

ICS 35.040
L 80
备案号:38309—2013



中华人民共和国密码行业标准

GM/T 0011—2012

可信计算 可信密码支撑平台功能与接口规范

Trusted computing—Functionality and interface specification of
cryptographic support platform

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、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	3
4 可信计算密码支撑平台功能原理	3
4.1 平台体系结构	3
4.1.1 平台功能与密码的关系	3
4.1.2 平台组成结构	4
4.1.3 可信密码模块	5
4.1.4 TCM 服务模块	5
4.2 密码算法要求	6
4.2.1 SM2	6
4.2.2 SM3	6
4.2.3 HMAC	6
4.2.4 SM4	7
4.2.5 随机数	7
4.3 功能原理	8
4.3.1 平台完整性	8
4.3.2 平台身份可信	9
4.3.3 平台数据安全保护	11
5 可信计算密码支撑平台功能接口	14
5.1 概述	14
5.2 上下文管理	15
5.2.1 概述	15
5.2.2 创建上下文	15
5.2.3 关闭上下文	16
5.2.4 设置上下文属性(整型参数)	16
5.2.5 获取上下文属性(整型参数)	17
5.2.6 设置上下文属性(变长参数)	18
5.2.7 获取上下文属性(变长参数)	19
5.2.8 连接上下文	20
5.2.9 释放上下文	20
5.2.10 获取上下文默认策略	21
5.2.11 创建对象	21

5.2.12	关闭对象	22
5.2.13	获取平台功能特性	22
5.2.14	获取 TCM 对象句柄	24
5.2.15	通过密钥属性加载密钥	24
5.2.16	通过密钥 ID 加载密钥	25
5.2.17	注册密钥	26
5.2.18	销毁密钥	26
5.2.19	通过密钥 ID 获取密钥	27
5.2.20	通过公钥获取密钥	27
5.2.21	通过 ID 获取注册密钥	28
5.2.22	设置传输会话加密密钥	29
5.2.23	关闭传输会话	29
5.3	策略管理	30
5.3.1	设置策略类属性(整型参数)	30
5.3.2	获取上下文属性(整型参数)	31
5.3.3	设置上下文属性(变长参数)	32
5.3.4	获取上下文属性(变长参数)	33
5.3.5	设置策略授权	34
5.3.6	清除策略授权	34
5.3.7	绑定策略对象	35
5.4	可信密码模块(TCM)管理	35
5.4.1	概述	35
5.4.2	创建平台身份和证书请求	35
5.4.3	激活平台身份和获取 PIK 证书	36
5.4.4	创建 PEK 请求	37
5.4.5	获取 PEK 证书	38
5.4.6	导入 PEK 密钥	38
5.4.7	创建不可撤销的密码模块密钥	39
5.4.8	获取密码模块密钥公钥	40
5.4.9	创建可撤销的密码模块密钥	40
5.4.10	撤销密码模块密钥	41
5.4.11	创建密码模块所有者	42
5.4.12	清除可信密码模块所有者	42
5.4.13	设置操作者授权	43
5.4.14	设置可信密码模块状态	43
5.4.15	查询设置可信密码模块状态	44
5.4.16	获取可信密码模块特性	46
5.4.17	可信密码模块完全自检	49
5.4.18	获取可信密码模块自检结果	49
5.4.19	获取可信密码模块产生的随机数	50
5.4.20	获取可信密码模块单个事件	50
5.4.21	获取可信密码模块一组事件	51
5.4.22	获取可信密码模块事件日志	51

5.4.23	可信密码模块 PCR 扩展	52
5.4.24	读取可信密码模块 PCR 值	53
5.4.25	重置可信密码模块 PCR	53
5.4.26	引证 PCR	54
5.4.27	读可信密码模块计数器	54
5.4.28	读可信密码模块当前时钟	55
5.4.29	获取可信密码模块审计摘要值	55
5.4.30	设置可信密码模块命令审计状态	56
5.5	密钥管理	57
5.5.1	概述	57
5.5.2	改变实体授权数据	57
5.5.3	获取策略对象	57
5.5.4	设置密钥属性(整型参数)	58
5.5.5	获取密钥属性(整型参数)	59
5.5.6	设置密钥属性(变长参数)	61
5.5.7	获取设置密钥属性(变长参数)	61
5.5.8	加载密钥	63
5.5.9	卸载密钥	63
5.5.10	获取密钥公钥	64
5.5.11	签署密钥	64
5.5.12	创建密钥	65
5.5.13	封装密钥	65
5.5.14	创建迁移授权	66
5.5.15	创建迁移密钥数据块	66
5.5.16	导入迁移密钥数据块	67
5.6	数据加密与解密	68
5.6.1	改变实体授权	68
5.6.2	获取策略对象	69
5.6.3	获取数据属性(整型参数)	69
5.6.4	设置数据属性(变长参数)	70
5.6.5	获取数据属性	70
5.6.6	数据加密	71
5.6.7	数据解密	72
5.6.8	数据封装	73
5.6.9	数据解封	74
5.6.10	数字信封封装	74
5.6.11	数字信封解密	75
5.7	PCR 管理	75
5.7.1	概述	75
5.7.2	设置 PCR Locality 属性	76
5.7.3	获取 PCR Locality 属性	76
5.7.4	获取 PCR 摘要	77
5.7.5	设置 PCR 值	77

5.7.6	获取 PCR 值	78
5.7.7	选择 PCR 索引	78
5.8	非易失性存储管理	79
5.8.1	设置非易失性存储区属性(整型参数)	79
5.8.2	获取非易失性存储区属性(整型参数)	80
5.8.3	获取非易失性存储区属性(变长参数)	81
5.8.4	创建非易失性存储区空间	82
5.8.5	释放非易失性存储区空间	83
5.8.6	数据写入非易失性存储区	83
5.8.7	从非易失性存储区读取数据	84
5.9	杂凑操作	85
5.9.1	设置杂凑对象属性(整型参数)	85
5.9.2	获取杂凑对象属性(整型参数)	86
5.9.3	设置杂凑对象属性(变长参数)	87
5.9.4	对用户数据进行杂凑操作	87
5.9.5	设置杂凑值	88
5.9.6	获取杂凑值	89
5.9.7	更新杂凑值	89
5.9.8	对杂凑值签名	90
5.9.9	验证杂凑值签名	90
5.9.10	给杂凑类加时间戳	91
5.10	密钥协商	92
5.10.1	创建会话	92
5.10.2	获取会话密钥	92
5.10.3	释放会话	94
附录 A (规范性附录)	接口规范数据结构	95
附录 B (规范性附录)	数字证书格式	118
附录 C (规范性附录)	主板应用接口	120
参考文献	129

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、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、范琴。

引 言

本标准以我国可信计算密码技术要求与应用方案为指导,描述了可信计算密码支撑平台的功能原理与要求,并定义了可信计算密码支撑平台为应用层提供服务的接口规范,用以指导我国相关可信计算产品开发和应用。

本标准凡涉及密码算法相关内容的,按照国家有关规定实施。

可信计算

可信密码支撑平台功能与接口规范

1 范围

本标准描述了可信计算密码支撑平台的功能原理与要求,并详细定义了可信计算密码支撑平台的密码算法、密钥管理、证书管理、密码协议、密码服务等应用接口规范。

本标准适用于可信计算密码支撑平台相关产品的研制、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 信息技术 词汇 第8部分:安全(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 0009 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

3 术语、定义和缩略语

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

部件 component

计算系统中可被度量的硬件和/或软件模块。

3.1.2

存储主密钥 storage master key

用于保护平台身份密钥和用户密钥的主密钥。

3.1.3

对象 object

可信计算密码支撑平台内可以被实体访问的各类资源,包括密钥数据、运行环境数据、敏感数据等。

3.1.4

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。

3.1.5

可信计算密码支撑平台 cryptographic support platform for trusted computing

可信计算平台的重要组成部分,包括密码算法、密钥管理、证书管理、密码协议、密码服务等内容,为