



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	V
引言	VI
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 可信密码模块接口符合性测试	2
4.1 概述	2
4.2 常量值	3
4.3 测试策略	4
4.4 测试方法	5
5 命令依赖关系	6
5.1 启动命令集	6
5.2 状态保存命令集	6
5.3 自检命令集	6
5.4 TCM 工作模式设置命令集	7
5.5 Owner 管理命令集	7
5.6 属性管理命令集	7
5.7 升级与维护命令集	7
5.8 授权值管理命令集	7
5.9 非易失存储管理命令集	7
5.10 运行环境管理命令集	8
5.11 审计命令集	8
5.12 时钟命令集	8
5.13 计数器命令集	8
5.14 TCM 背书密钥管理命令集	8
5.15 平台身份密钥管理命令集	9
5.16 数据保护操作命令集	9
5.17 密钥管理命令集	9
5.18 密钥协商命令集	10
5.19 密钥迁移命令集	10
5.20 密码服务命令集	11
5.21 传输会话命令集	11
5.22 授权协议命令集	11
5.23 平台配置寄存器管理命令集	12
6 向量命令	12
6.1 TCM_Startup	12

6.2	TCM_SelfTestFull	13
6.3	TCM_ContinueSelfTest	13
6.4	TCM_GetTestResult	14
6.5	TCM_SetOwnerInstall	14
6.6	TCM_OwnerSetDisable	15
6.7	TCM_PhysicalEnable	16
6.8	TCM_PhysicalDisable	17
6.9	TCM_SetTempDeactivated	17
6.10	TCM_PhysicalSetDeactivated	18
6.11	TCM_TakeOwnership	18
6.12	TCM_OwnerClear	21
6.13	TCM_ForceClear	23
6.14	TCM_DisableOwnerClear	23
6.15	TCM_DisableForceClear	25
6.16	TCM_GetCapability	25
6.17	TCM_SetCapability	26
6.18	TCM_ResetLockValue	27
6.19	TCM_ChangeAuth	28
6.20	TCM_ChangeAuthOwner	30
6.21	TCM_NV_DefineSpace	32
6.22	TCM_NV_WriteValue	34
6.23	TCM_NV_ReadValue	35
6.24	TCM_FlushSpecific	36
6.25	TCM_GetAuditDigest	37
6.26	TCM_GetAuditDigestSigned	38
6.27	TCM_SetOrdinalAuditStatus	40
6.28	TCM_GetTicks	41
6.29	TCM_TickStampBlob	42
6.30	TCM_ReadPubEK	43
6.31	TCM_OwnerReadInternalPub	44
6.32	TCM_MakeIdentity	46
6.33	TCM_ActivatePEKCert	49
6.34	TCM_ActivatePEK	51
6.35	TCM_Seal	53
6.36	TCM_Unseal	56
6.37	TCM_CreateWrapKey	59
6.38	TCM_LoadKey	61
6.39	TCM_GetPubKey	64
6.40	TCM_WrapKey	65
6.41	TCM_CertifyKey	69
6.42	TCM_AuthorizeMigrationKey	70
6.43	TCM_CreateMigratedBlob	71
6.44	TCM_ConvertMigratedBlob	74

6.45	TCM_SM3Start	77
6.46	TCM_SM3Update	78
6.47	TCM_SM3Complete	79
6.48	TCM_SM3CompleteExtend	79
6.49	TCM_Sign	80
6.50	TCM_SM4Encrypt	82
6.51	TCM_SM4Decrypt	84
6.52	TCM_SM2Decrypt	86
6.53	TCM_GetRandom	88
6.54	TCM_APCreate	89
6.55	TCM_APTerminate	90
6.56	TCM_Extend	91
6.57	TCM_PCRRead	92
6.58	TCM_Quote	93
6.59	TCM_PCR_Reset	95
7	脚本向量	96
7.1	TCM_SaveState	96
7.2	TCM_SaveContext	96
7.3	TCM_LoadContext	99
7.4	TCM_FiledUpgrade	101
	参考文献	102

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。