ICS 35.040
L 80
备案号:38310—2013

GM

中华人民共和国密码行业标准

GM/T 0012—2012

可信计算　可信密码模块接口规范

Trusted computing——Interface specification of trusted cryptography module

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　　发 布

中华人民共和国密码
行业标准
可信计算　可信密码模块接口规范
GM/T 0012—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址:www.gb168.cn
服务热线:010-68522006
2013年1月第一版
*
书号:155066·2-24380

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：联想控股有限公司、国民技术股份有限公司、同方股份有限公司、中国科学院软件所、北京兆日技术有限责任公司、瑞达信息安全产业股份有限公司、长春吉大正元信息技术股份有限公司、方正科技集团股份有限公司、北京信息科技大学、中国长城计算机深圳股份有限公司、成都卫士通信息产业股份有限公司、无锡江南信息安全工程技术中心、中国人民解放军国防科学技术大学。

本标准主要起草人：吴秋新、杨贤伟、范琴、邹浩、余发江、宁晓魁、王梓、郑必可、林洋、李伟平、尹洪兵、徐震、严飞、刘韧、李丰、许勇、贾兵、王蕾、顾健、何长龙、秦宇、刘鑫、王正鹏。

引　言

本标准描述了可信计算可信密码模块接口规范，用以指导可信密码模块的产品开发和应用。

本标准凡涉及密码算法相关内容，按照国家有关规定实施。

可信计算　可信密码模块接口规范

1　范围

本标准描述可信计算可信密码模块接口规范，详细定义了可信密码模块的功能及命令函数接口。

本标准适用于可信密码模块相关产品的研制、生产、测评与应用开发。

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　信息系统　词汇　第8部分：安全(GB/T 5271.8—2001，idt ISO/IEC 2382-8：1998)

GM/T 0002　SM4分组密码算法

GM/T 0003(所有部分)　SM2椭圆曲线公钥密码算法

GM/T 0004　SM3密码杂凑算法

GM/T 0005　随机性检测规范

GM/T 0011　可信计算　可信密码支撑平台功能与接口规范

3　术语和定义、缩略语

3.1　术语和定义

GB/T 5271.8中界定的以及下列术语和定义适用于本文件。

3.1.1

平台配置寄存器　platform configuration register

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。

3.1.2

授权数据　authorization data

执行一个命令操作的权限值。

3.1.3

可信密码模块　trusted cryptography module

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。

3.2　缩略语

下列缩略语适用于本文件

EK	密码模块密钥	(endorsement key)
NV	非易失性	(non-volatility)
PCR	平台配置寄存器	(platform configuration register)
TCM	可信密码模块	(trusted cryptography module)