ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0102—2020

密码设备应用接口符合性检测规范

Cryptographic device application interface test specification

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：卫士通信息产业股份有限公司、四川大学、深圳文鼎创数据科技有限公司、山东大学、格尔软件股份有限公司、国家密码管理局商用密码检测中心、山东得安信息技术有限公司。

本文件主要起草人：罗俊、龚勋、胡显荃、刘伟丰、孔凡玉、郑强、罗鹏、马洪富。

密码设备应用接口符合性检测规范

1 范围

本文件规定了GB/T 36322—2018的符合性检测要求和检测方法。

本文件适用于按照GB/T 36322—2018实现的密码设备应用接口的检测，也可用于指导基于该接口规范的密码设备、模块、固件和软件产品的研制和应用开发。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

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

GB/T 33560 信息安全技术 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

GB/T 36322—2018 信息安全技术 密码设备应用接口规范

GB/T 36968 信息安全技术 IPSec VPN技术规范

GM/T 0024 SSL VPN技术规范

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013和GB/T 36322—2018界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

API 应用程序接口(Application Program Interface)

ECB (分组密码的)电子密本(工作方式)(Electronic Codebook)

ECC 椭圆曲线算法(Elliptic Curve Cryptography)

EPK 外部加密公钥(External Public Key)

IPK 内部加密公钥(Internal Public Key)

ISK 内部加密私钥(Internal PrⅣate Key)

KEK 密钥加密密钥(Key Encrypt Key)

注：本文件中的ECC专指SM2算法。