商用密码产品认证目录（第二批）

| **序号** | **产品种类** | **产品描述** | **认证依据** |
| --- | --- | --- | --- |
| 1 | 可信密码模块 | 可信计算密码支撑平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。 | GM/T 0012《可信计算可信密码模块接口规范》  GM/T 0028《密码模块安全技术要求》 |
| 2 | 智能IC卡密钥管理系统 | 针对智能IC卡应用所需的密钥生命周期统一管理系统，为使用密钥的智能IC卡相关业务系统提供密钥服务功能。 | GM/T 0107《智能IC卡密钥管理系统基本技术要求》 |
| 3 | 云服务器密码机 | 在云计算环境下，采用虚拟化技术，以网络形式，为多个租户的应用系统提供密码服务的服务器密码机。 | GM/T 0104《云服务器密码机技术规范》  GM/T 0028《密码模块安全技术要求》 |
| 4 | 随机数发生器 | 软件随机数发生器：产生随机二元序列的程序。  硬件随机数发生器：产生随机二元序列的器件。 | 软件随机数发生器：  GM/T 0103《随机数发生器总体框架》  GM/T 0105《软件随机数发生器设计指南》  GM/T 0028《密码模块安全技术要求》 |
| 硬件随机数发生器：  GM/T 0078《密码随机数生成模块设计指南》  GM/T 0103《随机数发生器总体框架》  GM/T 0028《密码模块安全技术要求》 |
| 5 | 区块链密码模块 | 以区块链技术为核心，用于用户安全、共识安全、账本保护、对等网络安全、计算和存储安全、隐私保护、身份认证和管理等的密码模块。 | GM/T 0111 《区块链密码应用技术要求》  GM/T 0028《密码模块安全技术要求》 |
| 6 | 安全浏览器密码模块 | 具有浏览器内核、浏览器界面、密码算法/传输层密码协议逻辑运算模块等组成的浏览器密码模块。 | GM/T 0087《浏览器密码应用接口规范》  GM/T 0028《密码模块安全技术要求》  GB/T 38636《信息安全技术传输层密码协议（TLCP）》 |