ICS 35.040
L 80
备案号:38311—2013

GM

中华人民共和国密码行业标准

GM/T 0013—2012

可信计算　可信密码模块接口符合性测试规范

Trusted computing—Trusted cryptography module interface compliance

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　　发布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准起草单位：中国科学院软件研究所、国民技术股份有限公司、联想控股有限公司、同方股份有限公司、北京信息科技大学。

本标准主要起草人：秦宇、吴秋新、常德显、初晓博、徐震、刘鑫、宁晓魁、郑必可、刘韧、李昊、张倩颖、汪丹、刘孜文、于爱民。

引　言

为了推动我国可信计算技术的发展，GM/T 0012—2012《可信计算　可信密码模块接口规范》和GM/T 0011—2012《可信计算　可信密码支撑平台功能与接口规范》用于指导我国相关可信计算产品开发和应用。然而，不同厂商生产的产品规格和技术指标可能有所差别，因此必须对相关产品进行完整的符合性测试，以保证产品之间的兼容性。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

可信计算　可信密码模块接口符合性测试规范

1　范围

本标准以 GM/T 0011—2012《可信计算　可信密码支撑平台功能与接口规范》为基础，定义了可信密码模块的命令测试向量，并提供有效的测试方法与灵活的测试脚本。

本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查。可信密码模块的安全性检测需要按照其他相关规范来进行。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 5271.8—2001　信息技术　词汇　第8部分：安全

GB/T 16264.8—2005　信息技术　开放系统互连　目录　第8部分：公钥和属性证书框架

GB 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 18336(所有部分)　信息技术　安全技术　信息技术安全性评估准则

GM/T 0002—2012　SM4 分组密码算法

GM/T 0003—2012(所有部分)　SM2 椭圆曲线公钥密码算法

GM/T 0004—2012　SM3 密码杂凑算法

GM/T 0011—2012　可信计算　可信密码支撑平台功能与接口规范

GM/T 0012—2012　可信计算　可信密码模块接口规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

可信计算平台　trusted computing platform

构建在计算系统中，用于实现可信计算功能的支撑系统。

3.2

可信密码模块　trusted cryptography module；TCM

可信计算平台的硬件模块，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。

3.3

平台配置寄存器　platform configuration register；PCR

可信密码模块内部用于存储平台完整性度量值的存储单元。

3.4

TCM 背书密钥　TCM endorsement key；EK

可信密码模块的初始密钥。