# 表《商用密码产品认证目录》（第一批） 2020

为贯彻落实《中华人民共和国密码法》,建立完善商用密码产品认证体系,根据《国家密码管理局市场监管总局关于调整商用密码产品管理方式的公告》(国家密码管理局市场监管总局公告第39号)、《市场监管总局国家密码管理局关于开展商用密码检测认证工作的实施意见》(国市监认证〔2020〕50号),现对《商用密码产品认证目录(第一批)》《商用密码产品认证规则》予以发布,自发布之日起实施。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品种类** | **产品描述** | **认证依据** | **检测机构** |
| 1 | 智能密码钥匙 | 实现密码运算、密钥管理功能的终端密码设备，一般使用USB接口形态。 | GM/T 0027《智能密码钥匙技术规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 2 | 智能IC卡 | 智能IC卡：实现密码运算和密钥管理功能的含CPU（中央处理器）的集成电路卡，包括应用于金融等行业领域的智能IC卡。 | GM/T 0041《智能IC卡密码检测规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 3 | POS密码应用系统  ATM密码应用系统  多功能密码应用互联网终端 | 为金融终端设备提供密码服务的密码应用系统。 | GM/T 0028《密码模块安全技术要求》  JR/T 0025-2018《中国金融集成电路（IC）卡规范第7部分：借记贷记应用安全规范》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 4 | PCI-E/PCI密码卡 | 具有密码运算功能和自身安全保护功能的PCI硬件板卡设备。 | 《PCI 密码卡技术规范》  GM/T 0018《密码设备应用接口规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 5 | IPSec VPN产品/安全网关 | 基于IPSec协议，在通信网络中构建安全通道的设备。 | IPSec VPN产品：  GM/T 0022《IPSec VPN技术规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| IPSec VPN安全网关：  GM/T 0023《IPSec VPN 网关产品规范》  GM/T 0028《密码模块安全技术要求》 |
| 6 | SSL VPN产品/安全网关 | SSL VPN产品/安全网关：基于SSL/TLS协议，在通信网络中构建安全通道的设备。 | SSL VPN产品:  GM/T 0024《SSL VPN技术规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| SSL VPN安全网关:  GM/T 0025《SSL VPN 网关产品规范》  GM/T 0028《密码模块安全技术要求》 |
| 7 | 安全认证网关 | 采用数字证书为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服务的设备。 | GM/T 0026《安全认证网关产品规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 8 | 密码键盘 | 用于保护PIN输入安全并对PIN进行加密的独立式密码模块。包括POS主机等设备的外接加密密码键盘和无人值守（自助）终端的加密PIN键盘。 | GM/T 0049《密码键盘密码检测规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司、 |
| 9 | 金融数据密码机 | 用于确保金融数据安全，并符合金融磁条卡、IC卡业务特点的，主要实现PIN加密、PIN转加密、MAC产生和校验、数据加解密、签名验证以及密钥管理等密码服务功能的密码设备。 | GM/T 0045《金融数据密码机技术规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司 |
| 10 | 服务器密码机 | 服务器密码机：能独立或并行为多个应用实体提供密码运算、密钥管理等功能的设备。 | GM/T 0030《服务器密码机技术规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 11 | 签名验签服务器 | 用于服务端的，为应用实体提供基于PKI体系和数字证书的数字签名、验证签名等运算功能的服务器。 | GM/T 0029《签名验签服务器技术规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 12 | 时间戳服务器 | 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设备。 | GM/T 0033《时间戳接口规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司  智巡密码（上海）检测技术有限公司  豪符密码检测技术（成都）有限责任公司 |
| 13 | 安全门禁系统 | 采用密码技术，确定用户身份和用户权限的门禁控制系统。 | GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司 |
| 14 | 动态令牌  动态令牌认证系统 | 动态令牌：生成并显示动态口令的载体。  动态令牌认证系统：对动态口令进行认证，对动态令牌进行管理的系统。 | 动态令牌：  GM/T 0021《动态口令密码应用技术规范》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司 |
| 动态令牌认证系统：  GM/T 0021《动态口令密码应用技术规范》 |
| 15 | 安全电子签章系统 | 提供电子印章管理、电子签章/验章等功能的密码应用系统。 | GM/T 0031《安全电子签章密码技术规范》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司 |
| 16 | 电子文件密码应用系统 | 在电子文件创建、修改、授权、阅读、签批、盖章、打印、添加水印、流转、存档和销毁等操作中提供密码运算、密钥管理等功能的应用系统。 | GM/T 0055《电子文件密码应用技术规范》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司 |
| 17 | 可信计算密码支撑平台 | 可信计算密码支撑平台：采取密码技术，为可信计算平台自身的完整性、身份可信性和数据安全性提供密码支持。其产品形态主要表现为可信密码模块和可信密码服务模块。 | GM/T 0011《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》  GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司 |
| 18 | 证书认证系统  证书认证密钥管理系统 | 证书认证系统：对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。  证书认证密钥管理系统：对生命周期内的加密证书密钥对进行全过程管理的系统。 | 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》 | 国家密码管理局商用密码检测中心 |
| 19 | 对称密钥管理产品 | 为密码应用系统生产、分发和管理对称密钥的系统及设备。 | GM/T 0051《密码设备管理对称密钥管理技术规范》 | 国家密码管理局商用密码检测中心 |
| 20 | 安全芯片 | 含密码算法、安全功能，可实现密钥管理机制的集成电路芯片。 | GM/T 0008《安全芯片密码检测准则》 | 国家密码管理局商用密码检测中心 |
| 21 | 电子标签芯片 | 采用密码技术，载有与预期应用相关的电子识别信息，用于射频识别的芯片。 | GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》 | 国家密码管理局商用密码检测中心  鼎铉商用密码测评技术（深圳）有限公司 |
| 22 | 其他密码模块 | 实现密码运算、密钥管理等安全功能的软件、硬件、固件及其组合，包括软件密码模块、硬件密码模块等。 | GM/T 0028《密码模块安全技术要求》 | 国家密码管理局商用密码检测中心 |

注：1.上述产品中的密码算法应为符合GM/T 0001《祖冲之序列密码算法》、GM/T 0002《SM4分组密码算法》、GM/T 0003《SM2椭圆曲线公钥密码算法》、GM/T 0004《SM3密码杂凑算法》、GM/T 0009《SM2密码算法使用规范》、GM/T 0010《SM2密码算法加密签名消息语法规范》、GM/T 0004《SM9标识密码算法》等国家密码管理要求的密码算法。

2.上述产品的随机数检测应遵循GM/T 0005《随机性检测规范》、GM/T 0062《密码产品随机数检测要求》。

3.上述标准如未特别注明年代号，原则上应执行其最新版本（包括所有的修改单）。

# 表《商用密码产品认证目录》（第二批）2022

《国家市场监督管理总局国家密码管理局关于发布〈商用密码产品认证目录（第二批）〉的公告》（国家市场监督管理总局、国家密码管理局公告2022年第24号）

