块组成和接口规范，通过该类接口规范，向应用层提供统一的 TCM 密码应用服务，为可信计算应用的开发、使用及检测提供标准依据和指导，有利于提高可信计算产业发展水平。

(3) 内容概要

该标准主要包括 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 章软件架构中定义了 TCM 服务模块软件架构。

第 6 章中详细定义和描述了 TCM 应用服务的操作命令与函数接口规范。TSP 向应用程序提供 TCM 的服务，提供高层的 TCM 函数，使应用程序只关注它本身的特性，依靠 TSP 执行 TCM 提供的可信函数。TSP 还提供了一些方便功能操作的辅助函数，这些函数不是由 TCM 提供，如：签名验证功能。

第 7 章 TCM 核心服务中，详细定义和描述了 TCM 核心服务的操作命令与函数接口规范。

第 8 章 TCM 设备驱动中，详细定义和描述了上层应用与可信密码模块数据传输的操作命令与函数接口规范。包括设备的打开、关闭、数据发送/接收、数据传输取消、可信密码模块属性设置/读取以及可信密码模块状态获取等功能。

附录 A 是规范性附录，该部分详细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。

2.2 数据格式接口

2.2.1 GM/T 0017 智能密码钥匙密码应用接口数据格式规范

(1) 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。

(2) 用途与适用范围

该标准对智能密码钥匙的应用数据接口进行规范，用于指导智能密码钥匙的数据层互操作。

该标准用于规范智能密码钥匙的 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产品的研制、使用和检测。

(3) 内容概要

该标准主要包括 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 章给出了正文中用到的记号。

第 6 章给出了智能密码钥匙的结构模型，并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，定义了命令报文的响应报文的数据结构。

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 章给出了智能密码钥匙的 APDU 指令的详细编码并给出了 APDU 响应的编码。

第 10 章给出了智能密码钥匙支持的设备协议。

该标准中对 APDU 指令编码按照指令用途进行了分类。APDU 指令

包含设备管理、访问控制、应用管理、文件管理、容器管理和密码服务等指令。为了保证智能密码钥匙的设备接入能力，该标准还明确了使用 USB Mass Storage、HID、CCID 通信协议时协议编码相关内容。

3. 设备管理

3.1 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

该标准制定了统一的密码设备管理技术规范，实现了设备管理应用与具体密码设备的无关性、与密码设备用途的无关性。依据该标准设计、开发的密码设备，可以实现统一管理、统一配置的目的。

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，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和开发，也可用于指导密码设备管理系统、密码设备的检测。

(3) 内容概要

该标准共分为 9 个章节，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 章详细介绍了密码设备管理的体系结构。在该体系中，以数字证书机制为基础，在密码设备管理平台和底层被管设备之间建立一条安全通道，完成双方身份的鉴别和会话密钥的协商。通过该安全通道，设备管理平台可确认底层密码设备的位置，对其进行安全的基础管理。各种上层的管理应用如：远程密钥管理、远程设备监控、远程

设备回归性检查等以该安全通道为载体与底层密码设备之间进行信息交互。此外，本章还详细介绍了设备管理平台体系中各层的具体功能、设备管理信息的具体内容、设备证书的申请/更新管理要求、设备注册流程等内容。

第6章定义了设备管理中心与密码设备管理代理之间的管理信息交互应用安全协议，内容包括安全通道协议的消息格式定义、安全通道的建立时机和安全通道的使用等。

第7章定义了可管理的密码设备信息的层次结构、数据类型定义及管理属性对象的定义。

第8章定义了各级设备管理中心之间、各级设备管理中心和被管设备之间通过安全通道交互的密码设备管理消息格式。

第9章定义了设备管理平台对上层管理应用提供的接口。

附录A定义了关键错误代码。

附录B具体描述了建立安全通道的协议。

3.2 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统一的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。

(3) 内容概要

该标准共分为 9 个章节，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。

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，对称密钥管理系统结构和功能，并从管理端、传输和终端三个组成部分详细描述了设计要求。

第 7 章描述了密钥管理系统与被管设备间的协议、指令以及密钥管理系统的接口标准、数据结构标准。

附录 A 定义了关键错误码，支持扩展。

附录 B 定义了通用密钥产生装置所要求的密钥导入格式和专用密钥产生装置生成密钥的参数格式。

3.3 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

该标准旨在对 VPN 设备的使用行为进行有序、可控地管理，规范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

该标准共有 7 个章节，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 章依据 GM/T 0050《密码设备管理 设备管理技术规范》中定义的密码设备管理体系结构，规范了 VPN 设备的监察管理体系结构和管理流程。

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 章描述了 VPN 设备管理应用层和监察设备之间的网络通信消息。

3.4 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

该标准在 GM/T 0050《密码设备管理 设备管理技术规范》定义的密码设备管理体系基础上，对密码设备的远程监控、设备合规性检验等管理应用的接口数据进行规范。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，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

该标准共分为 6 个章节，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 章定义了密码设备管理体系。此体系遵循 GM/T 0050，该标准主要涉及密码设备管理平台层和密码设备层的管理应用接口，包括

远程监控、设备合规性检验等。

第6章在GM/T 0050定义的密码设备管理应用体系基础上，规范了远程监控、设备合规性检验等管理应用的详细消息格式。

4. 技术规范

4.1 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

该标准对IPSec VPN的技术协议、产品的功能、性能和管理以及检测进行了规定，用于指导IPSec VPN产品的研制、检测、使用和管理。

该规范的协议部分主要依据RFC4301、RFC4302、RFC4303、RFC4308、RFC4309等标准制定。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，对密钥协商、密码算法及使用、某些功能项的实施方法提出了一些特定的要求。

(3) 内容概要

该标准主要包括8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章介绍了密码算法和密钥种类。

第5章规定了密钥交换协议和安全报文协议。密钥交换协议包括交换阶段及模式、NAT穿越、密钥交换的载荷格式、数据包格式等；

安全报文协议包括鉴别头协议 AH、封装安全载荷 ESP、NAT 穿越、和匹配安全策略等。

第 6 章 IPSec VPN 产品要求，规定了 IPSec VPN 产品的功能要求、性能要求和安全管理要求。功能要求规定了随机数生成、工作模式、密钥交换、安全报文封装、NAT 穿越、鉴别方式、IP 协议版本支持、抗重放攻击、密钥更新等要求；产品性能要求规定了加解密吞吐率、加解密时延、加解密丢包率、每秒新建连接数等要求；安全管理要求规定了密钥管理、数据管理、人员管理、设备管理等要求。

第 7 章 IPSec VPN 产品检测，规定了 IPSec VPN 产品的功能检测、性能检测和安全管理检测要求。

第 8 章合格判定，规定了 IPSec VPN 产品合格判定的要求。

4.2 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

该标准对 SSL VPN 的技术协议、产品的功能、性能和管理以及检测进行了规定，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。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。

(3) 内容概要

该标准共包括 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章描述了规范中使用的密码算法和密钥种类。

第6章详细介绍了SSL VPN协议包括的握手协议、密码规格变更协议、报警协议、网关到网关协议和记录层协议的内容。

第7章从产品功能、产品性能、安全管理等方面对SSL VPN网关产品提出了具体要求。

第8章根据第7章的产品要求，介绍了如何检测SSL VPN网关产品。

第9章说明了产品的合格判定标准。

4.3 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，详细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。

该标准阐明了智能密码钥匙应该遵循的各方面要求，相当于智能密码钥匙产品的白皮书。智能密码钥匙研制者通过查阅该标准，能够获得关于智能密码钥匙应遵循所有标准的综合性索引。该标准适用于智能密码钥匙的研制、使用，也可用于指导智能密码钥匙的检测。

(3) 内容概要

该标准包括11个章节，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

化和使用初始化能力、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，包括电路接口、芯片等。

第 7 章描述了智能密码钥匙的软件要求，主要是对 GM/T 0017 的遵循要求。

第 8 章给出了智能密码钥匙的性能要求，具体技术指标在附录 A 给出。

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、软件防护等。

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 为资料性附录，给出了智能密码钥匙应达到的具体性能指标。

4.4 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

该标准定义了签名验签服务器的相关术语，规定了签名验签服务器的功能要求、安全要求、接口要求、检测要求和消息协议语法规范等有关内容。

该标准规范了签名验签服务器的服务功能，包括无格式和有格式的数字签名服务、无格式和有格式的签名验证服务、数字证书的验证

服务等。该标准规范了三种服务模式下的服务接口，包括函数调用方式、消息请求方式和 WEB 方式。签名验签服务器是提供外包式运算的设备，为应用系统提供签名验签运算服务。

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，对外提供的安全服务接口，支持的密码算法、密钥管理等方面强制技术要求。

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 8 章内容，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。

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。

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。

第 8 章给出了合格判定的标准。

该标准的附录 A、B、C 都是资料性附录，其中附录 A 给出了签名验签服务器的消息协议语法规范，附录 B 给出了基于 HTTP 的签名消息协议语法规范，附录 C 给出了响应码定义和说明。

4.5 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

该标准适用于服务器密码机的研制、使用，也可用于指导服务器密码机的检测，规定了服务器密码机的功能要求、硬件要求、软件要求、安全性要求及检测要求，保证服务器密码机基本技术规格的一致性，尽可能实现不同厂家提供的服务器密码机在具体应用中的设备通用性，避免重复开发，便于用户的使用，同时也有利于主管部门的统一测评、认证和管理。

该标准规定了服务器密码机在研发、生产、使用过程中，必须遵循的技术要求，规定了服务器密码机需提供的功能，对外提供的安全服务接口，支持的密码算法、密钥管理等方面的技术要求；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。

(3) 内容概要

该标准主要包括 10 章内容，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。

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。

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。

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。

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。

第10章是合格判定。

4.6 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等有关内容，可用于指导金融数据密码机技术规范的研制、检测、使用和管理。

该标准侧重于金融业务数据的安全保护，以及相应的密钥管理技术，适用于金融数据密码机的研制、运行、维护管理，以及密码机自身的安全保护。

遵循该标准，有利于节省产品开发商的开发成本和开发难度，实现各厂家产品之间的互联互通；有利于最终用户对金融数据密码机产品的正确选择并降低用户选用产品的技术门槛，提升用户对产品的规范使用和管理水平；有利于主管部门对该类产品的管理以及相关检测机构对该类产品的规范化检测。

(3) 内容概要

该标准主要包括10章内容，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章缩略语。

第5章规定了金融数据密码机的功能要求，其中包括密码算法，密钥管理、访问控制和设备管理等功能方面的要求。密码算法包括对称算法、非对称算法、密码杂凑算法；密钥管理中，包括密钥全生命周期的管理以及随机数产生进行了规定；访问控制包括物理访问控制和逻辑访问控制；设备管理包括设备自检和设备中的日志审计等方面内容。

第6章规定了金融数据密码机的硬件要求，其中包括设备的物理接口、状态指示、随机数发生器、环境适应性和可靠性。

第7章规定了金融数据密码机必须提供的安全业务要求，描述了金融数据密码机必须提供的安全机制、安全服务功能和应用编程接口等的技术要求；根据不同的金融业务类型，描述了磁条卡业务、IC卡业务和基础密码运算服务等金融业务的要求。

第8章规定了金融数据密码机的安全性要求，应符合GM/T 0028。

第9章规定了金融数据密码机的检测要求，提出了相应的检测方法和检测标准，包括设备的外观和结构检查、提交的研发和设计文档检查、功能检测、性能检测以及环境适应性等方面。

第10章规定了金融数据密码机的合格性判定标准。

5. 产品规范

5.1 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

该标准对IPSec VPN网关产品的功能、性能、管理、合规性和检

测方法进行了规范，规定了 IPSec VPN 的功能要求、硬件要求、软件要求、安全性要求和检测要求等有关内容，可用于指导 IPSec VPN 网关产品的研制、检测、使用和管理。

遵循该标准研制和生产 IPSec VPN 产品，有利于主管部门对 IPSec VPN 设备的管理以及相关检测机构对该类产品的规范化检测；有利于各最终用户对 IPSec VPN 网关产品的正确选择并降低用户选用产品的技术门槛，提升用户对产品的规范使用和管理水平，同时可以节省产品开发商的开发成本和开发难度；有利于各厂家产品之间的互联互通，实现行业范围内多家 IPSec VPN 设备提供商的市场竞争格局。

（3）内容概要

该标准主要包括 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 章介绍了密码算法和密钥种类。

第 5 章规定了 IPSec VPN 网关产品要求，提出了随机数生成、工作模式、密钥协商、安全报文封装、密钥更新等 10 大项主要功能要求；明确了加解密吞吐率、时延、丢包率、每秒新建隧道数和最大并发隧道数等五项性能指标要求；从密钥管理、硬件安全和软件安全三大方面提出了安全性要求；从配置管理、人员管理、设备管理三各层次对管理维护方面进行了说明；加入了远程管理部分，对 IPSec VPN 网关产品的远程合规性验证、远程配置管理、远程监控功能要求进行了详细的描述；硬件要求方面，除了对外接口、密码部件和随机数发生器的要求，还细化了环境适应性和可靠性要求，增加了电磁兼容性要求部分。

第 6 章 IPSec VPN 网关产品检测，根据第 5 章的功能要求、性能

要求和管理要求，提出了对应的检测方法。

第 7 章规定了 IPSec VPN 网关产品的合格性判定标准。

5.2 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

标准对 SSL VPN 网关产品的功能、性能、管理、合规性和检测方法进行了规范。

标准规定了 SSL VPN 的功能要求、硬件要求、软件要求、安全性要求和检测要求等有关内容，可用于指导 SSL VPN 网关产品的研制、检测、使用和管理。

(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 章术语和缩略语。

第 4 章介绍了产品中使用的密码算法和密钥种类。

第 5 章 SSL VPN 网关产品要求为重点章节，详细描述了 SSL VPN 网关产品功能要求、产品性能要求、安全性要求、管理要求、设备管理以及硬件要求。

第 6 章为相应的产品检测要求。

第 7 章为合格性判定。

5.3 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

标准对安全认证网关产品的功能、性能、管理、合规性和检测方法进行了规范。

标准规定了安全认证网关产品的密码算法和密钥要求、功能要求、硬件要求、软件要求、安全性要求和检测要求等有关内容,可用于指导安全认证网关产品的研制、检测、使用和管理。

(3) 内容概要

标准共分为 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 章给出了安全认证网关产品的概述。

第 6 章列出了规范中使用的密码算法和密钥种类。

第 7 章从产品功能、产品性能、安全性要求和管理要求等方面对安全认证网关产品提出了具体要求。

第 8 章根据第 7 章的产品要求,规定了安全认证网关产品须完成的检测。

第 9 章说明了产品的合格判定标准。

六 应用支撑类标准

1. 通用支撑

1.1 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。

通用密码服务接口向典型密码服务层和应用系统提供各类通用的密码服务，有利于密码服务接口产品的开发，有利于应用系统在密码服务过程中的集成和实施，有利于实现各应用系统的互联互通。

该标准规定的接口标准，在接口框架层次上类似于国际上PKCS#11或CSP接口标准。

该标准适用于密码应用服务的开发，密码应用支撑平台的研制及检测，也可用于指导使用密码设备的应用系统的开发。

(3) 内容概要

该标准主要包括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，第四章符号和缩略语。

第5章算法标识和数据结构，主要包括密码服务接口定义、密码服务接口数据结构定义和说明等。

第6章密码服务接口，主要阐述了密码服务接口在公钥密码基础设施应用技术框架的位置、接口的组成和功能说明。

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。

2. 典型支撑

2.1 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准是 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

该标准阐明了可信计算密码支撑平台功能原理与要求，并详细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，用以指导我国相关可信计算产品的开发和应用。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。

该标准所规定的可信密码支撑平台的功能及相应的接口可分为三类：身份标识、完整性存储和引证以及安全存储。身份标识相关功能和接口主要用于建立平台硬件身份标识。完整性存储和引证功能及其接口主要用于安全的存储平台完整性度量值，并根据需要提供度量值的数字签名。安全存储功能和接口主要用于进行数据加密、解密、封装、解封装等。

上述功能和接口通常由可信软件模块基于可信密码模块芯片实

现，安全应用开发人员可调用这些接口和功能，便捷、高效的实现可信应用程序。相比于 GM/T 0012《可信计算 可信密码模块接口规范》（以下简称《TCM 规范》）中所规定的接口，该标准所规定的接口抽象度更高、易用性更强，特别适用于普通的可信应用开发人员或专业的 TCM 服务模块开发人员使用。

该标准以《可信计算平台密码技术方案》为指导。《可信计算平台密码技术方案》体现了三个原则：以商用密码算法作为平台各类功能的基础基础，采用我国自主研发、拥有自主知识产权的 SM2/3/4 等公钥密码、杂凑密码和分组密码算法；结合国内安全需求与产业市场，充分考虑我国法律、监管、市场等各方面的特殊性，在平台特定功能中体现这些要求和特殊性；借鉴国际先进的可信计算技术框架与技术理念并自主创新。

（3）内容概要

该标准分为 5 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 章可信计算密码支撑平台功能原理，从平台体系结构、密码算法要求和功能原理三个方面进行了说明，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，分上下文管理、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，详细说明了各功能接口的作用、参数以及与其他接口的关系。

附录 A、B、C 都是规范性附录，附录 A 定义了第 5 章接口中所使

用的各类数据结构；附录 B 定义了第 5 章接口中所使用的数字证书格式，该格式遵守 GB/T 20518 定义的数字证书格式，并定义了证书可信计算扩展域 TCMExtension；附录 C 给出了主板应用接口，即在计算机主板上可信密码模块通过 UEFI 对外提供的功能接口。

2.2 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

证书应用综合服务接口主要为上层的证书应用系统提供简洁、易用的调用接口，屏蔽了各类密码设备（服务器密码机和智能密码钥匙等）的设备差异性，屏蔽了各类密码设备的密码应用接口之间的差异性，实现应用与密码设备无关性，可简化应用开发的复杂性。

证书应用综合服务接口分成客户端接口和服务器端接口两类，可满足 B/S 和 C/S 等多种架构的应用系统的调用需求，有利于密码服务接口产品的开发，有利于应用系统在密码服务过程中的集成和实施，有利于实现各应用系统的互联互通。

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。

该标准适用于公钥密码应用技术体系下密码应用服务产品的开发，密码应用支撑平台的研制及检测，也可用于指导直接使用密码设备和密码服务的应用系统的集成和开发。

(3) 内容概要

该标准主要包括 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 章算法标识和数据结构，规定了标识和数据结构的定义和说明。

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。

第 7 章证书应用综合服务接口函数定义，分别对客户端控件接口函数、服务器端 COM 组件接口函数、JAVA 组件接口函数的每个函数列表进行定义和说明。

该标准附录 A 是规范性附录，给出了证书应用综合服务接口的错误代码定义。

附录 B 为资料性附录，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。

2.3 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

该标准规范了基于角色的授权与访问控制框架的具体实现，遵循这一规范，访问控制系统的开发者能够容易地实现规范的、安全的、与应用无关的、基于角色的访问控制服务，应用开发者能够容易地实现与规范的访问控制系统联接的应用。

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。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。

该标准的总体思路就是使访问控制系统和应用系统能够方便的互联，实现统一的、支持异构环境的授权与访问控制。遵循规范开发的访问控制系统与具体应用系统无关，与应用系统开发商无关，与具体用户无关。只要应用系统同样遵循这一标准，就可以互联。

(3) 内容概要

该标准分为 9 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，由应用开发商实现。即由应用开发商描述应用中的每个具体资源可以由何种角色在何种条件下进行什么操作。

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，由用户单位的权限主管部门（如人力资源部门）实现，给具体的用户分配角色。

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，主要包括权限定义、授权管理、权限获取、访问控制方面的 API 定义，由访问控制产品开发商实现。

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。

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：

——标准中的属性管理系统可以是属性证书系统，也可以是属性数据库等其他形式。

——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。

——对访问控制策略签名后形成的策略证书被加载到访问控制决策部件。对授权信息签名后，访问控制决策部件通过访问控制请求中的发起者查询LDAP，得到授权信息。

——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。

2.4 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，使基础设施能够为应用系统提供标准、权威、可靠的时间戳服务，有利于应用系统的互联互通。

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。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和开发，以及时间戳服务的集成和实施。

(3) 内容概要

该标准分为 9 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的 ASN.1 编码方式。

第 8 章定义了时间戳服务与时间戳服务机构的五种通讯方式，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 章描述了七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。环境函数类中包含初始化环境和清除环境函数，时间戳服务函数类中包含生成时间戳请求、生成时间戳应答、验证时间戳有效性、获取时间戳主要信息、解析时间戳详细信息。并详细描述了各个接口函数，包括各函

数的原型、描述、参数说明、返回值说明及备注等详细信息。

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。

2.5 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

该标准依托 GM/T 0044《SM9 标识密码算法》标准，适用于应用系统中基于 IBC 技术和 SM9 算法进行身份鉴别时涉及到的鉴别需求。参照 GB/T 18794.2-2002《信息技术 开放系统互连开放系统安全框架 第 2 部分鉴别框架》中的协议，根据标识密码技术的特点进行了参数的重新定义。

该标准规定了两种单向身份鉴别要求和一个双向身份鉴别要求。在附录中给出了利用 IBC 技术进行鉴别时需要访问公开参数服务(PPS)的基本流程和相关密码数据结构，用于公开参数和标识状态查询；由于 SM9 密码算法使用、加密消息语法等标准规范尚未发布，为便于实现具体协议内容，还给出了 SM9 算法密钥格式以及签名格式定义。

(3) 内容概要

该标准分为 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 章定义了标识密码中的标识结构。

第 6 章定义了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) 和双向身份鉴别协议, 及其数据格式。

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 算法密钥数据结构和签名加密数据结构。

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

(1) 版本

GB/T 32922-2016《信息安全技术 IPSec VPN 安全接入基本要求与实施指南》是当前的最新版本。

(2) 用途与适用范围

该标准明确了采用 IPSec VPN 技术实现安全接入的场景, 提出了 IPSec VPN 安全接入应用过程中有关网关、客户端以及安全管理等方面的要求, 同时给出了 IPSec VPN 安全接入的实施过程指导。

现有的密码行业标准对 IPSec VPN 的技术协议、产品功能、性能和管理以及检测进行了规定, 该标准则定位于对 IPSec VPN 部署和实施层面的指导。该标准要求遵循 GB/T 36968《信息安全技术 IPSec VPN 技术规范》, GM/T 0023《IPSec VPN 网关产品规范》, GB/T 35291《信息安全技术 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》等密码行业标准, 并在此基础上提出对 IPSec VPN 设备的安全接入要求、安全管理要求和实施指南。

该标准适用于采用 IPSec VPN 技术开展安全接入应用的机构, 指导其进行基于 IPSec VPN 技术开展安全接入平台或系统的需求分析、方案设计、配置实施、测试与备案、运行管理, 也适用于设备厂商参考其进行产品的设计和开发。

(3) 内容概要

该标准提出了利用 IPSec VPN 技术实现安全接入的相关技术要求，同时给出了实施 IPSec VPN 安全接入的过程指导。主要内容包括：IPSec VPN 安全接入应用过程中有关网关、客户端以及安全管理方面的基本要求；基于 IPSec VPN 技术安全接入平台或系统建设过程中的实施指南。

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 章术语和定义，第 4 章缩略语。

第 5 章安全接入场景，描述了 IPSec VPN 安全接入应用的两种场景。

第 6 章安全接入基本要求，从 IPSec VPN 安全接入应用实施的角度，提出 IPSec VPN 网关的功能和性能、IPSec VPN 客户端等的技术要求，以及安全管理要求。

第 7 章实施指南，主要从需求分析、方案设计、配置实施、测试与备案、运行管理等 5 个方面规范基于 IPSec VPN 技术的安全接入平台或系统建设的实施过程。

附录 A 是典型应用案例，描述了政务外网基于 IPSec VPN 的典型应用案例。通过部署 IPSec VPN 安全接入系统，为政务外网用户提供从互联网等公众网络可信接入政务外网的安全隧道，满足不具备专线接入条件的部门接入政务外网和政务用户出差或移动办公的接入需求，延伸政务外网的覆盖范围。

附录 B 是 IPv6 过渡技术。根据实现机制的不同，过渡技术主要包括双栈、隧道技术和翻译技术。在实际应用中，一般会综合考虑网络、用户、业务、升级成本等诸多因素，将三种过渡技术结合使用，

以制定合理的网络过渡解决方案。

七 密码应用类标准

1. 应用要求

1.1 GM/T 0054 信息系统密码应用基本要求

(1) 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。

(2) 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、规范和评估信息系统中的商用密码应用。在网络安全等级保护和关键信息基础设施保护中，该标准是对信息系统中密码技术应用的基线性要求。

(3) 内容概要

该标准共有9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章中主要是从密码算法、密码技术、密码产品、密码服务等四方面提出了总体要求。

第6章提出了用密码技术保障网络和信息系统的机密性、完整性、真实性和不可否认性，是信息系统密码应用的安全保障目标，并给出了具体的密码功能要求。

第7章是标准的主体，重点从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、应用和数据安全四个层面提出了不同级别的密码技术应用要求。以密码技术实施的角度为主线，可灵活扩展至等保四级，并在条款的要求力度上，逐级增强。在控制点和要

求项上，也是逐级增强。

第 8 章明确了不同等级的密钥管理要求。

第 9 章明确了不同等级的安全管理要求。

附录 A 和附录 B 均为资料性附录。

2. 典型应用

2.1 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，例如 Web 系统登录、金融支付等。

一般地，动态口令的客户端/服务端同步机制可分为时间同步和事件同步两种，该标准对于二者均有涉及。

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、密钥管理系统等的内容，适用于动态口令相关产品的研制、生产、使用，以及指导相关产品的检测。

(3) 内容概要

该标准共包括 9 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。

第 5 章介绍了动态口令系统的组成和原理。

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，为动态令牌的产品制造提出了要求。

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。密钥管理系统在动态口令应用中具有关键地位，它负责设定和分发令牌，以及将相应的种子密钥提供给认证系统。

2.2 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

该标准是电子签章产品的技术要求，为电子签章产品的实现方和使用方提供依据和指导，规范了所用的数据结构和密码处理流程，有利于该类产品的标准化和互联互通。

该标准适用于电子签章产品的研发、应用和检测。

(3) 内容概要

该标准共有 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 章中提供了电子签章应用的安全机制。电子签章将传统印章与电子签名技术进行结合，通过采用密码技术、图像技术以及组件技术，以电子形式对电子文档进行数字签名及签章，以图像形式对文档来源的真实性以及文档的完整性进行展示，用以防止用户对电子文档的误用。

第6章中提供了电子签章的密码应用协议，是该标准的主体部分。本章中采用逐层细化的方式定义了电子印章的数据格式，明确了电子印章的验证流程；定义了电子签章的数据格式，明确了电子签章的生成流程和电子签章的验证流程。

该标准使用了ASN.1的形式对数据进行描述。

2.3 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》，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，规定了该标准涵盖的射频识别密码应用系统的范围；同时也规定了射频识别系统密码安全级别及各级别的要求。射频识别系统密码保护安全框架包括射频识别标准体系框架中的电子标签、电子标签和读写器间通信、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等。射频识别系统密码安全级别共分为4级，

从低到高分别对应第一到第四级。划分的依据是根据应用对安全性的需求。各级别的差距主要体现在身份鉴别、访问控制、机密性、完整性、抗抵赖和审计等安全机制的综合运用上。本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技术要求和密码安全要素。其中电子标签芯片和读写器的密码安全要素包括机密性、完整性、抗抵赖、身份鉴别、访问控制、审计记录、密码配置和其他安全措施等方面，读写器和电子标签通信密码安全要素包括身份鉴别、传输信息的机密性、传输信息的完整性等。根据该标准第1部分所规定的射频识别系统密码安全级别，不同的安全级别的密码安全技术要求不同。

该标准第3部分对使用了密码技术的射频识别系统，在电子标签、读写器及通信等部分规定了相关密钥管理要求，其中包括密钥体制、对称密钥管理模型、对称密钥管理通用要求和对称密钥使用通用要求。密钥体制包括对称密钥和非对称密钥。对称密钥管理模型从密钥生命周期来看可以分为密钥生成、密钥分发注入、密钥使用和密钥销毁/注销等步骤。本部分适用于指导射频识别系统密钥管理的设计、实现与应用。

(3) 内容概要

该标准分为3个部分，描述了在一个统一框架下对射频识别系统的芯片、读写器、通信和密钥管理的要求，3个部分相对独立，下面分别对每个部分予以介绍内容。

该标准第1部分共包含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 章主要规定射频识别系统密码安全保护框架、射频识别系统密码应用技术标准框架和安全级别。射频识别系统密码保护安全框架包括射频识别标准体系框架中的电子标签、电子标签和读写器间通信、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等。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等 4 部分。密码应用技术标准框架包含密码协议标准、密码设备标准和基础设施标准等三部分。

第 6 章主要规定安全级别共划分为 4 级，从低到高分别是第一到第四级，划分依据是应用对安全需求的不同。每个级别对安全技术要求不同，主要体现在身份鉴别、访问控制、机密性、完整性、抗抵赖和审计等安全机制的综合运用上。技术要求部分详细规定了身份鉴别等安全机制的不同要求。

第 7 章主要规定要使用国家密码管理部门认可的对称密码、非对称密码和杂凑密码。

本部分附录 A 为资料性附录，即电子标签防伪应用密码安全解决方案，规定典型电子标签防伪应用系统安全架构图、密码防伪应用安全体系，并从电子标签芯片密码安全技术及其实现、电子标签读写器密码安全技术及其实现、电子标签与读写器通信安全技术、密码算法及密码管理等方面阐述解决方案。

该标准第 2 部分共包含 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 章主要规定了电子标签、读写器及二者通信的安全要素。

第7章主要规定根据该标准第1部分所规定的射频识别系统密码安全级别划分，给出了不同的安全级别的电子标签、读写器及通信的密码安全技术要求。

第8章主要规定传输信息的机密性、传输信息的完整性和身份鉴别的实现方式。其中传输信息的机密性主要包括传输密钥和实现方法，传输密钥包括协商密钥模式和固定密钥加密模式，实现方式则采用对称密码算法加密，包括流密码加密和分组密码加密；传输信息的完整性主要规定采用CBC-MAC和HMAC两种方式进行完整性校验和身份认证的具体方法；身份鉴别主要规定唯一标识符鉴别、单向身份鉴别和双向身份鉴别的具体流程，单向身份鉴别包括读写器对电子标签的挑战响应鉴别和电子标签对读写器的挑战响应鉴别，双向身份鉴别包括采用对称密码算法鉴别和采用非对称密码算法鉴别。

本部分附录A为资料性附录，给出了电子标签芯片设计实例。首先规定电子标签分类，然后以防伪类电子标签为例规定功能特性、安全特性、功能框图，并规定数据存储结构、唯一标识符、数据访问控制权限、密码算法、身份鉴别、通信加密、密钥管理和全部指令集等内容。

本部分附录B为资料性附录，给出读写器密码应用安全实例。首先以用于某赛事的电子门票的射频识别系统为例，规定系统框架图、系统描述、安全级别、读写器密码安全需求，并从SAM指令集、密钥管理、访问控制、读写器与电子标签的双向身份鉴别、机密性和完整性等方面进行阐述。

本部分附录C和附录D为资料性附录，附录C“采用对称分组密码算法的双向身份鉴别与流加密应用”规定采用分组密码算法进行读

写器和电子标签间双向身份鉴别的流程和具体实现，并规定了流加密的应用；附录 D “采用非对称密码算法的双向身份鉴别和密钥协商” 规定采用非对称密码算法的双向身份鉴别并同时实现密钥协商的流程和具体实现。

该标准第 3 部分共包含 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 章符号和缩略语。

第 5 章主要规定对称密钥体制和非对称密钥体制。其中对称密钥体制适用于电子标签和读写器间的身份鉴别、访问控制、机密性和完整性的安全保护，根据对称密钥产生方式的不同可以把对称密钥分为根密钥、分散密钥和传输保护密钥；非对称密钥适用于电子标签和读写器间涉及的抗抵赖、身份鉴别、访问控制、机密性和完整性等安全保护。

第 6 章主要规定对称密钥的管理模型，包含了密钥生命周期中的密钥生成、密钥分发、密钥使用和密钥销毁/注销等主要过程。

第 7 章主要规定存储在电子标签/读写器内的对称密钥不能被读出，系统必须有必要的安全保护措施以保障密钥安全，在密钥管理中的各个步骤都要符合国家密码管理主管部门的相关要求。

第 8 章主要规定对称密钥的使用要求，包括身份鉴别、访问控制、机密性、完整性等。其中身份鉴别包括唯一标识符鉴别和挑战响应鉴别；访问控制要求用于访问控制的密钥必须唯一，访问权限不同对应的密钥不同；机密性包括存储加密和传输加密，存储加密要求对自身存储数据的加密密钥应由随机数发生器产生，且安全存储不能被导出。传输加密密钥负责加密传输数据，该密钥可是固定密钥，也可由电子标签和读写器协商产生，通信结束后该密钥相应被丢弃；完整性包括

存储完整性和传输完整性，对密码算法的要求同机密性相关要求。

本部分附录 A 为资料性附录，即射频识别系统的密钥管理示例。从系统的设计要求、密钥管理设计实现等方面规定，其中密钥管理设计实现包括密钥生成、密钥分散、密钥分发和注入、密钥存储、密钥备份、密钥验证、密钥更新与销毁、密钥的使用等流程。

2.4 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的技术要求。

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

该标准共包含 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。应用系统一般由门禁卡、门禁卡读卡器和后台管理系统构成，通过各系统内的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，密钥管理子系统完成生成密钥、初始化密钥模块、向密码模块注入密钥等功能。发卡子系统完成门禁卡初始化、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。密码应用方案应遵循相关密码算法使用要求；密码设备包括应用系统密码模块、密钥管理及发卡系统密码模块，密码设备应具备物理防护能力，并遵循相应密码算法使用要求；密码算法使用必须符合国家密码管理主管部门的要求，密码算法应用方案应遵循相应密码算法使用标准；密码协议是指门禁读卡器或后台管理系统之间的通信，应遵循 GM/T 0035.4；密钥管理包括密钥生成的机密性和随机性，密钥注入要防止明文密钥的泄漏，在保证密钥或敏感数据安全的情况下，密钥才能加载到密码设备中，在密钥生成、注入、更新及存储等过程中应保证密钥不被泄露。

第7章提供了两种密码应用方案，分别是附录A给出的基于国产密码算法SM7的非接触逻辑加密卡方案，附录B给出的基于国产密码算法SM1/SM4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，基于SM7算法的非接触式逻辑加密卡方案包括系统构成、方案原理、密码安全应用流程、密码产品现状、改造内容和方案特点等6个方面，其中密码安全应用流程包括密钥管理及发卡系统、门禁控制等2个流程。

附录B是资料性附录，基于SM1/SM4算法的非接触式IC卡方案包括系统构成、方案原理、密码安全应用流程、改造内容和方案特点等5个方面，其中密码安全应用流程包括密钥管理及发卡系统、门禁控制等2个流程。

2.5 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

该标准不限制具体的文件类型，也不规定特定的应用系统，而是站在通用的角度，对电子文件保护所涉及的密码技术予以规范性描述。

该标准适用于关注文件对象自身安全的相关标准规范和应用，也适用于安全电子文件密码服务中间件的开发和检测，可用于指导使用该中间件的应用系统的开发。

(3) 内容概要

该标准共分为 10 个章节，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 章是安全电子文件密码应用的总体设计，该章阐述了基于安全电子文件密码服务中间件及标签实现的文件安全控制机制，描述了中间件的基本架构、标签的逻辑结构、标签与文件的控制与绑定关系等内容，叙述了中间件响应应用系统密码服务请求的过程以及中间件与基础密码服务和个性密码服务的关系。基于标签的安全电子文件系统的应用系统架构如下图所示：

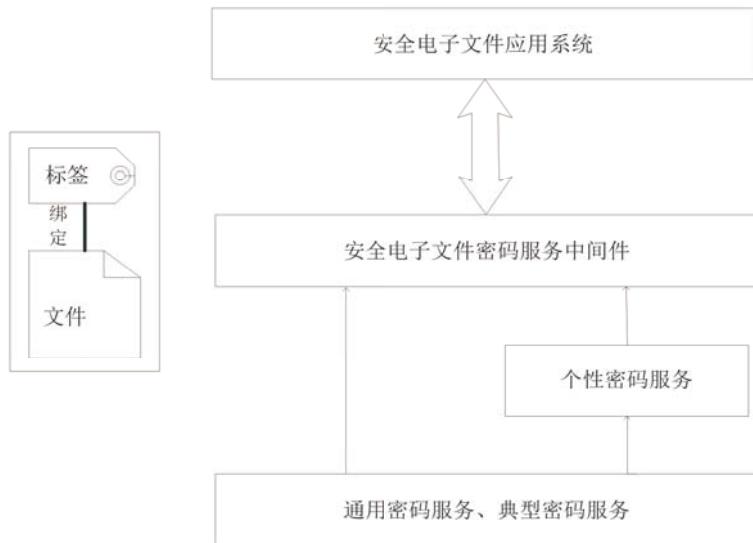


图 3 基于标签的安全电子文件系统的应用系统架构

第 6 章明确了该标准使用的密码算法和密钥对象，中间件通过调用通用密码服务、典型密码服务和个性密码服务来实现对电子文件的密码操作，其中：通用密码服务和典型密码服务由密码基础设施提供，包括加密、解密、签名、验证。个性密码服务包括电子印章服务、数字水印服务、指纹服务，个性密码服务需要的密码服务由密码基础设施提供。

密钥对象为操作者密钥，操作者是对文件进行密码操作的主体。

对标签修改操作仅能由中间件进行，操作者与应用系统都不能直接对标签进行操作。

第 7 章对标签的结构和属性进行了定义。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，并对每项标签属性进行了详细定义。

标签与文件的关联关系分为内联式与外联式两种，内联式将文件嵌入标签体中，组成独立的文件；外联式标签与文件在物理存储上各自独立。

标签与文件的绑定关系是通过计算文件摘要，将该摘要放入标签体中并与标签一起进行完整性签名。

标签通过属性对文件进行控制，其中：权限属性对文件的操作权限进行控制；内容属性对文件的存储地址、文件名、文件大小和文件失效日期等信息进行控制；日志属性对文件的操作行为记录进行控制；扩展属性由应用系统自行定义并使用。

第8章对中间件向应用系统提供的密码服务中的基础密码操作进行定义，基础密码操作包括：标签的完整性与文件绑定关系的建立和验证；文件的对称加密、对称解密、摘要、签名和验证等操作。

第9章定义了向应用系统提供的接口函数，包括函数的接口定义、参数的数据类型、参数的描述、函数的返回值和错误信息等。

该章定义的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、密码操作函数等组合而成，共分为四类八十二个函数。

附录A、B均为资料性附录，分别概要说明了水印和指纹等个性密码服务的原理和总体描述。

八 密码检测类标准

1. 随机性检测

1.1 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准是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

该标准是随机数发生器所产生随机数序列的质量检测规范，用于对所有的随机数发生软硬件产品所产生的随机数进行检测，并判断其质量是否合规。

该标准适用于随机数发生器软硬件产品的生产和检测，或含有随机数发生器单元的密码产品的生产和检测。产品厂商可利用该标准来自测随机数质量是否合规，检测机构利用该标准对送检产品的随机数质量进行检测，检测结果是否符合该标准的要求将作为产品认证的重要依据。

(3) 内容概要

该标准共包含 5 章，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，即二进制随机数序列样本的检测方法，包括其数据格式、样本长度、显著性水平等要求。对于二元序列采用的检测项目共有 15 项，分别为单比特频数检测、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产品的检测过程，包括采样、存储、检测和判定。

该标准的附录 A 为资料性附录，描述了 15 种二元序列检测项目的技术原理。

附录 B 为资料性附录，给出了随机性检测参数设置表。

附录 C 为资料性附录，给出了随机性检测结果分析表。

1.2 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

随机数发生器是指产生随机数的专用集成器件或者器件中的随机数生成部件。该标准将随机数检测划分为五个不同产品形态，对每个产品形态的随机数检测划分为四个不同应用阶段，并对每种产品形态的各应用阶段提出了随机数检测要求。

该标准针对随机数发生器的使用提出检测要求，为使用符合应用与环境安全要求的随机数发生器提供依据，亦可为随机数发生器的研制提供指导，有利于相关检测机构对密码产品的随机数进行规范化检测，以保障密码产品中的随机数的正确可靠使用。

(3) 内容概要

该标准的主要内容有 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 章为随机数检测的有关说明。在本章中，对随机数检测划分为 A 类、B 类、C 类、D 类、E 类五个不同产品形态类别进行说明。对随机数检测划分为送样检测、出厂检测、上电检测、使用检测四个不同应用阶段进行说明。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 章规定了 A 类产品随机数检测要求。在本章中，对 A 类产品的送样检测、出厂检测、上电检测、使用检测（包括周期检测和单次检测）规定了具体的检测要求。检测要求从检测量、检测项目、检测

判断标准三个方面规定。

第 6 章规定了 B 类产品随机数检测要求。在本章中，对 B 类产品的送样检测、出厂检测、上电检测、使用检测（包括周期检测和单次检测）规定了具体的检测要求。检测要求从检测量、检测项目、检测判断标准三个方面规定。

第 7 章规定了 C 类产品随机数检测要求。在本章中，对 C 类产品的送样检测、出厂检测、上电检测、使用检测（包括周期检测和单次检测）规定了具体的检测要求。检测要求从检测量、检测项目、检测判断标准三个方面规定。

第 8 章规定了 D 类产品随机数检测要求。在本章中，对 D 类产品的送样检测、出厂检测、上电检测、使用检测（包括周期检测和单次检测）规定了具体的检测要求。检测要求从检测量、检测项目、检测判断标准三个方面规定。

第 9 章规定了 E 类产品随机数检测要求。在本章中，对 E 类产品的送样检测、出厂检测、上电检测、使用检测（包括周期检测和单次检测）规定了具体的检测要求。检测要求从检测量、检测项目、检测判断标准三个方面规定。

2. 算法与协议检测

2.1 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

三元对等架构是我国自主提出的普适性网络安全技术架构，其核

心技术已被国际标准化组织接纳。该标准的主要目的就是针对基于三元对等架构的密码安全协议提出一套框架性测试要求及方法，为三元对等密码安全协议的设计提供参考，为符合三元对等密码安全性协议的相关产品提供测试依据，提高产品的互操作性。

该标准主要包括密码算法实现的正确性和一致性技术要求及测试方法、协议实现的符合性和互操作性基本技术要求及测试方法。

(3) 内容概要

该标准分为 9 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 章基本技术要求，从密码算法实现的正确性和一致性要求、协议实现的符合性和互操性要求两部分进行介绍。

第 6 章测试环境要求，从测试设备、测试拓扑两方面进行介绍，其中测试拓扑部分会针对被测设备是 REQ、AAC、AS 三种不同情况进行介绍。

第 7 章三元对等密码安全协议测试统一规范，为统一封装数据结构给出定义；涉及字段的细节内容在附录 B 中进行介绍。

第 8 章密码算法实现的正确性和一致性测试方法，涉及对称密码算法、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、随机数等 7 项测试内容。

第 9 章协议实现一致性和互操作性测试方法，涉及端口控制、TAEP 协议封装、TAEPoL 协议封装、TCP/UDP 端口等 4 项测试内容。

附录 A、B、C、D 都是资料性附录，附录 A 说明了 TAEP 协议封装 Request 和 Response 分组格式中 Type 字段的定义；附录 B 说明了三元对等密码安全协议测试统一封装数据元素 ID 定义，以及每个数据

元素的含义解释；附录 C 说明了证书中的设备命名规则；附录 D 给出了测试向量。

2.2 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》和 GB/T 20518《信息安全技术 公钥基础设施 数字证书格式规范》的要求，规定了数字证书的格式和互操作检测要求。

该标准适用于对证书认证系统签发的数字证书的格式进行检测，并检测不同证书认证系统签发的数字证书在具体的证书应用上是否能够互操作。

(3) 内容概要

该标准分为 9 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 章对检测规范中的检测对象进行了描述。

第 6 章对送检的材料清单及要求进行了描述。

第 7 章对检测内容进行了详细描述，包含两大类：一类是入根检测，包含 CA 证书申请功能检测、CA 证书申请文件符合性检测、CA 证书导入功能检测、入根后签发功能检测；另一类是证书互操作检测，包含数字证书格式符合性检测、证书信任链建立检测、CRL 格式符合性检测、证书扩展项符合性检测、签名证书互操作检测、加密证书互操作检测。

第 8 章对检测内容所对应的检测方法进行了详细描述，以便指导

检测人员进行检测。

第 9 章对检测合格的判断依据进行了描述。

3. 产品检测

3.1 功能检测

3.1.1 GM/T 0013 可信密码模块接口符合性测试规范

(1) 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。

(2) 用途与适用范围

该标准用于指导厂商、测评机构、用户等对可信密码模块的规范符合性进行测试。

该标准以 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》和 GM/T 0012《可信计算 可信密码模块接口规范》为基础，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。需要注意，该标准只适用于可信密码模块的符合性测试，不能取代其安全性检测。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。

(3) 内容概要

该标准分为 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，说明了对可信密码模块实施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，说明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，说明了适用于多数可信密码模块的向量命令测试方法。对于多数可信密码模块命令来说，其依赖的命令成功执行之后，可以直接采用测试向量的方式对其进行符合性测试，即给定输入，然后检测其输出是否与规范一致。本章说明了对于此类功能和命令实施符合性测试所需的测试向量，即输入、输出及其对应关系。

第 7 章脚本向量，说明了部分命令所需的较为复杂的测试方法。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。本章说明了对这一类命令进行测试时所使用的脚本，所述脚本以第 6 章中的向量为基础。

3.1.2 GM/T 0037 证书认证系统检测规范

(1) 版本

GM/T 0037-2014《证书认证系统检测规范》是当前的最新版本。

(2) 用途与适用范围

该标准规定了证书认证系统的检测内容与检测方法，适用于在中华人民共和国境内，为电子签名提供电子认证服务，按照 GB/T 25056 研制或建设的证书认证服务运营系统的检测，也可为其它证书认证系统的检测提供参考。

(3) 内容概要

该标准分为 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 章定义了产品和项目两种检测对象。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，按照 GM/T 0034 要求建设的证书认证服务运营系统。需要注意

的是，物理区域、安全管理、多层结构支持、数据备份和恢复、第三方安全产品等项测试内容只适用于项目检测，不适用于产品检测；系统初始化、CA 证书更新等测试内容只适用于产品检测，不适用于项目检测。

第 6 章规定了测试大纲编制的原则。标准中提供的测试大纲只是基本框架，实际编制测试大纲时应对每一项的测试进行细化。

第 7 章确定了产品和项目的检测环境。产品检测环境需要按产品设计要求搭建模拟环境，项目检测环境是证书认证服务运营系统的实际环境。

第 8 章从场地、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、算法等十三项详细规定了检测内容。

第 9 章规定了十三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最低条件。产品检测中网络结构、密码机、系统初始化、证书下载、证书签发、入根、证书格式、算法、协议为关键项，其中任何一项检测不通过即判定为不合格。项目检测中物理区域、网络结构、密码机、证书下载、证书签发、入根、证书格式、证书链、算法、协议为关键项，其中任何一项检测不通过即判定为不合格。规范中 CRL 签发和证书状态查询为组合关键项，其检测结果均不通过即判定为不合格。除上述项外，其它项累计 5 项不符合相应检测要求的，即判定为不合格。

附录 A 是资料性附录，提供了可供参考的测试大纲的示例。

附录 B 和附录 C 是资料性附录，提供了证书认证系统网络结构、证书认证系统机房布局及设备位置摆放的示例，供国内 PKI 厂商和运

营商参考。

3.1.3 GM/T 0038 证书认证密钥管理系统检测规范

(1) 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。

(2) 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，适用于在中华人民共和国境内，为电子签名提供电子认证服务，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，也可为其它证书认证密钥管理系统的检测提供参考。

(3) 内容概要

该标准分为9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章定义了产品和项目两种检测对象。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，按照GB/T 25056第9章要求建设的证书认证密钥管理系统。需要注意，物理区域、安全管理、数据备份和恢复、第三方安全产品等项测试内容只适用于项目检测，不适用于产品检测；系统初始化、支持多个CA等项测试内容只适用于产品检测，不适用于项目检测。

第5章规定了测试大纲编制的原则。标准中提供的测试大纲只是基本框架，实际编制测试大纲时应对每一项的测试进行细化。

第6章确定了产品和项目的检测环境。产品检测环境需要按产品设计要求搭建模拟环境，项目检测环境是证书认证密钥管理运营系统的实际环境。

第7章从场地、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、第三方安全产品等九项详细规定了检测内容。

第8章规定了九项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最低条件。产品检测中网络结构、密码机、系统初始化、密钥生成、密钥恢复为关键项，其中任何一项检测不通过即判定为不合格。项目检测中物理区域、网络结构、密码机、密钥生成、密钥恢复为关键项，其中任何一项检测不通过即判定为不合格。除上述项外，其它项累计3项不符合相应检测要求的，即判定为不合格。

附录A是资料性附录，提供了可供参考的测试大纲的示例。

附录B和附录C是资料性附录，提供了密钥管理系统网络结构、密钥管理系统机房布局及设备位置摆放的示例，供国内PKI厂商和运营商参考。

3.1.4 GM/T 0040 射频识别标签模块密码检测准则

(1) 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。

(2) 用途和适用范围

该标准是针对射频识别标签模块密码安全和服务功能的检测，对RFID的空口不做约束。

该标准适用范围包括但不限于：

- 采用 IS014443 协议和 SM7 密码算法的高频 RFID 标签模块；
- 采用 IS015693 协议和 SM7 密码算法的高频 RFID 标签模块；
- 采用 GB/T 29768 协议和 SM7 密码算法的超高频 RFID 标签模块；
- 采用 GB/T 28925 协议的微波 RFID 标签模块。

(3) 内容概要

该标准共包含 6 个章节，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，其中 II-B 类支持传输的机密性和完整性。

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。一般要求规定检测按照 GB/T 37033.1、GB/T 37033.2 和该标准开展，标签模块应明确声明产品类型及密码功能，且各项密码功能正确有效；密码算法包括算法实现正确性和随机数测试，分别规定了 I 类和 II 类模块的具体检测方案和判定准则；密码服务包括身份鉴别测试、数据传输机密性测试、数据存储机密性测试、数据传输完整性测试、数据存储完整性测试，分别规定了 I 类和 II 类模块的具体检测方案和判定准则；密码性能包括鉴别性能测试和数据交互性能测试，分别规定了 I 类和 II 类模块的具体检测方案和判定准则；敏感信息保护包括口令保护测试和敏感信息保护测试，分别

规定了 I 类和 II 类模块的具体检测方案和判定准则；抗抵赖包括抗原发抵赖测试，分别规定了 I 类和 II 类模块的具体检测方案和判定准则；生命周期安全包括标签模块灭活测试、防非法指令测试、防初始使用权欺骗测试和防生命周期越界测试，分别规定了 I 类和 II 类模块的具体检测方案和判定准则；审计包括标签模块唯一标识测试，分别规定了 I 类和 II 类模块的具体检测方案和判定准则；密码管理包括密钥生成、密钥存储、密钥使用、密钥更新、密钥导入和密钥清除，分别规定了 I 类和 II 类模块的具体检测方案和判定准则；开发环境保障包括文档管理、开发环境安全、隐蔽通道声明、人员管理和源文件管理，分别规定了 I 类和 II 类模块的具体检测方案和判定准则。

附录 A 为规范性附录，提供了“射频识别标签模块密码检测项”表格，列举了不同种类的射频识别标签模块需检测的内容。

3.1.5 GM/T 0041 智能 IC 卡密码检测规范

(1) 版本

GM/T 0041-2015《智能 IC 卡密码检测规范》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。

(3) 内容概要

该标准分为 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章检测项目包含7个部分：COS安全管理功能检测、COS安全机制检测、密钥的素性检测、随机数质量检测、密码算法实现正确性检测、密码算法实现性能检测和设备安全性测试。

第6章检测方法分别针对上一章节涉及到的检测项目进行详细说明，明确检测步骤和方法。

第7章合格性判定准则对测试结果的合规性进行了补充说明。

3.1.6 GM/T 0046 金融数据密码机检测规范

(1) 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。

(2) 用途与适用范围

该标准是对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等进行了规范，规定了检测项目、检测方法，以及产品是否合格的判定标准等方面的内容。

该标准指导各生产厂商研发具有统一产品规范的金融数据密码机，提升金融数据密码机产品的安全性和产品质量，保证配备金融数据密码机的用户信息系统的安全稳定运行；同时也为用户选择金融数据密码机提供测评的标准和依据。

该标准适用于金融数据密码机的研发、应用和检测。

(3) 内容概要

该标准分为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章详细规定了金融数据密码机检测环境的配置。

第6章说明了金融数据密码机的检测内容及检测方法。检测内容包括外观和结构、文档、功能、性能、环境适应性和稳定性检测等。

功能检测主要包括初始化、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、数据报文接口等内容；性能检测主要包括 PIN 加密、PIN 转加密、MAC 计算、ARQC 验证、对称密码算法加解密、非对称密码算法加解密、数据杂凑算法、随机数产生、非对称密钥生成、非对称算法签名和验签等测试内容。

第 7 章说明了必须具备的送检文档资料。

第 8 章描述了测试结果合格判定条件。

附录 A 为规范性附录，以表格的方式描述了各测试项目。具体项目包括：外观和结构测试、初始化检测、密码运算检测、密钥管理检测、随机数检测、访问控制检测、设备管理检测、日志审计检测、设备自检检测、数据报文接口（API）检测、性能检测、设备安全性测试、环境适应性检测、可靠性检测。

3.1.7 GM/T 0047 安全电子签章密码检测规范

(1) 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。

(2) 用途与适用范围

该标准规范了按照 GM/T 0031《安全电子签章密码技术规范》研制的安全电子签章的密码检测内容、检测要求、检测方法以及合格判定准则。该标准的制定将会促进安全电子签章提供商开发满足 GM/T 0031 标准的产品，有利于相关检测机构对该类产品的规范化检测。

该标准适用于按照 GM/T 0031 研制的安全电子签章系统密码技术的检测。

(3) 内容概要

该标准共分为 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 章描述了检测对象，以及数字签名算法检测、电子印章数据检测、电子印章验证检测、电子签章数据检测、电子签章验证检测等五个方面检测内容的要求。

第 6 章围绕数字签名算法检测、电子印章数据检测、电子印章验证检测、电子签章数据检测、电子签章验证检测等五个方面检测内容，规范了检测方法与步骤。

第 7 章为送检技术文档要求。

第 8 章明确了检测结果的合格判定要求。

3.1.8 GM/T 0048 智能密码钥匙密码检测规范

(1) 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。

(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，详细描述了智能密码钥匙的检测环境、检测内容和检测方法等有关内容。

该标准适用于智能密码钥匙密码检测，也可用于指导智能密码钥匙的研制和使用。

该标准的制定将会促进智能密码钥匙提供商开发满足 GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》、GM/T 0017《智能密码钥匙密码应用接口数据格式规范》和 GM/T 0027《智能密码钥匙技术规范》标准的产品，有利于相关检测机构对该类产品的规范化检测。

(3) 内容概要

该标准共分为 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 章规定了智能密码钥匙产品的检测环境，包括检测环境拓扑图、检测仪器和检测软件的要求。

第 6 章规定了智能密码钥匙产品的检测内容，包括功能检测、性能检测和安全性检测内容的要求。

第 7 章规定了智能密码钥匙产品的检测方法，包括功能检测、性能检测和安全性检测方法的要求。

3.1.9 GM/T 0049 密码键盘密码检测规范

(1) 版本

GM/T 0049-2016《密码键盘密码检测规范》是当前的最新版本。

(2) 用途与适用范围

密码键盘是金融终端产品（例如 POS、ATM 等）的关键密码部件。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。

该标准是针对采用国家自主的商用密码算法而制定的密码键盘检测标准，目的是保证商用密码算法的安全性和密钥的安全性，以保障我国自主的商用密码算法能够安全顺利的在密码键盘行业中应用。

(3) 内容概要

该标准的主要内容有 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 章规定了密码键盘按安全能力划分为依次递增的 4 个安全等级。其中安全 1 级最低，安全 4 级最高。

第6章规定了检测内容及检测方法，根据产品的安全管理功能、密码算法、密钥素性、随机数质量、环境失效保护、密码算法稳定性、算法性能、设备安全性和安全要求等项开展检测。检测须先通过基本检测项目的检测，并通过安全机制相应项目的检测，才能得出安全等级的最终结论。

第7章给出了合格判定条件。

3.1.10 GM/T 0059 服务器密码机检测规范

(1) 版本

GM/T 0059-2018《服务器密码机检测规范》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。通过该标准检测的服务器密码机，符合产品标准，能够为应用提供规范的基础密码服务。

该标准的制定将会促进各服务器密码机生产厂商形成统一的产品标准，有利于主管部门对服务器密码机的管理，以及相关检测机构对该类产品的规范化检测，有利于各厂家产品之间的互联互通，实现行业范围内多家服务器密码机提供商的市场竞争格局。

(3) 内容概要

该标准的主要内容有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章中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，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、网络适应性等方面检测方法和内容。

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。

3.1.11 GM/T 0060 签名验签服务器检测规范

(1) 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。

(2) 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。

(3) 内容概要

该标准共 7 个章节，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，并分别给予了网络部署示意图。

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。

第 7 章送检技术文档要求，规定了提交检测前需要准备的技术文档。

附录 A 测试项目列表，是规范性附录，为检测实施人提供了记录

项参考。

3.1.12 GM/T 0061 动态口令密码应用检测规范

(1) 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。

(2) 用途与适用范围

动态口令是一种多因素身份鉴别技术，在金融等领域得到广泛应用。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及安全功能检测。

该标准是针对采用国家自主的商用密码算法的动态口令系统而制定的密码应用检测标准，目的是保证实现商用密码算法的安全性、正确性，保证动态口令系统使用的密钥的安全性，保障我国自主的商用密码算法能够安全顺利的在产业中应用。

(3) 内容概要

该标准的主要内容有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章为检测内容和检测方法。根据动态口令系统的构成从动态口令生成算法、动态令牌、动态令牌认证、密钥管理四个部分展开，每一部分又包含若干个检测项目。每个检测项目由检测目的、检测条件、检测方法和流程以及合格性判定条件组成。

第6章为送检技术文档要求。

3.1.13 GM/T 0063 智能密码钥匙密码应用接口检测规范

(1) 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。

(2) 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。

(3) 内容概要

该标准的主要内容有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章为送检材料说明，列出了送检厂商检测时应提交的文档资料。

第6至第8章为规范的关键章节，详细规定了智能密码钥匙密码应用接口的检测环境、检测内容和检测方法。根据产品使用的实际情况按照以下内容进行检测：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。

3.1.14 GM/T 0064 限域通信(RCC)密码检测要求

(1) 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。

(2) 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。为了保证 RCC 产品使用的密码算法的正确有效及安全性，保障国产商用密码算法能够得到安全合规的应用，该标准针对采用密码技术的限域通信（RCC）产品，规定了其密码和安全方面的检测内容及要求。RCC 产品的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。

（3）内容概要

该标准包括 6 章正文，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 RCC 产品的分类，RCC 密码检测对象包括：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 章规定了 RCC 产品的具体检测内容及要求，针对每个检测项目提出检测要求以及合格判定准则。本章确定的主要检测内容包括：密码算法（随机数、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 为资料性附录。本附录针对 RCC 发起方产品和 RCC 响应方产品，分别给出了相应的参考测试系统。附录 A 还给出了 RCC 测试环境参考要求。

附录 B 为资料性附录。本附录给出了基于 RCC 产品的应用密钥管理方面的参考要求，以及 RCC 开发安全保障方面的参考要求。

3.2 安全检测

3.2.1 GM/T 0008 安全芯片密码检测准则

(1) 版本

GM/T 0008-2012《安全芯片密码检测准则》是当前的最新版本。

(2) 用途与适用范围

该标准中的安全芯片是指实现了一种或多种密码算法，直接或间接地使用密码技术来保护密钥和敏感信息的集成电路芯片。

该标准在密码算法、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证等九个部分考察安全芯片的安全能力，对每个部分的安全能力划分为安全性依次递增的三个安全等级，并对每个安全等级提出了安全性要求。安全芯片的安全等级定为该安全芯片所具有的各部分的安全能力的最低安全等级。

该标准可以为选择满足应用与环境安全要求的适用安全等级的安全芯片提供依据，亦可为安全芯片的研制提供指导。

(3) 内容概要

该标准共分为 13 个章节，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 章安全等级的划分，介绍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合。

第 5 章至第 13 章对安全芯片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证提出了具体的安全性要求。

3.2.2 GM/T 0039 密码模块安全检测要求

(1) 版本

GM/T 0039-2015《密码模块安全检测要求》是当前的最新版本。

(2) 用途与适用范围

该标准旨在描述可供检测机构检测密码模块是否符合GM/T 0028《密码模块安全技术要求》的一系列方法。这些方法是为了保证在检测过程中的客观性，并确保各检测机构测试结果的一致性。

该标准可为送检单位提供依据，用来判定密码模块是否符合GB/T 37092-2018《信息安全技术 密码模块安全要求》。

(3) 内容概要

该标准分为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章为规范的文档结构介绍，对第6章安全检测要求的描述方法和思路进行了总体介绍。

第6章为规范的安全检测要求，从不同领域详细描述了遵循该标准的密码模块应满足的安全要求和对应的检测要求。这些安全要求和检测要求涵盖了密码模块设计与实现的各个领域，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。

该标准的附录A到附录F为规范性附录，附录G为资料性附录。各附录分别对文档要求，密码模块安全策略，核准的安全功能，核准的敏感安全参数生成和建立方法，核准的鉴别机制，非入侵式攻击及

常用的缓解方法，不同检测要求的安全等级对应表等几个方面进行了补充介绍和说明。

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。

九 密码管理类标准

截止 2018 年 12 月，此类标准空缺。

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	20
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	21
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	49
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	11
6.	GB/T 32915 信息安全技术 二元序列随机性检测方法	72
7.	GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法	12
8.	GB/T 32922 信息安全技术 IPSec VPN 安全接入基本要求与实施指南	57
9.	GB/T 33133 信息安全技术 祖冲之序列密码算法	9
10.	GB/T 33560 信息安全技术 密码应用标识规范	7
11.	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
12.	GB/T 35276 信息安全技术 SM2 密码算法使用规范	16
13.	GB/T 35291 信息安全技术 智能密码钥匙应用接口规范	27
14.	GB/T 36322 信息安全技术 密码设备应用接口规范	28
15.	GB/T 36968 信息安全技术 IPSec VPN 技术规范	37
16.	GB/T 37033 信息安全技术 射频识别系统密码应用技术要求	63
17.	GB/T 37092 信息安全技术 密码模块安全要求	23

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	9
2.	GM/T 0002 SM4 分组密码算法	11
3.	GM/T 0003 SM2 椭圆曲线公钥密码算法	12
4.	GM/T 0004 SM3 密码杂凑算法	15
5.	GM/T 0005 随机性检测规范	72
6.	GM/T 0006 密码应用标识规范	7
7.	GM/T 0008 安全芯片密码检测准则	95
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范	17
10.	GM/T 0011 可信计算 可信密码支撑平台功能与接口规范	49
11.	GM/T 0012 可信计算 可信密码模块接口规范	25
12.	GM/T 0013 可信密码模块接口符合性测试规范	78
13.	GM/T 0014 数字证书认证系统密码协议规范	18
14.	GM/T 0015 基于 SM2 密码算法的数字证书格式规范	20
15.	GM/T 0016 智能密码钥匙密码应用接口规范	27
16.	GM/T 0017 智能密码钥匙密码应用接口数据格式规范	32
17.	GM/T 0018 密码设备应用接口规范	28
18.	GM/T 0019 通用密码服务接口规范	48
19.	GM/T 0020 证书应用综合服务接口规范	51
20.	GM/T 0021 动态口令密码应用技术规范	61
21.	GM/T 0022 IPsec VPN 技术规范	37
22.	GM/T 0023 IPsec VPN 网关产品规范	44

序号	标准名称	页码
23.	GM/T 0024 SSL VPN 技术规范	38
24.	GM/T 0025 SSL VPN 网关产品规范	46
25.	GM/T 0026 安全认证网关产品规范	46
26.	GM/T 0027 智能密码钥匙技术规范	39
27.	GM/T 0028 密码模块安全技术要求	23
28.	GM/T 0029 签名验签服务器技术规范	40
29.	GM/T 0030 服务器密码机技术规范	42
30.	GM/T 0031 安全电子签章密码技术规范	62
31.	GM/T 0032 基于角色的授权管理与访问控制技术规范	52
32.	GM/T 0033 时间戳接口规范	54
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	21
34.	GM/T 0035 射频识别系统密码应用技术要求	63
35.	GM/T 0036 采用非接触卡的门禁系统密码应用技术指南	68
36.	GM/T 0037 证书认证系统检测规范	79
37.	GM/T 0038 证书认证密钥管理系统检测规范	81
38.	GM/T 0039 密码模块安全检测要求	95
39.	GM/T 0040 射频识别标签模块密码检测准则	82
40.	GM/T 0041 智能 IC 卡密码检测规范	84
41.	GM/T 0042 三元对等密码安全协议测试规范	75
42.	GM/T 0043 数字证书互操作检测规范	77
43.	GM/T 0044 SM9 标识密码算法	13
44.	GM/T 0045 金融数据密码机技术规范	43

序号	标准名称	页码
45.	GM/T 0046 金融数据密码机检测规范	85
46.	GM/T 0047 安全电子签章密码检测规范	86
47.	GM/T 0048 智能密码钥匙密码检测规范	87
48.	GM/T 0049 密码键盘密码检测规范	88
49.	GM/T 0050 密码设备管理 设备管理技术规范	33
50.	GM/T 0051 密码设备管理 对称密钥管理技术规范	34
51.	GM/T 0052 密码设备管理 VPN 设备监察管理规范	35
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	36
53.	GM/T 0054 信息系统密码应用基本要求	60
54.	GM/T 0055 电子文件密码应用技术规范	70
55.	GM/T 0056 多应用载体密码应用接口规范	29
56.	GM/T 0057 基于 IBC 技术的身份鉴别规范	56
57.	GM/T 0058 可信计算 TCM 服务模块接口规范	30
58.	GM/T 0059 服务器密码机检测规范	89
59.	GM/T 0060 签名验签服务器检测规范	90
60.	GM/T 0061 动态口令密码应用检测规范	91
61.	GM/T 0062 密码产品随机数检测要求	74
62.	GM/T 0063 智能密码钥匙密码应用接口检测规范	91
63.	GM/T 0064 限域通信(RCC)密码检测要求	92
64.	GM/Z 4001 密码术语	7

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范》。

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。