

ICS 35.040
L 80
备案号:38310—2013



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.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 8.25 字数 251 千字
2013年1月第一版 2013年1月第一次印刷

*

书号: 155066·2-24380 定价 100.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	1
4 概述	2
5 可信密码模块管理功能	2
5.1 启动	3
5.2 状态保存 TCM_SaveState	4
5.3 自检	4
5.4 工作模式设置	6
5.5 所有者管理	12
5.6 属性管理	16
5.7 升级与维护	18
5.8 授权值管理	19
5.9 非易失性存储管理	22
5.10 运行环境管理	29
5.11 审计	31
5.12 时钟	34
5.13 计数器	36
6 平台身份标识与认证功能	41
6.1 密码模块密钥管理	41
6.2 平台身份密钥管理	44
7 平台数据保护	50
7.1 数据保护操作	50
7.2 密钥管理	53
7.3 密钥协商	60
7.4 密钥迁移	64
7.5 密码服务	69
7.6 传输会话	75
7.7 授权协议	79
8 完整性度量与报告功能	81
8.1 概述	81