

ICS 35.040
L 80
备案号: 62993—2018



中华人民共和国密码行业标准

GM/T 0058—2018

可信计算 TCM 服务模块接口规范

Trusted computing—TCM service module interface specification

2018-05-02 发布

2018-05-02 实施

国家密码管理局 发布

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	1
4 缩略语	3
5 软件架构	3
6 TCM 应用服务	5
6.1 类定义	5
6.2 类与对象的关系	5
6.3 接口	7
6.3.1 通用接口	7
6.3.2 上下文管理	11
6.3.3 管理策略类	25
6.3.4 TCM 管理类	31
6.3.5 密钥管理类	53
6.3.6 数据加解密类	65
6.3.7 PCR 操作类	74
6.3.8 NV 存储管理类	77
6.3.9 杂凑计算类	83
6.3.10 密钥协商类	90
6.3.11 回调函数类	93
7 TCM 核心服务	97
7.1 TCM 核心服务管理	97
7.1.1 上下文管理	97
7.1.2 密钥管理	100
7.1.3 事件管理	104
7.2 可信密码模块管理	106
7.2.1 TCM 测试	106
7.2.2 工作模式设置	107
7.2.3 所有者管理	110
7.2.4 属性管理	113
7.2.5 升级与维护	114
7.2.6 授权管理	115
7.2.7 非易失性存储管理	117
7.2.8 审计	121

- 7.2.9 时钟 123
- 7.2.10 计数器 124
- 7.3 平台身份标识与认证 127
 - 7.3.1 密码模块密钥管理 127
 - 7.3.2 平台身份密钥管理 130
- 7.4 平台数据保护 133
 - 7.4.1 数据保护操作 133
 - 7.4.2 密钥管理 135
 - 7.4.3 密钥协商 139
 - 7.4.4 密钥迁移 142
 - 7.4.5 密码学服务 144
 - 7.4.6 传输会话 147
 - 7.4.7 授权协议 150
- 7.5 完整性度量与报告 151
 - 7.5.1 平台配置寄存器管理 151
- 8 TDDL 设备驱动库 153
 - 8.1 TDDL 架构 153
 - 8.2 TDDL 内存管理 154
 - 8.3 TDDL 错误码与定义 154
 - 8.4 TDDL 接口 154
 - 8.4.1 Tddli_Open 154
 - 8.4.2 Tddli_Close 155
 - 8.4.3 Tddli_Cancel 155
 - 8.4.4 Tddli_GetCapability 156
 - 8.4.5 Tddli_SetCapability 157
 - 8.4.6 Tddli_GetStatus 157
 - 8.4.7 Tddli_TransmitData 158
- 附录 A (规范性附录) 接口数据结构 160
 - A.1 基础定义 160
 - A.2 数据结构 179
 - A.3 授权数据处理 184
 - A.4 返回码定义 184

前 言

本标准按照 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。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：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、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、北京工业大学。

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、刘鑫、林洋、李伟平、尹洪兵、徐震、严飞、付月朋、明明、刘韧、李丰、许勇、贾兵、王蕾、顾健、何长龙、秦宇。

引 言

可信计算标准体系包含以下标准：

- GM/T 0011—2012 可信计算 可信密码支撑平台功能与接口规范
- GM/T 0012—2012 可信计算 可信密码模块接口规范
- GM/T 0013—2012 可信计算 可信密码模块接口符合性测试规范
- GM/T 0058—2018 可信计算 TCM 服务模块接口规范

上述四个标准中,本标准的接口介于 GM/T 0012—2012 之上,向上为应用程序提供接口调用,中间定义了如何实现服务模块接口,向下调用 GM/T 0012—2012 中的接口,本标准以 GM/T 0011—2012 为基础及核心,技术内容基本未做改动,GM/T 0013—2012 为可信密码模块产品的符合性检测提供依据,四个规范形成一套完整的可信计算体系标准。

本标准描述了可信计算 TCM 服务模块接口规范,目标是制定统一的可信计算 TCM 服务模块组成和接口规范,通过该类接口规范,向应用层提供统一的 TCM 密码应用服务,适用于可信计算应用的开发、使用及检测提供标准依据和指导,有利于提高可信计算产业发展水平。

本标准凡涉及密码算法的相关内容,按国家有关法规实施;凡涉及采用密码技术解决保密性、完整性、真实性、不可否认性需求的应遵循密码相关国家标准和行业标准。

可信计算 TCM 服务模块接口规范

1 范围

本标准规定了 TCM 服务模块的组成和接口标准,包含 TSP、TCS 和 TDDL,是面向 TCM 应用层的接口标准。

本标准适用于基于 TCM 的应用开发。

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 32905—2016 SM3 密码杂凑算法

GB/T 32907—2016 SM4 分组密码算法

GB/T 32918.2—2016 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法

GB/T 32918.4—2016 SM2 椭圆曲线公钥密码算法 第 4 部分:公钥加密算法

GM/T 0005—2012 随机性检测规范

GM/T 0009—2012 SM2 密码算法使用规范

GM/T 0015—2012 基于 SM2 密码算法的数字证书格式规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

部件 component

计算系统中可被度量的硬件和/或软件模块。

3.2

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,是可信存储根的一种实现形式。

3.3

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。

3.4

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。

3.5

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,为可信计算平台自身的完整性、身份可信性和数据安全性提供密码支持。其产品形态主要表现为可信密码模块和可信密码服务模块。