ICS 35.040
L 80
备案号：

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.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 0.00　字数 00 千字
2012年　月第一版　2012年　月第一次印刷
*
书号:155066·-　定价 00.00 元

GM 0012-2012

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规范。

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(eqv ISO/IEC 2382-8-1998)

GM/T 0002　SM4 分组密码算法

GM/T 0003　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 AAAA　SM2 密码算法使用规范

GM/T BBBB　基于 SM2 密码算法的数字证书格式规范

GM/T CCCC　可信计算　可信密码支撑平台功能与接口规范

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合本文件。

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

是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	(TCM 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)

4　概述

TCM 是构建可信计算的关键基础部件,它自身能够建立独立、受保护的安全运算环境,是硬件和固件的集合。

硬件组成的部件包括 4 类:

1)　执行引擎,即 CPU;

2)　密码算法引擎(包括 SM4、SM2、SM3、随机数发生器),提供独立的密码运算支撑;

3)　存储器,分易失性存储器和非易失性存储器 2 种,非易失性存储器存储重要安全参数,包括固件和密钥之类;

4)　I/O 接口,即与主机平台的接口。

固件组成的部件包括 3 类:

1)　运行管理程序,即 TCM 的操作系统;

2)　功能命令程序,是固件的核心与主体;

3)　与主机程序交互的函数接口。

TCM 的核心功能体系就是基于自主密码算法构建可信计算 3 个维度的功能,包括:平台完整性度量与验证、平台可信身份标识与鉴别、平台数据保护。相关内容已在 GM/T CCCC 中详细描述,本规范就不再赘诉。而 TCM 的 I/O 接口与平台有关,需针对平台专门定义,本规范不涉及这部分内容。

本规范主要定义 TCM 固件中功能命令及对应函数接口。主要内容包括 4 个方面:

1)　TCM 管理功能,建立了包括启动、状态保存、自检、工作模式设置、所有者管理、属性管理、授权值管理、非易失性存储管理、运行环境管理、审计、时钟、计数器、升级与维护 13 个方面的 43 个功能命令与接口规范;

2)　平台身份标识功能,建立了包括密码模块密钥管理和平台身份密钥管理 2 个方面的 9 个功能命令与接口规范;

3)　平台数据保护功能,建立了包括数据操作保护、密钥管理、密钥协商、密钥迁移、密码服务、传输会话、授权协议 7 个方面的 27 个功能命令与接口规范;

4)　完整性度量与报告功能,建立了包括写入 PCR、读取 PCR、引用 PCR、PCRReset4 个方面的 4 个功能命令与接口。报告功能需要结合签名操作来实现。

在每个功能命令与接口描述中,主要给出功能描述与接口定义,至于功能命令内部逻辑不做严格定义。

下面各章将详细描述 TCM 的功能命令与接口规范。

5　可信密码模块管理功能

数据描述格式如下:

输入/输出数据格式:

参数 1	参数 2	…	参数 n
2B	4B	4B	2B

——参数 1 参数至参数 n 表示输入字节流的最左端到最右端

——XB,参数数据长度,单位为字节

输入/输出授权数据验证码格式：

命令码	抗重放数据	序列号
4B	32B	4B
1S	2S	2Hn

——XB，参数数据长度，单位为字节

——XS，参与 SM3 运算的参数编号

——2Hn，该参数时 HMAC 运算的第二个参数，n 表示第 n 个授权会话使用该参数，本标准支持 n 为 1，2

授权数据验证码计算：

本标准采用 HMAC 运算进行授权数据验证码计算。

1） 输入授权数据验证码等于：HMAC(密钥，输入参数摘要||2Hn)；

2） 输出授权数据验证码等于：HMAC(密钥，输出参数摘要||2Hn)；

3） 输入参数摘要或输出参数摘要＝SM3(1S||2S||3S||…)；

4） 密钥：取值参见具体命令授权数据验证码描述。

5.1 启动

5.1.1 TCM 初始化 TCM_Init

功能描述：

TCM_Init 是一个用于初始化 TCM 的物理方法。由 TCM_Init 信号通知 TCM 平台开始初始化。TCM_Init 把 TCM 置于等待 TCP_Startup 命令执行的状态。

具体实现方法由厂商自定义。

5.1.2 TCM 启动 TCM_Startup

功能描述：

TCM_Startup 在 TCM_Init 之后执行，以如下三种模式执行启动：

1） Clear：所有变量设置为缺省值，需设置的向量至少包括：

a） 设置＜TCM_RESOURCE_TYPE＞资源句柄无效；

b） 重置 TCM_STCLEAR_DATA 结构；

c） 重置 TCM_STCLEAR_FLAGS 结构；

2） Save：使 TCM 恢复到以前执行 TCM_SaveState 所保存的值；

3） Deactivate：使 TCM 无效，需重新执行 TCM_Init，才能使 TCM 进入一个正常工作状态。

接口：

输入数据格式：

标识	数据长度	命令码	启动类型
2B	4B	4B	2B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_Startup 所定义的固定值

——启动类型为 TCM_ST_CLEAR、TCM_ST_STATE、TCM_ST_DEACTIVED 中的一种，分别对应上述描述的三种启动模式

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)

5.2 状态保存 TCM_SaveState

功能描述：

用于在进入低电或没电状态前，通知 TCM 保存当前临时变量到非易失性存储中，以便下次启动时，恢复到当前保存的状态。

需要保存的值必须是非易失性的。如果保存的值已在非易失性存储介质中，则无需保存。TCM 必须能够检查被保存值的有效性。

需要保存的临时变量至少应包括：

1) PCR 值(PCR 属性 pcrReset 为 TRUE，或者标识为 DEBUG 的 PCR 值除外)
2) TCM_STCLEAR_DATA 中的所有值；
3) TCM_STCLEAR_FLAGS 中的所有值；
4) 若密钥的 parentPCRStatus 属性为 FALSE，则需要保存已载入密钥的值。

auditDigest 的值，保存时需要先根据审计要求进行处理，对本命令的输出参数不进行审计(可选)。

接口：

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_SaveState 所定义的固定值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)

5.3 自检

TCM 启动时需要自动对内部的基本功能模块进行检测，包括随机数发生器、EK 完整性、HASH 功能等。

5.3.1 启动自检

5.3.1.1 完全自检 TCM_SelfTestFull

功能描述：

该命令测试 TCM 的全部功能能否正常运行。

接口：

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SelfTestFull 所定义的固定值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

5.3.1.2 异步自检 TCM_ContinueSelfTest

功能描述：

测试 TCM 初始化时未被测试的模块。

接口：

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 CM_ORD_ContinueSelfTest 所定义的固定值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

5.3.2 获取自检结果 TCM_GetTestResult

功能描述：

该命令提供自检结果信息。该命令可以在故障模式下运行是为了让 TCM 生产商获得诊断信息。TCM 应返回最近一次自检结果的信息块。且这些信息不能包含任何能唯一鉴别某个 TCM 的数据。

接口：

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_GetTestResul 所定义的固定值
输出数据格式：

标识	数据长度	返回码	输出数据长度	输出数据
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——输出数据长度为厂商定义的测试信息的字节数
——输出数据是有厂商指定的测试信息

5.4 工作模式设置

5.4.1 所有者可创建模式 TCM_SetOwnerInstall

功能描述：
当 TCM 处于使能状态且没有所有者的情况下，该命令在确认物理现场后，设置 TCM 允许或拒绝创建所有者。操作如下：
1) 这个命令需要在物理现场下进行；
2) 需要对 TCM_PERMANENT_FLAGS. ownership 的值进行设置。
接口：
输入数据格式：

标识	数据长度	命令码	状态位
2B	4B	4B	1B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_SetOwnerInstall 所定义的固定值
——状态位，为一个布尔值：TRUE 表示允许 TCM 创建所有者，FALSE 则相反
输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)如果 TCM 已处于 owner 操作状态，命令将直接返回 TCM_SUCCESS

5.4.2 所有者设置 TCM 模式 TCM_OwnerSetDisable

功能描述：

TCM 所有者设置 TCM 处于工作或禁用模式。

1） 验证所有者授权；

2） 需要对 TCM_PERMANENT_FLAGS.disable 的值进行设置。

接口：

输入数据格式：

标识	数据长度	命令码	状态位	授权会话句柄	授权数据验证码
2B	4B	4B	1B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_OwnerSetDisable 所定义的固定值

——状态位，标识使能(TRUE)或禁用(FALSE)TCM

——授权会话句柄为所有者的授权会话句柄

——授权数据验证码

输出数据格式：

标识	数据长度	返回码	授权数据验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——授权数据验证码

授权数据验证码：

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	状态位	序列号
4B	1B	4B
1S	2S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	32B
1S	2S	2H1

5.4.3 物理现场设置可用模式 TCM_PhysicalEnable

功能描述：

使用物理现场作为授权使能 TCM。

1） 这个命令需要在现场下进行；

2） 需要对 TCM_PERMANENT_FLAGS.disable 的值进行设置 FALSE。

接口：

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_PhysicalEnable 所定义的固定值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

5.4.4 物理现场设置禁用模式 TCM_PhysicalDisable

功能描述：

使用物理现场作为授权禁用 TCM。

1) 这个命令需要在现场下进行；

2) 需要对 TCM_PERMANENT_FLAGS. disable 的值进行设置 TRUE。

接口：

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_PhysicalDisable 所定义的固定值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

5.4.5 临时无效模式 TCM_SetTempDeactivated

功能描述：

TCM 的操作者使 TCM 暂时无效，下一次平台启动时 TCM 恢复到有效状态。该命令的授权可以是物理现场也可以是操作者授权。

1) 这个命令需要在物理现场下进行；

2) 需要对 TCM_STCLEAR_FLAGS. deactivated 的值进行设置 TRUE。

接口：

1) 物理现场授权

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SetTempDeactivated 所定义的固定值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

2) 操作者授权

输入数据格式：

标识	数据长度	命令码	授权会话句柄	授权数据验证码
2B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SetTempDeactivated 所定义的固定值

——授权会话句柄为操作者的授权会话句柄

——授权数据验证码

输出数据格式：

标识	数据长度	返回码	授权数据验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——授权数据验证码

授权数据验证码:操作者授权

密钥为操作者使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	序列号
4B	4B
1S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.4.6 物理现场授权设置无效模式 TCM_PhysicalSetDeactivated

功能描述：

使用物理现场授权设置 TCM 为无效工作模式。

1) 这个命令需要在现场下进行；

2） 需要对 TCM_PERMANENT_FLAGS. deactivated 的值进行设置。

接口：

本接口只有零授权一种情况。

输入数据格式：

标识	数据长度	命令码	状态位
2B	4B	4B	1B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_PhysicalSetDeactivated 所定义的固定值

——状态位为是否设置物理现场作为授权标识的状态值，TRUE 表明可以使用物理现场作为授权方式，FALSE 表明不可以

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果（见返回码定义表）

5.4.7 设置操作者授权数据 TCM_SetOperatorAuth

功能描述：

用于设置 TCM 的操作者的授权数据。

1） 这个命令需要在物理现场下进行；

2） 需要对 TCM_PERMANENT_DATA－＞operatorAuth 的值进行设置；

3） 需要设置 TCM_PERMANENT_FLAGS－＞operator 的值为 TRUE，代表需要进行对操作者身份进行判断。

接口：

输入数据格式：

标识	数据长度	命令码	授权数据
2B	4B	4B	32B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SetOperatorAuth 所定义的固定值

——授权数据为设置的操作者的授权数据

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果（见返回码定义表）

5.4.8 设置物理现场 TSC_PhysicalPresence

功能描述：

TCM 某些命令操作需要物理现场，用来保证平台所有者身份证明或非远程软件对 TCM 的操作。这个命令有 2 个功能，第一个是启用或永久使用硬件/软件物理现场；另一个是如果启用软件物理现场后，是否允许使用物理现场。

物理现场的制定原则：

1） TCM_PERMANENT_FLAGS -> physicalPresenceLifetimeLock 为 FLASE 时才能设置物理现场值；

2） 硬件、软件物理现场不能同时存在；

3） TCM_PERMANENT_FLAGS -> physicalPresenceCMDEnable 为 FALSE 时软件物理现场不能存在；

4） TCM_STCLEAR_FLAGS -> physicalPresenceLock 为 FLASE 时才能设置物理现场值。

各个厂商在生产过程中需要定义 TCM 这些状态来绑定在某平台上如何使用。

接口：

输入数据格式：

标识	数据长度	命令码	状态
2B	4B	4B	2B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TSC_ORD_PhysicalPresence 所定义的固定值

——状态为可以设置的物理现场各种状态，使用 TCM_PHYSICAL_PRESENCE 类型表示，所包含值包括：

名称	值	操作
TCM_PHYSICAL_PRESENCE_HW_DISABLE	0x0200h	设置 TCM_PERMANENT_FLAGS -> physicalPresenceHWEnable 为 FALSE
TCM_PHYSICAL_PRESENCE_CMD_DISABLE	0x0100h	设置 TCM_PERMANENT_FLAGS -> physicalPresenceCMDEnable 为 FALSE
TCM _ PHYSICAL _ PRESENCE _ LIFETIME _LOCK	0x0080h	设置 TCM_PERMANENT_FLAGS -> physicalPresenceLifetimeLock 为 TRUE
TCM_PHYSICAL_PRESENCE_HW_ENABLE	0x0040h	设置 TCM_PERMANENT_FLAGS -> physicalPresenceHWEnable 为 TRUE
TCM_PHYSICAL_PRESENCE_CMD_ENABLE	0x0020h	设置 TCM_PERMANENT_FLAGS -> physicalPresenceCMDEnable 为 TRUE
TCM_PHYSICAL_PRESENCE_NOTPRESENT	0x0010h	设置 TCM_STCLEAR_FLAGS -> PhysicalPresence 为 FALSE
TCM_PHYSICAL_PRESENCE_PRESENT	0x0008h	设置 TCM_STCLEAR_FLAGS -> PhysicalPresence 为 TRUE
TCM_PHYSICAL_PRESENCE_LOCK	0x0004h	设置 TCM_STCLEAR_FLAGS -> PhysicalPresenceLock 为 TRUE

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)

5.5 所有者管理

5.5.1 获取所有权 TCM_TakeOwnership

功能描述:

用于在 TCM 内部创建所有者的命令,平台所有者只能有一个,需要平台已经创建了密码模块密钥(EK);

1) TCM 判断平台没有所有者,使用 EK 私钥解密得到所有者授权数据;
2) 验证所有者授权数据;
3) TCM 验证输入存储主密钥(SMK)的密钥信息参数,保证符合国家密码规范定义的算法(SM4)和长度要求(128);TCM 使用 EK 私钥解密输入的存储主密钥的加密授权数据参数,并验证其合法性;根据密钥参数创建 SMK;
4) 将 SMK 保存在 TCM_PERMANENT_DATA ->smk,所有者授权数据保存在 TCM_PERMANENT_DATA ->ownerAuth;
5) 返回存储主密钥信息数据。

接口:

本接口只有一个授权。

输入数据格式:

标识	数据长度	命令码	协议 ID	所有者授权数据长度	所有者授权数据	SMK 授权数据长度	SMK 授权数据	SMK 结构数据	<续>
2B	4B	4B	2B	4B	可变	4B	可变	可变	

授权会话句柄	授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_TakeOwnership 所定义的固定值
——协议 ID 为使用协议类型,这里等于 TCM_PID_OWNER
——所有者授权数据长度为为用 EK 公钥加密后的授权数据的长度
——所有者授权数据为用 EK 公钥加密后的授权数据
——SMK 授权数据长度为 EK 公钥加密后的授权数据的长度
——SMK 授权数据为用 EK 公钥加密后的授权数据
——SMK 结构数据为带有 SMK 创建的密钥参数的 TCM_KEY 结构,其中包括了采用的算法、密钥长度等密钥属性
——授权会话句柄为在该命令之前创建的 AP 协议会话句柄
——授权数据验证码

输出数据格式：

标识	数据长度	返回码	SMK 结构数据	＜续＞
2B	4B	4B	可变	

所有者授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——SMK 结构数据为创建的 SMK 密钥的 TCM_KEY 结构,其中包括了密钥属性

——所有者授权数据验证码

授权数据验证码:所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	协议 ID	所有者授权数据长度	所有者授权数据	SMK 授权数据长度	SMK 授权数据	SMK 结构数据	序列号
4B	2B	4B	可变	4B	可变	可变	4B
1S	2S	3S	4S	5S	6S	7S	2H1

输出验证码计算：

返回码	命令码	SMK 结构数据	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

5.5.2 清除所有权

5.5.2.1 所有者授权清除 TCM_OwnerClear

功能描述：

该命令在所有者授权下执行清除(clear)操作。DisableOwnerClear 可以设置该命令是否可用。

1) 首先验证所有者授权是否正确；

2) 卸载(Unload)所有密钥以及重置其他数据等操作。

接口：

本接口只有一个授权。

输入数据格式：

标识	数据长度	命令码	＜续＞
2B	4B	4B	

授权会话句柄	授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数
——命令码为 TSC_ORD_OwnerClear 所定义的固定值
——授权会话句柄为在该命令之前创建的 AP 协议会话的会话句柄
——授权数据验证码
输出数据格式：

标识	数据长度	返回码	＜续＞
2B	4B	4B	

授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——授权数据验证码
授权数据验证码:所有者授权
密钥为所有者使用 AP 会话产生的共享秘密数据。
输入验证码计算：

命令码	序列号
4B	4B
1S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.5.2.2 强制清除 TCM_ForceClear

功能描述：
该命令在物理现场的条件下执行清除所有者操作。
1） 这个命令需要在物理现场授权下进行；
2） 执行 TCM_OwnerClear 的操作。
接口：
输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_ForceClear 所定义的固定值
输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)

5.5.1 禁用清除权

5.5.1.1 禁用所有者授权清除权 TCM_DisableOwnerClear

功能描述:

该命令使 TCM_OwnerClear 命令无效,只有通过物理现场才能进行 TCM 的清除所有者的操作。在执行 TCM_ForceClear 后,TCM_ownerClear 又会有效。操作如下:

1) 检测所有者授权的正确性,只有授权数据正确才能进行这个操作;
2) 设置 TCM_PERMANENT_FLAGS -> disableOwnerClear 为 TRUE;

接口:

本接口只有一个授权。

输入数据格式:

标识	数据长度	命令码	<续>
2B	4B	4B	

授权会话句柄	授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_DisableOwnerClear 所定义的固定值
——授权会话句柄为在该命令之前创建的 AP 协议会话的会话句柄
——授权数据验证码

输出数据格式:

标识	数据长度	返回码	<续>
2B	4B	4B	

所有者授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——所有者授权数据验证码

授权数据验证码:所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	序列号
4B	4B

1S　　2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.5.1.2　禁用强制清除权 TCM_DisableForceClear

功能描述：

该命令使 ForceClear 命令无效直到下一个 startup 周期。

1）　这个命令需要在物理现场状态下进行；

2）　TCM_STCLEAR_FLAGS. disableForceClear 需要设置为 TRUE。

接口：

输入数据格式：

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_DisableForceClear 所定义的固定值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

5.6　属性管理

5.6.1　获取属性 TCM_GetCapability

功能描述：

该命令返回 TCM 的当前属性信息。

接口：

输入数据格式：

标识	数据长度	命令码	属性参数	子属性参数长度	子属性参数
2B	4B	4B	4B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_GetCapability 所定义的固定值

——属性域参数为需要查询的 TCM 当前信息的属性参数，参考 TCM_CAPABILITY_AREA 结构描述

——子属性参数长度为需要查询的 TCM 当前信息的子属性参数数据长度

——子属性参数为需要查询的 TCM 当前信息的子属性参数数据，参考 TCM_CAPABILITY_AREA 结构描述

输出数据格式：

标识	数据长度	返回码	属性值长度	属性值
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——属性值长度为查询的 TCM 当前信息的属性值长度

——子属性参数为查询的 TCM 当前信息的属性值，参考 TCM_CAPABILITY_AREA 结构描述

5.6.2 设置属性 TCM_SetCapability

功能描述：

该命令用于设置 TCM 的属性值。

TCM 需要检查输入的属性范围值与子范围值的有效性。如果这两个域都有效，设置相关的标志/数据。

接口：

本接口有零授权和一个授权两种情况。

1)、零授权

输入数据格式：

标识	数据长度	命令码	属性参数	子属性参数长度	子属性参数	属性值长度	属性值
				度		长度	
2B	4B	4B	4B	4B	可变	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SetCapability 所定义的固定值

——属性域参数为需要查询的 TCM 当前信息的属性参数，参考 TCM_CAPABILITY_AREA 结构描述

——子属性参数长度为需要查询的 TCM 当前信息的子属性参数数据长度

——子属性参数为需要查询的 TCM 当前信息的子属性参数数据，参考 TCM_CAPABILITY_AREA 结构描述

——属性值长度为输入的值的长度

——属性值为需要设置的具体值

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

2)、一个授权

输入数据格式：

标识	数据长度	命令码	属性参数	子属性参数长度	子属性参数	属性值长度	属性值	＜续＞
2B	4B	4B	4B	4B	可变	4B	可变	

所有者授权会话句柄	所有者授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_SetCapability 所定义的固定值
——属性域参数为需要查询的 TCM 当前信息的属性参数，参考 TCM_CAPABILITY_AREA 结构描述
——子属性参数长度为需要查询的 TCM 当前信息的子属性参数数据长度
——子属性参数为需要查询的 TCM 当前信息的子属性参数数据，参考 TCM_CAPABILITY_AREA 结构描述
——属性值长度为输入的值的长度
——属性值为需要设置的具体值
——所有者授权会话句柄
——所有者授权数据验证码

输出数据格式：

标识	数据长度	返回码	所有者授权 数据验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果（见返回码定义表）
——所有者授权数据验证码

授权数据验证码：所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	属性参数	子属性参数长度	子属性参数	属性值长度	属性值	序列号
4B	4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	6S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.7 升级与维护

5.7.1 固件升级 TCM_FieldUpgrade

功能描述：

该命令用于升级 TCM 的固件。这个命令为可选命令，各厂商可决定如何实现这个命令。

当实现这个命令时，必须遵守如下规则：

1. TCM 的升级机制不能依靠 TCM 保持一个全局的秘密值来实现。全局秘密的定义时不能由一个秘密值被多个 TCM 共享。
2. 不能使用 EK 用于升级过程的鉴别与加密。
3. 可以使用预生成的公钥来验证升级包。
4. 仅能升级固件本身，不能破坏用户数据。用户数据包括当前已加载的密钥、当前的 PCR 信息等等。
5. 当所有者不存在需要物理现场操作。所有者存在时必须有所有者授权。

5.7.2 重置锁定时间 TCM_ReSetLockValue

功能描述：

该命令用于重置 TCM 字典攻击次数。

由厂商自定义 TCM 防字典攻击机制。防字典攻击可以包括设置周期等待状态、重启、以及其他防攻击策略。

接口：

输入数据格式：

标识	数据长度	命令码	授权会话句柄	授权数据验证码
2B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReSetLockValue 所定义的固定值

——授权会话句柄是使用所有者授权会话句柄

——授权数据验证码

输出数据格式：

标识	数据长度	返回码	授权数据验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——授权数据验证码

授权数据验证码：所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	序列号
4B	4B
1S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.8 授权值管理

5.8.1 更改实体授权值 TCM_ChangeAuth

功能描述：

本命令允许一个实体的所有者改变这个实体的授权数据。操作如下：

1)、不能使用这个命令改变 SMK 的授权数据，验证实体类型值必须为 TCM_ET_DATA、TCM_ET_KEY 这两种类型之一，否则返回 TCM_WRONG_ENTITYTYPE。

2)、验证父密钥授权会话类型为 AP，否则返回 TCM_BAD_MODE。

3)、验证实体授权会话类型为 AP—〉(TCM_NONE)。否则返回 TCM_BAD_MODE。

4)、encData 必须是 TCM_STORED_DATA 或者 TCM_KEY 结构中对应的 encData 部分。

5)、新的授权数据使用父密钥的创建的 AP 会话共享秘密数据进行解密得到。

6)、验证父密钥授权。

7)、验证 parentHandle -> keyUsage 为 TCM_KEY_STORAGE，否则返回 TCM_INVALID_KEYUSAGE。

8)、使用父密钥授权解密 encData，并验证其结构为 TCM_STORE_ASYMKEY 或者 TCM_SEALED_DATA，同时检查 tag、length、authValue 是否匹配，否则返回 TCM_INVALID_STRUCTURE。

9)、使用新授权数据替代原实体授权数据。

10)、使用父密钥加密新的实体授权数据。

11)、终止实体对应的所有会话。

接口：

输入数据格式：

标识	数据长度	命令码	父密钥句柄	协议ID	加密后的新授权数据	实体类型	要改变授权数据的实体数据长度	要改变授权数据的实体数据	<续>
2B	4B	4B	4B	2B	32B	2B	4B	可变	

父密钥授权会话句柄	父密钥授权数据验证码	实体授权会话句柄	实体授权数据验证码
4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ChangeAuth 所定义的固定值

——父密钥句柄为实体的父密钥的句柄 TCM_KEY_HANDLE

——协议 ID 为 TCM_PID_AP 所定义的固定值

——加密后的新授权数据 TCM_ENCAUTH

——实体类型为 TCM_ET_DATA，TCM_ET_KEY 中一种

——要改变授权数据的实体数据大小 UINT32

——要改变授权数据的实体数据 BYTE[]

——父密钥授权会话句柄 TCM_AUTHHANDLE

——父密钥授权数据验证码

——实体授权会话句柄

——实体授权数据验证码

输出数据格式：

标识	数据长度	返回码	实体数据长度	实体数据	父密钥授权数据验证码	实体授权数据验证码
2B	4B	4B	4B	可变	32B	32B

——标识为 TCM_TAG_RSP_AUTH2_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——实体数据长度为实体数据的长度　UINT32
——实体数据为改变后的,经过加密的实体数据 BYTE[]
——父密钥授权数据验证码
——实体授权数据验证码
授权数据验证码:父密钥授权
　　密钥为父密钥使用 AP 会话产生的共享秘密数据。
输入验证码计算：

命令码	协议 ID	加密后的新授权数据	实体类型	要改变授权数据的实体数据长度	要改变授权数据的实体数据	序列号
4B	2B	32B	2B	4B	可变	4B
1S	2S	3S	4S	5S	6S	2H1

输出验证码计算：

返回码	命令码	实体数据长度	实体数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

授权数据验证码:原实体授权
　　密钥为原实体授权使用 AP 会话产生的共享秘密数据。
输入验证码计算：

命令码	协议 ID	加密后的新授权数据	实体类型	要改变授权数据的实体数据长度	要改变授权数据的实体数据	序列号
4B	2B	32B	2B	4B	可变	4B
1S	2S	3S	4S	5S	6S	2H2

输出验证码计算：

返回码	命令码	实体数据长度	实体数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H2

5.8.2　更改所有者/存储主密钥授权数据 TCM_ChangeAuthOwner

功能描述：

本命令 TCM 所有者改变所有者或 SMK 的授权数据。操作如下：

1)、验证 Owner 授权会话。

2)、这个命令改变 Owner、SMK 的授权数据，实体类型为 TCM_ET_OWNER 或 TCM_ET_SMK，否则返回 TCM_WRONG_ENTITYTYPE。

3)、使用 Owner 创建 AP 会话的共享秘密数据解密新授权数据。

4)、终止当前 Owner 授权会话。

5)、替代实体授权数据。

6)、终止 AP 相关所有会话。

接口：

输入数据格式：

标识	数据长度	命令码	协议 ID	新授权数据	实体类型	所有者授权会话句柄	所有者授权数据验证码
2B	4B	4B	2B	32B	2B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ChangeAuthOwner 所定义的固定值

——协议 ID 为 TCM_PID_AP 所定义的固定值

——新授权数据为被加密传输授权实体授权数据 TCM_ENCAUTH

——实体类型为需要改变实体的类型，值为 TCM_ET_OWNER 或 TCM_ET_SMK。TCM_ENTITY_TYPE

——所有者授权会话句柄 TCM_AUTHHANDLE

——所有者授权数据验证码

输出数据格式：

标识	数据长度	返回码	所有者授权数据验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——所有者授权数据验证码

授权数据验证码：所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	协议 ID	新授权数据	实体类型	序列号
4B	2B	32B	2B	4B
1S	2S	3S	4S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.9 非易失性存储管理

5.9.1 存储区定义 TCM_NV_DefineSpace

功能描述：

该命令定义 NV 空间。操作如下：

1） 如果输入的 pubInfo -> nvIndex 等于 TPM_NV_INDEX_LOCKandtag＝TPM_TAG_RQU_COMMAND;则设置 TPM_PERMANENT_FLAGS -> nvLocked 标记位为 TRUE;返回 TCM_SUCCESS;

2） 如果 TPM_PERMANENT_FLAGS -> nvLocked 为 FALSE,则只验证 NV 允许的最大写次数;

3） 如果输入的 pubInfo -> nvIndex 对应的 D 标记为 1 或者 pubInfo -> nvIndex＝＝TPM_NV_INDEX0 则返回错误;

4） 如果 tag＝TPM_TAG_RQU_AUTH1_COMMAND

则验证 Owner 授权会话,并使用授权会话共享密钥解密 NV 授权数据;

否则验证验证物理现场授权;

验证没有 Owner 下 NV 允许的最大写次数;

这种条件下输入的授权数据为明文。

5） 如果 pubInfo -> nvIndex 指向一个已定义的 NV 空间;

a） 根据该空间创建 TPM_NV_DATA_SENSITIVED1;

b） 如果 D1 -> attributes 指定了 TPM_NV_PER_GLOBALLOCK 属性,如果 TPM_STCLEAR_FLAGS -> bGlobalLock 为真则返回 TPM_AREA_LOCKED;

c） 如果 D1 -> attributes 指定 TPM_NV_PER_WRITE_STCLEAR 属性,如果 D1 -> pubInfo -> bWriteSTClear 为真则返回 TPM_AREA_LOCKED;

d） 无效 D1 对应的 NV 空间,无效 D1 相关的会话;

e） 如果 pubInfo -> dataSize 为零表明释放该 NV 空间成功。

6） 验证 PCR 信息;

7） 验证 NV 属性;

8） 创建 TPM_NV_DATA_SENSITIVE 结构,设置其授权数据,分配 NV 空间。

接口：

本接口有物理现场授权和一个授权两种情况。

1） 物理现场授权

输入数据格式：

标识	数据长度	命令码	NV 空间的公开信息	加密的授权数据
2B	4B	4B	可变	32B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_DefineSpace 所定义的固定值。

——定义的 NV 空间的公开信息,参照 TCM_NV_DATA_PUBLIC 数据结构

——加密的授权数据,用于设置该部分空间的授权数据

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

1) 一个授权

输入数据格式:

标识	数据长度	命令码	NV 空间的公开信息	加密的授权数据	授权会话句柄	授权数据验证码
2B	4B	4B	可变	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_DefineSpace 所定义的固定值。

——定义的 NV 空间的公开信息,参照 TCM_NV_DATA_PUBLIC 数据结构

——加密的授权数据,用于设置该部分空间的授权数据

——授权会话句柄

——所有者授权数据验证码

输出数据格式:

标识	数据长度	返回码	授权数据验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——所有者授权数据验证码

授权数据验证码:所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	NV 空间的公开信息	加密的授权数据	序列号
4B	可变	32B	4B
1S	2S	3S	2H1

输出验证码计算:

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.9.2 数据写入

5.9.2.1 所有者/物理现场授权数据写入 TCM_NV_WriteValue

功能描述:

该命令向指定 NV 区域写入数据,操作如下:

1) 如果 TCM_PERMANENT_FLAGS -> nvLocked 为 FALSE

则只验证 NV 允许的最大写次数;

2) 如果 nvIndex 为 TCM_NV_INDEX0 则:

a. 如果 dataSize 不等于 0,则返回 TPM_BADINDEX;

b. 设置 TCM_STCLEAR_FLAGS -> bGlobalLock 为 TRUE;

c. 返回 TCM_SUCCESS。

3) 定位 nvIndex 对应的 NV 空间 TCM_NV_DATA_AREAD1

如果 tag=TCM_TAG_RQU_AUTH1_COMMAND 则

a. 如果 D1 -> permission -> TCM_NV_PER_OWNERWRITE 为 FALSE 则返回 TCM_AUTH_CONFLICT;

b. 验证 Owner 授权。

否则

a. 如果 D1 -> permission -> TCM_NV_PER_OWNERWRITE 为 FALSE 则返回 TCM_AUTH_CONFLICT;

b. 验证没有 Owner 下 NV 允许的最大写次数。

4) 验证指定的 NV 属性,如 TCM_NV_PER_PPWRITE、TCM_NV_PER_PPWRITE 等;

5) 验证 PCR 信息;

6) 把数据写入 nvindex 和偏移量指定的 NV 空间。

接口:

本接口有零授权和一个授权两种情况。

1) 零授权

输入数据格式:

标识	数据长度	命令码	NV 索引	偏移量	要写入的数据长度	要写入的数据
2B	4B	4B	4B	4B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_WRITEVALUE 所定义的固定值

——要写入的 NV 空间索引

——NV 空间的偏移量

——要写入的数据大小

——要写入的数据

输出数据格式:

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

1) 一个授权

输入数据格式:

标识	数据长度	命令码	NV 空间索引	偏移量	要写入的数据大小	要写入的数据	授权会话句柄	授权会话验证码
2B	4B	4B	4B	4B	4B	可变	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_WRITEVALUE 所定义的固定值

——要写入的 NV 空间索引

——NV 空间的偏移量

——要写入的数据大小

——要写入的数据

——Owner 授权会话的句柄

——所有者授权数据验证码

输出数据格式：

标识	数据长度	返回码	Owner 授权会话验证信息
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——所有者授权数据验证码

授权数据验证码:所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	NV 空间索引	偏移量	要写入的数据大小	要写入的数据	序列号
4B	4B	4B	4B	可变	4B
1S	2S	3S	4S	5S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.9.2.2 NV 授权数据写入 TCM_NV_WriteValueAuth

功能描述：

该命令向指定 NV 区域写入数据,操作如下：

1) 定位 nvIndex 对应的 NV 空间 TCM_NV_DATA_AREAD1；

2) 如果 D1 -> permission -> TCM_NV_PER_OWNERWRITE 为 FALSE 则返回 TCM_AUTH_CONFLICT；

3) 验证 NV 空间授权数据；

4) 验证 PCR 信息；

5) 验证指定的 NV 属性,如 TCM_NV_PER_PPWRITE、TCM_NV_PER_PPWRITE、TCM_NV_PER_GLOBALLOCK、TCM_NV_PER_WRITE_STCLEAR 等；

6) 把数据写入 nvindex 和偏移量指定的 NV 空间。

接口：

输入数据格式：

标识	数据长度	命令码	NV 索引	偏移量	要写入的输入数据大小	要写入的输入数据	授权会话句柄	授权会话验证码
2B	4B	4B	4B	4B	4B	可变	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_WRITEVALUEAUTH 所定义的固定值
——要写入的 NV 空间索引
——NV 空间的偏移量
——要写入的数据大小
——要写入的数据
——NV 空间授权会话的句柄
——NV 空间授权数据验证码

输出数据格式：

标识	数据长度	返回码	NV 授权会话验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——NV 空间授权数据验证码

授权数据验证码：NV 空间授权

密钥为使用 NV 空间授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	NV 空间索引	偏移量	要写入的数据大小	要写入的数据	序列号
4B	4B	4B	4B	可变	4B
1S	2S	3S	4S	5S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.9.3 数据读出

5.9.3.1 所有者/物理现场授权数据读出 TCM_NV_ReadValue

功能描述：

该命令读取指定 NV 区域的数据，操作如下：

1) 验证 Owner 授权会话，如果没有 Owner，则验证其它的保护属性；
2) 从 NV 空间读取数据；
3) 如果 TPM_PERMANENT_FLAGS－＞nvLocked 为 FALSE

则只验证 NV 允许的最大写次数；

4） 定位 nvIndex 对应的 NV 空间 TPM_NV_DATA_AREAD1；

5） 如果 tag＝TPM_TAG_RQU_AUTH1_COMMAND 则

a. 如果 D1 -> TPM_NV_PER_OWNERREAD 为 FALSE，则返回 TPM_AUTH_CONFLICT；

b. 验证 Owner 授权会话。

否则：

a. 如果 D1 -> TPM_NV_PER_AUTHREAD 为真，则返回 TPM_AUTH_CONFLICT；

b. 如果 D1 -> TPM_NV_PER_OWNERREAD 为真，则返回 TTPM_AUTH_CONFLICT。

6） 验证指定的 NV 属性，如 TPM_NV_PER_PPREAD、TPM_NV_PER_READ_STCLEAR 等。

7） 验证 PCR 信息。

8） 从 nvindex、偏移量对应的 NV 空间读取数据。

接口：

本接口有零授权和一个授权两种情况。

1） 零授权

输入数据格式：

标识	数据长度	命令码	NV 索引	偏移量	要读取的数据大小
2B	4B	4B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReadValue 所定义的固定值

——要写入的 NV 空间索引

——NV 空间的偏移量

——要读取的数据大小

输出数据格式：

标识	数据长度	返回码	读取的数据大小	读取的数据
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果（见返回码定义表）

——读取的数据大小

——读取的数据。

1） 一个授权

输入数据格式：

标识	数据长度	命令码	NV 索引	偏移量	要读取数据大小	授权会话句柄	授权会话验证码
2B	4B	4B	4B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReadValue 所定义的固定值

——要写入的 NV 空间索引

——NV 空间的偏移量

——要读取的数据大小

——Owner 授权会话的句柄

——Owner 授权数据验证码

输出数据格式：

标识	数据长度	返回码	要读取的数据大小	读取的数据	Owner 授权会话验证信息
2B	4B	4B	4B	可变	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——读取的数据大小

——读取的数据

——Owner 授权数据验证码

授权数据验证码:所有者授权

密钥为使用所有者授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	NV 索引	偏移量	要读取数据大小	序列号
4B	4B	4B	4B	4B
1S	2S	3S	4S	2H1

输出验证码计算：

返回码	命令码	要读取的数据大小	读取的数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

5.9.3.2 NV 授权数据读出 TCM_NV_ReadValueAuth

功能描述：

该命令读取指定 NV 区域的数据,操作如下：

1) 定位 nvIndex 对应的 NV 空间 TPM_NV_DATA_AREAD1；

2) 如果 D1 -> TPM_NV_PER_AUTHREAD 为 FALSE 则返回 TPM_AUTH_CONFLICT；

3) 验证 NV 空间授权数据；

4) 验证 PCR 信息；

5) 验证指定的 NV 属性,如 TPM_NV_PER_PPREAD 等；

6) 从 nvindex、偏移量对应的 NV 空间读取数据。

接口：

输入数据格式：

标识	数据长度	命令码	NV 索引	偏移量	读取数据大小	授权会话句柄	授权会话验证码
2B	4B	4B	4B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_READVALUEAUTH 所定义的固定值
——要写入的 NV 空间索引
——NV 空间的偏移量
——要读取的数据大小
——NV 授权会话的句柄
——NV 空间授权数据验证码

输出数据格式：

标识	数据长度	返回码	读取的数据大小	读取的数据	NV 授权会话验证码
2B	4B	4B	4B	可变	32B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——读取的数据大小
——读取的数据
——NV 空间授权数据验证码

授权数据验证码：NV 空间授权

密钥为使用 NV 空间授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	NV 索引	偏移量	要读取数据大小	序列号
4B	4B	4B	4B	4B
1S	2S	3S	4S	2H1

输出验证码计算：

返回码	命令码	要读取的数据大小	读取的数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

5.10 运行环境管理

5.10.1.1 保存上下文 TCM_SaveContext

功能描述：

该命令将内部资源保存到 TCM 外部。成功执行此命令后 TCM 自动释放会话。

1) TCM_CONTEXT_SENSITIVE 信息由厂家自定义；

2) 使用 TCM_TakeOwnership 产生的 TCM_PERMANENT_DATA -> contextKey 加密 TCM

_CONTEXT_SENSITIVE；

3） 填充 TPM_CONTEXT_BLOB 保存到 TCM 外部。

接口：

输入数据格式：

标识	数据长度	命令码	资源句柄	资源类型	标签
2B	4B	4B	4B	4B	16B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SaveContext 所定义的固定值

——资源句柄为即将要保存的资源的句柄

——资源类型为即将要保存资源的类型。资源类型包括 TCM_RT_KEY、TCM_RT_AUTH 和 TCM_RT_TRANS 这三种类型

——标签为表征保存会话的标识

输出数据格式：

标识	数据长度	返回码	输出的要保存数据长度	输出的要保存数据
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果

——输出的要保存数据长度为已被保存到外部的所有实际数据长度

——输出的要保存数据

5.10.1.2 加载上下文 TCM_LoadContext

功能描述：

此命令将先前存储到 TCM 外部的内容再载入到 TCM 内部。操作如下：

1） 使用 TCM_PERMANENT_DATA -> contextKey 解密 TCM_CONTEXT_SENSITIVE；

2） 从新加载之前保存的 TPM_RT_KEY 或者 contextNonce；

3） 判断 keepHandle 是否恢复为以前使用的句柄，否则重新产生新的句柄；

4） 将生成的句柄返回。

接口：

输入数据格式：

标识	数据长度	命令码	实体句柄	保存句柄	以前保存的数据长度	以前保存的数据
2B	4B	4B	4B	1B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节长度

——命令码为 TCM_ORD_LoadContext 所定义的固定值

——实体句柄为 TCM 用来定位会话密钥的句柄

——以前保存的数据长度

——以前保存的数据

输出数据格式：

标识	数据长度	返回码	资源句柄
2B	4B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果
——资源句柄为最终生成的句柄

5.10.1.3 释放资源 TCM_FlushSpecific

功能描述：
该命令释放指定句柄的资源。
接口：
输入数据格式：

标识	数据长度	命令码	资源句柄	资源类型
2B	4B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_FlushSpecSetic 所定义的固定值
——资源句柄为指向将要被释放的资源的句柄
——资源类型为将要被释放的资源的类型，资源类型包括 TCM_RT_CONTEXT、TCM_RT_KEY、TCM_RT_AUTH 和 TCM_RT_TRANS 这四种类型

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)

5.11 审计

该功能可选，由厂商自行定义。

5.11.1.1 获取审计摘要 TCM_GetAuditDigest

功能描述：
该命令返回当前的审计摘要以及审计列表。
1) 设置审计摘要为 TCM_STANY_DATA -> auditDigest；
2) 设置设计单调计数器为 TCM_PERMANENT_DATA -> auditMonotonicCounter；
3) 根据输入参数 startOrdinal 决定要返回的审计列表；
4) 如果审计列表没有全部返回则设置全部返回标记为 TRUE。
接口：
输入数据格式：

标识	数据长度	命令码	开始序列号
2B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_GetAuditDigest 所定义的固定值
——开始序列号表明从何处开始返回审计列表
输出数据格式：

标识	数据长度	返回码	审计单调计数器	审计摘要	是否全部返回的标记	返回的命令列表长度	返回的命令列表
2B	4B	4B	10B	32B	1B	4B	可变

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——返回设计单调计数器当前值
——审计摘要
——指明返回命令列表是否包含所有请求命令
——返回的命令列表长度
——返回的命令列表内容

5.11.1.2 获取带签名审计摘要 TCM_GetAuditDigestSigned

功能描述：
返该命令返回当前的审计命令列表及其签名。
1) 验证签名密钥授权数据；
2) 创建签名结构 TCM_SIGN_INFOD1；
3) 创建审计命令列表 D3,返回审计列表摘要为 D4＝SM3(D3)；
4) 返回审计事件摘要为 TCM_STANY_DATA -> auditDigest；
5) 返回审计计数器为 TCM_PERMANENT_DATA -> auditMonotonicCounter；
6) 创建 D2＝auditDigest||counterValue||D4；
   - 设置 D1 -> data 为 D2；
   - 使用签名密钥签名 D1,作为返回的签名数据。
7) 根据 closeAudit 标记决定是否重新开始审计,也即设置 TCM_STANY_DATA -> auditDigest＝NULLS。

接口：
本接口只有一个授权。
输入数据格式：

标识	数据长度	命令码	签名密钥句柄	审计摘要结束标记	抗重放参数	授权会话句柄	授权数据验证码
2B	4B	4B	4B	1B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_GetAuditDigestSigned 所定义的固定值

——用于标记签名摘要信息是否重新开始计算
——用于抗重放攻击
——授权会话的句柄
——授权会话的校验值
——授权数据验证码
输出数据格式：

标识	数据长度	返回码	审计单调计数器	审计事件摘要	审计命令摘要
2B	4B	4B	10B	32B	32B

签名数据长度	签名值	授权数据验证码
4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果
——计数值为审计计数器的值
——审计事件摘要为所有的审计事件日志
——审计命令摘要为所有审计命令的摘要
——签名数据长度
——签名值为对当前域进行的签名
——授权数据验证码

授权数据验证码：密钥授权
密钥为载入的可进行数字签名的密钥。
输入验证码计算：

命令码	审计摘要结束标记	抗重放　参数	序列号
4B	1B	32B	4B
1S	2S	3S	2H1

输出验证码计算：

返回码	命令码	审计单调计数器	审计事件摘要	审计命令摘要	签名数据长度	签名值	序列号
4B	4B	10B	32B	32B	4B	可变	4B
1S	2S	3S	4S	5S	6S	7S	2H1

5.11.1.3　设置命令审计状态　TCM_SetOrdinalAuditStatus

功能描述：
设置一个给定命令的审计标志，必须判断指定命令是否可被设置。
命令号为 TCM_ORD_GetAuditDigest 的命令是不能被设置为被审计的。
接口：
本接口只有一个授权的情况。
输入数据格式：

标识	数据长度	命令码	审计命令码	审计标志	所有者授权会话句柄	所有者授权数据验证码
2B	4B	4B	4B	1B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_SetOrdinalAuditStatus 所定义的固定值
——审计命令码为需要设置的命令号
——审计标志:“1”代表需要被审计,“0”代表不需要被审计。
——所有者授权会话句柄
——所有者授权数据验证码
输出数据格式:

标识	数据长度	返回码	所有者授权数据验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——所有者授权数据验证码

授权数据验证码:所有者授权
密钥为所有者使用 AP 会话产生的共享秘密数据。
输入验证码计算:

命令码	审计命令码	审计状态	序列号
4B	4B	1B	4B
1S	2S	3S	2H1

输出验证码计算:

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.12 时钟

5.12.1.1 获取时钟节拍 TCM_GetTicks

功能描述:
获取 TCM 的当前时钟节拍。
接口:
输入数据格式:

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_GetTicks 所定义的固定值

输出数据格式：

标识	数据长度	返回码	时钟节拍
2B	4B	4B	44B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——时钟节拍为一个 TCM_CURRENT_TICKS 的数据结构

5.12.1.2 设置时间戳 TCM_TickStampBlob

功能描述：

对一块数据进行时间戳操作。

1) 创建一个 TCM_SIGN_INFO 结构的变量,假设为 H;

2) 将 H 的成员变量设置成默认的数据,然后设置 H1 ->fixed="TSTP";设置 H1 -> replay=反重放攻击数据;设置 H1 -> data=摘要||当前时钟节拍;设置 H1 -> dataLen=H1 -> data 的长度。最后对 H 进行签名作为计算的时间戳。

接口：

本接口有零授权和一个授权两种情况。

1) 零授权

输入数据格式：

标识	数据长度	命令码	签名密钥句柄	抗重放攻击数据	摘要
2B	4B	4B	4B	32B	32B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_TickStampBlob 所定义的固定值

——签名密钥句柄为执行签名操作的密钥的 TCM 内部句柄

——抗重放攻击数据

——摘要为需要被执行时间戳的数据

输出数据格式：

标识	数据长度	返回码	时间戳	签名长度	签名信息	
2B	4B	4B	44B	4B	可变	

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——时间戳为 TCM 当前的时间信息

——签名长度为签名信息的长度

——签名信息为本操作的签名结果

2) 一个授权

输入数据格式：

标识	数据长度	命令码	签名密钥句柄	抗重放攻击数据	摘要	密钥授权会话句柄	密钥授权数据验证码
2B	4B	4B	4B	32B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_TickStampBlob 所定义的固定值
——签名密钥句柄为执行签名操作的密钥的 TCM 内部句柄
——抗重放攻击数据
——摘要为执行时间戳的对象数据
——密钥授权会话句柄
——密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	时间戳	签名长度	签名信息	密钥授权数据验证码
2B	4B	4B	32B	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——时间戳为 TCM 当前的时间信息
——签名长度为签名信息的长度
——签名信息为本操作的签名结果
——密钥授权数据验证码

授权数据验证码：密钥授权

密钥为签名密钥使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	抗反重放攻击数据	摘要	序列号
4B	32B	32B	4B
1S	2S	3S	2H1

输出验证码计算：

返回码	命令码	时钟节拍	签名长度	签名信息	序列号
4B	4B	32B	4B	可变	4B
1S	2S	3S	4S	5S	2H1

5.13 计数器

5.13.1.1 创建计数器 TCM_CreateCounter

功能描述：

创建一个新的单调计数器，并赋予这个计数器授权数据与标签。每次创建一个新的计数器时，赋予内部最大计数器的值。TCM 至少支持同时拥有 4 个计数器。

计数器信息是一个 TCM_COUNTER_VALUE 的数据结构，包含计数器标签与计数器初始值。

授权数据使用所有者使用 AP 会话产生的共享秘密数据生成的公享秘密数据进行加密。

接口：

本接口只有一个授权的情况。

输入数据格式：

标识	数据长度	命令码	被加密的计数器授权数据	标签	所有者授权数据验证码
2B	4B	4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_CreateCounter 所定义的固定值
——被加密的计数器授权数据
——标签为计数器的标签
——所有者授权数据验证码
输出数据格式：

标识	数据长度	返回码	计数器 ID	计数器值信息	所有者授权数据验证码
2B	4B	4B	4B	10B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——计数器 ID 为新创建的计数器的 ID
——计数器值信息为计数器的初始值
——所有者授权数据验证码

授权数据验证码：密钥授权

密钥为签名密钥使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	授权数据	标签	序列号
4B	32B	4B	4B
1S	2S	3S	2H1

输出验证码计算：

返回码	命令码	计数器 ID	计数器值信息	序列号
4B	4B	4B	10B	4B
1S	2S	3S	4S	2H1

5.13.1.2 计数器递增 TCM_IncrementCounter

功能描述：
将一个计数器的值增加 1，并且选择这个计数器。输入 ID 为零时，采用当前计数器。使用 TCM_Startup(ST_CLEAR)命令后，可以重新选择。
接口：
本接口只有一个授权的情况。
输入数据格式：

标识	数据长度	命令码	计数器 ID	计数器授权数据验证码
2B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_IncrementCounter 所定义的固定值

——计数器 ID 为需要增加/选定的计数器 ID

——计数器授权数据验证码

输出数据格式：

标识	数据长度	返回码	计数器值	计数器授权数据验证码
2B	4B	4B	10B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——计数器值为增加后的计数器的值

——计数器授权数据验证码

授权数据验证码:计数器授权

密钥为计数器使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	计数器 ID	序列号
4B	4B	4B
1S	2S	2H1

输出验证码计算：

返回码	命令码	计数器值信息	序列号
4B	4B	10B	4B
1S	2S	3S	2H1

5.13.1.3 读取计数器 TCM_ReadCounter

功能描述：

读取计数器中的计数值,操作如下：

1） 验证待读取的计数器是否有效。

2） 读取计数器的计数值。

接口：

输入数据格式：

标识	数据长度	命令码	计数器 ID
2B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReadCounter 所定义的固定值

——计数器 ID 为待读取的计数器编号

输出数据格式：

标识	数据长度	返回码	计数器值
2B	4B	4B	10B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——计数值为返回的计数器的计数值。

5.13.1.4 释放计数器

5.13.1.4.1 计数器授权释放 TCM_ReleaseCounter

功能描述:

使用计数器授权数据释放计数器,操作如下:

1) 验证计数器授权数据建立的授权会话;

2) 无效该计数器相关的信息,包括授权会话等;

3) 如果 TCM_STCLEAR_DATA -> countID 指定的计数器为该计数器,则设置 TCM_STCLEAR_DATA -> countID 指向一个非法值。

接口:

本接口只有一个授权。

输入数据格式:

标识	数据长度	命令码	计数器 ID	计数器授权句柄	计数器授权会话验证码
2B	4B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReleaseCounter 所定义的固定值

——要释放的计数器 ID

——计数器的授权会话对应的句柄

——计数器授权数据验证码

输出数据格式:

标识	数据长度	返回码	计数器授权会话验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——计数器授权数据验证码

授权数据验证码:计数器授权

密钥为使用计数器授权 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	计数器 ID	序列号
4B	4B	4B
1S	2S	2H1

输出验证码计算:

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

5.13.1.4.2 所有者授权释放 TCM_ReleaseCounterOwner

功能描述：

使用 Owner 授权数据释放计数器，操作如下：

1） 验证 Owner 授权数据建立的授权会话；

2） 无效该计数器相关的信息，包括授权会话等；

3） 如果 TCM_STCLEAR_DATA -> countID 指定的计数器为该计数器，则设置 TCM_STCLEAR_DATA -> countID 指向一个非法值。

接口：

本接口只有一个授权。

输入数据格式：

标识	数据长度	命令码	计数器 ID	Owner 授权句柄	Owner 授权会话验证码
2B	4B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReleaseCounterOwner 所定义的固定值

——要释放的计数器 ID

——Owner 的授权会话对应的句柄

——Owner 授权数据验证码

输出数据格式：

标识	数据长度	返回码	Owner 授权会话验证码
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——Owner 授权数据验证码

授权数据验证码：所有者授权

密钥为使用所有者授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	计数器 ID	序列号
4B	4B	4B
1S	2S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B

1S	2S	2H1

6 平台身份标识与认证功能

6.1 密码模块密钥管理

6.1.1 创建密码模块密钥

6.1.1.1 创建不可撤销秘密模块密钥 TCM_CreateEndorsementKeyPair

功能描述：

创建不可撤消 EK，操作如下：

1） 如果 EK 已存在，则返回错误；

2） 验证输入的 EK 参数；

3） 产生 EK 并保存；

4） 计算校验和 checksum＝SM3(PUBEK||antiReplay)；

5） 设置 TCM_PERMANENT_FLAGS -> CEKPUsed 为 TRUE；

6） 设置 TCM_PERMANENT_FLAGS -> enableRevokeEK 为 FALSE。

接口：

输入数据格式：

标识	数据长度	命令码	防重放参数	输入的密钥参数
2B	4B	4B	32B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_CreateEndorsementKeyPair 所定义的固定值

——防重放参数，用于计算校验和

——用于创建 EK 的密钥参数结构 TCM_KEY_PARMS

输出数据格式：

标识	数据长度	返回码	EK 公钥信息	校验值
2B	4B	4B	可变	32

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——返回的 EK 公钥结构 TCM_PUBKEY

——返回的校验值，用于防止重放攻击

6.1.1.2 创建可撤消的密码模块密钥 TCM_CreateRevocableEK

功能描述：

创建可撤销 EK，操作如下：

1） 如果 EK 已存在，则返回错误；

2） 执行 TCM_CreateEndorsementKeyPair；

3） 设置 TCM_PERMANENT_FLAGS -> enableRevokeEK 为 TRUE；

4） 如果标记位为 TRUE；

则设置 TCM_PERMANENT_DATA -> EKreset 为随机数；

否则设置 TCM_PERMANENT_DATA -> EKreset 为 inputEKreset。

接口：

输入数据格式：

标识	数据长度	命令码	防重放参数	密钥信息	标记位	验证信息
2B	4B	4B	32B	可变	1B	32B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_CreateEndorsementKeyPair 所定义的固定值

——防重放参数，用于计算校验和

——用于创建 EK 的密钥参数

——标记位，用来决定输出的验证信息是随机产生还是通过输入

——输入的验证信息，用于撤销 EK 时验证

输出数据格式：

标识	数据长度	返回码	EK 公钥信息	校验和	验证信息
2B	4B	4B	可变	32	32

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——返回的 EK 公钥

——返回的校验值，用于防止重放攻击

——返回的验证信息，用于撤销 EK 时验证

6.1.2 撤消密码模块密钥 TCM_RevokeTrust

功能描述：

该命令清除 EK 并把 TCM 设置为一个缺省状态，操作如下：

1) 验证 TCM_PERMANENT_FLAGS -> enableRevokeEK 是否为真，若不为真则不能撤销 EK；
2) 验证输入的 EKReset 是否等于 TCM_PERMANENT_DATA -> EKReset，如不等则返回错误；
3) 需要物理现场验证；
4) 执行 TCM_OwnerClear(无需 Owner 授权)；
5) 清除 EK 及其相关状态。

接口：

该命令需要物理现场授权。

输入数据格式：

标识	数据长度	命令码	验证信息
2B	4B	4B	32B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_RevokeTrust 所定义的固定值

——用户撤销 EK 时的验证信息

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

6.1.3 读取密码模块密钥公钥

6.1.3.1 不授权读秘码模块密钥公钥 TCM_ReadPubEK

功能描述：

返回 EK 的公钥部分,操作如下：

1) 如果 TCM_PERMANENT_FLAGS -> readPubek 为 FALSE,则返回错误 TCM_DISABLED_CMD；

2) 如果 EK 不存在则返回 TCM_NO_ENDORSEMENT；

3) 计算校验和 SM3(EK 公钥||抗重放参数)；

4) 返回 EK 公钥。

接口：

输入数据格式：

标识	数据长度	命令码	抗重放参数
2B	4B	4B	32B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReadPubek 所定义的固定值

——用于防止重放攻击

输出数据格式：

标识	数据长度	返回码	EK 公钥	校验和
2B	4B	4B	可变	32

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——返回的 EK 公钥信息

——返回的校验和,用于防止重放攻击

6.1.3.2 授权读秘码模块密钥公钥 TCM_OwnerReadInternalPub

功能描述：

在 Owner 授权的条件下,读取 EK 的公钥部分,操作如下：

1) 验证 Owner 授权数据；

2) 验证 keyHandle 是否为 TCM_KH_EK,若是则返回 EK 公钥。

接口：

本接口只有一个授权。

输入数据格式：

标识	数据长度	命令码	EK 密钥句柄	授权句柄	授权会话验证码
2B	4B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_OwnerReadInternalPub 所定义的固定值

——EK 的固定密钥句柄

——授权会话产生的授权句柄

输出数据格式：

标识	数据长度	返回码	EK 公钥	授权会话验证码
2B	4B	4B	可变	32

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——返回的 EK 公钥

授权会话验证码:所有者授权

密钥为使用所有者授权 AP 会话产生的共享秘密数据

输入验证码计算：

命令码	EK 密钥句柄	序列号
4B	4B	4B
1S	2S	2H1

输出验证码计算：

返回码	命令码	EK 公钥	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

6.2 平台身份密钥管理

6.2.1 创建平台身份 TCM_MakeIdentity

功能描述：

创建 PIK 密钥及 PIK 证书请求,操作如下：

1) 验证输入的 PIK 密钥参数 idKeyParams；
2) 验证 Owner 授权；
3) 验证 SMK 授权；
4) 验证密钥属性,keyUsage 必须为 TCM_SM2KEY_IDENTITY,migratable 必须为 FALSE；
5) 解密 PIK 授权数据；
6) 创建 TCM_KEY 结构,设置其 PCR 属性；
7) 创建 PIK 密钥,设置其迁移授权数据为 TCM_PERMANENT_DATA -> TCMProof,设置其授权数据为解密后的授权数据；
8) 使用 SMK 加密 PIK 私钥；

9) 创建证书请求的相关信息，使用 PIK 私钥签名 TCM_IDENTITY_CONTENTS，TCM_IDENTITY_CONTENTS 结构包括输入的身份标识和可信方公钥的摘要以及 PIK 公钥。

接口：

本接口有两个授权。

输入数据格式：

标识	数据长度	命令码	加密的 PIK 授权数据	身份标识和可信方公钥的摘要	PIK 密钥参数	SMK 授权会话句柄	SMK 授权数据验证码	Owner 授权会话句柄	Owner 授权数据验证码
2B	4B	4B	32B	32B	可变	4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_MakeIdentity 所定义的固定值

——加密的 PIK 授权数据，用于给 PIK 设置授权数据

——身份标识和可信方公钥的摘要，用于产生证书请求，为 TCM_CHOSENID_HASH 结构数据的摘要值

——PIK 密钥参数，为 TCM_KEY 结构数据

——SMK 授权会话句柄

——SMK 授权数据验证码

——Owner 的授权会话句柄

——Owner 授权数据验证码

输出数据格式：

标识	数据长度	返回码	PIK	用于产生证书请求的信息大小	用于产生证书请求的信息	SMK 授权会话验证码	Owner 授权会话验证码
2B	4B	4B	可变	4B	可变	32B	32B

——标识为 TCM_TAG_RSP_AUTH2_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——PIK 密钥，为 TCM_KEY 结构数据。

——用于产生证书请求的信息大小

——用于产生证书请求的信息，是对 TCM_IDENTITY_CONTENTS 结构数据用 PIK 进行签名的结果

——SMK 授权数据验证码

——Owner 授权数据验证码

授权会话验证码：PIK 授权

密钥为使用 PIK 授权 AP 会话产生的共享秘密数据

输入验证码计算：

命令码	PIK 密钥句柄	可信方返回的加密信息大小	可信方返回的加密信息	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

输出验证码计算

返回码	命令码	对称密钥	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

授权会话验证码:所有者授权

密钥为使用 Owner 授权 AP 会话产生的共享秘密数据

输入验证码计算:

命令码	加密的 PIK 授权数据	身份标识和可信方公钥的摘要	PIK 密钥参数	序列号
4B	32B	32B	4B	4B
1S	2S	3S	4S	2H2

输出验证码计算:

返回码	命令码	PIK	用于产生证书请求的信息大小	用于产生证书请求的信息	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H2

6.2.2 激活平台身份 TCM_ActivateIdentity

功能描述:

获取加密 PIK 证书的对称密钥,操作如下:

1) 验证 Owner 授权会话;
2) 验证 PIK 密钥的使用属性是否为 TCM_SM2KEY_IDENTITY;
3) 验证 PIK 授权会话;
4) 计算 SM3(PIK 公钥)得到 H1,使用 EK 私钥解密可信方返回的加密信息得到 B1,验证 H1 是否等于 B1 -> idDigest,如果等于则设置返回对称密钥为 B1 -> sessionKey。

接口:

本接口有两个授权。

输入数据格式:

标识	数据长度	命令码	PIK 密钥句柄	可信方返回的加密信息大小	可信方返回的加密信息	PIK 密钥授权句柄	PIK 密钥授权会话校验码	Owner 授权句柄	Owner 授权会话校验码
2B	4B	4B	4B	4B	可变	4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ActivateIdentity 所定义的固定值。

——已加载的 PIK 密钥句柄。

——可信方返回的加密信息长度。

——可信方返回的加密信息,可信方用 EK 公钥对 TCM_ASYM_CA_CONTENTS 结构数据进行加密的结果。

——PIK 的授权会话对应的句柄

——PIK 授权数据验证码

——Owner 的授权会话对应的句柄

——Owner 授权数据验证码计算如下

输出数据格式：

标识	数据长度	返回码	对称密钥	PIK 授权会话验证码	Owner 授权会话验证码
2B	4B	4B	可变	32B	32B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——返回的对称密钥,为 TCM_SYMMETRIC_KEY 结构数据,用于解密 PIK 证书

——PIK 授权数据验证码

——Owner 授权数据验证码

授权数据验证码:PIK 授权

密钥为使用 PIK 授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	PIK 密钥句柄	可信方返回的加密信息大小	可信方返回的加密信息	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

输出验证码计算

返回码	命令码	对称密钥	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

授权数据验证码:Owner 授权

密钥为使用 Owner 授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	PIK 密钥句柄	可信方返回的加密信息大小	可信方返回的加密信息	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H2

输出验证码计算：

返回码	命令码	对称密钥	序列号
4B	4B	可变	4B
1S	2S	3S	2H2

6.2.3 激活平台加密密钥证书 TCM_ActivatePEKCert

功能描述：

获取加密 PEK 证书的对称密钥,操作如下：

1） 验证 Owner 授权会话；

2） 使用 EK 私钥解密获取对称密钥。

接口：

本接口只有一个授权。

输入数据格式：

标识	数据长度	命令码	可信方返回的加密信息大小	可信方返回的加密信息	Owner 授权句柄	Owner 授权会话验证码
2B	4B	4B	4B	可变	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ActivatePEKCert 所定义的固定值

——可信方返回的加密信息长度

——可信方返回的加密信息，可信方用 EK 公钥加密的 TCM_SYMMETRIC_KEY 结构数据

——Owner 的授权会话对应的句柄

——Owner 授权数据验证码

输出数据格式：

标识	数据长度	返回码	对称密钥	Owner 授权会话验证码
2B	4B	4B	24B	32

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果（见返回码定义表）

——产生的对称密钥，为 TCM_SYMMETRIC_KEY 结构数据，用于解密 PEK 证书

——Owner 授权数据验证码

授权数据验证码：所有者授权

密钥为使用所有者授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	可信方返回的加密信息大小	可信方返回的加密信息	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

输出验证码计算：

返回码	命令码	对称密钥	序列号
4B	4B	24B	4B
1S	2S	3S	2H1

6.2.4 激活平台加密密钥 TCM_ActivatePEK

功能描述：

导入 PEK，并使用 SMK 加密，操作如下：

1） 验证 Owner 授权会话；

2） 验证 SMK 授权会话；

3） 使用 EK 私钥解密获取对称密钥；

4） 用对称密钥解密获取 PEK；

5） 设置 PEK 的迁移授权数据、使用授权数据以及 PCR 信息；

6） 用 SMK 加密 PEK 私钥部分。

接口：

本接口有两个授权。

输入数据格式：

标识	数据长度	命令码	加密的使用授权密钥	PEK 密钥信息	加密的 PEK 大小	加密的 PEK	＜续＞
2B	4B	4B	32B	可变	4B	可变	

加密的对称密钥大小	加密的对称密钥	SMK 授权句柄	SMK 授权会话验证码	Owner 授权句柄	Owner 授权会话校验值
4B	可变	4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ActivatePEK 所定义的固定值。

——加密的使用授权密钥，用于设置 PEK 使用授权数据

——PEK 密钥信息，TCM_KEY 结构数据

——加密的 PEK 大小。

——加密的 PEK（TCM_KEY 结构数据）

——加密的对称密钥长度。

——加密的对称密钥数据。

——SMK 的授权会话对应的句柄。

——SMK 授权数据验证码

——Owner 的授权会话对应的句柄。

——Owner 授权数据验证码

输出数据格式：

标识	数据长度	返回码	PEK	SMK 授权会话验证码	Owner 授权会话验证码
2B	4B	4B	可变	32B	32

——标识为 TCM_TAG_RSP_AUTH2_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果（见返回码定义表）

——返回的 PEK（TCM_KEY 结构数据）

——SMK 授权数据验证码

——Owner 授权数据验证码

授权数据验证码：SMK 授权

密钥为使用 SMK 授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	加密的使用授权密钥	PEK 密钥信息	加密的 PEK 大小	加密的 PEK	加密的对称密钥大小	加密的对称密钥	序列号
4B	32B	可变	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	6S	7S	2H1

输出验证码计算：

返回码	命令码	PEK	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

授权数据验证码：所有者授权

密钥为使用所有者授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	加密的使用授权密钥	PEK 密钥信息	加密的 PEK 大小	加密的 PEK	加密的对称密钥大小	加密的对称密钥	序列号
4B	32B	可变	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	6S	7S	2H1

输出验证码计算：

返回码	命令码	PEK	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

7 平台数据保护

7.1 数据保护操作

7.1.1 数据密封 TCM_Seal

功能描述：

将数据与特定的平台配置信息(PCR 值)及平台验证信息(TCM_Proof)绑定在一起生成封装数据 sealedData。操作如下：

1) 验证 sealedData 为 TCM_STORED_DATA 结构数据，TCM_STORED_DATA 主要由 TCM_PCR_INFO 结构和加密后的 TCM_SEALED_DATA 组成。
2) 将当前的指定 PCR 值的摘要存储在 TCM_PCR_INFO 结构中，将 TCM_STORED_DATA 的摘要值、平台验证信息 TCM_Proof、待封装的数据和待封装数据的授权数据存储在 TCM_SEALED_DATA 结构中并用封装操作密钥加密；
3) 最终返回 TCM_STORED_DATA 结构数据。

接口：

输入数据格式：

标识	数据长度	命令码	封装操作密钥句柄	加密的授权数据	PCR信息长度	PCR信息	待封装数据长度	待封装数据	＜续＞
2B	4B	4B	4B	32B	4B	可变	4B	可变	

授权会话句柄	授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_Seal 所定义的固定值
——封装操作密钥句柄
——加密的授权数据为被加密的封装对象的授权数据，其中加密密钥为授权会话句柄指向的共享会话密钥
——PCR 信息长度为 PCR 信息参数的长度。如果为 0，则表明无可用的 PCR 寄存器
——PCR 信息为 TCM_PCR_INFO 结构数据
——待封装数据长度为待封装数据参数的长度
——待封装数据为待封装到平台和特定 PCR 寄存器上的数据
——授权会话句柄为执行封装操作密钥的授权会话句柄
——授权数据验证码

输出数据格式：

标识	数据长度	返回码	封装数据块	＜续＞
2B	4B	4B	可变	

授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——封装数据块为经过加密的被封装数据，是 TCM_STORED_DATA 结构数据。
——授权数据验证码

授权数据验证码：密钥授权

密钥为使用封装操作密钥 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	加密的授权数据	PCR信息长度	PCR信息	待封装数据长度	待封装数据	序列号
4B	32B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	6S	2H1

输出验证码计算：

返回码	命令码	封装数据	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

7.1.2 数据解封 TCM_Unseal

功能描述：

当封装数据中的平台配置信息(PCR 值)及平台验证信息(TCM_Proof)与当前 PCR 值和 TCM_Proof 值一致时，将 TCM_Seal 命令生成的封装数据解密。操作如下：

1) 输入数据对应 TCM_STORED_DATA 结构数据，将其中加密过的 TCM_SEALED_DATA 用解封操作密钥进行解密；
2) 验证 TCM_Proof 和封装数据的授权是否正确；
3) 验证存储在 TCM_PCR_INFO 结构中的平台配置摘要值与指定的当前 PCR 寄存器的摘要值是否一致；
4) 如果这些验证都通过，则返回 TCM_SEALED_DATA 结构中的被封装数据。

接口：

输入数据格式：

标识	数据长度	命令码	解封操作密钥句柄	待解封数据	＜续＞
2B	4B	4B	4B	可变	

解封操作密钥授权会话句柄	解封操作密钥授权数据验证码	封装数据授权会话句柄	封装数据授权数据验证码
4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_Unseal 所定义的固定值
——解封操作密钥句柄为执行解封操作的密钥的句柄
——待解封数据为由 TCM_Seal 命令生成的封装数据块
——解封操作密钥授权会话句柄为执行解封操作的密钥的授权会话句柄
——解封操作密钥授权数据验证码
——封装数据授权会话句柄为被封装数据的授权会话句柄
——封装数据授权数据验证码

输出数据格式：

标识	数据长度	返回码	输出数据长度	输出数据	＜续＞
2B	4B	4B	4B	可变	

解封操作密钥授权数据验证码	封装数据授权数据验证码
32B	32B

——标识为 TCM_TAG_RSP_AUTH2_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——输出数据长度为解封后的被封装数据的长度
——输出数据为解封后的被封装数据

——解封操作密钥授权数据验证码

——封装数据授权数据验证码

授权数据验证码:解封操作密钥授权

密钥为使用解封操作密钥 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	输入数据	序列号
4B	可变	4B
1S	2S	2H1

输出验证码计算:

返回码	命令码	输出数据长度	输出数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

授权数据验证码:封装数据授权

密钥为使用封装数据 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	输入数据	序列号
4B	可变	4B
1S	2S	2H2

输出验证码计算:

返回码	命令码	输出数据长度	输出数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H2

7.2 密钥管理

7.2.1 密钥创建 TCM_CreateWrapKey

功能描述:

请求 TCM 依据输入的 TCM_KEY 结构要求的密钥属性生成密钥,操作如下:

1) 验证保护操作密钥的授权;
2) 判断密钥属性的合法性;
3) 解密得到该密钥的使用授权数据和迁移授权数据,如果密钥可迁移,其迁移授权数据为解密得到的迁移授权数据;如果密钥不可迁移,其迁移授权数据为 TCM_Proof;
4) 密钥可以与指定的 PCR 寄存器的摘要值进行绑定;
5) 对非对称密钥的私钥部分或者对称密钥用保护操作密钥进行加密保护;
6) 返回 TCM_KEY 结构数据。

接口:

输入数据格式:

标识	数据长度	命令码	保护操作密钥句柄	加密的使用授权数据	加密的迁移授权数据	密钥信息	<续>
2B	4B	4B	4B	32B	32B	可变	

保护操作密钥授权会话句柄	保护操作密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_CreateWrapKey 所定义的固定值
——保护操作密钥句柄
——加密的使用授权数据,加密密钥为使用保护操作密钥 AP 会话产生的共享会话密钥
——加密的迁移授权数据,加密密钥为使用保护操作密钥 AP 会话产生的共享会话密钥
——密钥信息为 TCM_KEY 结构的数据
——保护操作密钥授权会话句柄
——保护操作密钥授权数据验证码

输出数据格式:

标识	数据长度	返回码	创建的密钥	<续>
2B	4B	4B	可变	

保护操作密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——创建的密钥为 TCM_KEY 结构的数据
——保护操作密钥授权数据验证码

授权数据验证码:密钥授权

密钥为使用保护操作密钥 AP 会话产生的共享秘密。

输入验证码计算:

命令码	加密的使用授权数据	加密的迁移授权数据	密钥信息	序列号
4B	32B	32B	可变	4B
1S	2S	3S	4S	2H1

输出验证码计算:

返回码	命令码	创建的密钥	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

7.2.2 密钥加载 TCM_LoadKey

功能描述：

该命令把一个受保护的密钥导入 TCM 中，TCM 分配密钥句柄，操作如下：

1） 验证保护操作密钥的授权，并判断其合法性；

2） 用保护操作密钥对被加载密钥的加密部分进行解密，判断被加载密钥的属性，如果为非对称密钥，存为 TCM_STORE_ASYMKEY，如果为对称密钥，存为 TCM_STORE_SYMKEY；

3） 判断载入密钥的正确性、属性合法性、所绑定的 PCR 信息与当前平台的 PCR 值的一致性；

4） 载入密钥继承保护操作密钥是否与平台配置信息相绑定的状态；

5） 为载入密钥分配一个句柄。

接口：

本接口有零授权和一个授权两种情况。

1） 零授权

输入数据格式：

标识	数据长度	命令码	保护操作密钥句柄	被加载密钥
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_LoadKey 所定义的固定值

——保护操作密钥句柄

——被加载密钥为一个 TCM_KEY 结构数据

输出数据格式：

标识	数据长度	返回码	被加载密钥句柄
2B	4B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——被加载密钥句柄为 TCM 内部句柄

2） 一个授权

输入数据格式：

标识	数据长度	命令码	保护操作密钥句柄	被加载密钥	<续>
2B	4B	4B	4B	可变	

保护操作密钥授权会话句柄	保护密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_LoadKey 所定义的固定值

——保护操作密钥句柄

——被加载密钥为一个 TCM_KEY 结构数据

——保护操作密钥授权会话句柄

——保护操作密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	被加载密钥句柄	＜续＞
2B	4B	4B	4B	

保护操作授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——被加载密钥句柄为 TCM 内部句柄

——保护操作授权数据验证码

授权数据验证码:密钥授权

密钥为使用保护操作密钥 AP 会话产生的共享秘密。

输入验证码计算：

命令码	被加载密钥	序列号
4B	可变	4B
1S	2S	2H1

输出验证码计算：

返回码	命令码	序列号
4B	4B	4B
1S	2S	2H1

7.2.3 获取公钥 TCM_GetPubKey

功能描述：

获取一个已经载入到 TCM 中的非对称密钥的公钥部分,判断给定的密钥句柄指向的密钥所绑定的平台配置信息是否与平台当前配置信息一致。

接口：

该命令有零授权和一个授权两种情况。

1) 零授权。

输入数据格式：

标识	数据长度	命令码	密钥句柄
2B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_GetPubKey 所定义的固定值

——密钥句柄为密钥的 TCM 内部句柄

输出数据格式：

标识	数据长度	返回码	密钥公钥部分
2B	4B	4B	可变

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——密钥公钥部分为 TCM_PUBKEY 结构数据

2） 一个授权。

输入数据格式：

标识	数据长度	命令码	密钥句柄	<续>
2B	4B	4B	4B	

密钥授权会话句柄	密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_GetPubKey 所定义的固定值
——密钥句柄为密钥的 TCM 内部句柄
——密钥授权会话句柄
——密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	密钥公钥部分	<续>′
2B	4B	4B	可变	

密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——密钥公钥部分为 TCM_PUBKEY 结构数据
——密钥授权数据验证码

授权数据验证码:密钥授权

密钥为使用该密钥 AP 会话产生的共享秘密。

输入验证码计算：

命令码	序列号
4B	4B
1S	2H1

输出验证码计算：

返回码	命令码	密钥公钥部分	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

7.2.4 密钥导入 TCM_WrapKey

功能描述：

导入一个由外部生成的 TCM_KEY 结构密钥，并指定其保护操作密钥，操作如下：

1） 验证保护操作密钥的授权，保护操作密钥必须是对称密钥；

2） 判断密钥属性的合法性；

3） 如果密钥可迁移，其迁移授权数据为输入的迁移授权数据；如果密钥不可迁移，其迁移授权数据为 TCM_Proof；

4） 密钥可以与指定的 PCR 寄存器的摘要值进行绑定；

5） 对非对称密钥的私钥部分或者对称密钥用保护操作密钥进行加密保护；

6） 返回 TCM_KEY 结构数据。

接口：

输入数据格式：

标识	数据长度	命令码	保护操作密钥句柄	使用授权数据	迁移授权数据	密钥信息	＜续＞
2B	4B	4B	4B	32B	32B	可变	

保护操作密钥授权会话句柄	保护操作密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_CreateWrapKey 所定义的固定值

——保护操作密钥句柄

——加密的使用授权数据，数据结构为 TCM_AuthData

——加密的迁移授权数据，数据结构为 TCM_AuthData

——密钥信息为 TCM_KEY 结构的数据

——保护操作密钥授权会话句柄

——保护操作密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	密钥信息	＜续＞
2B	4B	4B	可变	

保护操作密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——密钥信息为 TCM_KEY 结构的数据
——保护操作密钥授权数据验证码
授权数据验证码:密钥授权
密钥为使用保护操作密钥 AP 会话产生的共享秘密。
输入验证码计算:

命令码	使用授权数据	迁移授权数据	密钥信息	序列号
4B	32B	32B	可变	4B
1S	2S	3S	4S	2H1

输出验证码计算:

返回码	命令码	密钥信息	序列号
4B	4B	可变	4B
1S	2S	3S	2H1

7.2.5 密钥证明 TCM_CertifyKey

功能描述:
该命令使用一个密钥来验证另外一个密钥,须遵循如下原则:
1) 验证密钥和待验证密钥是非对称密钥;
2) 如果验证密钥是身份密钥,待验证密钥不可迁移;
3) 待验证密钥绑定的平台配置信息应与当前平台配置信息相匹配;
4) 将待验证密钥的公钥的摘要值及相关信息填入 TCM_CERTIFY_INFO 结构,计算出该结构数据的摘要值,并用验证密钥对该摘要值签名。
接口:
该命令有零授权、一个授权和两个授权三种情况。
1) 零授权
输入数据格式:

标识	数据长度	命令码	验证密钥句柄	待验证密钥句柄	抗重放数据
2B	4B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_CertifyKey 所定义的固定值
——验证密钥句柄
——待验证密钥句柄
——抗重放数据为 32 字节的随机数
输出数据格式:

标识	数据长度	返回码	验证信息	验证信息签名的长度	验证信息的签名
2B	4B	4B	可变	4B	可变

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)
——验证信息为 TCM_CERTIFY_INFO 结构数据
——验证信息签名的长度
——验证信息的签名

2) 一个授权

输入数据格式:

标识	数据长度	命令码	验证密钥句柄	待验证密钥句柄	抗重放数据	<续>
2B	4B	4B	4B	4B	32B	

验证密钥授权会话句柄	验证密钥授权数据验证码	<续>
4B	32B	

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_CertifyKey 所定义的固定值
——验证密钥句柄
——待验证密钥句柄
——抗重放数据为 32 字节的随机数
——验证密钥授权会话句柄
——验证密钥授权数据验证码

输出数据格式:

标识	数据长度	返回码	验证信息	验证信息签名的长度	验证信息的签名	<续>
2B	4B	4B	可变	4B	可变	

验证密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——验证信息为 TCM_CERTIFY_INFO 结构数据
——验证信息签名的长度
——验证信息的签名

3) ——验证密钥授权数据验证码两个授权

输入数据格式:

标识	数据长度	命令码	验证密钥句柄	待验证密钥句柄	抗重放数据	<续>
2B	4B	4B	4B	4B	32B	

验证密钥授权会话句柄	验证密钥授权数据验证码	<续>
4B	32B	

待验证密钥授权会话句柄	待验证密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_CertifyKey 所定义的固定值
——验证密钥句柄
——待验证密钥句柄
——抗重放数据为 32 字节的随机数
——验证密钥授权会话句柄
——验证密钥授权数据验证码
——待验证密钥授权会话句柄
——待验证密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	验证信息	验证信息签名的长度	验证信息的签名	＜续＞
2B	4B	4B	可变	4B	可变	

验证密钥授权数据验证码	＜续＞
32B	

待验证密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH2_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——验证信息为 TCM_CERTIFY_INFO 结构数据
——验证信息签名的长度
——验证信息的签名
——验证密钥授权数据验证码
——待验证密钥授权数据验证码

授权数据验证码：验证密钥授权输入验证码计算：

命令码	抗重放数据	序列号
4B	32B	4B
1S	2S	2H1

输出验证码计算：

返回码	命令码	验证信息	验证信息签名长度	验证信息签名	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H1

授权数据验证码：待验证密钥授权

密钥为使用待验证密钥 AP 会话产生的共享秘密。

输入验证码计算：

命令码	抗重放数据	序列号
4B	32B	4B
1S	2S	2H2

输出验证码计算：

返回码	命令码	验证信息	验证信息签名长度	验证信息签名	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H2

7.3 密钥协商

该功能用于协商一个对称密钥。

7.3.1 创建会话 TCM_CreateKeyExchange

功能描述：

密钥协商双方 A 与 B 使用这个函数生成临时点分别为 Ra,Rb。用户 A 将 Ra 传送给用户 B,用户 B 将 Rb 传送给用户 A,再使用 Tspi_Exchange_GetKeyExchange 进行密钥协商计算。操作如下：

1） 验证所有者授权；

2） 创建会话,生成非对称密钥对,并将私钥存储在会话中；

3） 返回公钥信息。

接口：

本接口只有一个授权。

输入数据格式：

标识	数据长度	命令码	所有者授权会话句柄	所有者授权数据验证码
2B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节长度

——命令码为 TCM_ORD_CreateKeyExchange 所定义的固定值

——所有者授权会话句柄

——所有者授权数据验证码

输出数据格式：

标识	数据长度	返回码	协商会话句柄	Rx 数据长度	Rx	所有者授权数据验证码
2B	4B	4B	4B	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果

——协商会话句柄

——Rx 数据长度

——Rx 表示为 TCM 生成的临时非对称密钥(临时的 ECC 曲线上的点,按照 SM2 算法规定的未

压缩编码形式的字符串)的公钥信息用来发送给对方

——所有者授权数据验证码。

授权数据验证码:所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	序列号
4B	4B
1S	2H1

输出验证码计算:

返回码	命令码	会话句柄	Rx 数据长度	Rx	序列号码
4B	4B	4B	4B	可变	4B
1S	2S	3S	4S	5S	2H1

7.3.2 获取会话密钥 TCM_GetKeyExchange

功能描述:

输入对方传送来信息,结合本地信息,协商出对称密钥以及验证码。操作如下:

1)、验证本地加载静态密钥授权数据;

2)、将对方发送来的密钥信息和个人信息,以及本地密钥信息和个人信息采用 TCM_CreateKeyExchange 创建会话过程中的临时非对称密钥私钥按照协商算法计算出对称密钥;

3)、生成给对方验证协商过程完整性验证码,以及自己用来验证对方协商过程完整性验证码。

接口:

输入数据格式:

标识	数据长度	命令码	本地静态密钥句柄	会话句柄	协商标识	产生密钥的使用授权	产生的密钥结构属性	<续>
2B	4B	4B	4B	4B	1B	32B	可变	

对方静态密钥公钥信息长度	对方静态密钥公钥信息	本地个人信息摘要长度	本地个人信息摘要	对方个人信息摘要长度	对方个人信息摘要	对方临时密钥公钥信息长度	对方临时密钥公钥信息	<续>
4B	可变	4B	32B	4B	32B	4B	32B	

本地静态密钥授权会话句柄	本地静态密钥授权验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_GetKeyExchange 所定义的固定值

——本地静态密钥句柄是已经加载的密钥句柄

——会话句柄为 TCM_CreateKeyExchange 返回的会话句柄

——协商标识为密钥协商的身份标识,1 代表发起方,2 代表响应方

——产生的密钥的使用授权

——产生的密钥结构属性，是 TCM_KEY 的密钥结构，用来作为生成密钥的的存储结构
——对方静态密钥公钥信息长度
——对方静态密钥公钥信息（ECC 曲线上的点，按照 SM2 密码算法规定的未压缩编码形式的字符串。）
——本地个人信息摘要长度
——本地个人信息摘要
——对方个人信息摘要长度
——对方个人信息摘要
——对方临时密钥公钥信息长度
——对方临时密钥公钥信息（ECC 曲线上的点，按照国标密码算法规定的未压缩编码形式的字符串。）
——本地静态密钥授权会话句柄
a)——本地静态密钥授权验证码

输出数据格式：

标识	数据长度	返回码	产生的密钥结构	本地验证数据	提供对方验证数据	本地静态密钥授权验证码
2B	4B	4B	可变	32B	32B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果（见返回码定义表）
——产生的密钥结构是协商出来的对称密钥，以 TCM_KEY 结构输出
——本地验证数据长度
——本地验证数据，与对方提供的协商结果验证码进行比较，如果相同说明验证通过
——提供对方验证数据长度
——提供对方验证数据，是提供给对方进行协商结果验证的数据
——本地静态密钥授权验证码
授权数据验证码：密钥授权
密钥为本地静态密钥使用 AP 会话产生的共享秘密数据。
输入验证码计算：

命令码	协商标识	产生的密钥的使用授权	产生的密钥结构属性	对方静态密钥公钥信息长度	对方静态密钥公钥信息	本地个人信息摘要长度	本地个人信息摘要	＜续＞
4B	1B	32B	可变	4B	可变	4B	可变	
1S	2S	3S	4S	5S	6S	7S	8S	

对方个人信息摘要长度	对方个人信息摘要	对方临时密钥公钥信息长度	对方临时密钥公钥信息	序列号码
4B	可变	4B	可变	4B
9S	10S	11S	12S	2H1

输出验证码计算：

返回码	命令码	产生的密钥结构	本地验证数据长度	本地验证数据	提供对方验证数据长度	提供对方验证数据	序列号码
4B	4B	可变	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	6S	7S	2H1

7.3.3 释放会话 TCM_ReleaseExchangeSession

功能描述：

该命令用来释放 TCM 协商过程会话。

接口：

输入数据格式：

标识	数据长度	命令码	会话句柄
2B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ReleaseExchangeSession 所定义的固定值

——会话句柄是 TCM_CreateKeyExchange 返回的会话句柄

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果

7.4 密钥迁移

7.4.1 创建迁移授权 TCM_AuthorizeMigrationKey

功能描述：

验证授权并指定迁移方式。

1） 验证 Owner 授权会话；

2） 创建迁移授权结构 TCM_MIGRATIONKEYAUTH，填充该结构并返回。

接口：

输入数据格式：

标识	数据长度	命令码	迁移模式	迁移密钥公钥	Owner 授权句柄	Owner 授权会话验证码
2B	4B	4B	2B	可变	4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_AuthorizeMigrationKey 所定义的固定值

——迁移模式可以是 TCM_MS_MIGRATE 或者 TCM_MS_REWRAP

——迁移密钥公钥是用于迁移的密钥公钥,数据结构为 TCM_PUBKEY

——Owner 授权句柄为给所有者授权的会话句柄

——Owner 授权会话验证码

输出数据格式:

标识	数据长度	返回码	迁移认证数据	Owner 授权会话验证码
2B	4B	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果

——迁移认证数据包括公钥和会话摘要,数据结构为 TCM_MIGRATIONKEYAUTH

——Owner 授权会话验证码

授权数据验证码:所有者授权

密钥为所有者使用 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	迁移模式	迁移密钥公钥	序列号
4B	2B	可变	32B
1S	2S	3S	2H1

输出验证码计算:

返回码	命令码	迁移认证数据	序列号
4B	4B	可变	32B
1S	2S	3S	2H1

7.4.2 创建迁移密钥数据块 TCM_CreateMigratedBlob

功能描述:

创建迁移数据块,操作如下:

1) 验证待迁移密钥父密钥授权会话;
2) 使用父密钥解密待迁移密钥;
3) 验证迁授权会话;
4) 判断迁移类型:

如果 migrationType 等于 TCM_MS_MIGRATE 则:

创建对称密钥加密待迁移密钥的私有部分;

使用迁移公钥加密对称密钥。

如果 migrationType 等于 TCM_MS_REWRAP

直接使用迁移公钥加密待迁移密钥的私有部分。

接口:

输入数据格式:

标识	数据长度	命令码	待迁移密钥父密钥句柄	迁移模式	迁移密钥认证数据	待迁移的密钥数据长度	待迁移的密钥数据	<续>
2B	4B	4B	4B	2B	可变	4B	可变	

待迁移密钥父密钥授权会话句柄	待迁移密钥父密钥授权会话验证码	待迁移密钥迁移授权会话句柄	待迁移密钥迁移授权会话验证码
4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_CreateMigratedBlob 所定义的固定值

——待迁移密钥的父密钥句柄

——迁移模式

——迁移密钥认证数据为迁移目标平台执行 TCM_AuthorizeMigrationKey 生成的结果

——待迁移的密钥数据长度

——待迁移的密钥数据，数据结构是 TCM_STORE_ASYMKEY 或 TCM_STORE_SYMKEY 加密后的数据

——待迁移密钥父密钥授权会话句柄

——待迁移密钥父密钥授权会话验证码

——待迁移密钥迁移授权会话句柄

——待迁移密钥迁移授权会话验证码

输出数据格式：

标识	数据长度	返回码	用对称密钥加密的待迁移密钥大小	用对称密钥加密的待迁移密钥	用迁移公钥加密的数据大小	用迁移公钥加密的数据	待迁移密钥父密钥授权会话验证码	待迁移密钥迁移授权会话验证码
2B	4B	4B	4B	可变	4B	可变	32B	32B

——标识为 TCM_TAG_RSP_AUTH2_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果（见返回码定义表）

——用对称密钥加密的待迁移密钥大小，如果是 TCM_MS_REWRAP 模式则＝0，直接用迁移迁移公钥加密的待迁移密钥，下个参数为 NULL

——用对称密钥加密的待迁移密钥

——用迁移公钥加密的数据大小：如果是 TCM_MS_REWRAP 模式这个参数是用迁移公钥加密的待迁移密钥大小；如果是 TCM_MS_MIGRATE 模式，则这个参数是用迁移公钥加密的对称密钥大小

——用迁移公钥加密的数据：如果是 TCM_MS_REWRAP 模式这个参数是用迁移公钥加密的待迁移密钥（TCM_KEY）；如果是 TCM_MS_MIGRATE 模式，则这个参数是用迁移公钥加密的对称密钥（TCM_KEY）

——待迁移密钥父密钥授权会话验证码

——待迁移密钥迁移授权会话验证码

授权数据验证码：待迁移密钥父密钥授权

密钥为待迁移密钥的父密钥使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	迁移模式	迁移密钥公钥数据	待迁移的密钥数据长度	待迁移的密钥数据	序列号
4B	2B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H1

输出验证码计算：

返回码	用对称密钥加密的待迁移密钥大小	用对称密钥加密的待迁移密钥	用迁移公钥加密的数据大小	用迁移公钥加密的数据	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H1

授权数据验证码：待迁移密钥迁移授权

密钥为待迁授权会话密钥使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	迁移模式	迁移密钥公钥数据	待迁移的密钥数据长度	待迁移的密钥数据	序列号
4B	2B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H2

输出验证码计算：

返回码	用对称密钥加密的待迁移密钥大小	用对称密钥加密的待迁移密钥	用迁移公钥加密的数据大小	用迁移公钥加密的数据	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H2

7.4.3 导入迁移数据块 TCM_ConvertMigratedBlob

功能描述：

将迁移块转换为可以被 LoadKey 命令使用的密钥，操作如下：

1） 验证目标方父密钥授权数据；

2） 验证迁移密钥授权；

3） 用迁移密钥解密(用迁移密钥公钥加密的对称密钥)得到对称密钥；

4） 用对称密钥解密得到待迁移密钥的私有部分；

5） 用目标方父密钥加密待迁移密钥的私有部分。

接口：

本接口有两个授权。

输入数据格式：

标识	数据长度	命令码	迁移密钥句柄	迁移目标父密钥句柄	用对称密钥加密的待迁移密钥大小	用对称密钥加密的待迁移密钥	用迁移公钥加密的数据大小	用迁移公钥加密的数据	<续>
2B	4B	4B	4B	4B	4B	可变	4B	可变	

迁移密钥授权会话句柄	迁移密钥授权会话验证码	迁移目标父密钥授权会话句柄	迁移目标父密钥授权会话验证码
4B	32B	4B	32B

——标识为 TCM_TAG_RQU_AUTH2_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ConvertMigrationBlob 所定义的固定值

——已加载的迁移密钥句柄

——迁移目标父密钥句柄

——用对称密钥加密的待迁移密钥大小，如果是 TCM_MS_REWRAP 模式则＝0，直接用迁移迁移公钥解密的待迁移密钥，下个参数为空

——用对称密钥加密的待迁移密钥

——用迁移公钥加密的数据大小，如果是 TCM_MS_REWRAP 模式这个参数是用迁移公钥加密的待迁移密钥大小；如果是 TCM_MS_MIGRATE 模式，则这个参数是用迁移公钥加密的对称密钥大小

——用迁移公钥加密的数据，如果是 TCM_MS_REWRAP 模式这个参数是用迁移公钥加密的待迁移密钥(TCM_KEY)；如果是 TCM_MS_MIGRATE 模式，则这个参数是用迁移公钥加密的对称密钥(TCM_SYMMETRIC_KEY)

——迁移密钥授权会话句柄

——迁移密钥授权数据验证码

——迁移目标父密钥授权会话句柄

——迁移目标父密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	加密的私钥或对称密钥大小	加密的私钥或对称密钥	迁移密钥授权会话验证码	迁移目标父密钥授权会话验证码
2B	4B	4B	4B	可变	32B	32B

——标识为 TCM_TAG_RSP_AUTH2_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——加密的私钥或对称密钥大小

——加密的私钥或对称密钥，非对称密钥数据结构为 TCM_STORE_ASYMKEY，对称密钥数据结构为 TCM_STORE_SYMKEY

——迁移密钥授权数据验证码

——迁移目标父密钥授权数据验证码

授权数据验证码:迁移密钥授权

密钥为使用迁移密钥授权 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	用对称密钥加密的待迁移密钥大小	用对称密钥加密的待迁移密钥	用迁移公钥加密的数据大小	用迁移公钥加密的数据	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H1

输出验证码计算:

返回码	命令码	加密的私钥或对称密钥大小	加密的私钥或对称密钥	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

授权数据验证码:目标父密钥授权

密钥为使用迁移目标父密钥授权 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	用对称密钥加密的待迁移密钥大小	用对称密钥加密的待迁移密钥	用迁移公钥加密的数据大小	用迁移公钥加密的数据	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H2

输出验证码计算:

返回码	命令码	加密的私钥或对称密钥大小	加密的私钥或对称密钥	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H2

7.5 密码服务

7.5.1 哈希

7.5.1.1 哈希初始化 TCM_SM3Start

功能描述:

启动一个计算 SM3 哈希值会话。

接口:

输入数据格式:

标识	数据长度	命令码
2B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SM3Start 所定义的固定值

输出数据格式：

标识	数据长度	返回码	可以发给 TCM_SM3Update 的最大比特数
2B	4B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——返回可以发给 TCM_SM3Update 的最大比特数

7.5.1.2 哈希运算 TCM_SM3Update

功能描述：

该命令输入哈希计算需要的数据块。

接口：

输入数据格式：

标识	数据长度	命令码	数据块大小	数据块
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SM3Update 所定义的固定值

——待 hash 的数据块大小

——待 hash 的数据块

输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

7.5.1.3 完成哈希运算 TCM_SM3Complete

功能描述：

该命令完成 SM3 会话。

接口：

输入数据格式：

标识	数据长度	命令码	数据块大小	数据块
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SM3Complete 所定义的固定值。

——最后需要计算 hash 的数据大小

——最后需要计算 hash 的数据,小于等于 64 字节

输出数据格式：

标识	数据长度	返回码	Hash 结果
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——Hash 计算的结果

7.5.1.4 完成哈希运算并写入平台寄存器 TCM_SM3CompleteExtend

功能描述：

完成当前 SM3 会话并将结果值扩展到指定的 PCR 中,操作如下：

1) 计算 hash 值；

2) 写入指定的 PCR。

接口：

输入数据格式：

标识	数据长度	命令码	指定的 PCR	数据块大小	数据块
2B	4B	4B	4B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SM3CompleteExtend 所定义的固定值

——指定的 PCR

——最后需要计算 hash 的数据大小

——最后需要计算 hash 的数据,小于等于 64 字节

输出数据格式：

标识	数据长度	返回码	Hash 结果	PCR 结果
2B	4B	4B	32	32

——标识为 TCM_TAG_RSP_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——hash 计算的结果

——写 PCR 以后,PCR 的当前值

7.5.2 签名 TCM_Sign

功能描述：

利用指定的密钥执行数字签名操作并返回其数字签名。参照国标 ECC 算法指定的签名算法。

1) 验证签名密钥授权数据；

2) 验证待签名数据长度,如果为 0 则返回 TCM_BAD_PARAMETER；

3) 验证签名密钥属性,其 keyUsage 必须为 TCM_KEY_SIGNING,否则返回 TCM_INVALID_KEYUSAGE；

4） 计算签名。

接口：

输入数据格式：

标识	数据长度	命令码	签名密钥句柄	待签名摘要数据长度	待签名摘要数据	＜续＞
2B	4B	4B	4B	4B	32B	

签名密钥授权会话句柄	签名密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_Sign 所定义的固定值

——签名密钥句柄为可以用来签名的密钥加载在 TCM 中后返回的句柄

——待签名数据长度，上层摘要后的结果（32 字节）

——待签名数据

——签名密钥授权会话句柄

——签名密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	签名数据长度	签名数据	签名密钥授权数据验证码
2B	4B	4B	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果

——签名数据长度

——签名数据，直接使用国标 SCH 计算

——签名密钥授权数据验证码

授权数据验证码：签名密钥授权

密钥为使用签名密钥授权 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	待签名摘要数据长度	待签名摘要数据	序列号
4B	4B	32B	4B
1S	2S	3S	2H1

输出验证码计算：

返回码	命令码	签名数据长度	签名	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

7.5.3 加解密

7.5.3.1 SM4 加密 TCM_SM4Encrypt

功能描述：

该命令利用已经加载的密钥对输入数据进行对称加密。

数据加密方式采用 TCM_ES_SM4_CBC 模式,数据填充原则如下:

a) 填充完的数据长度必须是 16 的整数倍;

b) 缺少几个字节(d1)就填充 d1 个字节,每个字节内容均是 d1;

c) 如果 d1=0 则填充 16 个字节,每个字节内容均是 16

加密采用上层传递的 IV。

接口

输入数据格式:

标识	数据长度	命令码	密钥句柄	CBC 模式使用的 IV	待加密数据长度	待加密数据	<续>
2B	4B	4B	4B	16B	4B	可变	

加密密钥的授权会话句柄	加密密钥的授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的节数

——命令码为 TCM_ORD_SM4Encrypt 所定义的固定值

——密钥句柄为可进行 SM4 加密操作的密钥的句柄

——CBC 模式使用的 IV

——待加密数据长度

——待加密数据

——加密密钥的授权会话句柄

——加密密钥的授权数据验证码

输出数据格式:

标识	数据长度	返回码	已加密数据长度	已加密数据	加密密钥的授权数据验证码
2B	4B	4B	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果。

——已加密数据长度

——已加密数据

——加密密钥的授权数据验证码

授权数据验证码:加密密钥授权

密钥为加密密钥的授权 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	CBC 模式使用的 IV	待加密数据长度	待解密数据	序列号
4B	16B	4B	可变	32B
1S	2S	3S	4S	2H1

输出验证码计算：

返回码	命令码	已加密数据长度	已加密数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

7.5.3.2 SM4 解密 TCM_SM4Decrypt

功能描述：

该命令利用已经加载的密钥对输入数据进行对称解密。。数据解密采用 TCM_ES_SM4_CBC 模式。数据还原方法如下：

a) 根据解密后最后一个字节内容(d1)，删除解密后数据最后 d1 个字节；

b) 如果 d1＝16，则解密数据的最后一个分组删除。

解密采用上层传递的 IV。

接口：

输入数据格式：

标识	数据长度	命令码	密钥句柄	CBC 模式使用的 IV	待解密数据长度	待解密数据
2B	4B	4B	4B	16B	4B	可变

解密密钥的授权会话句柄	解密密钥的授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SM4Decrypt 所定义的固定值

——密钥句柄为能进行解密操作的密钥的句柄

——CBC 模式使用的 IV

——待解密数据长度

——待解密数据

——解密密钥的授权会话句柄

——解密密钥的授权数据验证码

输出数据格式：

标识	数据长度	返回码	输出数据长度	解密后数据	解密密钥的授权数据验证码
2B	4B	4B	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果

——输出数据长度

——解密后数据

——解密密钥的授权数据验证码

授权数据验证码:解密密钥授权

密钥为解密密钥的授权 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	CBC 模式使用的 IV	被解密数据长度	被解密数据	序列号
4B	16B	4B	可变	32B
1S	2S	3S	4S	2H1

输出验证码计算:

返回码	命令码	输出数据长度	解密后数据	序列号
4B	4B	4B	可变	4B
1S	2S	3S	4S	2H1

7.5.3.3 SM2 解密 TCM_SM2Decrypt

功能描述:

利用指定的非对称密钥执行解密操作并返回其解密结果,加密操作可以在上层实现。算法参照国标算法指定加解密算法。

接口:

输入数据格式:

标识	数据长度	命令码	密钥句柄	待解密数据长度	待解密数据
2B	4B	4B	4B	4B	可变

解密密钥的授权会话句柄	解密密钥的授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_SM2Decrypt 所定义的固定值

——密钥句柄

——待解密数据长度

——待解密数据

——解密密钥的授权会话句柄

——解密密钥的授权数据验证码

——解密密钥的授权会话句柄

——解密密钥的授权数据验证码

输出数据格式:

标识	数据长度	返回码	解密后数据长度	解密后数据	授权数据验证码
2B	4B	4B	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果
——解密后数据长度
——解密后数据
——授权数据验证码
授权数据验证码:解密密钥授权
密钥为解密密钥的授权 AP 会话产生的共享秘密数据。
输入验证码计算:

命令码	待解密数据长度	待解密数据	序列号
4B	4B	可变	32B
1S	2S	3S	2H1

输出验证码计算:

返回码	命令码	解密后数据长度	解密后数据	序列号
4B	4B	4B	可变	32B
1S	2S	3S	4S	2H1

7.5.4 获取随机数 TCM_GetRandom

功能描述:
返回一个指定长度的随机数。
接口:
输入数据格式:

标识	数据长度	命令码	随机数据长度
2B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_GetRandom 所定义的固定值
——随机数据长度
输出数据格式:

标识	数据长度	返回码	随机数据长度	随机数据
2B	4B	4B	4B	可变

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果
——随机数据长度为返回的随机数的字节数
——随机数据

7.6 传输会话

7.6.1 创建会话 TCM_EstablishTransport

功能描述:
建立传输会话。操作如下:
1) 用传输保护密钥解密得到临时会话密钥;

2） TCM 创建传输会话句柄和防重放攻击的初始序列号；

3） 定义传输保护的算法和加密操作方式；

4） 返回 locality 和当前时钟节拍值。

接口：

输入数据格式：

标识	数据长度	命令码	传输保护密钥句柄	传输描述信息	加密的临时会话密钥长度	加密的临时会话密钥	＜续＞
2B	4B	4B	4B	可变	4B	可变	

传输保护密钥授权会话句柄	传输保护密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_EstablishTransport 所定义的固定值

——传输保护密钥句柄

——传输描述信息是 TCM_TRANSPORT_PUBLIC 结构的数据

——加密的临时会话密钥长度

——加密的临时会话密钥，为对称密钥

——传输保护密钥授权会话句柄

——传输保护密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	传输会话句柄	locality	当前时钟节拍值	传输会话序列号	＜续＞
2B	4B	4B	4B	4B	8B	4B	

传输保护密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——传输会话句柄

——locality

——当前时钟节拍值

——传输会话序列号

——传输保护密钥授权数据验证码

授权数据验证码：保护密钥授权

密钥为使用传输保护密钥 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	传输描述信息	加密的临时会话密钥长度	秘加密的临时会话密钥	序列号
4B	可变	4B	可变	4B
1S	2S	3S	4S	2H1

输出验证码计算：

返回码	命令码	locality	当前时钟节拍值	传输会话序列号	序列号
4B	4B	4B	8B	4B	4B
1S	2S	3S	4S	5S	2H1

7.6.2 使用会话 TCM_ExecuteTransport

功能描述：

该命令负责命令的传输保护，操作如下：

1） 利用传输会话密钥解密输入的受保护命令数据包；

2） TCM 执行完该命令；

3） 用传输会话密钥加密命令的响应数据包；

4） 返回 locality 和当前时钟节拍值。

接口：

输入数据格式：

标识	数据长度	命令码	受保护命令数据长度	受保护命令数据	＜续＞
2B	4B	4B	4B	可变	

传输会话句柄	传输保护密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_ExecuteTransport 所定义的固定值

——受保护命令数据长度

——受保护命令数据

——传输会话句柄

——传输保护密钥授权数据验证码

输出数据格式：

标识	数据长度	返回码	locality	当前时钟节拍值	加密的命令响应数据长度	加密的命令响应数据	＜续＞
2B	4B	4B	4B	可变	4B	可变	

传输保护密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果(见返回码定义表)

——locality

——当前时钟节拍值

——加密的命令响应数据长度

——加密的命令响应数据

——传输保护密钥授权数据验证码

授权数据验证码:保护密钥授权

密钥为使用传输保护密钥 AP 会话产生的共享秘密数据。

输入验证码计算:

命令码	受保护命令数据长度	受保护命令数据	传输会话序列号
4B	4B	可变	4B
1S	2S	3S	2H1

输出验证码计算:

返回码	命令码	locality	当前时钟节拍值	加密的命令响应数据长度	加密的命令响应数据	传输会话序列号
4B	4B	4B	8B	4B	可变	4B
1S	2S	3S	4S	5S	6S	2H1

7.6.3 释放会话 TCM_Releasetransport

功能描述:

释放与指定的传输会话相关的资源,结束传输会话。

接口:

输入数据格式:

标识	数据长度	命令码	<续>
2B	4B	4B	

传输会话句柄	传输保护密钥授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND

——数据长度为输入数据总的字节数

——命令码为 TCM_ORD_Releasetransport 所定义的固定值

——传输会话句柄

——传输保护密钥授权数据验证码计算如下:

a) 输入数据格式:

命令码	传输会话序列号
4B	4B
1S	2H1

b) 密钥为使用传输保护密钥 AP 会话产生的共享秘密数据

输出数据格式:

标识	数据长度	返回码	locality	当前时钟节拍值	<续>
2B	4B	4B	4B	44B	

传输保护密钥授权数据验证码
32B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——locality
——当前时钟节拍值
授权数据验证码:保护密钥授权
密钥为使用传输保护密钥 AP 会话产生的共享秘密数据。
输入验证码计算:

命令码	传输会话序列号
4B	4B
1S	2H1

输出验证码计算:
无

7.7 授权协议

7.7.1 创建授权协议会话 TCM_APCreate

功能描述:
授权协议发起命令,建立授权会话。操作如下:
1) 如果实体类型为 TCM_NONE 转 3),否则验证调用者是否拥有对某一实体的权限和输入参数的完整性;
2) 基于共享的授权数据 authData、调用者输入的随机数 callerNonce 和 TCM 生成的随机数 TCMNonce 来创建共享秘密数据 shareSecret=HMAC(authData,callerNonce||TCMNonce)和共享会话密钥 sessionKey=KDF(shareSecret);
3) 创建会话和相应的授权会话句柄;
4) 生成防重放攻击的初始序列号;
5) 生成授权数据验证码。
接口:
输入数据格式:

标识	数据长度	命令码	实体类型	实体值	调用者 nonce	实体授权数据验证码
2B	4B	4B	2B	4B	32B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_APCreate 所定义的固定值
——实体类型为使用的实体的类型,实体类型包括:

值	实体类型	句柄	注释
0x01	TCM_ET_KEYHANDLE		密钥句柄
0x02	TCM_ET_OWNER	0x40000001	TCM 所有者
0x03	TCM_ET_DATA		数据
0x04	TCM_ET_SMK	0x40000000	存储主密钥 SMK

值	实体类型	句柄	注释
0x05	TCM_ET_KEY		密钥
0x06	TCM_ET_REVOKE	0x40000002	可撤销 EK
0x0A	TCM_ET_COUNTER		计数器
0x0B	TCM_ET_NV		NV 索引
0x11	TCM_ET_KEYSM4		对称密钥
0x12	TCM_ET_NONE		
0x13	TCM_ET_AUTHDATA_ID		授权数据标识
0x40	TCM_ET_RESERVED_HANDLE		保留

——实体值为基于实体类型的选择值，如密钥句柄号，根据实体类型和实体值可确定欲访问实体的授权数据

——调用者 nonce 为调用者生成的随机数

——实体授权数据验证码

输出数据格式：

标识	数据长度	返回码	授权会话句柄	TCM nonce	序列号	实体授权数据验证码
2B	4B	4B	4B	32B	4B	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND

——数据长度为输出数据总的字节数

——返回码为本操作的结果（见返回码定义表）

——授权会话句柄

——TCMnonce 为 TCM 生成的随机数

——序列号

——实体授权数据验证码

授权数据验证码：实体授权

密钥为通过授权数据生成的共享秘密数据。

输入验证码计算：

命令码	实体类型	调用者 nonce
4B	2B	32B
1S	2S	2H1

输出验证码计算：

返回码	命令码	TCM nonce	序列号
4B	4B	32B	4B
1S	2S	3S	2H1

7.7.2 释放授权协议会话 TCM_APTerminate

功能描述：

该命令终止授权协议。通过授权数据验证后，释放指定的授权会话及相关资源。

接口：

输入数据格式：

标识	数据长度	命令码	＜续＞
2B	4B	4B	

实体授权会话句柄	实体授权数据验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_APTerminate 所定义的固定值
——实体授权会话句柄
——实体授权数据验证码
输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
授权数据校验码:实体授权
密钥为 TCM_APCreate 中生成的共享秘密数据。
输入校验码计算：

命令码	序列号
4B	4B
1S	2H1

输出校验码计算：
无

8 完整性度量与报告功能

8.1 平台配置寄存器管理

8.1.1 写入平台配置寄存器 TCM_Extend

功能描述
在 PCR 寄存器中增加一个度量值。操作如下：
1） 根据指定的 PCR 索引值读出 PCR 寄存器的内容；
2） 将所读出的内容与输入摘要值进行拼接；
3） 用 SCH 算法哈希得到的新度量值记入相应的 PCR 寄存器中。
接口
输入数据格式：

标识	数据长度	命令码	PCR 索引	输入摘要值
2B	4B	4B	4B	32B

——标识为 TCM_TAG_RQU_COMMAND

——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_Extend 所定义的固定值
——PCR 索引
——输入摘要值为被度量部件的特征数据的 256 比特位的哈希值
输出数据格式：

标识	数据长度	返回码	新的度量值
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——新的度量值

8.1.2 读取平台配置寄存器 TCM_PCRRead

功能描述
读取指定 PCR 寄存器的当前值。
接口
输入数据格式：

标识	数据长度	命令码	PCR 索引
2B	4B	4B	4B

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_PCRRead 所定义的固定值
——PCR 索引
输出数据格式：

标识	数据长度	返回码	PCR 值
2B	4B	4B	32B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)
——PCR 值为指定 PCR 寄存器的当前值

8.1.3 引用平台配置寄存器 TCM_Quote

功能描述：
对指定的 PCR 值,返回给定密钥的签名,操作如下：
1) 验证签名密钥的授权；
2) 验证目标 PCR 数据结构 TCM_PCR_SELECTION；
3) 创建 TCM_QUOTE_INFO 数据结构,并填充；
4) 返回对 TCM_QUOTE_INFO 数据结构签名值；
5) 签名算法参照国标算法指定签名算法。
接口：
输入数据格式：

标识	数据长度	命令码	密钥句柄	防重放攻击数据	目标 PCR	＜续＞
2B	4B	4B	4B	32B	可变	

授权会话句柄	密钥授权验证码
4B	32B

——标识为 TCM_TAG_RQU_AUTH1_COMMAND
——数据长度为输入数据的总字节数
——命令码为 TCM_ORD_Quote 所定义的固定值
——密钥句柄
——防重放攻击数据
——目标 PCR,数据结构为 TCM_PCR_SELECTION
——授权会话句柄
——密钥授权验证码

输出数据格式：

标识	数据长度	返回码	PCR 数据	签名数据长度	签名数据	密钥授权验证码
2B	4B	4B	可变	4B	可变	32B

——标识为 TCM_TAG_RSP_AUTH1_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果
——PCR 数据,数据结构为 TCM_PCR_COMPOSITE
——签名数据长度
——签名数据
——密钥授权验证码

授权数据验证码:密钥授权

密钥为签名密钥使用 AP 会话产生的共享秘密数据。

输入验证码计算：

命令码	防重放攻击数据	目标 PCR	序列号
4B	32B	可变	4B
1S	2S	3S	2H1

输出验证码计算：

返回码	命令码	PCR 数据	签名数据长度	签名数据	序列号
4B	4B	可变	4B	可变	4B
1S	2S	3S	4S	5S	2H1

8.1.4 复位平台配置寄存器 TCM_PCR_Reset

功能描述：

对于可重置的 PCR,设置为启动时的初始值,如果 TCM_STANY_FLAGS->TOSPresent 值为 TRUE 则重置 PCR 值为 0,否则重置 PCR 值为 0xff。

接口：

输入数据格式：

标识	数据长度	命令码	目标 PCR
2B	4B	4B	可变

——标识为 TCM_TAG_RQU_COMMAND
——数据长度为输入数据总的字节数
——命令码为 TCM_ORD_PCR_ReSets 所定义的固定值
——目标 PCR 为所选择的要进行重置的 PCR,数据结构为 TCM_PCR_SELECTION
输出数据格式：

标识	数据长度	返回码
2B	4B	4B

——标识为 TCM_TAG_RSP_COMMAND
——数据长度为输出数据总的字节数
——返回码为本操作的结果(见返回码定义表)

附 录 A
（规范性附录）
数 据 结 构

A.1 结构标记

名称	值	结构
TCM_TAG_CONTEXTBLOB	0x0001	TCM_CONTEXT_BLOB
TCM_TAG_CONTEXT_SENSITIVE	0x0002	TCM_CONTEXT_SENSITIVE
TCM_TAG_SIGNINFO	0x0005	TCM_SIGN_INFO
TCM_TAG_PCR_INFO	0x0006	TCM_PCR_INFO
TCM_TAG_PERSISTENT_FLAGS	0x0007	TCM_PERMANENT_FLAGS
TCM_TAG_VOLATILE_FLAGS	0x0008	TCM_VOLATILE_FLAGS
TCM_TAG_PERSISTENT_DATA	0x0009	TCM_PERSISTENT_DATA
TCM_TAG_EK_BLOB	0x000C	TCM_EK_BLOB
TCM_TAG_EK_BLOB_AUTH	0x000D	TCM_EK_BLOB_AUTH
TCM_TAG_COUNTER_VALUE	0x000E	TCM_COUNTER_VALUE
TCM_TAG_TRANSPORT_INTERNAL	0x000F	TCM_TRANSPORT_INTERNAL
TCM_TAG_AUDIT_EVENT_IN	0x0012	TCM_AUDIT_EVENT_IN
TCM_TAG_AUDIT_EVENT_OUT	0X0013	TCM_AUDIT_EVENT_OUT
TCM_TAG_CURRENT_TICKS	0x0014	TCM_CURRENT_TICKS
TCM_TAG_KEY	0x0015	TCM_KEY
TCM_TAG_STORED_DATA	0x0016	TCM_STORED_DATA
TCM_TAG_NV_ATTRIBUTES	0x0017	TCM_NV_ATTRIBUTES
TCM_TAG_NV_DATA_PUBLIC	0x0018	TCM_NV_DATA_PUBLIC
TCM_TAG_NV_DATA_SENSITIVE	0x0019	TCM_NV_DATA_SENSITIVE
TCM_TAG_TRANSPORT_AUTH	0x001D	TCM_TRANSPORT_AUTH
TCM_TAG_TRANSPORT_PUBLIC	0X001E	TCM_TRANSPORT_PUBLIC
TCM_TAG_PERMANENT_FLAGS	0X001F	TCM_PERMANENT_FLAGS
TCM_TAG_STCLEAR_FLAGS	0X0020	TCM_STCLEAR_FLAGS
TCM_TAG_STANY_FLAGS	0X0021	TCM_STANY_FLAGS
TCM_TAG_PERMANENT_DATA	0X0022	TCM_PERMANENT_DATA
TCM_TAG_STCLEAR_DATA	0X0023	TCM_STCLEAR_DATA
TCM_TAG_STANY_DATA	0X0024	TCM_STANY_DATA
TCM_TAG_CERTIFY_INFO	0X0029	TCM_CERTIFY_INFO
TCM_TAG_EK_BLOB_ACTIVATE	0X002B	TCM_EK_BLOB_ACTIVATE
TCM_TAG_CAP_VERSION_INFO	0X0030	TCM_CAP_VERSION_INFO
TCM_TAG_QUOTE_INFO	0X0036	TCM_QUOTE_INFO

A.2 类型

A.2.1 TCM_RESOURCE_TYPE

名称	值	描述
TCM_RT_KEY	0x00000001	密钥句柄,为 Loadkey 的操作返回结果
TCM_RT_AUTH	0x00000002	授权句柄,为授权协议返回结果
TCM_RT_HASH	0X00000003	保留
TCM_RT_TRANS	0x00000004	传输保护协议句柄,为创建传输会话的返回结果
TCM_RT_CONTEXT	0x00000005	上下文资源,在 TCM 外部缓存/加载
TCM_RT_COUNTER	0x00000006	保留

A.2.2 TCM_PAYLOAD_TYPE

名称	值	描述
TCM_PT_SYM	0x00	对称密钥类型
TCM_PT_ASYM	0x01	非对称密钥类型
TCM_PT_BIND	0x02	加密数据类型
TCM_PT_SEAL	0x05	封装数据类型
TCM_PT_SYM_MIGRATE	0x08	对称迁移类型
TCM_PT_ASYM_MIGRATE	0x09	非对称迁移类型
	0x09-0xFF	保留

A.2.3 TCM_ENTITY_TYPE

值	名称	描述
0x01	TCM_ET_KEYHANDLE	密钥句柄实体类型
0x02	TCM_ET_OWNER	TCM 所有者实体类型
0x03	TCM_ET_DATA	数据实体类型
0x04	TCM_ET_SMK	SMK 实体类型
0x05	TCM_ET_KEY	密钥实体类型
0x06	TCM_ET_REVOKE	可撤销密钥实体类型
0x0A	TCM_ET_COUNTER	计数器实体类型
0x0B	TCM_ET_NV	NV 索引实体类型
0x10	TCM_ET_KEYXOR	采用异或算法加密授权的密钥实体句柄
0x11	TCM_ET_KEYSM4	采用 SM4 对称加解密的密钥实体类型
0x12	TCM_ET_NONE	授权协议无实体创建

值	名称	描述
0x13	TCM_ET_AUTHDATA_ID	授权数据标识实体类型
0x14	TCM_ET_AUTHDATA	授权数据实体类型
0x15	TCM_ET_OPERATOR	操作者实体类型
0x16	TCM_ET_OWENERSM4	
0x17	TCM_ET_OWNERXOR	
0x40	TCM_ET_RESERVED_HANDLE	保留

A.2.4 KeyHandles 值

句柄	名称	描述
0x40000000	TCM_KH_SMK	SMKSMK 密钥句柄
0x40000001	TCM_KH_OWNER	TCM 所有者句柄
0x40000002	TCM_KH_REVOKE	可撤销 EK 句柄
0x40000003	TCM_KH_TRANSPORT	创建传输会话句柄
0x40000004	TCM_KH_OPERATOR	操作者授权句柄
0x40000006	TCM_KH_EK	EK 句柄

A.2.5 TCM_STARTUP_TYPE 值

值	名称	描述
0x0001	TCM_ST_CLEAR	TCM 采用所有变量设置为缺省值的启动方式
0x0002	TCM_ST_STATE	TCM 恢复到以前执行 TCM_SaveState 所保存的值的启动方式
0x0003	TCM_ST_DEACTIVATED	使 TCM 无效的启动方式

A.2.6 TCM_PROTOCOL_ID 值

值	事件名称	描述
0X0005	TCM_PID_OWNER	创建所有者会话协议
0x0007	TCM_PID_TRANSPORT	传输会话协议
0x0008	TCM_PID_AP	AP 授权协议

A.2.7 TCM_ALGORITHM_ID 值

值	名称	描述
0x00000007	TCM_ALG_KDF	KDF 算法
0x0000000A	TCM_ALG_XOR	异或算法
0x0000000B	TCM_ALG_SM2	SM2 算法

值	名称	描述
0x0000000C	TCM_ALG_SM4	SM4 算法
0x0000000D	TCM_ALG_SM3	SM3 算法
0x0000000E	TCM_ALG_HMAC	HAMC 算法

A.2.8 TCM_ENC_SCHEME 值

值	名称	描述
0x0006	TCM_ES_SM2	ECC 加密编码
0x0004	TCM_ES_SM2NONE	不能用于加密
0x0008	TCM_ES_SM4_CBC	SM4 对称 CBC 编码
0x000A	TCM_ES_SM4_ECB	SM4 对称 ECB 编码

A.2.9 TCM_SIG_SCHEME 值

值	名称	描述
0x0001	TCM_SS_SM2NONE	不能用于签名
0x0005	TCM_SS_SM2	SM2 签名

A.2.10 TCM_PHYSICAL_PRESENCE

名称	值	描述
TCM_PHYSICAL_PRESENCE_HW_DISABLE	0x0200h	设置 physicalPresenceHWEnable＝FALSE
TCM_PHYSICAL_PRESENCE_CMD_DISABLE	0x0100h	设置 physicalPresenceCMDEnable＝FALSE
TCM_PHYSICAL_PRESENCE_LIFETIME_LOCK	0x0080h	设置 physicalPresenceLifetimeLock＝TRUE
TCM_PHYSICAL_PRESENCE_HW_ENABLE	0x0040h	设置 physicalPresenceHWEnable＝TRUE
TCM_PHYSICAL_PRESENCE_CMD_ENABLE	0x0020h	设置 physicalPresenceCMDEnable＝TRUE
TCM_PHYSICAL_PRESENCE_NOTPRESENT	0x0010h	设置 PhysicalPresence＝FALSE
TCM_PHYSICAL_PRESENCE_PRESENT	0x0008h	设置 PhysicalPresence＝TRUE
TCM_PHYSICAL_PRESENCE_LOCK	0x0004h	设置 PhysicalPresenceLock＝TRUE

A.2.11 TCM_MIGRATE_SCHEME 值

名称	值	描述
TCM_MS_MIGRATE	0x0001	对称密钥加密并用迁移密钥公钥保护的迁移类型
TCM_MS_REWRAP	0x0002	使用迁移密钥公钥加密迁移类型

A.2.12 TCM_EK_TYPE

名称	值	描述
TCM_EK_TYPE_ACTIVATE	0x0001	EK 申请证书请求类型 TCM_EK_BLOB_ACTIVATE
TCM_EK_TYPE_AUTH	0x0002	EK 数据授权类型 TCM_EK_BLOB_AUTH

A.3 基本结构

A.3.1 TCM_STRUCT_VER

结构定义：

```
typedef struct tdTCM_STRUCT_VER {
    BYTE major;
    BYTE minor;
    BYTE revMajor;
    BYTE revMinor;
} TCM_STRUCT_VER;
```

参数说明：

类型	名称	描述
BYTE	Major	主版本号
BYTE	Minor	次版本号
BYTE	revMajor	保留
BYTE	revMinor	保留

A.3.2 TCM_VERSION

结构定义：

```
typedef struct tdTCM_VERSION {
    TCM_VERSION_BYTE major;
    TCM_VERSION_BYTE minor;
    BYTE revMajor;
    BYTE revMinor;
} TCM_VERSION;
```

参数说明：

类型	名称	描述
TCM_VERSION_BYTE	Major	TCM 主版本号
TCM_VERSION_BYTE	Minor	TCM 次版本号
BYTE	revMajor	等于 TCM_PERMANENT_DATA->revMajor 的值
BYTE	revMinor	等于 TCM_PERMANENT_DATA->revMinor 的值

A.3.3 TCM_DIGEST

结构定义：

```
typedef struct tdTCM_DIGEST {
    BYTE digest[digestSize];
} TCM_DIGEST;
```

参数说明：

类型	名称	描述
BYTE	digest	摘要信息

类型定义	名称	描述
TCM_DIGEST	TCM_CHOSENID_HASH	身份标识和 CA 公钥的摘要
TCM_DIGEST	TCM_COMPOSITE_HASH	PCR 索引和值的摘要
TCM_DIGEST	TCM_HMAC	HAMC 摘
TCM_DIGEST	TCM_PCRVALUE	PCR 值
TCM_DIGEST	TCM_AUDITDIGEST	审计摘要

A.3.4 TCM_NONCE

结构定义：

```
typedef struct tdTCM_NONCE {
    BYTE nonce[32];
  } TCM_NONCE;
```

参数说明：

类型	名称	描述
BYTE	Nonce	32 字节的随机数

A.3.5 TCM_SEQ

结构定义：

```
typedef UINT32 TCM_SEQ
```

参数说明：

类型	名称	描述
UINT32	TCM_SEQ	TCM 的 4 个字节的序列号

A.3.6 TCM_AUTHDATA

结构定义：

```
typedef BYTE tdTCM_AUTHDATA[32];
```

类型定义	名称	描述
TCM_AUTHDATA	TCM_SECRET	在授权过程中的授权数据
TCM_AUTHDATA	TCM_ENCAUTH	授权会话中加密的授权数据

A.3.7 TCM_KEY_HANDLE_LIST

结构定义：

```
typedef struct tdTCM_KEY_HANDLE_LIST {
    UINT16 loaded;
    [size_is(loaded)] TCM_KEY_HANDLE  handle[];
} TCM_KEY_HANDLE_LIST;
```

参数说明：

类型	名称	描述
UINT16	Loaded	TCM 当前加载的密钥的数量
UINT32	Handle	当前 TCM 加载的密钥句柄数组

A.3.8 TCM_KEY_USAGE 值

名称	值	描述
TCM_SM2KEY_SIGNING	0x0010	使用 ECC 算法进行签名的密钥类型
TCM_SM2KEY_STORAGE	0x0011	存储密钥类型
TCM_SM2KEY_IDENTITY	0x0012	身份密钥类型
TCM_SM2KEY_BIND	0x0014	采用 ECC 算法加密的密钥类型
TCM_SM2KEY_MIGRATE	0x0016	采用 ECC 算法进行迁移的密钥类型
TCM_SM2KEY_PEK	0x0017	采用 ECC 算法生成的 PEK 密钥类型
TCM_SM4KEY_STORAGE	0x0018	采用 SM4 算法的存储密钥类型
TCM_SM4KEY_BIND	0x0019	采用 SM4 算法进行加密的密钥类型
TCM_SM4KEY_MIGRATE	0x001A	采用 SM4 密钥是否可以迁移

A.3.9 TCM_AUTH_DATA_USAGE 值

名称	值	描述
TCM_AUTH_NEVER	0x00	不需要授权数据的实体使用方式
TCM_AUTH_ALWAYS	0x01	必须使用授权数据的实体使用方式
TCM_AUTH_PRIV_USE_ONLY	0x03	对私有数据必须授权数据的实体使用方式

A.3.10 TCM_KEY_FLAGS

TCM_KEY_FLAGS 值

名称	掩码值	描述
Migratable	0x00000002	可迁移密钥
isVolatile	0x00000004	易失性密钥，在启动(ST_Clear 方式)时不需要重新加载
pcrIgnoredOnRead	0x00000008	TRUE 时，在获取公钥时不检查 PCR FLASE 时，在获取公钥检查 PCR

A.3.11 TCM_CHANGEAUTH_VALIDATE

结构定义：

```
typedef struct tdTCM_CHANGEAUTH_VALIDATE {
    TCM_SECRET newAuthSecret;
    TCM_NONCE n1;
} TCM_CHANGEAUTH_VALIDATE;
```

参数说明：

类型	名称	描述
TCM_SECRET	newAuthSecret	新授权数据
TCM_NONCE	n1	用来表明授权数据已经更新

A.3.12 TCM_MIGRATIONKEYAUTH

结构定义：

```
typedef struct tdTCM_MIGRATIONKEYAUTH{
    TCM_PUBKEY migrationKey;
    TCM_MIGRATE_SCHEME migrationScheme;
    TCM_DIGEST digest;
} TCM_MIGRATIONKEYAUTH;
```

参数说明：

类型	名称	描述
TCM_PUBKEY	migrationKey	迁移公钥
TCM_MIGRATE_SCHEME	migrationScheme	迁移模式
TCM_DIGEST	digest	迁移公钥和迁移模式以及 TCMProof 的摘要

A.3.13 TCM_COUNTER_VALUE

结构定义：

```
typedef struct tdTCM_COUNTER_VALUE {
    TCM_STRUCTURE_TAG  tag;
    BYTE label[4];
    TCM_ACTUAL_COUNT counter;
} TCM_COUNTER_VALUE;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_COUNTER_VALUE
BYTE	label	计数器标签
TCM_ACTUAL_COUNT	counter	计数器值

A.3.14 TCM_SIGN_INFO

结构定义：

```
typedef struct tdTCM_SIGN_INFO {
    TCM_STRUCTURE_TAG tag;
    BYTE fixed[4];
    TCM_NONCE replay;
    UINT32 dataLen;
    [size_is (dataLen)] BYTE * data;
} TCM_SIGN_INFO;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	设置为 TCM_TAG_SIGNINFO
BYTE	fixed	固定值
TCM_NONCE	replay	防重放攻击随机数
UINT32	dataLen	待签名数据长度
BYTE	data	待签名数据

A.3.15 TCM_SELECT_SIZE

结构定义：

```
typedef struct tdTCM_SELECT_SIZE {
    BYTE major;
    BYTE minor;
    UINT16 reqSize;
} TCM_SELECT_SIZE;
```

参数说明：

类型	名称	描述
BYTE	Major	TCM 主版本号
BYTE	Minor	TCM 次版本号
UINT16	reqSize	TCM_SELECTION 结构中的 sizeOfSelect 字段值

A.3.16 TCM_CURRENT_TICKS

结构定义：

```
typedef struct tdTCM_CURRENT_TICKS {
    TCM_STRUCTURE_TAG  tag;
    UINT64 currentTicks;
    UINT16  tickRate;
    TCM_NONCE  tickNonce;
}TCM_CURRENT_TICKS;
```

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_CURRENT_TICKS
UINT64	currentTicks	时间戳开始计数
UINT16	tickRate	芯片内计数器,代表了微秒
TCM_NONCE	tickNonce	芯片生成的随机数反映时间戳为 0 时的值

A.4 命令标志

Tag	名称	描述
0x00C1	TCM_TAG_RQU_COMMAND	没有授权的命令
0x00C2	TCM_TAG_RQU_AUTH1_COMMAND	需要一个授权的命令
0x00C3	TCM_TAG_RQU_AUTH2_COMMAND	需要两个授权的命令
0x00C4	TCM_TAG_RSP_COMMAND	没有授权的命令返回
0x00C5	TCM_TAG_RSP_AUTH1_COMMAND	需要一个授权的命令返回
0x00C6	TCM_TAG_RSP_AUTH2_COMMAND	需要两个授权的命令返回

A.5 TCM 的内部数据

A.5.1 TCM_PERMANENT_FLAGS

结构定义:

```
typedef struct tdTCM_PERMANENT_FLAGS{
    TCM_STRUCTURE_TAG tag;
    BOOL disable;
    BOOL ownership;
    BOOL deactivated;
    BOOL readPubek;
    BOOL disableOwnerClear;
    BOOL physicalPresenceLifetimeLock;
    BOOL physicalPresenceHWEnable;
    BOOL physicalPresenceCMDEnable;
    BOOL CEKPUsed;
    BOOL TCMpost;
    BOOL TCMpostLock;
    BOOL operator;
    BOOL enableRevokeEK;
    BOOL nvLocked;
    BOOL TCMEstablished;
} TCM_PERMANENT_FLAGS;
```

参数说明:

类型	名称	描述	标志名
TCM_STRUCTURE_TAG	Tag	TCM_TAG_PERMANENT_FLAGS	
BOOL	Disable	禁用 TCM 标识，默认＝TRUE	TCM_PF_DISABLE
BOOL	ownership	存在所有者标识，默认＝TRUE	TCM_PF_OWNERSHIP
BOOL	deactivated	是否有效标识，默认＝TRUE	TCM_PF_DEACTIVATED
BOOL	readPubek	读取 EK 公钥是否需授权，默认＝TRUE	TCM_PF_READPUBEK
BOOL	disableOwnerClear	是否可以在所有者授权下清除所有者，默认＝FLASE	TCM _ PF _ DISABLEOWNERCLEAR
BOOL	physicalPresenceLifetimeLock	FLASE：代表通过软件和硬件设置可以设置物理现场；（默认） TRUE：代表通过软件和硬件设置不能设置物理现场；	TCM _ PF _ PHYSICALPRESENCELIFETIMELOCK
BOOL	physicalPresenceHWEnable	FLASE：禁止硬件修改物理现场状态；（默认） TRUE：允许硬件修改物理现场状态；	TCM _ PF _ PHYSICALPRESENCEHWENABLE
BOOL	physicalPresenceCMDEnable	FLASE：禁止软件修改物理现场状态；（默认） TRUE：允许软件修改物理现场状态；	TCM _ PF _ PHYSICALPRESENCECMDENABLE
BOOL	CEKPUsed	FLASE：TCM 中厂商自己生成 EK； TRUE：TCM 中通过 TCM_CreateEndorsementKeyPair 生成 EK；	TCM_PF_CEKPUSED
BOOL	TCMpost	TRUE；TCM 在启动后必须做全部自检； FLASE：不需要全部自检（默认）	TCM_PF_TCMPOST
BOOL	TCMpostLock	FALSE：TCMpost 值可以改变；（默认） TRUE：TCMpost 值不能改变	TCM_PF_TCMPOSTLOCK
BOOL	Operator	TRUE：操作者授权可用； FALSE：操作者授权没有被设置（默认）	TCM_PF_OPERATOR
BOOL	enableRevokeEK	TRUE：可以使用 TCM_RevokeTrust 撤销 EK； FALSE：不能使用 TCM_RevokeTrust 撤销 EK；	TCM_PF_ENABLEREVOKEEK
BOOL	nvLocked	TRUE：NV 空间授权必须检查 FALSE：NV 空间不检查（默认），除了检查没有所有者下最大可写次数	TCM_PF_NV_LOCKED
BOOL	TCMEstablished	FALSE：TCM_HASH_START 没有被执行过，可以使用 TCM_ResetEstablishmentBit 设置该状态	TCM_PF_TCMESTABLISHED

A.5.2 TCM_STCLEAR_FLAGS

结构定义：

```
typedef struct tdTCM_STCLEAR_FLAGS{
    TCM_STRUCTURE_TAG tag;
```

```
    BOOL deactivated;
    BOOL disableForceClear;
    BOOL physicalPresence;
    BOOL physicalPresenceLock;
    BOOL bGlobalLock;
} TCM_STCLEAR_FLAGS;
```

参数说明：

类型	名称	描述	标识名
TCM_STRUCTURE_TAG	tag	TCM_TAG_STCLEAR_FLAGS	
BOOL	deactivated	TCM 是否有效标识。 TCM_Startup 将其初始化 TCM_PERMANENT_FLAGS->deactivated 或者其他值。 TCM_SetTempDeactivated 将其设为 TRUE。	TCM_SF_DEACTIVATED
BOOL	disableForceClear	禁止物理现场清除，默认为 FALSE。 TCM_DisableForceClear 将其设为 TRUE。 其为 TRUE 时禁止 TCM_ForceClear 操作。	TCM_SF_DISABLEFORCECLEAR
BOOL	physicalPresence	所有者是否在物理现场的软件标识。 默认值为 FALSE。	TCM_SF_PHYSICALPRESENCE
BOOL	physicalPresenceLock	表示是否允许改变 physicalPresence 标示，TRUE 表示禁止，FALSE 表示允许。 Clear 模式的 TCM_Startup 将其设为默认值 FALSE。 TSC_PhysicalPresence 对其进行设置。	TCM_SF_PHYSICALPRESENCELOCK
BOOL	bGlobalLock	NV 全局锁标识。 Clear 模式的 TCM_Starup 将其设为 FALSE，表示允许写 NV。 写 NV_Index=0 成功时将其设为 TRUE，表示禁止写 NV。	TCM_SF_BGLOBALLOCK

A.5.3 TCM_STANY_FLAGS

结构定义：

```
typedef struct tdTCM_STANY_FLAGS{
    TCM_STRUCTURE_TAG tag;
    BOOL postInitialise;
    TCM_MODIFIER_INDICATOR localityModifier;
    BOOL transportExclusive;
    BOOL TOSPresent;
} TCM_STANY_FLAGS;
```

参数说明：

类型	名称	描述	标识
TCM_STRUCTURE_TAG	tag	TCM_TAG_STANY_FLAGS	
BOOL	postInitialise	是否初始化标识。 无默认值。 TCM_Init 将其设为 TRUE，TCM_Startup 将其设为 FALSE。	TCM_AF_POSTINITIALISE
TCM_MODIFIER_INDICATOR	localityModifier	表示命令是否与 locality 相关，须确保其值能反应使用命令的当前 locality。	TCM_AF_LOCALITYMODIFIER
BOOL	transportExclusive		TCM_AF_TRANSPORTEXCLUSIVE
BOOL	TOSPresent	TOS 是否存在标识。 默认值为 FALSE。 TCM_HASH_START 将其置为 TRUE，TCM_SetCapability 将其设为 FALSE。	TCM_AF_TOSPRESENT

A.5.4 TCM_PERMANENT_DATA

定义：

```
#define TCM_MIN_COUNTERS 4
#define TCM_NUM_PCR 16
#define TCM_MAX_NV_WRITE_NOOWNER 64
typedef struct tdTCM_PERMANENT_DATA{
    TCM_STRUCTURE_TAG           tag;
    BYTE                revMajor;
    BYTE                revMinor;
    TCM_NONCE               TCMProof;
    TCM_NONCE               ekReset;
    TCM_SECRET              ownerAuth;
    TCM_SECRET              operatorAuth;
    TCM_KEY                 endorsementKey;
    TCM_KEY                 smk;
    TCM_KEY                 contextKey;
    TCM_COUNTER_VALUE           auditMonotonicCounter;
    TCM_COUNTER_VALUE           monotonicCounter[TCM_MIN_COUNTERS];
    TCM_PCR_ATTRIBUTES          pcrAttrib[TCM_NUM_PCR];
    BYTE                ordinalAuditStatus[];
    BYTE *              rngState;
    UINT32              maxNVBufSize;
    UINT32              noOwnerNVWrite;
}TCM_PERMANENT_DATA;
```

参数说明：

类型	名称	描述	标识名
TCM_STRUCTURE_TAG	tag	TCM_TAG_PERMANENT_DATA	
BYTE	revMajor	TCM 主版本号。	TCM_PD_REVMAJOR
BYTE	revMinor	TCM 次版本号。	TCM_PD_REVMINOR
TCM_NONCE	TCMProof	平台验证信息。	TCM_PD_TCMPROOF
TCM_SECRET	ownerAuth	所有者授权数据。	TCM_PD_OWNERAUTH
TCM_SECRET	operatorAuth	操作者授权数据。	TCM_PD_OPERATORAUTH
TCM_KEY	endorsementKey	密码模块密钥 EK。	TCM_PD_ENDORSEMENTKEY
TCM_KEY	smk	TCM 存储主密钥。	TCM_PD_SMK
TCM_KEY	contextKey	运行环境保护密钥，可以是对称密钥或非对称密钥，其大小由具体算法决定。不能与 EK 或 SMK 相同。 TCM 所有者发生改变时，其必须被重置。	TCM_PD_CONTEXTKEY
TCM_COUNTER_VALUE	auditMonotonicCounter	审计单调计数器，按照审计规则从 0 开始累加。	TCM _ PD _ AUDITMONOTONICCOUNTER
TCM_COUNTER_VALUE	monotonicCounter	单调计数器，按照一定的规则从初始值开始累加。	TCM _ PD _ MONOTONICCOUNTER
TCM_PCR_ATTRIBUTES	pcrAttrib	PCR 属性。	TCM_PD_PCRATTRIB
byte	ordinalAuditStatus	命令是否需要审计列表。	TCM_PD_ORDINALAUDITSTATUS
BYTE *	rngState	随机数产生器状态信息。	TCM_PD_RNGSTATE
TCM_NONCE	ekReset	使用 TCM_CreateRevocableEK 创建可撤销的 EK 时所生成的随机数，在使用 TCM_RevokeTrust 撤销 EK 时对其进行验证。	TCM_PD_EKRESET
UINT32	maxNVBufSize	使用 TCM_NV_DefineSpace 时所能定义的最大空间。	TCM_PD_MAXNVBUFSIZE
UINT32	noOwnerNVWrite	所有者还未创建时，写 NV 的最大次数。在 TCM 制造或执行 TCM_OwnerClear 时其被设置为 0。TCM_NV_DefineSpace 和 TCM_NV_WriteValue 执行时其被累加，若超过 64，则返回 TCM_MAXNVWRITES。	TCM _ PD _ NOOWNERNVWRITE

A.5.5 TCM_STCLEAR_DATA

结构定义：

```
typedef struct tdTCM_STCLEAR_DATA{
    TCM_STRUCTURE_TAG      tag;
```

```
    TCM_NONCE           contextNonceKey;
    TCM_COUNT_ID        countID;
    UINT32              ownerReference;
    BOOL                disableResetLock;
}TCM_STCLEAR_DATA;
```

参数说明：

类型	名称	描述	标识名
TCM_STRUCTURE_TAG	tag	TCM_TAG_STCLEAR_DATA	
TCM_NONCE	contextNonceKey	密钥类型的运行环境保存防重放攻击随机数，Clear 模式的 TCM_Startup 执行时其被清空。	TCM_SD_CONTEXTNONCEKEY
TCM_COUNT_ID	countID	当前单调计数器句柄，Clear 模式的 TCM_Startup 执行时其被置为 NULL。	TCM_SD_COUNTID
UINT32	ownerReference		TCM_SD_OWNERREFERENCE
BOOL	disableResetLock	TRUE 表示禁止 TCM_ResetLockValue 设值允许重放攻击的次数，默认为 FALSE。	TCM_SD_DISABLERESETLOCK

A.5.6 TCM_STANY_DATA

定义：

```
#define TCM_MIN_SESSIONS 3
#define TCM_MIN_SESSION_LIST 16
typedef struct tdTCM_SESSION_DATA{
… // vendor specific
} TCM_SESSION_DATA;
typedef struct tdTCM_STANY_DATA{
    TCM_STRUCTURE_TAG   tag;
    TCM_NONCE           contextNonceSession;
    TCM_DIGEST          auditDigest;
    TCM_CURRENT_TICKS   currentTicks;
    UINT32              contextCount;
    UINT32              contextList[TCM_MIN_SESSION_LIST];
    TCM_SESSION_DATA    sessions[TCM_MIN_SESSIONS];
}TCM_STANY_DATA;
```

STANY_Data 参数说明：

类型	名称	描述	标识名
TCM_STRUCTURE_TAG	tag	TCM_TAG_STANY_DATA	

类型	名称	描述	标识名
TCM_NONCE	contextNonceSession	会话类型的运行环境保存防重放攻击随机数，Clear 模式的 TCM_Startup 执行时其必须被清空，其它模式的 TCM_Startup 执行时其可以被清空。	TCM_AD_CONTEXTNONCESESSION
TCM_DIGEST	auditDigest	审计日志的摘要值，每个审计会话开始时其被设置为 NULL。	TCM_AD_AUDITDIGEST
TCM_CURRENT_TICKS	currentTicks	当前的时钟节拍值。	TCM_AD_CURRENTTICKS
UINT32	contextCount	会话运行环境保存防重放攻击的计数值。Clear 模式的 TCM_Startup 执行时其必须被置为 0，其它模式的 TCM_Startup 执行时其可以被置为 0。	TCM_AD_CONTEXTCOUNT
UINT32	contextList	会话类型的运行环境保存的序列计数列表，Clear 模式的 TCM_Startup 执行时每一项必须被置为 0，其它模式的 TCM_Startup 执行时每一项可以被置为 0。	TCM_AD_CONTEXTLIST
TCM_SESSION_DATA	sessions	当前存在的会话列表。	TCM_AD_SESSIONS

A.6 PCR 结构

A.6.1 TCM_PCR_SELECTION

结构定义：

```
typedef struct tdTCM_PCR_SELECTION
{
    UINT16 sizeOfSelect;
    [size_is(sizeOfSelect)] BYTE pcrSelect[];
    } TCM_PCR_SELECTION;
```

参数说明：

类型	名称	描述
UINT16	sizeOfSelect	pcrSelect 的大小。
BYTE[]	pcrSelect	每个 bit 位表示对应的 PCR 被选择或未被选择。

A.6.2 TCM_PCR_COMPOSITE

结构定义：

```
typedef struct tdTCM_PCR_COMPOSITE {
    TCM_PCR_SELECTION select;
    UINT32 valueSize;
    [size_is(valueSize)] TCM_PCRVALUE pcrValue[];
```

} TCM_PCR_COMPOSITE;

参数说明：

类型	名称	描述
TCM_PCR_SELECTION	select	PCR 选择信息。
UINT32	valueSize	pcrValue 的大小。
TCM_PCRVALUE	pcrValue[]	选择的 PCR 值。

A.6.3 TCM_PCR_INFO

结构定义：

```
typedef struct tdTCM_PCR_INFO{
    TCM_STRUCTURE_TAG tag;
    TCM_LOCALITY_SELECTION localityAtCreation;
    TCM_LOCALITY_SELECTION localityAtRelease;
    TCM_PCR_SELECTION creationPCRSelection;
    TCM_PCR_SELECTION releasePCRSelection;
    TCM_COMPOSITE_HASH digestAtCreation;
    TCM_COMPOSITE_HASH digestAtRelease;
} TCM_PCR_INFO;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_PCR_INFO
TCM_LOCALITY_SELECTION	localityAtCreation	创建数据块时的 locality 信息。
TCM_LOCALITY_SELECTION	localityAtRelease	解封数据或使用一个密钥时的 locality 信息，不能为 0。
TCM_PCR_SELECTION	creationPCRSelection	创建数据块时的 PCR 选择信息。
TCM_PCR_SELECTION	releasePCRSelection	解封数据或使用一个密钥时的 PCR 选择信息。
TCM_COMPOSITE_HASH	digestAtCreation	创建数据块时的所选择的 PCR 值的摘要值。
TCM_COMPOSITE_HASH	digestAtRelease	解封与平台配置信息相绑定的数据或使用一个与平台配置信息相绑定的密钥时所选择的 PCR 值的摘要值。

A.6.4 TCM_LOCALITY_SELECTION

定义：

```
#define TCM_LOCALITY_SELECTION BYTE
```

比特位	名称	描述
7：5	Reserved	必须被设置为 0。
4	TCM_LOC_FOUR	Locality4
3	TCM_LOC_THREE	Locality3
2	TCM_LOC_TWO	Locality2
1	TCM_LOC_ONE	Locality1
0	TCM_LOC_ZERO	Locality0。

A.6.5 TCM_PCR_ATTRIBUTES

结构定义：

```
typedef struct tdTCM_PCR_ATTRIBUTES{
    BOOL pcrReset;
    TCM_LOCALITY_SELECTION pcrExtendLocal;
    TCM_LOCALITY_SELECTION pcrResetLocal;
} TCM_PCR_ATTRIBUTES;
```

PersistentData 类型：

类型	名称	描述
BOOL	pcrReset	TRUE 表示： PCR 默认值为 0xFF…FF 执行 TCM_Startup 时 PCR 值被重置 PCR 能被 TCM_PCR_Reset 命令重置 TCM_HASH_START 重置 PCR 值为 0x00…00 执行 TCM_SaveSatePCR 值不能被保存 FALSE 表示： PCR 默认值为 0x00…00 只有在执行 Clear 模式的 TCM_Startup 时 PCR 值被重置 PCR 不能被 TCM_PCR_Reset 命令重置 执行 TCM_SaveSatePCR 值被保存
TCM_LOCALITY_SELECTION	pcrResetLocal	可以重置本地 PCR 的 locality
TCM_LOCALITY_SELECTION	pcrExtendLocal	可以扩展本地 PCR 的 locality

A.7 存储结构

A.7.1 TCM_STORED_DATA

结构定义：

```
typedef struct tdTCM_STORED_DATA {
    TCM_STRUCTURE_TAG tag;
    TCM_ENTITY_TYPE et;
    UINT32 sealInfoSize;
    [size_is(sealInfoSize)] BYTE * sealInfo;
    UINT32 encDataSize;
    [size_is(encDataSize)] BYTE * encData;
} TCM_STORED_DATA;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_STORED_DATA
TCM_ENTITY_TYPE	et	数据块类型
UINT32	sealInfoSize	sealInfo 的大小

类型	名称	描述
BYTE *	sealInfo	TCM_PCR_INFO 结构数据
UINT32	encDataSize	encData 的大小
BYTE *	encData	加密的 TCM_SEALED_DATA 结构数据

A.7.2 TCM_SEALED_DATA

结构定义：

```
typedef struct tdTCM_SEALED_DATA {
    TCM_PAYLOAD_TYPE payload;
    TCM_SECRET authData;
    TCM_NONCE TCMProof;
    TCM_DIGEST storedDigest;
    UINT32 dataSize;
    [size_is(dataSize)] BYTE * data;
} TCM_SEALED_DATA;
```

参数说明：

类型	名称	描述
TCM_PAYLOAD_TYPE	payload	TCM_PT_SEAL
TCM_SECRET	authData	授权数据
TCM_NONCE	TCMProof	平台唯一标识 TCM_PERMANENT_DATA->TCMProof
TCM_DIGEST	storedDigest	除 encDataSize 和 encData 外的 TCM_STORED_DATA 结构数据的摘要信息。
UINT32	dataSize	Data 的大小。
BYTE *	data	被封装的数据。

A.7.3 TCM_SYMMETRIC_KEY

结构定义：

```
typedef struct tdTCM_SYMMETRIC_KEY {
    TCM_ALGORITHM_ID algId;
    TCM_ENC_SCHEME encScheme;
    UINT16 size;
    [size_is(size)] BYTE * data;
} TCM_SYMMETRIC_KEY;
```

参数说明：

类型	名称	描述
TCM_ALGORITHM_ID	algId	对称算法 ID。
TCM_ENC_SCHEME	encScheme	加密模式。
UINT16	Size	对称密钥数据长度。
BYTE *	Data	对称密钥数据。

A.7.4 TCM_BOUND_DATA

结构定义：

```
typedef struct tdTCM_BOUND_DATA {
    TCM_STRUCT_VER ver;
    TCM_PAYLOAD_TYPE payload;
    BYTE[] payloadData;
    } TCM_BOUND_DATA;
```

参数说明：

类型	名称	描述
TCM_STRUCT_VER	ver	1.1.0.0
TCM_PAYLOAD_TYPE	payload	TCM_PT_BIND
BYTE[]	payloadData	数据。

A.8 TCM_KEY 结构

A.8.1 TCM_KEY_PARMS

结构定义：

```
typedef struct tdTCM_KEY_PARMS {
    TCM_ALGORITHM_ID algorithmID;
    TCM_ENC_SCHEME encScheme;
    TCM_SIG_SCHEME sigScheme;
    UINT32 parmSize;
    [size_is(parmSize)] BYTE * parms;
} TCM_KEY_PARMS;
```

参数说明：

类型	名称	描述
TCM_ALGORITHM_ID	algorithmID	所使用的算法标识。
TCM_ENC_SCHEME	encScheme	加密模式。
TCM_SIG_SCHEME	sigScheme	签名模式。
UINT32	parmSize	parms 的大小。
BYTE[]	parms	根据算法模式指向采用 TCM_SM2_ASYMKEY_PARAMETERS 或 TCM_STORE_SYMKEY_PARMS 的结构数据。

A.8.2 TCM_SM2_ASYMKEY_PARAMETERS

结构定义：

```
typedef struct td TCM_SM2_ ASYMKEY_PARAMETERS {
    UINT32 keyLength;                    4byte
```

} TCM_SM2_ ASYMKEY_PARAMETERS;

参数说明：

类型	名称	描述
UINT32	keyLength	密钥长度

A.8.3 TCM_SYMMETRIC_KEY_PARMS

结构定义：

```
typedef struct tdTCM_SYMMETRIC_KEY_PARMS {
    UINT32 keyLength;
    UINT32 blockSize;
    UINT32 ivSize;
    [size_is(ivSize)] BYTE IV;
} TCM_SYMMETRIC_KEY_PARMS;
```

参数说明：

类型	名称	描述
UINT32	keyLength	密钥比特长度
UINT32	blockSize	分组大小
UINT32	ivSize	初始向量长度
BYTE[]	IV	初始向量

A.8.4 TCM_KEY

结构定义：

```
typedef struct tdTCM_KEY{
TCM_STRUCTURE_TAG tag;
UINT16 fill;
    TCM_KEY_USAGE keyUsage;
    TCM_KEY_FLAGS keyFlags;
    TCM_AUTH_DATA_USAGE authDataUsage;
    TCM_KEY_PARMS algorithmParms;
    UINT32 PCRInfoSize;
    BYTE* PCRInfo;
    TCM_STORE_PUBKEY    pubKey;
    UINT32 encDataSize;
    [size_is(encDataSize)] BYTE* encData;max
} TCM_KEY;                          max 参数说明：
```

类型	名称	描述
TCM_STRUCTURE_TAG	Tag	TCM_TAG_KEY
UINT16	Fill	等于 0x0000
TCM_KEY_USAGE	keyUsage	密钥用途，是否可存储、可加密等

类型	名称	描述
TCM_KEY_FLAGS	keyFlags	密钥属性,是否可迁移等
TCM_AUTH_DATA_USAGE	authDataUsage	是否需要授权数据
TCM_KEY_PARMS	algorithmParms	算法参数信息
UINT32	PCRInfoSize	PCR 信息长度
BYTE *	PCRInfo	TCM_PCR_INFO 结构数据
TCM_STORE_PUBKEY	pubKey	公钥
UINT32	encDataSize	加密数据长度
BYTE *	encData	TCM_STORE_ASYMKEY 或 TCM_STORE_SYMKEY 加密数据

A.8.5 TCM_PUBKEY

结构定义:

typedef struct tdTCM_PUBKEY{ TCM_KEY_PARMS algorithmParms; TCM_STORE_PUBKEY pubKey;

} TCM_PUBKEY;

参数说明:

类型	名称	描述
TCM_KEY_PARMS	algorithmParms	密钥参数
TCM_STORE_PUBKEY	pubKey	公钥

A.8.6 TCM_STORE_PUBKEY

结构定义:

typedef struct tdTCM_STORE_PUBKEY { UINT32 keyLength; 4byte

[size_is(kenLenght)]BYTE * key; max 65byte :1(04)+32+32

} TCM_STORE_PUBKEY; max 69byte

参数说明:

类型	名称	描述
UINT32	keyLength	密钥长度
BYTE[]	Key	公钥

A.8.7 TCM_STORE_ASYMKEY

结构定义:

typedef struct tdTCM_STORE_ASYMKEY {

TCM_PAYLOAD_TYPE payload;

TCM_SECRET usageAuth;

TCM_SECRET migrationAuth;

TCM_DIGEST pubDataDigest;

```
    TCM_STORE_PRIVKEY privKey;
} TCM_STORE_ASYMKEY;
```

参数说明：

类型	名称	描述
TCM_PAYLOAD_TYPE	payload	TCM_PT_ASYM
TCM_SECRET	usageAuth	密钥使用授权数据
TCM_SECRET	migrationAuth	迁移授权数据
TCM_DIGEST	pubDataDigest	公钥数据摘要
TCM_STORE_PRIVKEY	privKey	私钥数据

A.8.8 TCM_STORE_SYMKEY

结构定义：

```
typedef struct tdTCM_STORE_SYMKEY {
    TCM_PAYLOAD_TYPE payload;
    TCM_SECRET usageAuth;
    TCM_SECRET migrationAuth;
    UINT16 size;
    [size_is(size)] BYTE* data;
} TCM_STORE_SYMKEY;
```

参数说明：

类型	名称	描述
TCM_ALGORITHM_ID	algId	对称密钥标识
TCM_ENC_SCHEME	encScheme	加密模式
UINT16	size	数据长度
BYTE*	data	密钥数据

A.8.9 TCM_STORE_PRIVKEY

结构定义：

```
typedef struct tdTCM_STORE_PRIVKEY {
    UINT32 keyLength;
    [size_is(keyLength)] BYTE* key;
} TCM_STORE_PRIVKEY;
```

参数说明：

类型	名称	描述
UINT32	keyLength	私钥长度
BYTE*	key	私钥数据

A.9 签名结构

A.9.1 TCM_CERTIFY_INFO

结构定义：

```
typedef struct tdTCM_CERTIFY_INFO{   TCM_STRUCT_VER version;
    TCM_KEY_USAGE keyUsage;
    TCM_KEY_FLAGS keyFlags;
    TCM_AUTH_DATA_USAGE authDataUsage;
    TCM_KEY_PARMS algorithmParms;
    TCM_DIGEST pubkeyDigest;
    TCM_NONCE data;
    BOOL parentPCRStatus;
    UINT32 PCRInfoSize;
    [size_is(pcrInfoSize)] BYTE* PCRInfo;
} TCM_CERTIFY_INFO;
```

参数说明：

类型	名称	描述
TCM_STRUCT_VER	Version	等于 1
TCM_KEY_USAGE	keyUsage	密钥用途
TCM_KEY_FLAGS	keyFlags	密钥属性，是否可迁移等
TCM_AUTH_DATA_USAGE	authDataUsage	是否需要授权数据
TCM_KEY_PARMS	algorithmParms	算法参数
TCM_DIGEST	pubKeyDigest	公钥摘要
TCM_NONCE	Data	防重放攻击参数
BOOL	parentPCRStatus	表明父密钥是否和 PCR 绑定
UINT32	PCRInfoSize	PCR 信息长度
BYTE*	PCRInfo	PCR 信息

A.9.2 TCM_QUOTE_INFO

结构定义：

```
typedef struct tdTCM_QUOTE_INFO{
    TCM_STRUCTURE_TAG tag;
    BYTE fixed[4];
    TCM_NONCE externalData;
    TCM_PCR_INFO info;
} TCM_QUOTE_INFO;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_QUOTE_INFO
BYTE	fixed	固定值'QUOT'
TCM_NONCE	externalData	32 字节防重放攻击参数
TCM_PCR_INFO	info	PCR 信息

A.10 身份结构

A.10.1 TCM_EK_BLOB

结构定义：

```
typedef struct tdTCM_EK_BLOB{
    TCM_STRUCTURE_TAG  tag;
    TCM_EK_TYPE ekType;
    UINT32 blobSize;
    [size_is(blobSize)] byte * blob;
} TCM_EK_BLOB;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	Tag	TCM_TAG_EK_BLOB
TCM_EK_TYPE	EkType	数据块类型
UINT32	BlobSize	EK 数据块长度
BYTE *	Blob	EK 数据块

A.10.2 TCM_EK_BLOB_ACTIVATE

结构定义：

```
typedef struct tdTCM_EK_BLOB_ACTIVATE{
    TCM_STRUCTURE_TAG  tag;
    TCM_SYMMETRIC_KEY sessionKey;
    TCM_DIGEST idDigest;
    TCM_PCR_INFO pcrInfo;
} TCM_EK_BLOB_ACTIVATE;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	Tag	TCM_TAG_EK_BLOB_ACTIVATE
TCM_SYMMETRIC_KEY	SessionKey	CA 产生的对称会话密钥
TCM_DIGEST	IdDigest	TCM_PUBKEY 摘要
TCM_PCR_INFO	PcrInfo	PCR 信息

A.10.3 TCM_EK_BLOB_AUTH

结构定义：

```
typedef struct tdTCM_EK_BLOB_AUTH{
    TCM_STRUCTURE_TAG    tag;
    TCM_SECRET authValue;
} TCM_EK_BLOB_AUTH;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	Tag	TCM_TAG_EK_BLOB_AUTH
TCM_SECRET	AuthValue	EK 授权数据

A.10.4 TCM_CHOSENID_HASH

参数说明：

类型	名称	描述
BYTE[ ]	IdentityLabel	身份信息
TCM_PUBKEY	PrivacyCA	CA 的公钥数据

TCM_CHOSENID_HASH = SM3(identityLabel || privacyCA)

A.10.5 TCM_IDENTITY_CONTENTS

结构定义：

```
typedef struct tdTCM_IDENTITY_CONTENTS {
    TCM_STRUCT_VER          ver;
    UINT32                  ordinal;
    TCM_CHOSENID_HASH   labelPrivCADigest;
    TCM_PUBKEY              identityPubKey;
} TCM_IDENTITY_CONTENTS;
```

参数说明：

类型	名称	描述
TCM_STRUCT_VER	Ver	等于 1
UINT32	Ordinal	TCM_MakeIdentity 命令码
TCM_CHOSENID_HASH	LabelPrivCADigest	身份信息和公钥的摘要
TCM_PUBKEY	IdentityPubKey	PIK 公钥

A.10.6 TCM_IDENTITY_REQ

参数说明：

类型	名称	描述
UINT32	AsymSize	AsymBlob 的长度
UINT32	SymSize	SymBlob 的长度
TCM_KEY_PARMS	asymAlgorithm	非对称算法参数
TCM_KEY_PARMS	symAlgorithm	对称算法参数
BYTE *	AsymBlob	非对称加密数据区，可信方公钥对对称密钥进行加密的结果
BYTE *	SymBlob	对称加密数据区（TCM_IDENTITY_PROOF 结构加密数据）

A.10.7 TCM_PEK_REQ

参数说明：

类型	名称	描述
UINT32	AsymSize	AsymBlob 的长度
UINT32	SymSize	SymBlob 的长度
TCM_KEY_PARMS	asymAlgorithm	非对称算法参数
TCM_KEY_PARMS	symAlgorithm	对称算法参数
BYTE *	AsymBlob	非对称加密数据区，可信方公钥对对称密钥进行加密的结果
BYTE *	SymBlob	对称加密数据区（TCM_PEK_PROOF 结构加密数据）

A.10.8 TCM_IDENTITY_PROOF

类型	名称	描述
TCM_STRUCT_VER	Ver	等于 1
UINT32	LabelSize	平台身份标识长度
UINT32	IdentityBindingSize	身份绑定信息长度
UINT32	EndorsementSize	EK 证书长度
TCM_PUBKEY	IdentityKey	身份公钥
BYTE *	LabelArea	平台身份标识
BYTE *	IdentityBinding	TCM_IDENTITY_CONTENTS 的摘要
BYTE *	EndorsementCredential	EK 证书

A.10.9 TCM_PEK_PROOF

类型	名称	描述
TCM_STRUCT_VER	Ver	等于 1
UINT32	LabelSize	平台身份标识长度
UINT32	EndorsementSize	EK 证书长度
TCM_KEY_PARMS	IdentityKey	PEK 公钥参数
BYTE *	LabelArea	平台身份标识
BYTE *	EndorsementCredential	EK 证书

A.10.10 TCM_ASYM_CA_CONTENTS

结构定义：

```
typedef struct tdTCM_ASYM_CA_CONTENTS{
    TCM_SYMMETRIC_KEY sessionKey;
    TCM_DIGEST idDigest;
} TCM_ASYM_CA_CONTENTS;
```

参数说明：

类型	名称	描述
TCM_SYMMETRIC_KEY	SessionKey	CA 产生的对称会话密钥
TCM_DIGEST	IdDigest	TCM_PUBKEY 的摘要

A.10.11 TCM_ASYM_CA_PEK_CONTENTS

结构定义：

```
typedef struct tdTCM_ASYM_CA_CONTENTS{
    TCM_SYMMETRIC_KEY sessionKey;
} TCM_ASYM_CA_PEK_CONTENTS;
```

参数说明：

类型	名称	描述
TCM_SYMMETRIC_KEY	SessionKey	CA 产生的对称会话密钥

A.10.12 TCM_SYM_CA_ATTESTATION

类型	名称	描述
UINT32	credSize	证书参数长度
TCM_KEY_PARMS	algorithm	算法参数
BYTE *	credential	身份证书

A.11 传输结构

A.11.1 TCM _TRANSPORT_PUBLIC

结构定义：

```
typedef struct tdTCM_TRANSPORT_PUBLIC{
    TCM_STRUCTURE_TAG    tag;
    TCM_TRANSPORT_ATTRIBUTES transAttributes;
    TCM_ALGORITHM_ID algID;
    TCM_ENC_SCHEME encScheme;
} TCM_TRANSPORT_PUBLIC
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	Tag	TCM_TAG_TRANSPORT_PUBLIC
TCM_TRANSPORT_ATTRIBUTES	transAttributes	传输会话属性
TCM_ALGORITHM_ID	AlgId	算法标识
TCM_ENC_SCHEME	EncScheme	加密模式

A.11.2 TCM_TRANSPORT_INTERNAL

结构定义：

```
typedef struct tdTCM_TRANSPORT_INTERNAL{
    TCM_STRUCTURE_TAG    tag;
    TCM_AUTHDATA authData;
    TCM_TRANSPORT_PUBLIC tranPublic;
    TCM_TRANSHANDLE transHandle;
    TCM_NONCE transEven;
    TCM_DIGEST transDigest;
} TCM_TRANSPORT_INTERNAL;
```

A.11.3 TCM_TRANSPORT_AUTH

```
typedef struct tdTCM_TRANSPORT_AUTH {
    TCM_STRUCTURE_TAG    tag;
    TCM_AUTHDATA authData;
} TCM_TRANSPORT_AUTH;
```

A.12 命令码

命令码长度为32bit，只使用低16bit，使用0x0800-0x08ff。

A.13 上下文结构

A.13.1 TCM_CONTEXT_BLOB

结构定义：

```
typedef struct tdTCM_CONTEXT_BLOB {
    TCM_STRUCTURE_TAG tag;
    TCM_RESOURCE_TYPE resourceType;
    TCM_HANDLE handle;
    BYTE[16] label;
    UINT32 contextCount;
    TCM_DIGEST integrityDigest;
    UINT32 additionalSize;
    [size_is(additionalSize)] BYTE * additionalData;
    UINT32 sensitiveSize;5
```

```
    [size_is(sensitiveSize)] BYTE * sensitiveData;
}TCM_CONTEXT_BLOB;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	标记
TCM_RESOURCE_TYPE	resourceType	资源类型
TCM_HANDLE	handle	资源句柄
BYTE[16]	label	用于保存资源的标识
UINT32	contextCount	用于上下文防重放攻击，创建时等于 TCM_STANY_DATA -> contextCount
TCM_DIGEST	integrityDigest	整个结构的摘要
UINT32	additionalSize	厂商自定义信息大小
BYTE	additionalData	厂商自定义信息
UINT32	sensitiveSize	要保存的敏感信息大小
BYTE	sensitiveData	要保存的敏感信息

A.13.2 TCM_CONTEXT_SENSITIVE

结构定义：

```
typedef struct tdTCM_CONTEXT_SENSITIVE {
    TCM_STRUCTURE_TAG tag;
    TCM_NONCE contextNonce;
    UINT32 internalSize;
    [size_is(internalSize)] BYTE * internalData;
}TCM_CONTEXT_SENSITIVE;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_CONTEXT_SENSITIVE 标记
TCM_NONCE	contextNonce	防重放参数，如果保存的是 KEY，这个值等于 TCM_STCLEAR_DATA -> contextNonceKey 否则等于 TCM_STANY_DATA -> contextNonceSession
UINT32	internalSize	自定义敏感数据大小
BYTE	internalData	自定义敏感数据

A.14 非易失性存储结构

A.14.1 TCM_NV_INDEX

TCM_NV_INDEX 为 32 位值

		3						2		1	
1	0	9	8	7	6	5	4	3 2 1 0 9 8 7 6		5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0	
T	P	U	D	保留				Purview		索引	

T 为 TCM 制造商保留。

P 为平台制造商保留。

U 为平台用户保留。

D 为 1 表明该 Index 已经永久定义

部分固定的 TCM_NV_INDEX

值	索引名称	描述
0xFFFFFFFF	TCM_NV_INDEX_LOCK	设置 NV 授权保护，使用 TCM_NV_DefineSpace 来设置，其中输入的数据大小为 0
0x00000000	TCM_NV_INDEX0	用于设置 bGlobalLock 标记，使用 TCM_NV_WriteValue 来设置，其中输入的数据大小为 0

值	索引名称	描述
0x0000F000	TCM_NV_INDEX_EKCert	EK 证书
0x000111xx	TCM_NV_INDEX_TSS	保留给 TSM 使用
0x000112xx	TCM_NV_INDEX_PC	保留给 PC Client 使用
0x000113xx	TCM_NV_INDEX_SERVER	保留给 Server 使用
0x000114xx	TCM_NV_INDEX_MOBILE	保留给 mobile 使用
0x000115xx	TCM_NV_INDEX_PERIPHERAL	保留给 peripheral 使用
0x000116xx	TCM_NV_INDEX_GPIO_xx	保留给 GPIO 使用

A.14.2 TCM_NV_ATTRIBUTES

结构定义：

```
typedef struct tdTCM_NV_ATTRIBUTES{
    TCM_STRUCTURE_TAG tag;
    UINT32 attributes;
} TCM_NV_ATTRIBUTES;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	Tag	TCM_TAG_NV_ATTRIBUTES 标记
UINT32	attributes	属性数据

属性值

位	名称	描述
31	TCM_NV_PER_READ_STCLEAR	加锁前可读
30：19	Reserved	保留

位	名称	描述
18	TCM_NV_PER_AUTHREAD	需要授权才能读
17	TCM_NV_PER_OWNERREAD	Owner 授权才能读
16	TCM_NV_PER_PPREAD	物理现场授权才能读
15	TCM_NV_PER_GLOBALLOCK	全局锁标记
14	TCM_NV_PER_WRITE_STCLEAR	加锁前可写
13	TCM_NV_PER_WRITEDEFINE	定义后只能写一次
12	TCM_NV_PER_WRITEALL	把指定的 NV 空间填满
11：3	Reserved for write additions	保留
2	TCM_NV_PER_AUTHWRITE	需要授权才能写
1	TCM_NV_PER_OWNERWRITE	Owner 授权才能写
0	TCM_NV_PER_PPWRITE	物理现场授权才能写

A.14.3 TCM_NV_DATA_PUBLIC

结构定义：

```
typedef struct tdTCM_NV_DATA_PUBLIC {
    TCM_STRUCTURE_TAG tag;
    TCM_NV_INDEX nvIndex;
    TCM_PCR_INFO pcrInfoRead;
    TCM_PCR_INFO pcrInfoWrite;
    TCM_NV_ATTRIBUTES permission;
    BOOL bReadSTClear;
    BOOL bWriteSTClear;
    BOOL bWriteDefine;
    UINT32 dataSize;
} TCM_NV_DATA_PUBLIC;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_NV_DATA_PUBLIC 标记
TCM_NV_INDEX	nvIndex	NV 索引
TCM_PCR_INFO	pcrInfoRead	读取数据时的 PCR 信息
TCM_PCR_INFO	pcrInfoWrite	写入数据时的 PCR 信息
TCM_NV_ATTRIBUTES	permission	操作 NV 空间的权限
BOOL	bReadSTClear	TCM_Startup(ST_Clear)设为 TRUE，使用 ReadValue 或者 ReadValueAuth 设为 FALSE，输入数据长度为 0
BOOL	bWriteSTClear	TCM_Startup(ST_CLEAR) 设为 FALSE，使用 WriteValue 或者 WriteValueAuth 设为 TRUE，输入数据长度为 0
BOOL	bWriteDefine	TCM_NV_DefineSpace 设为 FALSE，使用 WriteValue 设为 TRUE，输入数据长度为 0
UINT32	dataSize	数据大小

A.14.4 TCM_NV_DATA_SENSITIVE

结构定义：

```
typedef struct tdTCM_NV_DATA_SENSITIVE {
    TCM_STRUCTURE_TAG tag;
    TCM_NV_DATA_PUBLIC pubInfo;
    TCM_AUTHDATA authValue;
    [size_is(dataSize)] BYTE * data;
} TCM_NV_DATA_SENSITIVE;
```

参数说明：

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_NV_DATA_SENSITIVE 标记
TCM_NV_DATA_PUBLIC	pubInfo	NV 公开信息
TCM_AUTHDATA	authValue	NV 空间授权数据
BYTE *	data	敏感数据

A.14.5 TCM_NV_DATA_AREA

该结构为内部数据，内容包含 TCM_NV_DATA_PUBLIC、TCM_NV_DATA_SENSITIVE 结构。

A.15 Capability 域

A.15.1 TCM_CAPABILITY_AREA

值	属性	子属性	描述
0x00000001	TCM_CAP_ORD	命令号	返回为真表示 TCM 支持该命令号。
0x00000002	TCM_CAP_ALG	TCM_ALGORITHM_ID	返回为真表示 TCM 支持该算法
0x00000003	TCM_CAP_PID	TCM_PROTOCOL_ID	返回为真表示 TCM 支持该协议
0x00000004	TCM_CAP_FLAG		
0x00000108	TCM_CAP_FLAG_PERMANENT	返回 TCM_PERMANENT_FLAGS 结构	
0x00000109	TCM_CAP_FLAG_VOLATILE	返回 TCM_STCLEAR_FLAGS 结构	
0x00000006	TCM_CAP_VERSION		返回 TCM 版本信息
0x00000007	TCM_CAP_KEY_HANDLE		返回当前 TCM 加载的所有密钥句柄，不包括 EK 和 SMK
0x00000008	TCM_CAP_CHECK_LOADED	TCM_KEY_PARMS	返回为真，表明 TCM 有足够的内存支持密钥加载，返回为假，表明 TCM 没有足够的内存。子域
0x00000009	TCM_CAP_SYM_MODE	TCM_SYM_MODE	返回为真表示支持对称算法
0x0000000C	TCM_CAP_KEY_STATUS	handle	返回真表明该密钥必须使用 Owner 逐出

值	属性	子属性	描述
0x0000000D	TCM_CAP_NV_LIST		返回 NV 索引列表
0x00000010	TCM_CAP_MFR		返回厂商自定义的 TCM 信息
0x00000011	TCM_CAP_NV_INDEX	TCM_NV_INDEX	返回 TCM_NV_DATA_PUBLIC 中指定的 NV 索引，如果索引不在 TCM_CA_NV_LIST 表中，返回 TCM_BAD_INDEX
0x00000012	TCM_CAP_TRANS_ALG	TCM_ALGORITHM_ID	返回为真，表明 TCM 支持 TCM_EstablishTransport，TCM _ ExecuteTransport and TCM_ReleaseTransport 中使用的算法
0x00000014	TCM_CAP_HANDLE	TCM_RESOURCE_TYPE	返回所有已加载的指定资源类型的句柄
0x00000015	TCM_CAP_TRANS_ES	TCM_ENC_SCHEME	布尔值，返回为真表明传输会话中支持该种加密模式
0x00000017	TCM_CAP_AUTH_ENCRYPT	TCM_ALGORITHM_ID	布尔值，返回为真表明 AP 会话授权数据的加密方式支持该加密算法
0x00000018	TCM_CAP_SELECT_SIZE	TCM_SELECT_SIZE	布尔值，返回为真表明 TCM 中 TCM_PCR_SELECT->sizeOfSelect 的 repSize 支持给定的版本
0x0000001A	TCM_CAP_VERSION_VAL		返回 TCM_CAP_VERSION_INFO 版本信息

A.15.2 CAP_PROPERTY

值	属性	描述
0x00000101	TCM_CAP_PROP_PCR	返回当前 PCR 数目
0x00000103	TCM_CAP_PROP_MANUFACTURER	返回制造商信息
0x00000104	TCM_CAP_PROP_KEYS	返回可加载的密钥数量
0x00000107	TCM_CAP_PROP_MIN_COUNTER	计数器加一的最小时间间隔，前提是计数器按照每秒十次的增长速度。
0x0000010A	TCM_CAP_PROP_AUTHSESS	返回支持的授权会话数量
0x0000010B	TCM_CAP_PROP_TRANSESS	返回支持的传输会话数量
0x0000010C	TCM_CAP_PROP_COUNTERS	返回支持的单调计数器数量
0x0000010D	TCM_CAP_PROP_MAX_AUTHSESS	返回 TCM 已加载的最大授权会话
0x0000010E	TCM_CAP_PROP_MAX_TRANSESS	返回 TCM 已加载的最大传输会话
0x0000010F	TCM_CAP_PROP_MAX_COUNTERS	返回使用 TCM_CreateCounter 创建的最大单调计数器数量
0x00000110	TCM_CAP_PROP_MAX_KEYS	返回 TCM 支持的密钥数量，该数量不包括 EK 或 SMK
0x00000111	TCM_CAP_PROP_OWNER	返回为真表明 TCM 成功创建 Owner
0x00000112	TCM_CAP_PROP_CONTEXT	返回可保存的会话数目，该值随环境改变
0x00000113	TCM_CAP_PROP_MAX_CONTEXT	返回最大的可保存的会话数目
0x00000116	TCM_CAP_PROP_STARTUP_EFFECT	返回 TCM_STARTUP_EFFECTS 结构

值	属性	描述
0x0000011B	TCM_CAP_PROP_CONTEXT_DIST	返回 context count 值的最大距离
0X0000011D	TCM_CAP_PROP_SESSIONS	返回可行的会话数目，包括授权会话、传输会话、协商会话，该值随环境改变
0x0000011E	TCM_CAP_PROP_MAX_SESSIONS	返回支持的最大会话数目，包括授权会话、传输会话、协商会话
0x000001220	TCM_CAP_PROP_DURATION	返回命令执行时间，可以为长、中、短三种
0x00000122	TCM_CAP_PROP_ACTIVE_COUNTER	返回当前计数器 ID
0x00000123	TCM_CAP_PROP_MAX_NV_AVAILABLE	返回 NV 最大可分配的空间，该值随环境改变
0x00000124	TCM_CAP_PROP_INPUT_BUFFER	返回 TCM 输入缓冲区的大小

A.15.3 TCM_CAPABILITY_AREA

值	参数名	子参数	描述
0x00000001	TCM_SET_PERM_FLAGS	TCM _ PERMANENT _ FLAGS structure	设置 TCM_PERMANENT_FLAGS 中的数据
0x00000002	TCM_SET_PERM_DATA	TCM _ PERMANENT _ DATA structure	设置 TCM_PERMANENT_DATA 中的数据
0x00000003	TCM_SET_STCLEAR_FLAGS	TCM_STCLEAR_FLAGS structure	设置 TCM _ STCLEAR _ FLAGS 中的数据
0x00000004	TCM_SET_STCLEAR_DATA	TCM_STCLEAR_DATA structure	设置 TCM_STCLEAR_DATA 中的数据
0x00000005	TCM_SET_STANY_FLAGS	TCM_STANY_FLAGS structure	设置 TCM_STANY_FLAGS 中的数据
0x00000006	TCM_SET_STANY_DATA	TCM_STANY_DATA structure	设置 TCM_STANY_DATA 中的数据
0x00000007	TCM_SET_VENDOR	Vendor specific	厂商自定义

A.15.4 SetCapability 子属性

A.15.4.1 TCM_PERMANENT_FLAGS

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+1 TCM_PF_DISABLE	Y	所有者授权或物理现场	TCM_OwnerSetDisable TCM_PhysicalEnable TCM_PhysicalDisable
+2 TCM_PF_OWNERSHIP	Y	无授权。没有执行创建所有者的操作。需声明物理现场 TCM 无效模式或禁用模式不能使用	TCM_SetOwnerInstall

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+3 TCM_PF_DEACTIVATED	Y	无授权,需声明物理存在 TCM 禁用模式不能使用	TCM_PhysicalSetDeactivated
+4 TCM_PF_READPUBEK	Y	所有者授权 TCM 无效模式或禁用模式不能使用	
+5 TCM_PF_DISABLEOWNER-CLEAR	Y	所有者授权。只能设置为 T 真.只有 ForceClear 操作能够重置该值为假。 TCM 无效模式或者禁用模式无能使用。	TCM_DisableOwnerClear
+6 TCM_PF_PHYSICALPRES-ENCELIFETIMELOCK	N		
+7 TCM_PF_PHYSICALPRES-ENCEHWENABLE	N		
+8 TCM_PF_PHYSICALPRES-ENCECMDENABLE	N		
+9 TCM_PF_CEKPUSED	N		
+10 TCM_PF_TCMPOST	N		
+11 TCM_PF_TCMPOSTLOCK	N		
+12 TCM_PF_OPERATOR	N		
+13 TCM_PF_ENABLEREVO-KEEK	N		
+14 TCM_PF_NV_LOCKED	N		
+15 TCM_PF_TCMESTAB-LISHED	Y	Locality 3 或 locality 4 仅能设置为 FALSE	
+16 TCM_PF_WRITEEKCERT-LOCK	N		

A.15.4.2 TCM_PERMANENT_DATA

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+1 TCM_PD_REVMAJOR	N		
+2 TCM_PD_REVMINOR	N		
+3 TCM_PD_TCMPROOF	N		
+4TCM_PD_EKRESET			
+5 TCM_PD_OWNERAUTH	N		
+6 TCM_PD_OPERATORAUTH	N		
+7 TCM_PD_ENDORSEMENTKEY	N		
+8 TCM_PD_SMK	N		
+9 TCM_PD_DELEGATEKEY	N		
+10 TCM_PD_CONTEXTKEY	N		

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+11 TCM_PD_AUDITMONOTONICCOUNTER	N		
+12 TCM_PD_MONOTONICCOUNTER	N		
+13 TCM_PD_PCRATTRIB	N		
+14 TCM_PD_ORDINALAUDITSTATUS	N		
+15 TCM_PD_RNGSTATE	N		
+16 TCM_PD_FAMILYTABLE	N		
+17 TCM_DELEGATETABLE	N		
+18 TCM_PD_EKRESET	N		
+19 TCM_PD_MAXNVBUFSIZE	N		
+20TCM_PD_LASTFAMILYID	N		
+21 TCM_PD_NOOWNERNVWRITE	N		

A.15.4.3 TCM_STCLEAR_FLAGS

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+1 TCM_SF_DEACTIVATED	N		
+2 TCM_SF_DISABLEFORCECLEAR	Y	TCM 无效模式或禁用模式不能使用。只能设置为真。	TCM_DisableForceClear
+3 TCM_SF_PHYSICALPRESENCE	N		
+4 TCM_SF_PHYSICALPRESENCELOCK	N		
+5 TCM_SF_BGLOBALLOCK	N		

A.15.4.4 TCM_STCLEAR_DATA

标识 SubCap 值 r 0x00000000+	设置	设置限制	行为来源
+1 TCM_SD_CONTEXTNONCEKEY	N		
+2 TCM_SD_COUNTID	N		
+3 TCM_SD_OWNERREFERENCE	N		
+4 TCM_SD_DISABLERESETLOCK	N		
+5 TCM_SD_PCR	N		
+6TCM_SD_DEFERREDPHYSICALPRESENCE	Y	只有在声明物理现场时能设置为真。任何权限都能设置为假。	TCM_SetCapability

A.15.4.5 TCM_STANY_FLAGS

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+1 TCM_AF_POSTINITIALISE	N		
+2 TCM_AF_LOCALITYMODIFIER	N		

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+3 TCM_AF_TRANSPORTEXCLUSIVE	N		
+4 TCM_AF_TOSPRESENT	Y	Locality 3 或 Locality4，仅能设置为 FALSE	
TCM 为失效或者禁用模式时不能执行			

A.15.4.6 TCM_STANY_DATA

标识 SubCap 值 0x00000000+	设置	设置限制	行为来源
+1 TCM_AD_CONTEXTNONCESESSION	N		
+2 TCM_AD_AUDITDIGEST	N		
+3 TCM_AD_CURRENTTICKS	N		
+4 TCM_AD_CONTEXTCOUNT	N		
+5 TCM_AD_CONTEXTLIST	N		
+6 TCM_AD_SESSIONS	N		

A.15.5 TCM_CAP_VERSION_INFO

结构定义：

```
typedef struct tdTCM_CAP_VERSION_INFO {
    TCM_STRUCTURE_TAG tag;
    TCM_VERSION version;
    UINT16 specLevel;
    BYTE errataRev;
    BYTE TCMVendorID[4];
    UINT16 vendorSpecificSize;
    [size_is(vendorSpecificSize)] BYTE * vendorSpecific;
} TCM_CAP_VERSION_INFO;
```

类型	名称	描述
TCM_STRUCTURE_TAG	tag	TCM_TAG_CAP_VERSION_INFO 标记
TCM_VERSION	version	主版本
UINT16	specLevel	文档版本
TCM_VERSION_BYTE	errataRev	修订版本
BYTE	TCMVendorID	厂商 ID
UINT16	vendorSpecificSize	厂商特定信息大小
BYTE *	vendorSpecific	厂商特定信息

A.16 返回码定义

注释：

TCM 有五种类型的返回码。一种表明操作成功，四种表明失败。TCM_SUCCESS(00000000)表示执行成功。失败的报告是：TCM 定义致命错误(00000001 至 000003FF)，供应商定义致命错误(00000400 至 000007FF)，TCM 定义非致命错误(00000800 至 00000BFF)，供应商定义的非致命错误(00000C00 到 00000FFF)。

描述：

1) 当一个命令因任何原因失败，TCM 必须只返回以下三个项目：
   a) tag (2 bytes，fixed at TCM_TAG_RSP_COMMAND)
   b) paramSize (4 bytes，fixed at 10)
   c) returnCode (4 bytes，never TCM_SUCCESS)
2) 当一个命令失败，TCM 必须返回合法的错误代码。否则，TCM 应返回 TCM_SUCCESS。如果 TCM 执行一条命令后返回一个错误代码，它应该由该命令制定的错误码或是与错误条件适应的合法错误码。
3) 一个致命的失败将终止相关的授权或传输会话。非致命失败不引起相关授权或传输会话终止。
4) 一个打包命令的致命失败不引起打包该命令的传输会话中断。例外情况是当该失败的导致 TCM 本身进入失败模式(自检失败，等等)
5) 返回码必须使用下面的基数。返回码可以是 TCM 规范定义的或供应商定义的。

A.16.1 Mask 参数说明

名称	值	描述
TCM_BASE	0x00000000	TCM 返回码起始值
TCM_SUCCESS	TCM_BASE	操作成功完成
TCM_VENDOR_ERROR	0x00000400	卖主定义码掩码
TCM_NON_FATAL	0x00000800	非致命失败错误码掩码

A.16.2 TCM 定义的致命的错误码

名称	值	描述
TCM_AUTHFAIL	TCM_BASE+1	授权失败
TCM_BADINDEX	TCM_BASE+2	指向 PCR 或者其他寄存器的索引错误
TCM_BAD_PARAMETER	TCM_BASE+3	一个或者更多的参数错误
TCM_AUDITFAILURE	TCM_BASE+4	操作正确完成但是审计操作失败
TCM_CLEAR_DISABLED	TCM_BASE+5	Clear disable 标识位被设置
TCM_DEACTIVATED	TCM_BASE+6	TCM 处于无效模式
TCM_DISABLED	TCM_BASE+7	TCM 处于禁用模式
TCM_DISABLED_CMD	TCM_BASE+8	目标命令被禁用
TCM_FAIL	TCM_BASE+9	操作失效
TCM_BAD_ORDINAL	TCM_BASE+10	不认识或者的命令序列
TCM_INSTALL_DISABLED	TCM_BASE+11	安装所有权的能力被禁用
TCM_INVALID_KEYHANDLE	TCM_BASE+12	密钥句柄不能被解读

名称	值	描述
TCM_KEYNOTFOUND	TCM_BASE+13	密钥句柄指向无效密钥
TCM_INAPPROPRIATE_ENC	TCM_BASE+14	不能接受的加密策略
TCM_MIGRATEFAIL	TCM_BASE+15	迁移授权失败
TCM_INVALID_PCR_INFO	TCM_BASE+16	PCR 信息不能被解读
TCM_NOSPACE	TCM_BASE+17	没有足够的空间加载密钥
TCM_NOSMK	TCM_BASE+18	没有安装 SMK
TCM_NOTSEALED_BLOB	TCM_BASE+19	加密数据块无效或不是该 TCM 产生的加密数据块
TCM_OWNER_SET	TCM_BASE+20	所有者已经存在
TCM_RESOURCES	TCM_BASE+21	TCM 没有足够的内部资源执行请求操作
TCM_SHORTRANDOM	TCM_BASE+22	随机字符串太短
TCM_SIZE	TCM_BASE+23	TCM 没有足够的空间执行该操作
TCM_WRONGPCRVAL	TCM_BASE+24	使用的 PCR 至于 TCM 当前 PCR 值不匹配
TCM_BAD_PARAM_SIZE	TCM_BASE+25	命令的 paramSize 参数值错误
TCM_SM3_THREAD	TCM_BASE+26	没有 SM3 线程
TCM_SM3_ERROR	TCM_BASE+27	SM3 线程出现错误,不能完成计算
TCM_FAILEDSELFTEST	TCM_BASE+28	自检失败,TCM 关闭
TCM_AUTH2FAIL	TCM_BASE+29	命令第二个密钥授权失败
TCM_BADTAG	TCM_BASE+30	命令 Tag 参数错误
TCM_IOERROR	TCM_BASE+31	传输信息给 TCM 时发生 I/O 错误
TCM_ENCRYPT_ERROR	TCM_BASE+32	加密过程出现问题
TCM_DECRYPT_ERROR	TCM_BASE+33	解密过程未完成
TCM_INVALID_AUTHHANDLE	TCM_BASE+34	使用无效句柄
TCM_NO_ENDORSEMENT	TCM_BASE+35	TCM 没有安装 EK
TCM_INVALID_KEYUSAGE	TCM_BASE+36	不被允许的 Key 用法
TCM_WRONG_ENTITYTYPE	TCM_BASE+37	不被允许的实体类型
TCM_INVALID_POSTINIT	TCM_BASE+38	TCM_Init 命令后发送了错误的命令序列,后续命令为 TCM_Startup
TCM_INAPPROPRIATE_SIG	TCM_BASE+39	签名数据不能包含 DER 信息
TCM_BAD_KEY_PROPERTY	TCM_BASE+40	TCM 的 TCM_KEY_PARM 结构不支持该密钥特性
TCM_BAD_MIGRATION	TCM_BASE+41	密钥迁移策略错误
TCM_BAD_SCHEME	TCM_BASE+42	密钥的签名或者加密策略错误
TCM_BAD_DATASIZE	TCM_BASE+43	密钥相关的数据大小不一致或者不匹配
TCM_BAD_MODE	TCM_BASE+44	参数模式不正确,\
TCM_BAD_PRESENCE	TCM_BASE+45	physicalPresence 或 physicalPresenceLock 位存在错误的值
TCM_BAD_VERSION	TCM_BASE+46	TCM 不能执行给定版本的能力

名称	值	描述
TCM_NO_WRAP_TRANSPORT	TCM_BASE+47	TCM 不允许掩护传输会话
TCM_AUDITFAIL_UNSUCCESSFUL	TCM_BASE+48	审计操作失败,后续命令进入返回错误
TCM_AUDITFAIL_SUCCESSFUL	TCM_BASE+49	审计操作成功,后续命令返回成功
TCM_NOTRESETABLE	TCM_BASE+50	尝试重置不具备重置属性的 PCR 寄存器
TCM_NOTLOCAL	TCM_BASE+51	尝试重置不在当前 Locality 下可重置的 PCR 寄存器
TCM_BAD_TYPE	TCM_BASE+52	错误的类型标识
TCM_INVALID_RESOURCE	TCM_BASE+53	预备保存的上下文与当前实际环境不一致
TCM_NO_NV_PERMISSION	TCM_BASE+56	使用非当前被操作 NV 许可的授权操作
TCM_REQUIRES_SIGN	TCM_BASE+57	操作需要签名的命令
TCM_AREA_LOCKED	TCM_BASE+60	NV 被锁,不能执行写操作
TCM_BAD_LOCALITY	TCM_BASE+61	当前 Locality 不能执行该操作
TCM_READ_ONLY	TCM_BASE+62	NV 只能读
TCM_PER_NOWRITE	TCM_BASE+63	当前 NV 不能被写
TCM_WRITE_LOCKED	TCM_BASE+65	NV 写操作已完成,不能执行写操作
TCM_BAD_ATTRIBUTES	TCM_BASE+66	NV 区域属性冲突
TCM_INVALID_STRUCTURE	TCM_BASE+67	结构的 tag 和 version 域无效或者不匹配
TCM_BAD_COUNTER	TCM_BASE+69	计数器句柄错误
TCM_NOT_FULLWRITE	TCM_BASE+70	写操作未完成
TCM_CONTEXT_GAP	TCM_BASE+71	被保存的上下文间隙太大
TCM_MAXNVWRITES	TCM_BASE+72	超过的没有所有者时最大的 NV 写限制
TCM_NOOPERATOR	TCM_BASE+73	没有设置操作者授权数据
TCM_RESOURCEMISSING	TCM_BASE+74	上下文指定的资源未被加载
TCM_TRANSPORT_NOTEXCLUSIVE	TCM_BASE+78	有命令在排外传输会话外执行
TCM_BAD_HANDLE	TCM_BASE+88	错误的句柄
TCM_BADCONTEXT	TCM_BASE+90	无效的上下文
TCM_TOOMANYCONTEXTS	TCM_BASE+91	需保存的上下文超过 TCM 允许数量
TCM_MA_TICKET_SIGNATURE	TCM_BASE+92	迁移授权验证失败
TCM_MA_DESTINATION	TCM_BASE+93	迁移目标未被授权
TCM_MA_SOURCE	TCM_BASE+94	被迁移数据不正确
TCM_MA_AUTHORITY	TCM_BASE+95	不正确的迁移授权
TCM_PERMANENTEK	TCM_BASE+97	尝试 撤销不可撤销 EK
TCM_BAD_SIGNATURE	TCM_BASE+98	错误的签名
TCM_NOCONTEXTSPACE	TCM_BASE+99	上下文列表中没有足够的空间

A.16.3 TCM 定义的非致命错误

名称	值	描述
TCM_RETRY	TCM_BASE+TCM_NON_FATAL	TCM 太忙,不能立即响应该命令,该命令可以稍后再提交。
TCM_NEEDS_SELFTEST	TCM_BASE+TCM_NON_FATAL+1	TCM_ContinueSelfTest 没有运行
TCM_DOING_SELFTEST	TCM_BASE+TCM_NON_FATAL+2	当前命令执行需要的资源未被测试,TCM 正在执行 TCM_ContinueSelfTest 命令测试该资源
TCM_DEFEND_LOCK_RUNNING	TCM_BASE+TCM_NON_FATAL+3	TCM 处于字典攻击锁定延时期

A.17 备注

TCM 内部使用的数据结构,本结构提供参考,厂商可自行实现。

参 考 文 献

http://www.trustedcomputinggroup.org/home:

[1] TCG TPM Specification Version 1.2 Revision 94

[2] TCG Specification Architecture Overview Specification Revision 1.4

[3] FIPS PUB 198,The Keyed-Hash Message Authentication Code (HMAC)