ICS 35.040
L 80
备案号：

GM

中华人民共和国密码行业标准

GM/T 0013—2012

可信密码模块接口符合性测试规范

Trusted cryptography module interface compliance

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
可信密码模块接口符合性测试规范
GM/T 0013—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
2013年 月第一版 2013年 月第一次印刷
*
书号:155066·2-0020 定价 00.00 元

GM/T 0013-2012

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：中国科学院软件研究所、国民技术股份有限公司、联想控股有限公司、同方股份有限公司。

本标准主要起草人：秦宇、吴秋新、常德显、初晓博、徐震、刘鑫、宁晓魁、郑必可、刘韧、李昊、张倩颖、汪丹、刘孜文、于爱民。

引　言

为了推动我国可信计算技术的发展，《GM/T AAAA—2012 可信计算 可信密码模块接口规范》和《GM/T BBBB-2012 可信计算　可信密码支撑平台功能与接口规范》用于指导我国相关可信计算产品开发和应用。然而，不同厂商生产的产品规格和技术指标可能有所差别，因此必须对相关产品进行完整的符合性测试，以保证产品之间的兼容性。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

可信密码模块接口符合性测试规范

1 范围

本标准以《GM/T BBBB—2012 可信计算　可信密码支撑平台功能与接口规范》为基础，定义了可信密码模块的命令测试向量，并提供有效的测试方法与灵活的测试脚本。

本标准只适用于可信密码模块的符合性测试，不能取代其安全性检查。可信密码模块的安全性检测需要按照其他相关规范来进行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999　计算机信息系统安全保护等级划分规则

GB/T 5271.8—2001　信息系统　词汇　第8部分：安全

GB/T 16264.8—2005　信息技术　开放系统互连　目录　公钥和属性证书框架

GB/T 18336(所有部分)　信息技术　安全技术　信息技术安全性评估准则

GM/T 0002—2012　SM4分组密码算法

GM/T 0003—2012　SM2椭圆曲线公钥密码算法

GM/T 0004—2012　SM3密码杂凑算法

GM/T AAAA—2012　可信计算　可信密码模块接口规范

GM/T BBBB—2012　可信计算　可信密码支撑平台功能与接口规范

3 术语和定义

下列术语和定义适用于本标准。

3.1

可信计算平台　trusted computing platform

构建在计算系统中，用于实现可信计算功能的支撑系统。

3.2

可信密码模块　trusted cryptography module；TCM

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。

3.3

平台配置寄存器　platform configuration register；PCR

可信密码模块内部用于存储平台完整性度量值的存储单元。

3.4

TCM背书密钥　TCM endorsement key；EK

可信密码模块的初始密钥。

3.5

存储主密钥　storage master key；SMK

用于保护平台身份密钥和用户密钥的主密钥。

3.6

基于杂凑函数的消息验证码　hash-based message authentication mode;HMAC

本标准采用 GM/T 0004-2012 规范提供的 SM3 杂凑算法生成消息验证码。

3.7

授权协议　authorization protocol;AP

是形成授权关系的过程。

3.8

字节流　byte stream

一个字节流是指以字节表示的一个流,每个字节都用十六进制表示,有时带有文字注解。字节的顺序遵循从左到右,从上到下的规则。表 1 为一个字节流示例,包含 9 个字节,采用十六进制的表示方式。00 表示第一个字节,08 表示最后一个字节。

表 1　字节流示例

注解	值
Description #1	00 01 02 03
	04 05
Description #2	06 07 08

在本标准的所有例子中,整数值只能用十六进制(0x)或者十进制来表示。整数值是非负的,0xff 表示 255 而非一个负数。

4　可信密码模块接口符合性测试

4.1　概述

标准 GM/T BBBB 定义了可信密码模块(TCM)的设计。可信密码模块接口符合性测试主要是测试不同厂商生产的可信密码模块实现的结构和命令与 GM/T BBBB 的一致性,确保这些可信密码模块产品都以相同的方式接收和运行命令,在测试时,与厂商无关的命令可直接通过测试向量进行测试,验证每条命令的参数格式、结构解析以及操作执行与规范的一致性。与厂商相关的命令以及需由若干命令组成的命令序列则由测试向量构成的测试脚本进行测试。本标准仅用于评估可信密码模块与 GM/T BBBB 的符合性,通过定义符合性测试方法和例子供厂商或者评估者来确保产品的符合性,并不检验规范中对于 TCM 的设计与描述是否安全。

本标准只提供 TCM 符合性测试的测试策略和测试方法,其中涉及的命令均来自标准 GM/T BBBB,由于命令输入参数的可选性以及 TCM 内部的随机化因素,使得厂商可自行实现命令的测试,因此本标准提供的测试向量仅供用户参考。

如果厂商将测试过程当作一个模式加入 TCM 产品中,那么当 TCM 处于这个模式时,就认为 TCM 处于测试状态。测试状态要求:

a)　在产品 TCM 的测试模式中不能与工作中 TCM 的其他信息发生冲突,也不能暴露这些信息。

b)　TCM 厂商和系统提供者必须确保只提供符合性模式的 TCM 不被植入产品系统中。

c)　当 TCM 处于符合性测试的状态时,必须提供证据证明 TCM 处于符合性测试状态。

　　1)　TCM 可以通过厂商特定的机制来提供证据。

2） 已知的机制有：

i. 非标准的版本信息。

ii. 固定的 EK。

4.2 常量值

本标准关于测试向量和测试脚本的举例会涉及一些值，这些值作用相同，可以统一起来并复用，有利于标准整体的统一。下列标准值将应用于整个标准中数字化计算 TCM 命令的例子。

4.2.1 密钥

非对称密钥：TCM 采用 GM/T 0003—2012 规范提供的 SM2 非对称密钥算法，本标准使用以下 4 个命名的 SM2 密钥。

keyA：主要负责密钥本身的相关操作，如获取公钥、加载密钥等操作以及 SM2 加解密操作。是由外部导入的 SM2 非对称密钥。

keyB：签名密钥，主要负责签名数据。由 TCM_MakeIdentity 命令产生。

keyC：封装密钥，主要负责封装和解封数据。由 TCM 内部产生。

keyD：迁移密钥，主要用于迁移相关的测试。由 TCM 内部产生。

对称密钥：TCM 采用 GM/T 0002-2012 规范提供的 SM4 对称密钥算法。本标准采用了一个命名的 SM4 密钥。

keyE：用于执行 SM4 加解密操作。由 TCM 内部产生。

另，在 TCM 中，SMK 也是一个 SM4 密钥，它具有固定的句柄为 40 00 00 00。

表 2-表 4 描述了上述密钥的具体信息、作用以及外部导入的密钥值。

表 2 密钥信息

密钥常量名	密钥使用类型（keyUsage）	授权数据使用类型（authDataUsage）	使用授权（usageAuth）	迁移授权（migrationAuth）	PCR 信息（pcrInfoSize）
keyA	TCM_ECCKEY_BIND	TCM_AUTH_ALWAYS	KEYAUTH	KEYAUTH	0
keyB	TCM_ECCKEY_IDENTITY	TCM_AUTH_NEVER	KEYAUTH	KEYAUTH	0
keyC	TCM_ECCKEY_STORAGE	TCM_AUTH_ALWAYS	KEYAUTH	KEYAUTH	0
keyD	TCM_ECCKEY_STORAGE	TCM_AUTH_ALWAYS	KEYAUTH	KEYAUTH	0
keyE	TCM_SMS4KEY_BIND	TCM_AUTH_ALWAYS	KEYAUTH	KEYAUTH	0

表 3 密钥作用

密钥常量名	作　　用
keyA	TCM_GetPubKey、TCM_SaveContext、TCM_LoadContext、TCM_FlushSpecific、TCM_EccDecrypt
keyB	TCM_GetAuditDigestSigned、TCM_Quote、TCM_Sign、TCM_TickStampBlob
keyC	TCM_Seal、TCM_Unseal
keyD	TCM_AuthorizeMigrationKey、TCM_CreateMigratedBlob、TCM_ConvertMigratedBlob
keyE	TCM_SMS4Encrypt、TCM_SMS4Decrypt

表 4　keyA 公私钥信息

密钥类型	密钥值
keyA 公钥	04 35 DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72
keyA 私钥	4F E0 6B CE 0C A3 A8 AF 92 18 C5 A2 EC 0E B5 1F 6A DD 7B 03 01 D9 F4 13 BC A1 02 85 C1 C6 31 9D

4.2.2　授权值

本标准对授权值进行统一的命名，以使不同的测试向量和脚本达到统一。表 5 为授权值表。

表 5　授权值表

授权类型名称	授权值
OWNERAUTH	“TCMAuth”
SMKAUTH	“TCMAuth”
TCMPROOF	“TCMAuth”
NVAUTH	“TCMAuth”
DATAAUTH	“TCMAuth”
KEYAUTH	“TCMAuth”
PIKAUTH	“TCMAuth”
PEKAUTH	“TCMAuth”
TEMPAUTH	“tempTCMAuth”

注：

a) 授权值的名字是本标准为描述方便采用的标记，其值为用户指定的口令，这些口令要经过哈希才得到真正的授权值。

b) TEMPAUTH 是改变授权值等类似操作中的新授权值，在改变授权值操作执行完成后，需要恢复成原来的授权值。

4.3　测试策略

TCM 提供的命令分为三大类：第一类是严格按照规范实现，与厂商具体实现无关的命令；第二类是与厂商具体实现相关，规范中并没有严格规定实现的命令；第三类是需要一个命令序列才能完成测试的命令。对于第一类命令，本标准采用测试向量的方式直接进行测试，主要测试每个命令的输入参数的位组合格式。第二类和第三类命令不能只简单使用测试向量方式测试，本标准采用测试脚本的方式进行测试。TCM 的符合性测试是通过测试向量或者测试脚本的方式来进行的，如图 1 所示。

为实现规范符合性测试，TCM 必须具备以下三种能力：

a) 能够创建静态测试向量；

b) 能够执行动态测试脚本；

c) 能够载入和执行来自至少一个其他 TCM 厂商的 TCM 数据。

本标准基于 TCM 产品的上述能力，对 TCM 产品与 GM/T BBBB 的符合程度进行测试。测试内

容主要为 TCM 产品所提供的单个命令在接收特定输入时，其输出是否符合规范中的描述，也包括了该命令执行的中间过程是否符合规范描述。

对厂商而言，TCM 符合性测试属于白盒测试，可以直接对这些命令执行的中间过程进行测试并展示其测试结果。为此，厂商应该展示 TCM 符合性测试的中间过程，这也符合应用密码学的标准化、公开性原则。

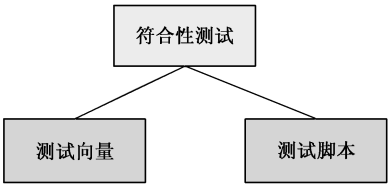

图 1　符合性测试分类

对 TCM 产品的评估者而言，TCM 符合性测试是一个灰盒或者黑盒测试，只能通过测试命令的输入和输出来检验是否符合 GM/T BBBB，无法对命令执行的中间过程进行测试。

基于 TCM 厂商和评估者的不同能力，本标准建议采取联合测试常量和变量的方式对 TCM 进行测试。常量主要是针对一些值被固定的密钥，将这些密钥的值设置为常量，可以减少命令输入参数中的不固定值的数目，便于测试的统一进行。变量主要是针对命令运行期间无法固定的中间值，但是对于厂商提供的符合性测试模式，这些值是可以统一且展示出来的，所以引入变量来指导厂商进行中间过程的组织和展示，而评估者可以通过这些变量来理解 TCM 对命令处理的过程。

4.4　测试方法

可信密码模块接口符合性测试包括单个命令和功能测试两个部分。其中，单个命令的测试用于检测该命令接收到输入参数后，验证其执行结果是否符合规范；而功能测试则是用于检测一组命令执行的结果是否完成了规范中规定的功能。因此，采用两种不同的测试方法：单个命令的测试采用测试向量来实施，而功能测试则采用测试脚本来实施。

许多 TCM 命令并不是孤立存在的，命令之间存在着依赖关系，因此测试脚本或者测试向量的编写都必须基于命令之间的依赖关系。本标准根据 TCM 命令间授权关系上的依赖和数据流关系上的依赖，给出了 TCM 命令依赖关系图。这些依赖关系，保证测试向量和测试脚本的正确编写。数据流之间的依赖关系，可以简单地通过命令参数的引用获得，例如某个命令的输入参数是另一个命令的输出，则此命令在数据流上依赖于另一命令。而授权关系上的依赖，则是通过分析 GM/T BBBB 中命令的多种授权方式获得。本标准可以正确反映这些依赖关系，采用实线型箭头表示一个命令拥有其他授权方式产生的依赖关系。

1. 测试向量

根据命令间的依赖关系，针对那些与厂商实现无关，并且可以独立测试的 TCM 命令，本标准定义了一组测试向量。这些测试向量展示了每个命令需要的位组合格式，但并非所有可能的组合格式。直接使用测试向量进行测试的命令是不需要厂商特定输入和输出的命令。测试向量一般由厂商实现为 TCM 产品的一个模式，静态创建。但这不是必须的，测试向量也可以由评估者在测试时自主开发。

测试向量的目的就是确保命令参数的格式正确，确保其结构解释正确，确保操作的执行与规范一致。在 TCM 产品中 TCM 不需要支持使用测试向量，但是这些测试向量在 TCM 自检时是推荐使用的。测试向量要求命令之间的交互最小化。使用授权会话的命令需要的是成功 AP 会话的输出，这将是其测试向量执行的默认前置条件。

2. 测试脚本

对于需要厂商特殊决定的命令，或者需要一组命令序列的命令，符合性测试将采取测试脚本的方

式。这部分测试脚本可以由厂商提供,也可以由评估者根据厂商的信息资料开发。TCM 要提供动态执行这些脚本的能力。简而言之,由于以上原因不能简单地由测试向量测试的命令,都是采用测试脚本来完成测试。本标准将给出需要在测试脚本中进行测试的 TCM 命令的部分示例数据,具体的脚本需要根据厂商实现及规范描述另行编写。

5 命令依赖关系

明确命令依赖关系是测试向量和测试脚本正确执行的根本保证。只有根据命令依赖关系确保命令执行的前置条件满足,才能保证其测试向量成功执行。与此相同,只有根据命令依赖关系正确组合测试向量生成测试脚本,才能保证测试脚本成功执行。由于命令依赖关系繁多复杂,本标准对 TCM 命令的分类见 GM/T BBBB,根据 TCM 成功执行不同命令之后所处的状态不同,将若干相近的命令划分到一个命令集合中。集合内部命令之间存在依赖关系,集合与集合之间也存在依赖关系,本标准就是通过这种方式来表述所有命令之间的依赖关系,使用实线箭头表示这种依赖关系,其中,箭尾命令依赖于箭头所指命令,具体如下所示:

5.1 启动命令集

有 2 个命令:TCM_Init、TCM_Startup,命令之间依赖关系如图 2 示:

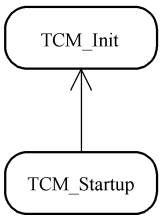

图 2 启动命令依赖关系

此集合不需要依赖其他集合。

5.2 状态保存命令集

只有 1 个命令 TCM_SaveState。

5.3 自检命令集

有 3 个命令,命令之间的依赖关系如图 3 示:

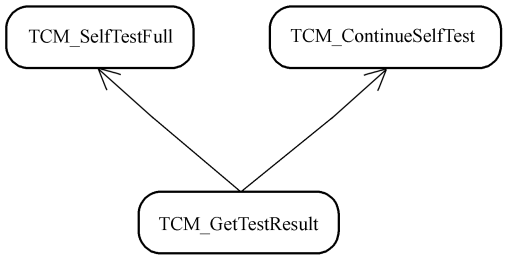

图 3 自检命令依赖关系

此集合依赖于启动命令集的完成,也就是依赖于 TCM_Startup 命令的成功执行。

5.4 TCM 工作模式设置命令集

共有 7 个命令：TCM_PhysicalDisable、TCM_PhysicalEnable、TCM_PhysicalSetDeactivated、TCM_SetOperatorAuth、TCM_SetOwnerInstall、TCM_SetTempDeactivated、TCM_OwnerSetDisable，命令之间没有依赖关系。

此集合中命令 TCM_OwnerSetDisable 依赖于 Owner 的存在，也就是依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。其他命令则依赖于启动命令集的 TCM_Startup 命令。

5.5 Owner 管理命令集

共有 5 个命令，其中，TCM_ForceClear、TCM_DisableForceClear 无依赖关系，TCM_TakeOwnership、TCM_OwnerClear、TCM_DisableOwnerClear 之间的依赖关系如图 4 示：

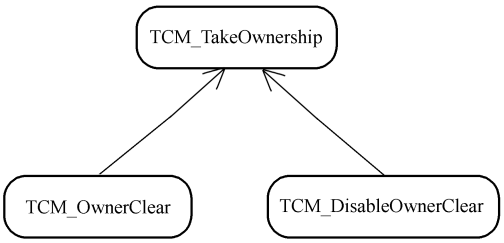

图 4 Owner 管理命令依赖关系

此命令集依赖于启动命令集的完成以及 TCM 背书密钥的存在。

5.6 属性管理命令集

共有 2 个命令：TCM_GetCapability、TCM_SetCapability，命令之间没有依赖关系。

此命令集依赖于启动命令集，TCM_SetCapability 命令存在多种授权方式，其中 Owner 的授权方式要求它依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。

5.7 升级与维护命令集

共有 2 个命令：TCM_FieldUpgrade、ReSetLockValue，命令之间没有依赖关系。

此命令集中的 TCM_ReSetLockValue 依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。

5.8 授权值管理命令集

共有两个命令：TCM_ChangeAuth、TCM_ChangeAuthOwner，命令之间没有依赖关系。

此命令集中的 TCM_ChangeAuthOwner 依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。TCM_ChangeAuth 要求父密钥和实体本身的授权，所以依赖于密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。

5.9 非易失存储管理命令集

共有 5 个命令，依赖关系如图 5 示：

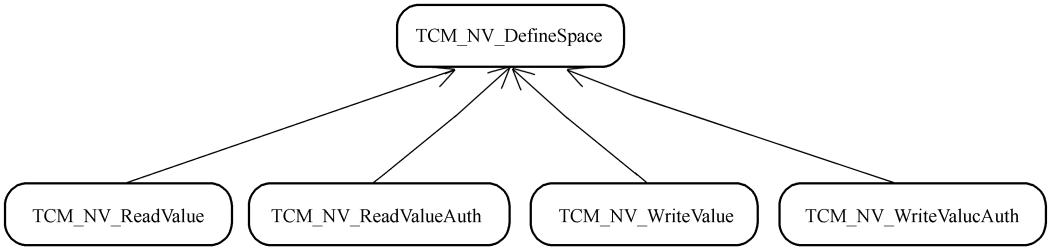

图 5　非易失存储管理命令依赖关系

此命令集合中的 TCM_NV_DefineSpace、TCM_NV_ReadValue、TCM_NV_WriteValue 有多种授权方式，其中一种依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。

5.10　运行环境管理命令集

共有 3 个命令：TCM_SaveContext、TCM_LoadContext、TCM_FlushSpecific，命令之间没有依赖关系。

此命令集合依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行，因为需要用到 TCM_TakeOwnership 命令产生的 TCM_PERMANENT_DATA->contextKey 加解密 TCM_CONTEXT_SENSITIVE。

5.11　审计命令集

共有 3 个命令：TCM_GetAuditDigest、TCM_GetAuditDigestSigned、TCM_SetOrdinalAuditStatus，命令之间没有依赖关系。

此命令集合中的 TCM_SetOrdinalAuditStatus 命令依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。TCM_GetAuditDigestSigned 命令依赖于一个已经加载的签名密钥。

5.12　时钟命令集

共有 2 个命令：TCM_GetTicks、TCM_TickStampBlob，命令之间没有依赖关系。

此命令集合中的 TCM_TickStampBlob 命令需要一个签名密钥，所以依赖于密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。

5.13　计数器命令集

共有 5 个命令，命令之间的依赖关系如图 6 示：

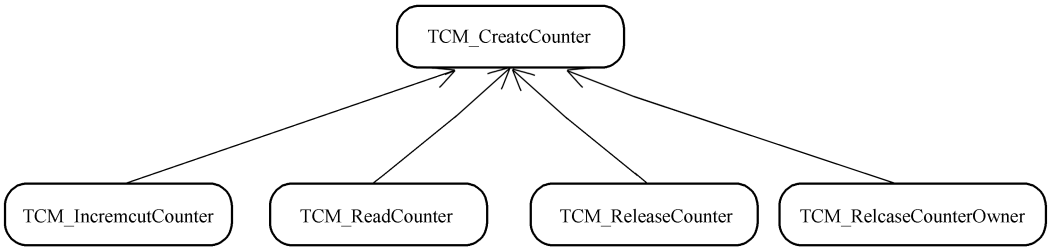

图 6　计数器命令依赖关系

此命令集合依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。

5.14　TCM 背书密钥管理命令集

共有 3 个命令，命令之间的依赖关系如图 7 示：

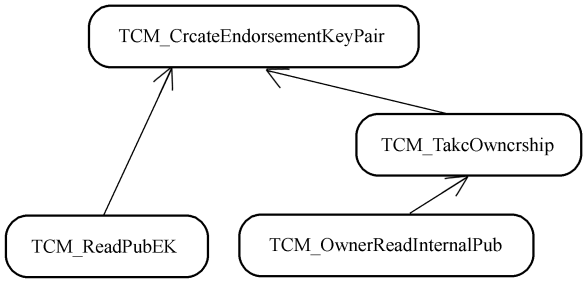

图 7　TCM 背书密钥管理命令依赖关系

此命令集合依赖于启动命令集的完成。但是其中 TCM_OwnerReadInternalPub 依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。

5.15　平台身份密钥管理命令集

共有 4 个命令：TCM_ActivatePEKCert、TCM_ActivatePEK、TCM_MakeIdentity 和 TCM_ActivateIdentity，其中 TCM_ActivatePEKCert、TCM_ActivatePEK 无命令依赖关系，TCM_MakeIdentity 和 TCM_ActivateIdentity 之间的依赖关系如图 8 示：

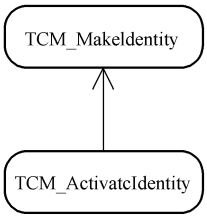

图 8　平台身份密钥管理命令依赖关系

此命令集合依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。

5.16　数据保护操作命令集

共有 2 个命令：TCM_Seal、TCM_Unseal，命令之间的依赖关系如图 9 示：

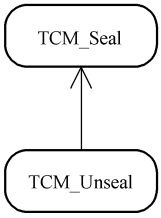

图 9　数据保护操作命令依赖关系

此命令集合需要一个封装密钥，所以依赖于密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。

5.17　密钥管理命令集

共有 5 个命令，命令之间的依赖关系如图 10 示：

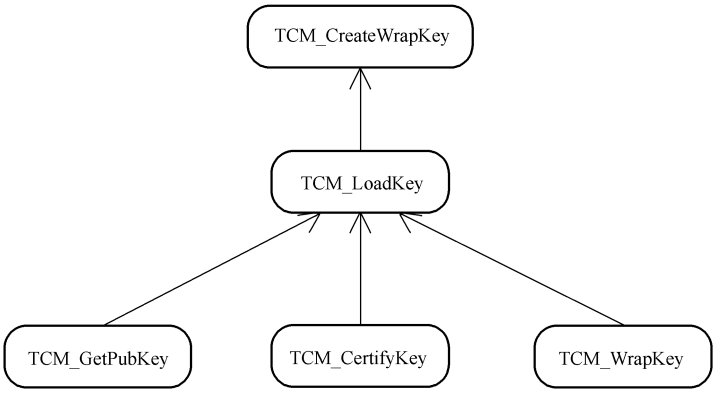

图 10　密钥管理命令依赖关系

此命令集合依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行。

5.18　密钥协商命令集

共有 3 个命令，命令之间的依赖关系如图 11 示：

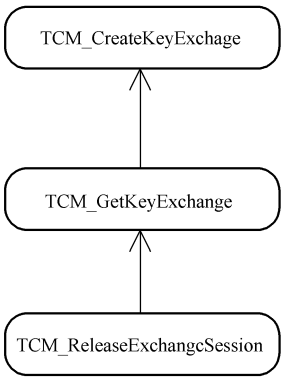

图 11　密钥协商命令依赖关系

此命令集合依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行以及密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。

5.19　密钥迁移命令集

共有 3 个命令，命令之间的依赖关系如图 12 示：

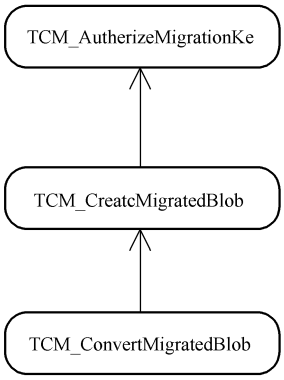

图 12　密钥迁移命令依赖关系

此命令集合依赖于 Owner 管理命令集中 TCM_TakeOwnership 命令的成功执行以及密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。

5.20 密码服务命令集

共有 9 个命令：TCM_GetRandom、TCM_Sign、TCM_SMS4Encrypt、TCM_EccDecrypt、TCM_SMS4Decrypt、TCM_SCHStart、TCM_SCHUpdate、TCM_SCHComplete、TCM_SCHCompleteExtend，其中前 5 个命令无依赖关系，后 4 个命令之间的依赖关系如图 13 示：

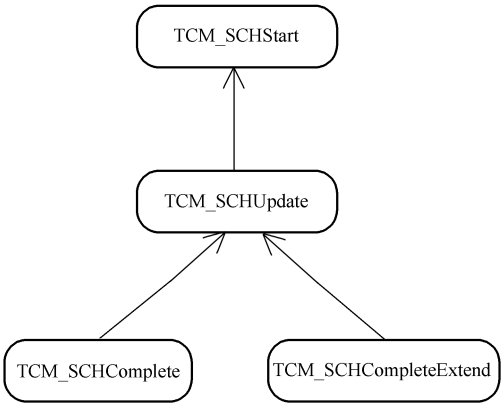

图 13 密码服务命令依赖关系

此命令集合只有 TCM_GetRandom 和 SCH 运算相关命令只需要依赖于启动命令集合的成功完成，其他命令都依赖于密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。

5.21 传输会话命令集

共有 3 个命令，命令之间的依赖关系如图 14 示：

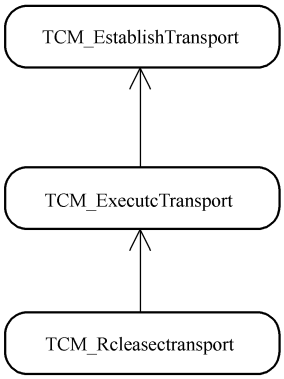

图 14 传输会话命令依赖关系

此命令集合依赖于密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。

5.22 授权协议命令集

共有 2 个命令，命令之间的依赖关系如图 15 示：

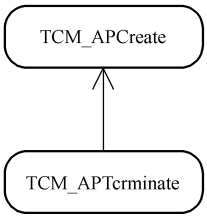

图 15　授权协议命令依赖关系

此命令集合依赖于某个实体的授权。

5.23　平台配置寄存器管理命令集

共有 4 个命令：TCM_Extend、TCM_PCRRead、TCM_Quote、TCM_PCR_Reset，命令之间没有依赖关系。

此命令集合中的 TCM_Quote 需要一个签名密钥，所以依赖于密钥管理命令集中的 TCM_CreateWrapKey 命令的成功执行。其他命令依赖于启动命令集的成功执行。

6　向量命令

对于与厂商实现无关的 TCM 命令，在其依赖的命令成功执行之后，可以直接采用测试向量的方式对其进行符合性测试，即给定输入，然后检测其输出是否与规范一致。下面是通过测试向量方式进行测试的 TCM 命令，其中的测试向量是由国内多款 TCM 芯片实际执行得到，其中的参数选择体现了符合性测试的原则，但以下测试向量不具有唯一排它性，仅仅作为测试 TCM 芯片的测试示例参考使用。

6.1　TCM_Startup

依赖于：

TCM_Init 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0C	
3	4	命令码	00 00 80 99	TCM_ORD_Startup
4	2	启动类型	00 01	也可以是 00 02 或者 00 03

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 99	TCM_ORD_Startup

输入 Blob：

00 C1 00 00 00 0C 00 00 80 99 00 01

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.2 TCM_SelfTestFull

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 50	TCM_ORD_SelfTestFull

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	参数长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 50	TCM_ORD_SelfTestFull

输入 Blob：

00 C1 00 00 00 0A 00 00 80 50

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.3 TCM_ContinueSelfTest

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 53	TCM_ORD_ContinueSelfTest

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	参数长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 53	TCM_ORD_ContinueSelfTest

输入 Blob：

00 C1 00 00 00 0A 00 00 80 53

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.4 TCM_GetTestResult

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 54	TCM_ORD_GetTestResult

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 12	总的字节数，受到输出数据的长度影响
3	4	返回码	00 00 00 00	
4	4	输出数据长度	00 00 00 04	厂商定义的测试信息的字节数
5	可变	输出数据	00 00 00 00	厂商指定的测试信息
		命令码	00 00 80 54	TCM_ORD_GetTestResult

输入 Blob：

00 C1 00 00 00 0A 00 00 80 54

输出 Blob：

00 C4 00 00 00 12 00 00 00 00 00 00 00 04 00 00 00 00

6.5 TCM_SetOwnerInstall

依赖于：

a) TCM_Startup 命令的成功执行。

b) 无所有者。

c) TCM 处于使能状态。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0B	
3	4	命令码	00 00 80 71	TCM_ORD_SetOwnerInstall
4	1	状态位	01	也可以是 00

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 71	TCM_ORD_SetOwnerInstall

输入 Blob：

00 C1 00 00 00 0B 00 00 80 71 01

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.6 TCM_OwnerSetDisable

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2F	
3	4	命令码	00 00 80 6E	TCM_ORD_OwnerSetDisable
4	1	状态位	01	也可以是 00
5	4	授权会话句柄	00 00 00 0F	
6	32	授权数据验证码	76 9D B3 FF 4C 0C 0B E9 B6 72 48 FF 99 6D FB 4C 2D AF 66 52 03 72 38 2F E3 6A E8 DA CF 21 CB FD	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	授权数据验证码	1C AD 05 EF 3A 07 87 EC 6B B6 4E F1 91 81 B4 4B AF 2B 19 16 96 B1 DB FB DE 87 93 07 A2 4B E9 20	
		命令码	00 00 80 6E	TCM_ORD_OwnerSetDisable

输入 Blob：

00 C2 00 00 00 2F 00 00 80 6E 01 00 00 00 0F 76 9D B3 FF 4C 0C 0B E9 B6 72 48 FF 99 6D FB 4C 2D AF 66 52 03 72 38 2F E3 6A E8 DA CF 21 CB FD

输出 Blob：

00 C5 00 00 00 2A 00 00 00 00 1C AD 05 EF 3A 07 87 EC 6B B6 4E F1 91 81 B4 4B AF 2B 19 16 96 B1 DB FB DE 87 93 07 A2 4B E9 20

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 6E	命令码
HASH IN 2	01	状态位
HASH OUT	CB 08 28 13 E1 4E 23 26 6E D9 75 AA D3 33 E6 C1 76 DA A3 8A BE DF D4 D0 B5 E5 19 EC BA DB 66 2E	HMAC IN 1
KEY	70 8B EF 6D E8 9A 80 65 DD 65 91 93 21 9F 6C 04 C5 9F 95 56 DE E7 53 B4 71 45 2A 8F 5C 15 3D C1	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	CB 08 28 13 E1 4E 23 26 6E D9 75 AA D3 33 E6 C1 76 DA A3 8A BE DF D4 D0 B5 E5 19 EC BA DB 66 2E	HASH OUT
HMAC IN 2	13 BA B5 F2	AP 会话的序列号
HMAC OUT	76 9D B3 FF 4C 0C 0B E9 B6 72 48 FF 99 6D FB 4C 2D AF 66 52 03 72 38 2F E3 6A E8 DA CF 21 CB FD	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c） Owner 授权数据

Owner 创建 AP 会话时，需要 Owner 授权数据。本标准采用 OWNERAUTH 常量值。

6.7 TCM_PhysicalEnable

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 6F	TCM_ORD_PhysicalEnable

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 6F	TCM_ORD_PhysicalEnable

输入 Blob：

00 C1 00 00 00 0A 00 00 80 6F

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.8 TCM_PhysicalDisable

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 70	TCM_ORD_PhysicalDisable

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 70	TCM_ORD_PhysicalDisable

输入 Blob：

00 C1 00 00 00 0A 00 00 80 70

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.9 TCM_SetTempDeactivated

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 73	TCM_ORD_SetTempDeactivated

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 73	TCM_ORD_SetTempDeactivated

输入 Blob：

00 C1 00 00 00 0A 00 00 80 73

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.10 TCM_PhysicalSetDeactivated

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0B	
3	4	命令码	00 00 80 72	TCM _ ORD _ PhysicalSetDeactivated
4	1	状态位	00	也可以是 01

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 72	TCM_ORD_PhysicalSetDeactivated

输入 Blob：

00 C1 00 00 00 0B 00 00 80 72 00

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.11 TCM_TakeOwnership

依赖于：

a) TCM 背书密钥的存在。

b) TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 01 79	
3	4	命令码	00 00 80 0D	TCM_TakeOwnership
4	28	协议 ID	00 05	
5	4	所有者授权数据长度	00 00 00 81	EK 公钥加密后的所有者授权数据的长度

序号	长度	名称	值	说明
6	可变	所有者授权数据	04 10 95 A0 8A 0E 9D 0B 1F 92 9F BE B8 54 35 E0 76 DA 2C 3F EA 27 62 CF 5D 3D ED F9 DD 2A 1D FD 96 BD 7B EA 51 F7 3F 0E D8 C8 7D 4E E4 55 A4 4B 3B 0E 1D A0 33 26 C9 0A 02 FA 2E 31 7F 91 78 EC BA EF A1 19 76 38 C6 EC C3 CB 2F D2 07 F1 EF F0 D0 52 43 1F 24 6A E4 89 EA CD 81 78 0E BB B7 C0 1A E0 29 FA 4E D4 26 A7 D4 B8 DC 5E 73 00 E1 B8 C8 7D D7 42 9C E0 80 08 99 30 62 9E F3 13 6A 79 6B	EK 公钥加密后的所有者授权数据
7	4	SMK 授权数据长度	00 00 00 81	EK 公钥加密后的授权数据的长度
8	可变	SMK 授权数据	04 E1 34 82 CD 80 CF 14 D2 54 84 8F E0 B4 7F 91 0C 9F 0F 0C 46 F2 5C 76 02 4B 86 A5 96 1E C2 97 7C 44 C3 73 96 ED AB D2 58 26 F8 C9 4D F0 D3 61 CF 0F 8D AB F1 8A 53 B2 E6 EC C6 C6 E8 A3 A3 EE ED C9 3E 2C A7 A5 8B 65 88 BC C0 F9 F8 B6 17 1D E5 AD 26 BC 1A B3 76 14 AF B8 14 36 12 5E BE 84 3C 4F 27 1D 75 B2 7A EC 05 2B A7 D9 D8 B3 45 07 CB E6 29 59 A1 BB D0 D2 37 92 79 D9 81 29 2C 14 E7	EK 公钥加密后的授权数据
9	可变	SMK 结构数据	00 15 00 00 00 18 00 00 00 00 01 00 00 00 0C 00 08 00 01 00 00 00 1C 00 00 00 80 00 00 00 80 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	带有 SMK 创建的密钥参数的 TCM_KEY 结构
10	4	授权会话句柄	00 00 00 03	
11	32	授权数据验证码	23 BC 6E 14 06 62 DC F2 E0 3A 6F 42 20 F4 37 5F FC 9F A0 A1 55 A8 96 21 F2 73 79 25 B0 72 E6 F4	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 69	
3	4	返回码	00 00 00 00	

序号	长度	名称	值	说明
4	可变	SMK 数据结构	00 15 00 00 00 18 00 00 00 00 01 00 00 00 0C 00 08 00 01 00 00 00 1C 00 00 00 80 00 00 00 80 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
5	32	授权数据验证码	1C 66 75 D3 C9 BF 1F 86 EA 48 DD E8 C1 50 5F 87 78 DF E6 A4 01 E8 DD 3D 6F 1C 32 9B FE 60 83 DA	
		命令码	00 00 80 0D	TCM_TakeOwnership

输入 Blob：

00 C2 00 00 01 79 00 00 80 0D 00 05 00 00 00 81 04 10 95 A0 8A 0E 9D 0B 1F 92 9F BE B8 54 35 E0 76 DA 2C 3F EA 27 62 CF 5D 3D ED F9 DD 2A 1D FD 96 BD 7B EA 51 F7 3F 0E D8 C8 7D 4E E4 55 A4 4B 3B 0E 1D A0 33 26 C9 0A 02 FA 2E 31 7F 91 78 EC BA EF A1 19 76 38 C6 EC C3 CB 2F D2 07 F1 EF F0 D0 52 43 1F 24 6A E4 89 EA CD 81 78 0E BB B7 C0 1A E0 29 FA 4E D4 26 A7 D4 B8 DC 5E 73 00 E1 B8 C8 7D D7 42 9C E0 80 08 99 30 62 9E F3 13 6A 79 6B 00 00 00 81 04 E1 34 82 CD 80 CF 14 D2 54 84 8F E0 B4 7F 91 0C 9F 0F 0C 46 F2 5C 76 02 4B 86 A5 96 1E C2 97 7C 44 C3 73 96 ED AB D2 58 26 F8 C9 4D F0 D3 61 CF 0F 8D AB F1 8A 53 B2 E6 EC C6 C6 E8 A3 A3 EE ED C9 3E 2C A7 A5 8B 65 88 BC C0 F9 F8 B6 17 1D E5 AD 26 BC 1A B3 76 14 AF B8 14 36 12 5E BE 84 3C 4F 27 1D 75 B2 7A EC 05 2B A7 D9 D8 B3 45 07 CB E6 29 59 A1 BB D0 D2 37 92 79 D9 81 29 2C 14 E7 00 15 00 00 00 18 00 00 00 00 01 00 00 00 0C 00 08 00 01 00 00 00 1C 00 00 00 80 00 00 00 80 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 23 BC 6E 14 06 62 DC F2 E0 3A 6F 42 20 F4 37 5F FC 9F A0 A1 55 A8 96 21 F2 73 79 25 B0 72 E6 F4

输出 Blob：

00 C5 00 00 00 69 00 00 00 00 00 15 00 00 00 18 00 00 00 00 01 00 00 00 0C 00 08 00 01 00 00 00 1C 00 00 00 80 00 00 00 80 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 66 75 D3 C9 BF 1F 86 EA 48 DD E8 C1 50 5F 87 78 DF E6 A4 01 E8 DD 3D 6F 1C 32 9B FE 60 83 DA

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 0D	命令码
HASH IN 2	00 05	协议 ID
HASH IN 3	00 00 00 81	所有者授权数据长度
HASH IN 4	04 10 95 A0 8A 0E 9D 0B 1F 92 9F BE B8 54 35 E0 76 DA 2C 3F EA 27 62 CF 5D 3D ED F9 DD 2A 1D FD 96 BD 7B EA 51 F7 3F 0E D8 C8 7D 4E E4 55 A4 4B 3B 0E 1D A0 33 26 C9 0A 02 FA 2E 31 7F 91 78 EC BA EF A1 19 76 38 C6 EC C3 CB 2F D2 07 F1 EF F0 D0 52 43 1F 24 6A E4 89 EA CD 81 78 0E BB B7 C0 1A E0 29 FA 4E D4 26 A7 D4 B8 DC 5E 73 00 E1 B8 C8 7D D7 42 9C E0 80 08 99 30 62 9E F3 13 6A 79 6B	所有者授权数据

输入域	输入域授权数据验证码	说明
HASH IN 5	00 00 00 81	SMK 授权数据长度
HASH IN 6	04 E1 34 82 CD 80 CF 14 D2 54 84 8F E0 B4 7F 91 0C 9F 0F 0C 46 F2 5C 76 02 4B 86 A5 96 1E C2 97 7C 44 C3 73 96 ED AB D2 58 26 F8 C9 4D F0 D3 61 CF 0F 8D AB F1 8A 53 B2 E6 EC C6 C6 E8 A3 A3 EE ED C9 3E 2C A7 A5 8B 65 88 BC C0 F9 F8 B6 17 1D E5 AD 26 BC 1A B3 76 14 AF B8 14 36 12 5E BE 84 3C 4F 27 1D 75 B2 7A EC 05 2B A7 D9 D8 B3 45 07 CB E6 29 59 A1 BB D0 D2 37 92 79 D9 81 29 2C 14 E7	SMK 授权数据
HASH IN 7	00 15 00 00 00 18 00 00 00 00 01 00 00 00 0C 00 08 00 01 00 00 00 1C 00 00 00 80 00 00 00 80 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SMK 结构数据
HASH OUT	45 48 F0 5F 28 D1 1F F5 73 00 84 C9 2B 10 9D 3C 24 69 14 DF C8 C1 17 8D 4E 93 52 0E 17 5F 68 2F	HMAC IN 1
KEY	0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50	Owner 授权数据
HMAC IN 1	45 48 F0 5F 28 D1 1F F5 73 00 84 C9 2B 10 9D 3C 24 69 14 DF C8 C1 17 8D 4E 93 52 0E 17 5F 68 2F	HASH OUT
HMAC IN 2	A9 EA 0C E9	AP 会话的序列号
HMAC OUT	23 BC 6E 14 06 62 DC F2 E0 3A 6F 42 20 F4 37 5F FC 9F A0 A1 55 A8 96 21 F2 73 79 25 B0 72 E6 F4	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码、命令码、SMK 结构数据做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为 Owner 授权数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) Owner 授权数据

执行本命令时，Owner 授权值采用的是 OWNERAUTH 常量值，SMK 授权值采用的是 SMKAUTH 常量值。

6.12 TCM_OwnerClear

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2E	
3	4	命令码	00 00 80 5B	TCM_ORD_OwnerClear
4	4	授权会话句柄	00 00 00 0B	

序号	长度	名称	值	说明
5	32	授权数据验证码	C7 35 B2 2D 70 1E 4C 29 78 38 5E 8F C4 BD 9A 0B 2A C1 74 8A 15 9B 7F 4C F6 67 65 87 E9 0D 01 29	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	授权数据验证码	F1 51 C0 F8 1A 94 8E 27 63 F7 60 81 FD A8 5C 8F B3 AA D8 8E 1D 58 41 48 40 AF 84 9F EA 1E A7 0A	
		命令码	00 00 80 5B	TCM_ORD_OwnerClear

输入 Blob：

00 C2 00 00 00 2E 00 00 80 5B 00 00 00 0B C7 35 B2 2D 70 1E 4C 29 78 38 5E 8F C4 BD 9A 0B 2A C1 74 8A 15 9B 7F 4C F6 67 65 87 E9 0D 01 29

输出 Blob：

00 C5 00 00 00 2A 00 00 00 00 F1 51 C0 F8 1A 94 8E 27 63 F7 60 81 FD A8 5C 8F B3 AA D8 8E 1D 58 41 48 40 AF 84 9F EA 1E A7 0A

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 5B	命令码
HASH OUT	C0 3B 4C BB 93 68 43 E0 1D AA 42 86 A5 A7 D9 CE 76 7B 6A D5 B5 A8 B2 76 64 52 B6 E5 13 D5 75 05	HMAC IN 1
KEY	B3 59 9C EB 84 F0 4B 5D 76 D1 EF E7 EC 5D 77 EB B8 75 DC 9B 33 33 B7 8E C9 AE 63 52 A6 1D 38 5D	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	C0 3B 4C BB 93 68 43 E0 1D AA 42 86 A5 A7 D9 CE 76 7B 6A D5 B5 A8 B2 76 64 52 B6 E5 13 D5 75 05	HASH OUT
HMAC IN 2	91 7B 87 C5	AP 会话的序列号
HMAC OUT	C7 35 B2 2D 70 1E 4C 29 78 38 5E 8F C4 BD 9A 0B 2A C1 74 8A 15 9B 7F 4C F6 67 65 87 E9 0D 01 29	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) Owner 授权数据

Owner 创建 AP 会话时,需要 Owner 授权数据。本标准采用是 OWNERAUTH 常量值。

6.13 TCM_ForceClear

依赖于:

TCM_Startup 命令的成功执行。

输入域:

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 5D	TCM_ORD_ForceClear

输出域:

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 5D	TCM_ORD_ForceClear

输入 Blob:

00 C1 00 00 00 0A 00 00 80 5D

输出 Blob:

00 C4 00 00 00 0A 00 00 00 00

6.14 TCM_DisableOwnerClear

依赖于:

a) TCM_Startup 命令的成功执行。

b) 有所有者,即 TCM_TakeOwnership 命令的成功执行。

输入域:

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2E	
3	4	命令码	00 00 80 5C	TCM_ORD_DisableOwnerClear
4	4	授权会话句柄	00 00 00 0D	
5	32	授权数据验证码	42 CA F7 BC 2C 1C 6C 92 D5 E3 C7 BF 4B A8 A6 0D 5B 07 0E 78 99 BF 8D 4C 3E 35 9C E6 F2 DB 9A D5	

输出域:

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	授权数据验证码	6E 60 EC EB FB 49 FC 75 D5 52 61 E5 8A 9A EC 28 E5 F5 42 CC 9F 45 36 79 F5 1D 35 F2 F1 71 24 ED	
		命令码	00 00 80 5C	TCM_ORD_DisableOwnerClear

输入 Blob：

00 C2 00 00 00 2E 00 00 80 5C 00 00 00 0D 42 CA F7 BC 2C 1C 6C 92 D5 E3 C7 BF 4B A8 A6 0D 5B 07 0E 78 99 BF 8D 4C 3E 35 9C E6 F2 DB 9A D5

输出 Blob：

00 C5 00 00 00 2A 00 00 00 00 6E 60 EC EB FB 49 FC 75 D5 52 61 E5 8A 9A EC 28 E5 F5 42 CC 9F 45 36 79 F5 1D 35 F2 F1 71 24 ED

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 5C	命令码
HASH OUT	BD 2F 59 B6 26 B7 39 E2 CE 6B 59 E9 49 D9 90 5E 60 73 A7 D3 A0 12 D3 71 7C FA BA FD 21 CD AA 0C	HMAC IN 1
KEY	4A B2 4D A7 B3 0D 73 5B 1C C3 91 B4 F6 F1 09 53 E9 CE D2 CB D1 60 95 51 04 FC 57 50 8A C6 B0 A1	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	BD 2F 59 B6 26 B7 39 E2 CE 6B 59 E9 49 D9 90 5E 60 73 A7 D3 A0 12 D3 71 7C FA BA FD 21 CD AA 0C	HASH OUT
HMAC IN 2	69 01 70 F3	AP 会话的序列号
HMAC OUT	42 CA F7 BC 2C 1C 6C 92 D5 E3 C7 BF 4B A8 A6 0D 5B 07 0E 78 99 BF 8D 4C 3E 35 9C E6 F2 DB 9A D5	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c） Owner 授权数据

Owner 创建 AP 会话时，需要 Owner 授权数据。本标准采用 OWNERAUTH 常量值。

6.15 TCM_DisableForceClear

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 5E	TCM_ORD_DisableForceClear

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 5E	TCM_ORD_DisableForceClear

输入 Blob：

00 C1 00 00 00 0A 00 00 80 5E

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.16 TCM_GetCapability

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 16	
3	4	命令码	00 00 80 65	TCM_ORD_GetCapability
4	4	属性参数	00 00 00 01	也可以是其他值，参看 GM/T BBBB 中 TCM_CAPABILITY_AREA 的描述
5	4	子属性参数长度	00 00 00 04	标识子属性参数的长度
6	可变	子属性参数	00 00 80 65	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0F	
3	4	返回码	00 00 00 00	
4	4	属性值长度	00 00 00 01	标识返回的属性值的长度
5	可变	属性值	01	
		命令码	00 00 80 65	TCM_ORD_GetCapability

输入 Blob：

00 C1 00 00 00 16 00 00 80 65 00 00 00 01 00 00 00 04 00 00 80 65

输出 Blob：

00 C4 00 00 00 0F 00 00 00 00 00 00 00 01 01

6.17 TCM_SetCapability

依赖于：

a） TCM_Startup 命令的成功执行。

b） 在需要 Owner 授权的授权方式下，还需要 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 1B	
3	4	命令码	00 00 80 3F	TCM_ORD_SetCapability
4	4	属性参数	00 00 00 05	也可以是其他值，参看 GM/T BBBB 中 TCM_CAPABILITY_AREA 的描述
5	4	子属性参数长度	00 00 00 04	标识子属性参数的长度
6	可变	子属性参数	00 00 00 04	也可以是其他 GM/T BBBB 描述的允许设置的子属性。
7	4	属性值长度	00 00 00 01	标识属性值的长度
8	可变	属性值	00	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 3F	TCM_ORD_SetCapability

输入 Blob：

00 C1 00 00 00 1B 00 00 80 3F 00 00 00 05 00 00 00 04 00 00 00 04 00 00 00 01 00

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

说明：

a） 此命令能够设置的属性是有限的，必须严格按照 GM/T BBBB 来设置。

b） GM/T BBBB 规定部分属性值的设置需要 Owner 授权，那么就应该使用带一个授权的测试向量组织方式。具体请参考 GM/T BBBB 来实施。

6.18 TCM_ResetLockValue

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2E	
3	4	命令码	00 00 80 40	TCM_ORD_ResetLockValue
4	4	授权会话句柄	00 00 00 0B	
5	32	授权数据验证码	F6 68 D9 B3 F7 1B FD 89 9B 54 6A A0 E1 B2 80 80 BD AE 3C BB CF 2F 42 86 89 9E 76 BF 6A 08 F1 AF	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	授权数据验证码	99 92 B6 9B CD D2 03 2D 2B 90 63 46 32 BB B6 6D F8 F4 BE F8 1A CE 5E 65 77 94 6B 0E BC 67 CD A9	
		命令码	00 00 80 40	TCM_ORD_ResetLockValue

输入 Blob：

00 C2 00 00 00 2E 00 00 80 40 00 00 00 0B F6 68 D9 B3 F7 1B FD 89 9B 54 6A A0 E1 B2 80 80 BD AE 3C BB CF 2F 42 86 89 9E 76 BF 6A 08 F1 AF

输出 Blob：

00 C5 00 00 00 2A 00 00 00 00 99 92 B6 9B CD D2 03 2D 2B 90 63 46 32 BB B6 6D F8 F4 BE F8 1A CE 5E 65 77 94 6B 0E BC 67 CD A9

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 40	命令码
HASH OUT	E3 94 82 E1 0E 05 09 0B 91 2C 13 BB C2 6F 19 6B AE 0B 15 C3 28 96 AF 25 EF 1F F0 19 54 1D F0 47	HMAC IN 1
KEY	B9 4A 5F F7 A2 7F D4 BF 10 53 89 9B B2 E5 0F D7 AA 47 A9 2C 39 92 1F 00 24 CD 3B 58 74 9C 7B 23	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	E3 94 82 E1 0E 05 09 0B 91 2C 13 BB C2 6F 19 6B AE 0B 15 C3 28 96 AF 25 EF 1F F0 19 54 1D F0 47	HASH OUT

输入域	输入域授权数据验证码	说明
HMAC IN 2	13 AF 54 E4	AP 会话的序列号
HMAC OUT	F6 68 D9 B3 F7 1B FD 89 9B 54 6A A0 E1 B2 80 80 BD AE 3C BB CF 2F 42 86 89 9E 76 BF 6A 08 F1 AF	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算,其结果再与序列号做 HMAC 计算,HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值,使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来,有助于整个符合性测试的展现。

c) Owner 授权数据

Owner 创建 AP 会话时,需要 Owner 授权数据。本标准采用 OWNERAUTH 常量值。

6.19 TCM_ChangeAuth

依赖于:

a) TCM_Startup 命令的成功执行。

b) 有所有者,即 TCM_TakeOwnership 命令的成功执行。

c) 要求父密钥和实体本身的授权,所以依赖于 TCM_CreateWrapKey 命令的成功执行。

输入域:

序号	长度	名称	值	说明
1	2	标识	00 C3	TCM _ TAG _ RQU _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 0E	
3	4	命令码	00 00 80 0C	TCM_ORD_ChangeAuth
4	4	父密钥句柄	40 00 00 00	
5	2	协议 ID	00 08	
6	32	加密后的新授权数据	F9 F2 4F 58 C1 E6 DA FB 79 51 40 8F 70 01 26 55 DF 1C 8D 01 8E 20 30 6B DE E1 CC 9D CC C8 28 9E	TEMPAUTH
7	2	实体类型	00 05	
8	4	要改变授权数据的实体数据长度	00 00 00 90	

序号	长度	名称	值	说明
9	可变	要改变授权数据的实体数据	E9 09 DF A1 53 E2 1F 23 D5 A4 3D CE F7 9D E8 1F 1C B1 41 71 8F 58 F1 20 E6 D4 77 E2 1C A1 75 C1 A2 47 3C 61 3C 16 56 CB D9 DA 89 D6 59 4C 6F 53 95 3A 7F 06 30 E6 A2 40 18 33 63 7A 92 1A B8 34 8E D3 E0 06 1F 36 87 D1 6A C2 8E 44 FB F1 11 CD 4F 5D 50 7D 59 04 0A 65 B6 AE 50 5F C2 8D EB 7A EA 09 67 E9 AD 48 06 B0 79 EA 8F 3A 4E B9 41 27 17 33 AC DA 8C A8 66 90 F9 5D 30 1A 2F 61 18 45 B2 CA E7 EA 7A F9 A9 4D DC 23 8E 98 5A F6 73 21	
10	4	父密钥授权会话句柄	00 00 00 0C	
11	32	父密钥授权数据验证码	E5 55 28 4F A8 F2 EC 3B 2F 7D 12 D7 32 35 EF 50 86 CD 69 4E B6 73 3E CC B5 BF 1C D0 31 9D 35 01	
12	4	实体授权会话句柄	00 00 00 0D	
13	32	实体授权数据验证码	BC BA 5C 1C 99 66 DE 6B 23 0A 61 DD CD 9A 50 F7 A5 91 79 A2 1E D5 33 9F 30 52 2F 69 C4 9E 04 8E	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C6	TCM _ TAG _ RSP _ AUTH2 _COMMAND
2	4	数据长度	00 00 00 DE	
3	4	返回码	00 00 00 00	
4	4	实体数据长度	00 00 00 90	
5	可变	实体数据	B1 41 71 E8 60 60 44 C8 17 72 3F 73 0E 6A 16 6E DE 00 35 DF 14 B5 98 F5 CC 28 28 B1 B6 0F 3E 80 E7 89 E0 C8 58 FE F1 11 B6 54 19 62 6B AB 63 82 86 4A A0 F7 C8 20 F2 0E C4 92 E5 16 78 B2 61 9F E3 7D 65 6C 00 26 4B 06 EB 55 E7 FD 03 8B 14 5C 82 1C EC 29 E7 BB 34 F6 72 47 6D 31 6C 39 72 40 58 BC FB 91 DA D6 3A 1E 37 77 2C A2 8B AD C9 23 1A 3A 34 A4 C6 B7 98 2F 98 33 6C 77 48 8E A2 4E B7 59 80 C2 60 09 21 87 F2 57 41 1E 4A 7A D0 15	

序号	长度	名称	值	说明
6	32	父密钥授权数据验证码	6A 70 29 5C 0E B2 3A 58 01 B8 6F 3D 9E 7C 09 67 C4 DF 6C D1 03 17 64 86 D6 8B BA 10 3D 07 2C 3E	
7	32	实体授权数据验证码	7D 6A 48 04 4A 67 40 A6 FF 9D 9B 64 62 EB 2F 9C 52 45 E1 6C 82 FB D9 CD 3D 65 6C FE 89 E1 6F 45	
		命令码	00 00 80 0C	TCM_ORD_ChangeAuth

输入 Blob：

00 C3 00 00 01 0E 00 00 80 0C 40 00 00 00 00 08 F9 F2 4F 58 C1 E6 DA FB 79 51 40 8F 70 01 26 55 DF 1C 8D 01 8E 20 30 6B DE E1 CC 9D CC C8 28 9E 00 05 00 00 00 90 E9 09 DF A1 53 E2 1F 23 D5 A4 3D CE F7 9D E8 1F 1C B1 41 71 8F 58 F1 20 E6 D4 77 E2 1C A1 75 C1 A2 47 3C 61 3C 16 56 CB D9 DA 89 D6 59 4C 6F 53 95 3A 7F 06 30 E6 A2 40 18 33 63 7A 92 1A B8 34 8E D3 E0 06 1F 36 87 D1 6A C2 8E 44 FB F1 11 CD 4F 5D 50 7D 59 04 0A 65 B6 AE 50 5F C2 8D EB 7A EA 09 67 E9 AD 48 06 B0 79 EA 8F 3A 4E B9 41 27 17 33 AC DA 8C A8 66 90 F9 5D 30 1A 2F 61 18 45 B2 CA E7 EA 7A F9 A9 4D DC 23 8E 98 5A F6 73 21 00 00 00 0C E5 55 28 4F A8 F2 EC 3B 2F 7D 12 D7 32 35 EF 50 86 CD 69 4E B6 73 3E CC B5 BF 1C D0 31 9D 35 01 00 00 00 0D BC BA 5C 1C 99 66 DE 6B 23 0A 61 DD CD 9A 50 F7 A5 91 79 A2 1E D5 33 9F 30 52 2F 69 C4 9E 04 8E

输出 Blob：

00 C6 00 00 00 DE 00 00 00 00 00 00 00 90 B1 41 71 E8 60 60 44 C8 17 72 3F 73 0E 6A 16 6E DE 00 35 DF 14 B5 98 F5 CC 28 28 B1 B6 0F 3E 80 E7 89 E0 C8 58 FE F1 11 B6 54 19 62 6B AB 63 82 86 4A A0 F7 C8 20 F2 0E C4 92 E5 16 78 B2 61 9F E3 7D 65 6C 00 26 4B 06 EB 55 E7 FD 03 8B 14 5C 82 1C EC 29 E7 BB 34 F6 72 47 6D 31 6C 39 72 40 58 BC FB 91 DA D6 3A 1E 37 77 2C A2 8B AD C9 23 1A 3A 34 A4 C6 B7 98 2F 98 33 6C 77 48 8E A2 4E B7 59 80 C2 60 09 21 87 F2 57 41 1E 4A 7A D0 15 6A 70 29 5C 0E B2 3A 58 01 B8 6F 3D 9E 7C 09 67 C4 DF 6C D1 03 17 64 86 D6 8B BA 10 3D 07 2C 3E 7D 6A 48 04 4A 67 40 A6 FF 9D 9B 64 62 EB 2F 9C 52 45 E1 6C 82 FB D9 CD 3D 65 6C FE 89 E1 6F 45

说明：

要改变的实体的授权数据采用 KEYAUTH 常量值，新的使用授权值采用 TEMPAUTH 常量值。向量测试完成后，再次恢复成为 TEMPAUTH 常量值。

6.20 TCM_ChangeAuthOwner

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 52	
3	4	命令码	00 00 80 10	TCM_ORD_ChangeAuthOwner

序号	长度	名称	值	说明
4	2	协议 ID	00 08	
5	32	新授权数据	3D 10 83 13 AB 7F A8 86 8F 83 74 65 D0 00 3F 27 61 A0 4A C6 25 BA 02 D5 31 DE 73 F3 69 CF 22 6F	TEMPAUTH
6	2	实体类型	00 04	也可以是 0x0002
7	4	授权会话句柄	00 00 00 0C	
8	32	授权数据验证码	BF 91 08 34 2D 66 5E 24 9F D4 A7 4C 98 9F 76 B7 B2 AF 28 A3 FD 03 3B E5 B2 1C 44 0E 91 E1 C2 98	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	授权数据验证码	0E 71 85 3B 09 D5 E9 2C 02 F4 8C 7F 3C 18 64 52 99 E0 A4 FA 4F 92 66 DA D5 6B B0 AB C1 52 4F 64	
		命令码	00 00 80 10	TCM_ORD_ChangeAuthOwner

输入 Blob：

00 C2 00 00 00 52 00 00 80 10 00 08 3D 10 83 13 AB 7F A8 86 8F 83 74 65 D0 00 3F 27 61 A0 4A C6 25 BA 02 D5 31 DE 73 F3 69 CF 22 6F 00 04 00 00 00 0C BF 91 08 34 2D 66 5E 24 9F D4 A7 4C 98 9F 76 B7 B2 AF 28 A3 FD 03 3B E5 B2 1C 44 0E 91 E1 C2 98

输出 Blob：

00 C5 00 00 00 2A 00 00 00 00 0E 71 85 3B 09 D5 E9 2C 02 F4 8C 7F 3C 18 64 52 99 E0 A4 FA 4F 92 66 DA D5 6B B0 AB C1 52 4F 64

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 10	命令码
HASH IN 2	00 08	协议 ID
HASH IN 3	3D 10 83 13 AB 7F A8 86 8F 83 74 65 D0 00 3F 27 61 A0 4A C6 25 BA 02 D5 31 DE 73 F3 69 CF 22 6F	新授权数据(加密的)
HASH IN 4	00 04	实体类型
HASH OUT	3B F9 60 3C 85 4C 71 8F 49 42 11 9F 47 FD 3B 8E 59 90 B2 A2 62 A1 E9 AD B5 E4 31 D4 F2 74 38 CD	HMAC IN 1

输入域	输入域授权数据验证码	说明
KEY	4A D2 78 9D A3 69 DC 6A 5A AC 8F 9B 5E B3 36 8F 32 39 1D 4D FB CC F8 FC B2 B4 A6 B4 C5 3C E8 3A	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	3B F9 60 3C 85 4C 71 8F 49 42 11 9F 47 FD 3B 8E 59 90 B2 A2 62 A1 E9 AD B5 E4 31 D4 F2 74 38 CD	HASH OUT
HMAC IN 2	37 1D 69 E7	AP 会话的序列号
HMAC OUT	BF 91 08 34 2D 66 5E 24 9F D4 A7 4C 98 9F 76 B7 B2 AF 28 A3 FD 03 3B E5 B2 1C 44 0E 91 E1 C2 98	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算,其结果再与序列号做 HMAC 计算,HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值,使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来,有助于整个符合性测试的展现。

c) Owner 授权数据

Owner 创建 AP 会话时,需要 Owner 授权数据。本标准采用“TCMAuth”定值。新的 SMK 使用授权值采用“tempTCMAuth”。向量测试完成后,再次恢复成为“TCMAuth”定值。

6.21 TCM_NV_DefineSpace

依赖于:

a) TCM_Startup 命令的成功执行。

b) 有所有者,即 TCM_TakeOwnership 命令的成功执行。

输入域:

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 F9	
3	4	命令码	00 00 80 CC	TCM_ORD_NV_DefineSpace
4	可变	NV 空间的公开信息	00 18 00 00 00 01 00 06 01 01 00 02 01 00 00 02 01 00 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 00 06 01 01 00 02 01 00 00 02 01 00 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 00 17 00 00 00 00 00 00 00 00 00 00 28	TCM _ NV _ DATA _ PUBLIC 数据结构

序号	长度	名称	值	说明
5	32	加密的授权数据	99 B7 05 D8 97 C4 8A 14 7C 6F 10 CF 9A 0D 91 B6 8D 17 74 09 5F 78 E5 C0 E3 C6 BC 22 3C 16 21 36	NVAUTH
6	4	授权会话句柄	00 00 00 0B	
7	32	授权数据验证码	C4 3F 47 1B ED 80 38 D3 F8 CD D3 74 0E 9C 41 D0 4E 63 B8 F3 0A 39 B3 49 FD FF 45 C3 10 A5 D0 D7	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	授权数据验证码	CC AF 6F 1C 86 17 55 69 84 3C B9 61 E7 0B 0B 3F 39 CB 79 DA B1 4E 57 84 C8 C0 33 C4 EF 97 41 7C	
		命令码	00 00 80 CC	TCM_ORD_NV_DefineSpace

输入 Blob：

00 C2 00 00 00 F9 00 00 80 CC 00 18 00 00 00 01 00 06 01 01 00 02 01 00 00 02 01 00 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 00 06 01 01 00 02 01 00 00 02 01 00 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 00 17 00 00 00 00 00 00 00 00 00 00 28 99 B7 05 D8 97 C4 8A 14 7C 6F 10 CF 9A 0D 91 B6 8D 17 74 09 5F 78 E5 C0 E3 C6 BC 22 3C 16 21 36 00 00 00 0B C4 3F 47 1B ED 80 38 D3 F8 CD D3 74 0E 9C 41 D0 4E 63 B8 F3 0A 39 B3 49 FD FF 45 C3 10 A5 D0 D7

输出 Blob：

00 C5 00 00 00 2A 00 00 00 00 CC AF 6F 1C 86 17 55 69 84 3C B9 61 E7 0B 0B 3F 39 CB 79 DA B1 4E 57 84 C8 C0 33 C4 EF 97 41 7C

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 CC	命令码
HASH IN 2	00 18 00 00 00 01 00 06 01 01 00 02 01 00 00 02 01 00 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 00 06 01 01 00 02 01 00 00 02 01 00 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 41 54 89 09 21 CE 19 0F 1E FC 8E AF 60 0D A0 19 7A 88 20 C1 67 80 79 BF 99 51 D1 1C D0 78 9E AF 00 17 00 00 00 00 00 00 00 00 00 00 28	NV 空间的公开信息
HASH IN 3	99 B7 05 D8 97 C4 8A 14 7C 6F 10 CF 9A 0D 91 B6 8D 17 74 09 5F 78 E5 C0 E3 C6 BC 22 3C 16 21 36	新授权数据(加密的)
HASH OUT	27 B3 08 48 60 43 5F 1B B4 6A 5E 3D 58 25 20 FF 9D A0 19 94 77 14 4D D9 4F 1D 1B 4F B4 DB 1D 9C	HMAC IN 1
KEY	29 56 74 ED 8B 08 C4 EF E3 8C 46 E2 54 8B B3 D6 8F 54 5A B4 04 AF 75 8B F7 61 46 88 BB 85 81 15	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	27 B3 08 48 60 43 5F 1B B4 6A 5E 3D 58 25 20 FF 9D A0 19 94 77 14 4D D9 4F 1D 1B 4F B4 DB 1D 9C	HASH OUT
HMAC IN 2	41 26 A8 FD	AP 会话的序列号
HMAC OUT	C4 3F 47 1B ED 80 38 D3 F8 CD D3 74 0E 9C 41 D0 4E 63 B8 F3 0A 39 B3 49 FD FF 45 C3 10 A5 D0 D7	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算,其结果再与序列号做 HMAC 计算,HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值,使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来,有助于整个符合性测试的展现。

c) Owner 授权数据

Owner 创建 AP 会话时,需要 Owner 授权数据。本标准采用 OWNERAUTH 定值。新的 NV 空间使用授权值采用 NVAUTH。

6.22 TCM_NV_WriteValue

依赖于:

a) TCM_Startup 命令的成功执行。

b) 需要 TCM_NV_DefineSpace 命令的成功执行。

输入域:

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 20	
3	4	命令码	00 00 80 CD	TCM_ORD_NV_WriteValue

序号	长度	名称	值	说明
4	4	NV 索引	00 00 00 01	也可以是其他值，参看 GM/T BBBB 中的描述
5	4	偏移量	00 00 00 00	
6	4	要写入的数据长度	00 00 00 0A	要写入的数据长度
7	可变	要写入的数据	01 01 01 01 01 01 01 01 01 01	也可以是其他值

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 CD	TCM_ORD_NV_WriteValue

输入 Blob：

00 C1 00 00 00 20 00 00 80 CD 00 00 00 01 00 00 00 00 00 00 00 0A 01 01 01 01 01 01 01 01 01 01

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.23 TCM_NV_ReadValue

依赖于：

a） TCM_Startup 命令的成功执行。

b） 需要 TCM_NV_DefineSpace 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 16	
3	4	命令码	00 00 80 CF	TCM_ORD_NV_ReadValue
4	4	NV 索引	00 00 00 01	也可以是其他值，参看 GM/T BBBB 中的描述
5	4	偏移量	00 00 00 00	
6	4	要读取的数据大小	00 00 00 05	要读取的数据长度

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 13	
3	4	返回码	00 00 00 00	
4	4	读取的数据大小	00 00 00 05	

序号	长度	名称	值	说明
5	可变	读取的数据	01 01 01 01 01	
		命令码	00 00 80 CF	TCM_ORD_NV_ReadValue

输入 Blob：

00 C1 00 00 00 16 00 00 80 CF 00 00 00 01 00 00 00 00 00 00 00 05

输出 Blob：

00 C4 00 00 00 13 00 00 00 00 00 00 00 05 01 01 01 01 01

6.24 TCM_FlushSpecific

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) KeyA 的存在。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 12	
3	4	命令码	00 00 80 BA	TCM_ORD_FlushSpecific
4	4	资源句柄	05 00 00 07	KeyA 的句柄，也可以是其他资源句柄
5	4	资源类型	00 00 00 01	TCM_RT_KEY，也可以是 TCM_RT_CONTEXT，TCM_RT_AUTH，或者 TCM_RT_TRANS

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 BA	TCM_ORD_FlushSpecific

输入 Blob：

00 C1 00 00 00 12 00 00 80 BA 05 00 00 07 00 00 00 01

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

6.25 TCM_GetAuditDigest

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0E	
3	4	命令码	00 00 80 85	TCM_ORD_GetAuditDigest
4	4	开始序列号	00 00 80 65	设定开始审计的命令

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 C9	
3	4	返回码	00 00 00 00	
4	10	审计单调计数器	00 0E 00 00 00 00 00 00 00 38	
5	32	审计摘要	B7 BD 0C A3 AF AD 8F 0F 97 D0 5D 16 82 DB 41 AD 44 DC DF CB 33 96 8E 59 DA 3A 17 4B AF B0 6A A3	
6	1	是否全部返回的标记	00	
7	4	返回的命令列表长度	00 00 00 90	
8	可变	返回的命令列表	00 00 80 6F 00 00 80 6F 00 00 80 72 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 72 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C	
		命令码	00 00 80 85	TCM_ORD_GetAuditDigest

输入 Blob：

00 C1 00 00 00 0E 00 00 80 85 00 00 80 65

输出 Blob：

00 C4 00 00 00 C9 00 00 00 00 00 0E 00 00 00 00 00 00 00 38 B7 BD 0C A3 AF AD 8F 0F 97 D0 5D 16 82 DB 41 AD 44 DC DF CB 33 96 8E 59 DA 3A 17 4B AF B0 6A A3 00 00 00 00 90 00 00 80 6F 00 00 80 6F 00 00 80 72 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 72 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C 00 00 80 6F 00 00 80 6F 00 00 80 7C

6.26 TCM_GetAuditDigestSigned

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c） 存在已经加载的签名密钥，即 TCM_LoadKey 的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 53	
3	4	命令码	00 00 80 86	TCM _ ORD _ GetAuditDigest-Signed
4	4	签名密钥句柄	05 00 00 06	keyB
5	1	审计摘要结束标记	01	
6	32	抗重放参数	01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01	
7	4	授权会话句柄	00 00 00 4D	
8	32	授权数据验证码	1E 11 EF E9 CC 9E D5 A3 E8 A2 69 56 5B 9E BB 97 F1 0D 56 89 FF 0E 72 4F 00 A9 93 4E 8F 95 DD 27	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 B8	
3	4	返回码	00 00 00 00	
4	10	审计单调计数器	00 0E 00 00 00 00 00 00 00 3C	
5	32	审计事件摘要	91 1E 4B 21 97 63 7F 80 DD D1 10 43 4A E2 FA BD DE 10 BE 99 49 5B 61 9C 56 86 FA BF 46 36 84 63	
6	32	审计命令摘要	73 3F 04 58 03 3A 45 59 35 8D 10 16 68 0E 27 A1 24 24 28 35 0A 7E 8C 52 15 F4 81 0E 6E C5 00 5A	
7	4	签名数据长度	00 00 00 40	

序号	长度	名称	值	说明
8	可变	签名值	47 6B 9D 47 B6 8E DD 64 1C 6E 10 89 5E 8F B5 20 4A 90 7A A9 DE 53 99 D3 BF 06 9E CC 1D 45 BC 96 04 69 9A AF 4A D3 0B C2 0C B8 36 12 F5 E6 71 86 80 3C EF 35 5F 95 C8 04 F1 65 48 D8 A1 0E 22 5E	
9	32	授权数据验证码	BB 70 2C 3E 9A 55 74 03 29 D8 08 D7 87 5D F2 18 4A D6 9F 4F 0D B4 2D 9A 6B 15 B1 D5 DC 39 20 73	
		命令码	00 00 80 86	TCM _ ORD _ GetAuditDigest-Signed

输入 Blob：

00 C2 00 00 00 53 00 00 80 86 05 00 00 06 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 00 00 00 4D 1E 11 EF E9 CC 9E D5 A3 E8 A2 69 56 5B 9E BB 97 F1 0D 56 89 FF 0E 72 4F 00 A9 93 4E 8F 95 DD 27

输出 Blob：

00 C5 00 00 00 B8 00 00 00 00 00 0E 00 00 00 00 00 00 00 3C 91 1E 4B 21 97 63 7F 80 DD D1 10 43 4A E2 FA BD DE 10 BE 99 49 5B 61 9C 56 86 FA BF 46 36 84 63 73 3F 04 58 03 3A 45 59 35 8D 10 16 68 0E 27 A1 24 24 28 35 0A 7E 8C 52 15 F4 81 0E 6E C5 00 5A 00 00 00 40 47 6B 9D 47 B6 8E DD 64 1C 6E 10 89 5E 8F B5 20 4A 90 7A A9 DE 53 99 D3 BF 06 9E CC 1D 45 BC 96 04 69 9A AF 4A D3 0B C2 0C B8 36 12 F5 E6 71 86 80 3C EF 35 5F 95 C8 04 F1 65 48 D8 A1 0E 22 5E BB 70 2C 3E 9A 55 74 03 29 D8 08 D7 87 5D F2 18 4A D6 9F 4F 0D B4 2D 9A 6B 15 B1 D5 DC 39 20 73

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 86	命令码
HASH IN 2	01	审计摘要结束标记
HASH IN 3	01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01	抗重放参数
HASH OUT	4E 2D 8D 1F A2 59 A4 CA 04 97 84 90 81 CB 22 C1 A3 CE 22 A3 AB BD 30 95 6E 9B 18 31 35 C6 76 DD	HMAC IN 1
KEY	DD 06 D5 64 FE D9 72 0B A3 29 AD 1E 50 39 4F 54 F4 CB 2E EF B4 99 04 A1 9E A8 D1 5C 41 9C AF E7	AP 会话的共享秘密数据
HMAC IN 1	4E 2D 8D 1F A2 59 A4 CA 04 97 84 90 81 CB 22 C1 A3 CE 22 A3 AB BD 30 95 6E 9B 18 31 35 C6 76 DD	HASH OUT
HMAC IN 2	E3 DD BD DC	AP 会话的序列号
HMAC OUT	1E 11 EF E9 CC 9E D5 A3 E8 A2 69 56 5B 9E BB 97 F1 0D 56 89 FF 0E 72 4F 00 A9 93 4E 8F 95 DD 27	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

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、签名数据长度和签名值做哈希计

算,其结果再与序列号做 HMAC 计算,HMAC 的密钥为 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值,使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来,有助于整个符合性测试的展现。

c) 授权数据

创建签名密钥 AP 会话时,需要签名密钥授权数据。本标准采用 KEYAUTH 定值。

6.27 TCM_SetOrdinalAuditStatus

依赖于:

a) TCM_Startup 命令的成功执行。

b) 有所有者,即 TCM_TakeOwnership 命令的成功执行。

输入域:

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 33	
3	4	命令码	00 00 80 8D	TCM_ORD_SetOrdinalAuditStatus
4	4	审计命令码	00 00 80 EF	
5	1	审计标志位	01	也可以是 00
6	4	所有者授权会话句柄	00 00 00 2E	
7	32	所有者授权数据验证码	39 F6 B3 D1 B3 9B 6D C1 BF 70 E3 83 56 F4 A5 D8 B6 07 AE B6 63 4C 04 B9 A6 30 B2 36 D4 46 3F 56	

输出域:

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	所有者授权数据验证码	CF 5C 28 3A 62 96 27 4D D6 50 AA 25 0B 22 33 1D B5 70 33 F3 44 C1 2E D8 13 F0 5A 13 7A 05 57 5B	
		命令码	00 00 80 8D	TCM_ORD_SetOrdinalAuditStatus

输入 Blob:

00 C2 00 00 00 33 00 00 80 8D 00 00 80 EF 01 00 00 00 2E 39 F6 B3 D1 B3 9B 6D C1 BF 70 E3 83 56 F4 A5 D8 B6 07 AE B6 63 4C 04 B9 A6 30 B2 36 D4 46 3F 56

输出 Blob:

00 C5 00 00 00 2A 00 00 00 00 CF 5C 28 3A 62 96 27 4D D6 50 AA 25 0B 22 33 1D B5 70 33 F3 44

C1 2E D8 13 F0 5A 13 7A 05 57 5B

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 8D	命令码
HASH IN 2	00 00 80 EF	审计命令码
HASH IN 3	01	审计状态
HASH OUT	D3 48 76 7B F8 25 4A D5 58 D0 51 E8 00 43 FD 1E B4 D2 2A 63 B9 7F 6C 3D C3 13 55 98 77 63 26 89	HMAC IN 1
KEY	C2 CE 4F 5C 25 CD 58 59 8B C2 32 1A C2 48 10 E1 DA 7A 91 E6 57 BB 65 CA 77 CB 66 47 46 D5 FB 1D	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	D3 48 76 7B F8 25 4A D5 58 D0 51 E8 00 43 FD 1E B4 D2 2A 63 B9 7F 6C 3D C3 13 55 98 77 63 26 89	HASH OUT
HMAC IN 2	E1 B6 0E E1	AP 会话的序列号
HMAC OUT	39 F6 B3 D1 B3 9B 6D C1 BF 70 E3 83 56 F4 A5 D8 B6 07 AE B6 63 4C 04 B9 A6 30 B2 36 D4 46 3F 56	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c） Owner 授权数据

Owner 创建 AP 会话时，需要 Owner 授权数据。在本标准中采用的都是 OWNERAUTH 常量值。

6.28 TCM_GetTicks

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 F1	TCM_ORD_GetTicks

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 36	
3	4	返回码	00 00 00 00	

序号	长度	名称	值	说明
4	44	时钟节拍	00 14 00 00 00 00 00 00 0F B6 00 01 0B 6A 72 88 29 44 53 29 CA DA 5A ED 76 F2 7C 7B 9E 6A 11 08 DC 48 69 EB 09 D5 3C 46 4C F4 E9 D0	
		命令码	00 00 80 F1	TCM_ORD_GetTicks

输入 Blob：

00 C1 00 00 00 0A 00 00 80 F1

输出 Blob：

00 C4 00 00 00 36 00 00 00 00 00 14 00 00 00 00 00 00 0F B6 00 01 0B 6A 72 88 29 44 53 29 CA DA 5A ED 76 F2 7C 7B 9E 6A 11 08 DC 48 69 EB 09 D5 3C 46 4C F4 E9 D0

6.29 TCM_TickStampBlob

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 存在已经加载的签名密钥，即 TCM_LoadKey 的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM _ TAG _ RQU _ AUTH _COMMAND
2	4	数据长度	00 00 00 4E	
3	4	命令码	00 00 80 F2	TCM_ORD_TickStampBlob
4	4	签名密钥句柄	05 00 00 06	keyB
5	32	抗重放攻击数据	01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01	
6	32	摘要	70 98 2D 05 13 1E 5E AE 64 40 00 D1 3A DE 39 BF 68 15 46 7E 75 A0 85 0F 40 6C CD 9A 65 BC E0 7A	需要被执行时间戳的数据

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM _ TAG _ RSP _ AUTH _COMMAND
2	4	数据长度	00 00 00 9A	
3	4	返回码	00 00 00 00	

序号	长度	名称	值	说明
4	44	时间戳	00 14 00 00 00 00 00 02 BE 0E 00 01 CF 44 78 AF EB 86 00 F8 4E 3E CF 1B 1B 3D 7C BD 98 83 C0 D0 46 90 98 E5 20 B0 D7 2B C8 67 DC DE	
5	4	签名长度	00 00 00 40	
6	可变	签名信息	4E A4 24 4A DE FD B0 2D 89 17 E6 1A 53 7D F3 79 83 37 A7 03 9C 85 C2 30 2F 78 CA 82 41 5A CC 75 93 A3 C1 88 4F 9D CC 40 00 0E 31 16 13 E8 AE D0 5A 2A E7 DA B7 F1 6A D5 9B A2 64 01 95 4D 7C 41 6F 76 A3 AC 75 45 A1 D5 AC 22 03 3D 5E A9 66 38 30 B1 8C D2 DA 1B 4C EE 1D 2A 22 B2 82 1A CB EA	
		命令码	00 00 80 F2	TCM_ORD_TickStampBlob

输入 Blob：

00 C1 00 00 00 4E 00 00 80 F2 05 00 00 06 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 70 98 2D 05 13 1E 5E AE 64 40 00 D1 3A DE 39 BF 68 15 46 7E 75 A0 85 0F 40 6C CD 9A 65 BC E0 7A

输出 Blob：

00 C4 00 00 00 9A 00 00 00 00 00 14 00 00 00 00 00 02 BE 0E 00 01 CF 44 78 AF EB 86 00 F8 4E 3E CF 1B 1B 3D 7C BD 98 83 C0 D0 46 90 98 E5 20 B0 D7 2B C8 67 DC DE 00 00 00 40 4E A4 24 4A DE FD B0 2D 89 17 E6 1A 53 7D F3 79 83 37 A7 03 9C 85 C2 30 2F 78 CA 82 41 5A CC 75 93 A3 C1 88 4F 9D CC 40 00 0E 31 16 13 E8 AE D0 5A 2A E7 DA B7 F1 6A D5 9B A2 64 01 95 4D 7C 41 6F 76 A3 AC 75 45 A1 D5 AC 22 03 3D 5E A9 66 38 30 B1 8C D2 DA 1B 4C EE 1D 2A 22 B2 82 1A CB EA

6.30 TCM_ReadPubEK

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 2A	
3	4	命令码	00 00 80 7C	TCM_ORD_ReadPubEK
4	32	抗重放参数	FC 21 C0 D7 CA DE 82 92 27 34 D4 65 CA DD D2 55 65 A6 1A D6 D4 A2 DF E4 3B A3 E2 33 96 9D D9 EA	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 7F	
3	4	返回码	00 00 00 00	
4	可变	EK 公钥	00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 E2 A8 7A BD 18 6A 58 F6 F9 59 F1 27 F8 39 6F D8 46 5B 05 37 FC 2C A7 57 68 BF B9 72 89 61 1C 1D 5F 11 06 0D B6 D5 BD 64 56 B1 2E C0 C3 2F D8 90 4F B9 E8 F4 19 58 2C C7 26 3C A1 E4 11 B5 3F CD	
5	32	校验和	B6 E9 75 42 56 26 BA 8E 69 D4 B3 1E E4 50 66 B7 23 B7 3E 12 77 F1 5A 3E 4F A9 E0 58 4C 00 92 8F	
		命令码	00 00 80 7C	TCM_ORD_ReadPubEK

输入 Blob：

00 C1 00 00 00 2A 00 00 80 7C FC 21 C0 D7 CA DE 82 92 27 34 D4 65 CA DD D2 55 65 A6 1A D6 D4 A2 DF E4 3B A3 E2 33 96 9D D9 EA

输出 Blob：

00 C4 00 00 00 7F 00 00 00 00 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 E2 A8 7A BD 18 6A 58 F6 F9 59 F1 27 F8 39 6F D8 46 5B 05 37 FC 2C A7 57 68 BF B9 72 89 61 1C 1D 5F 11 06 0D B6 D5 BD 64 56 B1 2E C0 C3 2F D8 90 4F B9 E8 F4 19 58 2C C7 26 3C A1 E4 11 B5 3F CD B6 E9 75 42 56 26 BA 8E 69 D4 B3 1E E4 50 66 B7 23 B7 3E 12 77 F1 5A 3E 4F A9 E0 58 4C 00 92 8F

6.31 TCM_OwnerReadInternalPub

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 32	
3	4	命令码	00 00 80 81	TCM_ORD_OwnerReadInternal-Pub
4	4	EK 密钥句柄	40 00 00 06	
5	4	授权会话句柄	00 00 00 28	

序号	长度	名称	值	说明
6	32	授权数据验证码	27 77 3D 7B 3A 6A 4C 81 B3 73 92 BD 47 67 18 89 A6 2B 38 92 A6 83 81 FD F3 F0 29 B7 69 4C 26 14	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 7F	
3	4	返回码	00 00 00 00	
4	可变	EK 公钥	00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 E2 A8 7A BD 18 6A 58 F6 F9 59 F1 27 F8 39 6F D8 46 5B 05 37 FC 2C A7 57 68 BF B9 72 89 61 1C 1D 5F 11 06 0D B6 D5 BD 64 56 B1 2E C0 C3 2F D8 90 4F B9 E8 F4 19 58 2C C7 26 3C A1 E4 11 B5 3F CD	
5	32	授权数据校验码	66 C8 41 50 5A AB 8F F6 6E EB 62 30 9D 4F BC C0 2D BA D7 37 E3 BE D6 3E 51 83 91 88 66 37 EE 1B	
		命令码	00 00 80 81	TCM_ORD_OwnerReadInternal-Pub

输入 Blob：

00 C2 00 00 00 32 00 00 80 81 40 00 00 06 00 00 00 28 27 77 3D 7B 3A 6A 4C 81 B3 73 92 BD 47 67 18 89 A6 2B 38 92 A6 83 81 FD F3 F0 29 B7 69 4C 26 14

输出 Blob：

00 C5 00 00 00 7F 00 00 00 00 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 E2 A8 7A BD 18 6A 58 F6 F9 59 F1 27 F8 39 6F D8 46 5B 05 37 FC 2C A7 57 68 BF B9 72 89 61 1C 1D 5F 11 06 0D B6 D5 BD 64 56 B1 2E C0 C3 2F D8 90 4F B9 E8 F4 19 58 2C C7 26 3C A1 E4 11 B5 3F CD 66 C8 41 50 5A AB 8F F6 6E EB 62 30 9D 4F BC C0 2D BA D7 37 E3 BE D6 3E 51 83 91 88 66 37 EE 1B

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 81	命令码
HASH IN 2	40 00 00 06	EK 密钥句柄
HASH OUT	95 64 12 EC 48 44 B6 9F 90 C7 E0 A4 10 88 E8 08 F9 32 25 1E 55 AD 6C 08 A1 B7 83 11 E3 39 37 12	HMAC IN 1

输入域	输入域授权数据验证码	说明
KEY	8E 51 7E C5 46 0B A1 CD 4D 83 68 8D 60 B7 79 8D 0B 75 62 96 21 CF 93 D0 CF 1A 06 5F 17 1E 32 7B	Owner 创建的 AP 会话的共享秘密数据
HMAC IN 1	95 64 12 EC 48 44 B6 9F 90 C7 E0 A4 10 88 E8 08 F9 32 25 1E 55 AD 6C 08 A1 B7 83 11 E3 39 37 12	HASH OUT
HMAC IN 2	F3 99 99 D4	AP 会话的序列号
HMAC OUT	27 77 3D 7B 3A 6A 4C 81 B3 73 92 BD 47 67 18 89 A6 2B 38 92 A6 83 81 FD F3 F0 29 B7 69 4C 26 14	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码、命令码和 EK 公钥做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为 Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) Owner 授权数据

Owner 创建 AP 会话时，需要 Owner 授权数据。本标准采用 OWNERAUTH 常量值。

6.32 TCM_MakeIdentity

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C3	TCM _ TAG _ RQU _ AUTH2 _COMMAND
2	4	数据长度	00 00 00 B9	
3	4	命令码	00 00 80 79	TCM_ORD_MakeIdentity
4	32	加密的 PIK 授权数据	FE D8 FE CB 19 3F C7 54 08 03 6C 1D 72 3C 5B F0 2D A0 28 08 71 71 10 FF 5B 90 68 64 C0 B5 30 26	PIKAUTH
5	32	身份标识和可信方公钥的摘要	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78	
6	可变	PIK 密钥参数	00 15 00 00 00 12 00 00 00 00 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
7	4	SMK 授权会话句柄	00 00 00 4B	
8	32	SMK 授权数据验证码	B9 8F DC 12 06 AE 1F 49 3B 5B CC FC 81 23 0A 11 90 DA F3 8D A4 AD 40 9E F4 E5 63 61 BA FE D2 98	

序号	长度	名称	值	说明
9	4	Owner 授权会话句柄	00 00 00 4A	
10	32	Owner 授权数据验证码	C8 BA F4 82 D3 B7 50 00 44 27 33 48 DB 08 6C 25 7B 7D 4B EA D3 9C 01 0A 01 E8 8A 13 64 60 12 85	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C6	TCM _ TAG _ RSP _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 86	
3	4	返回码	00 00 00 00	
4	可变	PIK	00 15 00 00 00 12 00 00 00 00 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 41 04 4B 41 F0 0F CD 66 FE B1 F1 3C F9 9C 23 32 CE F8 55 04 2D 93 F8 9B E5 47 30 3B 71 71 08 9F BE 49 E9 88 45 CC 84 73 E6 E4 87 DE 2E EB AA 0D A8 EC 81 32 42 D6 57 9E 2B 9D EB 26 16 CE 12 2E 16 63 00 00 00 90 3B F4 DF EE AC 66 25 D9 D8 9F 12 89 7D 29 22 00 24 F2 01 21 E0 C4 F4 A1 0D CD C1 ED E2 6D 91 7A 82 FE 62 35 13 E8 49 29 E6 5B C9 04 2C 9D DD 58 A1 73 7B 3C 84 6F 2C 32 7E BC 76 D0 2A 39 44 3E AA 9D F7 85 29 01 C8 FE 6C CB 2B 58 5C F2 16 E0 9C 83 6F 76 A3 AC 75 45 A1 D5 AC 22 03 3D 5E A9 66 38 30 B1 8C D2 DA 1B 4C EE 1D 2A 22 B2 82 1A CB EA DD 34 24 45 3E 27 76 76 6B 35 DA AB 23 4E E7 54 4D DC F0 9F 9D 83 C3 AA 2B AD D0 78 9C AB	keyB
5	4	用于产生证书请求的信息大小	00 00 00 40	
6	可变	用于产生证书请求的信息	EC 95 C5 22 7E BE 7B 31 4B 8E 74 98 CD 5B 8D DF 9C 3B 62 E8 34 35 6F 7D 25 60 16 D6 1B F8 F8 61 3C 15 0A D4 6B A0 20 52 CA 64 36 BC CB 4A 58 BD 75 B3 C0 D5 5A 82 D9 DE 4D CC 63 B8 8E 18 15 54	
7	32	SMK 授权会话验证码	03 A9 0F 55 D4 20 EC 8A A8 2E 3D 42 0B E0 44 83 96 08 7D D4 96 8F 99 FF DA 0D 99 C5 AD 01 A9 8D	

序号	长度	名称	值	说明
8	32	Owner 授权会话验证码	25 F5 52 7D EB AC 9D 36 C1 30 78 38 DA 3F 5D 74 2F 61 94 80 61 81 27 CB 73 3B DE CD AE 9A 58 FC	
		命令码	00 00 80 79	TCM_ORD_MakeIdentity

输入 Blob：

00 C3 00 00 00 B9 00 00 80 79 FE D8 FE CB 19 3F C7 54 08 03 6C 1D 72 3C 5B F0 2D A0 28 08 71 71 10 FF 5B 90 68 64 C0 B5 30 26 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 00 15 00 00 00 12 00 00 00 00 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4B B9 8F DC 12 06 AE 1F 49 3B 5B CC FC 81 23 0A 11 90 DA F3 8D A4 AD 40 9E F4 E5 63 61 BA FE D2 98 00 00 00 4A C8 BA F4 82 D3 B7 50 00 44 27 33 48 DB 08 6C 25 7B 7D 4B EA D3 9C 01 0A 01 E8 8A 13 64 60 12 85

输出 Blob：

00 C6 00 00 01 86 00 00 00 00 00 15 00 00 00 12 00 00 00 00 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 41 04 4B 41 F0 0F CD 66 FE B1 F1 3C F9 9C 23 32 CE F8 55 04 2D 93 F8 9B E5 47 30 3B 71 71 08 9F BE 49 E9 88 45 CC 84 73 E6 E4 87 DE 2E EB AA 0D A8 EC 81 32 42 D6 57 9E 2B 9D EB 26 16 CE 12 2E 16 63 00 00 00 90 3B F4 DF EE AC 66 25 D9 D8 9F 12 89 7D 29 22 00 24 F2 01 21 E0 C4 F4 A1 0D CD C1 ED E2 6D 91 7A 82 FE 62 35 13 E8 49 29 E6 5B C9 04 2C 9D DD 58 A1 73 7B 3C 84 6F 2C 32 7E BC 76 D0 2A 39 44 3E AA 9D F7 85 29 01 C8 FE 6C CB 2B 58 5C F2 16 E0 9C 83 6F 76 A3 AC 75 45 A1 D5 AC 22 03 3D 5E A9 66 38 30 B1 8C D2 DA 1B 4C EE 1D 2A 22 B2 82 1A CB EA DD 34 24 45 3E 27 76 76 6B 35 DA AB 23 4E E7 54 4D DC F0 9F 9D 83 C3 AA 2B AD D0 78 9C AB 00 00 00 40 EC 95 C5 22 7E BE 7B 31 4B 8E 74 98 CD 5B 8D DF 9C 3B 62 E8 34 35 6F 7D 25 60 16 D6 1B F8 F8 61 3C 15 0A D4 6B A0 20 52 CA 64 36 BC CB 4A 58 BD 75 B3 C0 D5 5A 82 D9 DE 4D CC 63 B8 8E 18 15 54 03 A9 0F 55 D4 20 EC 8A A8 2E 3D 42 0B E0 44 83 96 08 7D D4 96 8F 99 FF DA 0D 99 C5 AD 01 A9 8D 25 F5 52 7D EB AC 9D 36 C1 30 78 38 DA 3F 5D 74 2F 61 94 80 61 81 27 CB 73 3B DE CD AE 9A 58 FC

说明：

a) 输入域 SMK 授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 79	命令码
HASH IN 2	FE D8 FE CB 19 3F C7 54 08 03 6C 1D 72 3C 5B F0 2D A0 28 08 71 71 10 FF 5B 90 68 64 C0 B5 30 26	加密的 PIK 授权数据
HASH IN 3	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78	身份标识和可信方公钥的摘要
HASH IN 4	00 15 00 00 00 12 00 00 00 00 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PIK 密钥参数
HASH OUT	E9 C4 58 49 16 EC 5D 9D A7 22 C7 51 D3 12 8F F9 31 85 F5 3B 77 FA D2 1E BB B1 D2 4A EE EE 06 E4	HMAC IN 1
KEY	62 CE A9 7F 92 94 81 B2 75 37 76 EA D4 59 54 2A 87 3E 90 6A 23 4A 84 33 45 3C 6D 44 C1 2E DC 23	创建的 SMK AP 会话的共享秘密数据

输入域	输入域授权数据验证码	说明
HMAC IN 1	E9 C4 58 49 16 EC 5D 9D A7 22 C7 51 D3 12 8F F9 31 85 F5 3B 77 FA D2 1E BB B1 D2 4A EE EE 06 E4	HASH OUT
HMAC IN 2	63 49 21 C5	AP 会话的序列号
HMAC OUT	B9 8F DC 12 06 AE 1F 49 3B 5B CC FC 81 23 0A 11 90 DA F3 8D A4 AD 40 9E F4 E5 63 61 BA FE D2 98	输入域授权数据验证码

b) 输入域 Owner 授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 79	命令码
HASH IN 2	FE D8 FE CB 19 3F C7 54 08 03 6C 1D 72 3C 5B F0 2D A0 28 08 71 71 10 FF 5B 90 68 64 C0 B5 30 26	加密的 PIK 授权数据
HASH IN 3	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78	身份标识和可信方公钥的摘要
HASH IN 4	00 15 00 00 00 12 00 00 00 00 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PIK 密钥参数
HASH OUT	E9 C4 58 49 16 EC 5D 9D A7 22 C7 51 D3 12 8F F9 31 85 F5 3B 77 FA D2 1E BB B1 D2 4A EE EE 06 E4	HMAC IN 1
KEY	EA 32 C1 76 7C 16 3A 9D B6 45 82 93 08 1B 88 57 F9 7A 59 6C 07 8D E7 EA 94 1F C2 5E A3 01 4A 96	创建的 Owner AP 会话的共享秘密数据
HMAC IN 1	E9 C4 58 49 16 EC 5D 9D A7 22 C7 51 D3 12 8F F9 31 85 F5 3B 77 FA D2 1E BB B1 D2 4A EE EE 06 E4	HASH OUT
HMAC IN 2	F5 BD D2 C8	AP 会话的序列号
HMAC OUT	C8 BA F4 82 D3 B7 50 00 44 27 33 48 DB 08 6C 25 7B 7D 4B EA D3 9C 01 0A 01 E8 8A 13 64 60 12 85	输入域授权数据验证码

c) 输出域授权数据验证码的计算过程

参看 GM/T BBBB 的描述。

d) 授权数据

创建 Owner AP 会话时,需要 Owner 授权数据。本标准采用 OWNERAUTH 常量值。创建 SMK AP 会话时,需要 SMK 授权数据,使用的是 SMKAUTH 常量值。

6.33 TCM_ActivatePEKCert

依赖于:

a) TCM_Startup 命令的成功执行。

b) 有所有者,即 TCM_TakeOwnership 命令的成功执行。

输入域:

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 AB	

序号	长度	名称	值	说明
3	4	命令码	40 00 80 DA	TCM_ORD_ActivatePEKCert
4	4	可信方返回的加密信息的大小	00 00 00 79	PIKAUTH
5	可变	可信方返回的加密信息	04 B6 9E 45 6E 48 27 22 46 D9 97 4D 16 F5 FA 56 FA 08 72 11 BD BE 19 74 1E E1 2B 19 52 7B 42 D8 10 48 7A 9F B0 EE 2C 7D 5B 72 0E 17 44 0D 6A 8E 24 EA 8A 27 59 A5 7C 30 50 3C 10 79 5D 10 AF 19 95 39 AD 78 BE 6C 6F 70 CC 37 06 EE F4 1D 51 DF 83 28 FC 79 0B FD B1 5A F1 E5 BE FE 63 ED A6 9F 58 9B D4 7D 05 E9 72 56 A9 0D 79 59 A1 54 1A D1 9B CD 6B 7D F1 71 D4 88 AF	
6	4	Owner 授权会话句柄	00 00 00 25	
7	32	Owner 授权数据验证码	08 70 0E F5 A9 D8 CE E2 34 7D C8 23 1A 66 4A 85 0C EF FC 7C 02 FC F7 60 40 A7 47 C3 62 63 7E 32	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH2 _COMMAND
2	4	数据长度	00 00 00 42	
3	4	返回码	00 00 00 00	
4	24	对称密钥	00 00 00 0B 00 08 00 10 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78	
5	32	Owner 授权会话验证码	C8 26 D4 8C 93 D0 35 AC 49 4A 10 DD 16 F8 5A EA 7B FA 1B B6 9B 23 34 48 5A 74 2B 4E DD 6B 5B 54	
		命令码	40 00 80 DA	TCM_ORD_ActivatePEKCert

输入 Blob：

00 C2 00 00 00 AB 40 00 80 DA 00 00 00 79 04 B6 9E 45 6E 48 27 22 46 D9 97 4D 16 F5 FA 56 FA 08 72 11 BD BE 19 74 1E E1 2B 19 52 7B 42 D8 10 48 7A 9F B0 EE 2C 7D 5B 72 0E 17 44 0D 6A 8E 24 EA 8A 27 59 A5 7C 30 50 3C 10 79 5D 10 AF 19 95 39 AD 78 BE 6C 6F 70 CC 37 06 EE F4 1D 51 DF 83 28 FC 79 0B FD B1 5A F1 E5 BE FE 63 ED A6 9F 58 9B D4 7D 05 E9 72 56 A9 0D 79 59 A1 54 1A D1 9B CD 6B 7D F1 71 D4 88 AF 00 00 00 25 08 70 0E F5 A9 D8 CE E2 34 7D C8 23 1A 66 4A 85 0C EF FC 7C 02 FC F7 60 40 A7 47 C3 62 63 7E 32

输出 Blob：

00 C5 00 00 00 42 00 00 00 00 00 00 00 0B 00 08 00 10 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78 C8 26 D4 8C 93 D0 35 AC 49 4A 10 DD 16 F8 5A EA 7B FA 1B B6 9B 23 34 48 5A 74 2B 4E DD

6B 5B 54

6.34 TCM_ActivatePEK

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C3	TCM _ TAG _ RQU _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 AA	
3	4	命令码	40 00 80 D9	TCM_ORD_ActivatePEK
4	32	加密的使用授权密码	1C D1 19 2B BC FF F1 2A B8 39 EF 59 DF 24 70 2C A7 E5 B9 0B A7 46 78 6A 26 42 CB 2E C3 85 A9 5C	PEKAUTH
5	可变	PEK 密钥信息	00 15 00 00 00 10 00 00 00 00 01 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00	
6	4	加密的 PEK 大小	00 00 00 90	
7	可变	加密的 PEK	7B 87 21 44 86 C5 5D 99 51 6C 78 E7 71 CF B6 9C 45 D2 3D FB 9A 0A 65 7E 0D EE B3 32 DD CD 97 BB 62 21 31 DA CA 74 E6 3F 2B 71 E9 0E 87 02 D3 BA 12 92 E2 8E 6A C7 85 18 01 3B 64 63 F6 8A 22 82 99 33 34 F1 E3 53 A5 54 CA F4 D6 B5 80 0D B8 38 B3 16 5D B1 D2 D5 A3 5B FB 5C CC DD B5 81 F4 D2 59 5F 45 1B 07 E2 7C 24 07 BF A4 AD C3 C4 5F 30 5E CA AE 9E B4 31 B3 50 1A AE B0 31 C9 F1 F4 BC 3F 06 5D CC BC 50 96 06 3A BF 2C 0B 19 EC D5 0A	
8	4	加密的对称密钥大小	00 00 00 79	
9	可变	加密的对称密钥	04 06 C9 77 10 4E C6 92 5F 05 04 F7 5E FF EB 1E E8 A1 28 8E 50 CC 1B F4 EB 04 90 1E 80 93 B5 74 85 A2 BC 23 E3 A6 B6 02 5C 06 12 EC 27 B1 57 19 76 A0 78 D1 6F 26 F5 4C D0 7D 64 8C 03 60 D7 15 6E 9A BC C1 12 50 68 88 5E B8 FB EE 83 6B 84 12 9F F3 5A F5 07 3F ED CE 2D A3 06 9C B6 55 77 88 B2 CE 0C 73 1B 01 38 9B 88 2C 24 A8 6F DE B4 BC 4B 00 02 04 5A 69 6C A5 45	
10	4	SMK 授权句柄	00 00 00 3C	

序号	长度	名称	值	说明
11	32	SMK 授权会话验证码	E1 DB B4 84 F1 31 2F 97 4A F6 28 70 64 88 0B 0F B1 64 B4 72 0D AF D2 58 32 6F 10 B8 E7 0C A9 1C	
12	4	Owner 授权句柄	00 00 00 3D	
13	32	Owner 授权数据验证码	9A 3D 98 EF F2 1F 37 EA 63 8E 87 48 35 76 F2 46 73 09 A8 E9 39 08 98 80 3D B0 67 27 22 71 8D C8	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C6	TCM _ TAG _ RSP _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 01	
3	4	返回码	00 00 00 00	
4	可变	PEK	00 15 00 00 00 10 00 00 00 00 01 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 90 60 A6 D9 57 52 0C B1 70 B2 FB 21 60 08 48 96 C2 C6 70 B7 6C C9 CE F9 B0 FC 68 DB 1B 1A 49 F1 08 46 60 27 FC FF 8E D3 37 DE E1 19 49 2D 77 5F AD 1A 73 8E A3 38 BD A8 00 51 D6 0E 23 61 D2 24 04 A5 C4 5C 2C 2B 4E 78 F8 BC 3B B9 E3 D4 53 94 76 9B A7 62 99 04 60 E9 AA 74 F7 EE 53 6F F4 2E 80 FF 4A 58 2F 46 E5 67 7A 0B 0E 17 03 8D C2 C4 C9 80 D5 DC F4 6A 18 CC E8 FE B3 72 40 00 34 33 53 93 47 2D BD B9 84 A3 0F D7 C4 EB 4A 98 58 BD 26	
5	32	SMK 授权会话验证码	2A 6A 5A 40 D9 38 A2 AB 6A A4 75 72 5C 86 4D D6 AC 51 EB FA 7E 25 30 41 4B 39 CC FD 1B 81 75 40	
6	32	Owner 授权会话验证码	4B A4 AA 20 CF 5E D6 1E DA 63 1D 5E B0 68 E2 3A 28 42 6C CC BC A1 47 39 67 21 9A AA DA 84 B1 DD	
		命令码	40 00 80 D9	TCM_ORD_ActivatePEK

输入 Blob：

00 C3 00 00 01 AA 40 00 80 D9 1C D1 19 2B BC FF F1 2A B8 39 EF 59 DF 24 70 2C A7 E5 B9 0B A7 46 78 6A 26 42 CB 2E C3 85 A9 5C 00 15 00 00 00 10 00 00 00 00 01 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 7B 87 21 44 86 C5 5D 99 51 6C 78 E7 71 CF B6 9C 45 D2 3D FB 9A 0A 65 7E 0D EE B3 32 DD CD 97 BB 62 21 31 DA CA 74 E6 3F 2B 71

E9 0E 87 02 D3 BA 12 92 E2 8E 6A C7 85 18 01 3B 64 63 F6 8A 22 82 99 33 34 F1 E3 53 A5 54 CA F4 D6 B5 80 0D B8 38 B3 16 5D B1 D2 D5 A3 5B FB 5C CC DD B5 81 F4 D2 59 5F 45 1B 07 E2 7C 24 07 BF A4 AD C3 C4 5F 30 5E CA AE 9E B4 31 B3 50 1A AE B0 31 C9 F1 F4 BC 3F 06 5D CC BC 50 96 06 3A BF 2C 0B 19 EC D5 0A 00 00 00 79 04 06 C9 77 10 4E C6 92 5F 05 04 F7 5E FF EB 1E E8 A1 28 8E 50 CC 1B F4 EB 04 90 1E 80 93 B5 74 85 A2 BC 23 E3 A6 B6 02 5C 06 12 EC 27 B1 57 19 76 A0 78 D1 6F 26 F5 4C D0 7D 64 8C 03 60 D7 15 6E 9A BC C1 12 50 68 88 5E B8 FB EE 83 6B 84 12 9F F3 5A F5 07 3F ED CE 2D A3 06 9C B6 55 77 88 B2 CE 0C 73 1B 01 38 9B 88 2C 24 A8 6F DE B4 BC 4B 00 02 04 5A 69 6C A5 45 00 00 00 3C E1 DB B4 84 F1 31 2F 97 4A F6 28 70 64 88 0B 0F B1 64 B4 72 0D AF D2 58 32 6F 10 B8 E7 0C A9 1C 00 00 00 3D 9A 3D 98 EF F2 1F 37 EA 63 8E 87 48 35 76 F2 46 73 09 A8 E9 39 08 98 80 3D B0 67 27 22 71 8D C8

输出 Blob：

00 C6 00 00 01 01 00 00 00 00 00 15 00 00 00 10 00 00 00 00 01 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 90 60 A6 D9 57 52 0C B1 70 B2 FB 21 60 08 48 96 C2 C6 70 B7 6C C9 CE F9 B0 FC 68 DB 1B 1A 49 F1 08 46 60 27 FC FF 8E D3 37 DE E1 19 49 2D 77 5F AD 1A 73 8E A3 38 BD A8 00 51 D6 0E 23 61 D2 24 04 A5 C4 5C 2C 2B 4E 78 F8 BC 3B B9 E3 D4 53 94 76 9B A7 62 99 04 60 E9 AA 74 F7 EE 53 6F F4 2E 80 FF 4A 58 2F 46 E5 67 7A 0B 0E 17 03 8D C2 C4 C9 80 D5 DC F4 6A 18 CC E8 FE B3 72 40 00 34 33 53 93 47 2D BD B9 84 A3 0F D7 C4 EB 4A 98 58 BD 26 2A 6A 5A 40 D9 38 A2 AB 6A A4 75 72 5C 86 4D D6 AC 51 EB FA 7E 25 30 41 4B 39 CC FD 1B 81 75 40 4B A4 AA 20 CF 5E D6 1E DA 63 1D 5E B0 68 E2 3A 28 42 6C CC BC A1 47 39 67 21 9A AA DA 84 B1 DD

6.35 TCM_Seal

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 存在封装操作密钥。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 6A	
3	4	命令码	00 00 80 17	TCM_ORD_Seal
4	4	封装操作密钥句柄	05 00 00 02	KeyC
5	32	加密的授权数据	0A C4 6B F4 E2 E7 09 B8 AA 52 E5 19 2D D4 5E 0E 7C 85 BA 8D 58 A3 2B 79 82 54 3A B7 84 84 9A E9	DATAAUTH
6	4	PCR 信息长度	00 00 00 00	
7	可变	PCR 信息		也可以是其他 PCR
8	4	待封装数据长度	00 00 00 10	
9	可变	待封装数据	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 01	也可以是其他任意数据

序号	长度	名称	值	说明
10	4	授权会话句柄	00 00 00 2A	
11	32	授权数据验证码	51 16 B2 AF 7D B9 FD 22 14 65 D1 8A 17 A2 DB 98 D8 80 0C 62 8D 60 6B 49 B3 C1 A2 51 51 57 F9 0D	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 01 0C	
3	4	返回码	00 00 00 00	
4	可变	封装数据块	00 16 00 00 00 00 00 00 00 00 00 D6 04 69 EF 29 4A 63 57 0D DC B4 69 62 1D 87 ED D9 3E A6 D6 CE 98 81 34 F1 E4 CE 71 FB B8 E0 0C 6D 47 CF EF 6C 19 30 61 5E DD 79 51 03 A8 28 DC 40 DA 8E 83 B6 72 E3 32 5C 15 38 CF 3B E8 99 96 EA 02 BA 61 3B C1 96 E4 96 B1 27 3E 64 74 84 A4 89 D8 32 26 38 43 84 90 5F 47 95 5A D7 7B 16 A9 13 C9 E7 8E E5 F5 6D 04 0B E9 44 D2 71 7B 2D 79 32 A9 E8 99 4F FE E3 87 CF 49 D0 20 80 B9 18 D7 CD FC 92 3D 69 5F C7 60 AB 5B 36 79 80 5D 96 F9 F3 15 F8 85 D3 81 86 CB B1 48 06 14 6A EF E7 85 6B ED 27 9E D4 5A C1 49 71 BD AC BF CF 2D 82 47 AF BB CC 41 FC 7F 9D 6E 20 24 E2 BB 73 DC F0 F8 7A D5 6E 53 0C D7 6A 61 DF F2 27 22 C6 4A CE 5F B0 B7 00 C3 8C 43 CC	
5	32	授权数据验证码	FE 58 06 FA 3A 20 49 2C 31 B8 A4 9E B2 FF FF 5E A4 F4 EF 26 D0 31 8E 80 55 51 B2 6A AD 61 D9 C6	
		命令码	00 00 80 17	TCM_ORD_Seal

输入 Blob：

00 C2 00 00 00 6A 00 00 80 17 05 00 00 02 0A C4 6B F4 E2 E7 09 B8 AA 52 E5 19 2D D4 5E 0E 7C 85 BA 8D 58 A3 2B 79 82 54 3A B7 84 84 9A E9 00 00 00 00 00 00 00 10 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 01 00 00 00 2A 51 16 B2 AF 7D B9 FD 22 14 65 D1 8A 17 A2 DB 98 D8 80 0C 62 8D 60 6B 49 B3 C1 A2 51 51 57 F9 0D

输出 Blob：

00 C5 00 00 01 0C 00 00 00 00 00 16 00 00 00 00 00 00 00 00 00 D6 04 69 EF 29 4A 63 57 0D DC B4 69 62 1D 87 ED D9 3E A6 D6 CE 98 81 34 F1 E4 CE 71 FB B8 E0 0C 6D 47 CF EF 6C 19 30 61 5E

DD 79 51 03 A8 28 DC 40 DA 8E 83 B6 72 E3 32 5C 15 38 CF 3B E8 99 96 EA 02 BA 61 3B C1 96 E4 96 B1 27 3E 64 74 84 A4 89 D8 32 26 38 43 84 90 5F 47 95 5A D7 7B 16 A9 13 C9 E7 8E E5 F5 6D 04 0B E9 44 D2 71 7B 2D 79 32 A9 E8 99 4F FE E3 87 CF 49 D0 20 80 B9 18 D7 CD FC 92 3D 69 5F C7 60 AB 5B 36 79 80 5D 96 F9 F3 15 F8 85 D3 81 86 CB B1 48 06 14 6A EF E7 85 6B ED 27 9E D4 5A C1 49 71 BD AC BF CF 2D 82 47 AF BB CC 41 FC 7F 9D 6E 20 24 E2 BB 73 DC F0 F8 7A D5 6E 53 0C D7 6A 61 DF F2 27 22 C6 4A CE 5F B0 B7 00 C3 8C 43 CC FE 58 06 FA 3A 20 49 2C 31 B8 A4 9E B2 FF FF 5E A4 F4 EF 26 D0 31 8E 80 55 51 B2 6A AD 61 D9 C6

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 17	命令码
HASH IN 2	0A C4 6B F4 E2 E7 09 B8 AA 52 E5 19 2D D4 5E 0E 7C 85 BA 8D 58 A3 2B 79 82 54 3A B7 84 84 9A E9	加密的授权数据
HASH IN 3	00 00 00 00	PCR 信息长度
HASH IN 4		PCR 信息
HASH IN 5	00 00 00 10	待封装数据长度
HASH IN 6	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 01	待封装数据
HASH OUT	34 6D 13 36 0C 96 06 9C DC 62 95 6A 7C F5 08 58 FA A8 41 26 A0 D5 C1 92 E8 67 AD 37 11 C3 B1 D6	HMAC IN 1
KEY	0F 34 72 9A 84 19 02 DC 61 68 7A 86 15 AC 56 8E 49 B7 0A 32 EB CC 1B DE 38 C4 4E 8D AF E0 AE 68	封装操作密钥 AP 会话的共享秘密数据
HMAC IN 1	34 6D 13 36 0C 96 06 9C DC 62 95 6A 7C F5 08 58 FA A8 41 26 A0 D5 C1 92 E8 67 AD 37 11 C3 B1 D6	HASH OUT
HMAC IN 2	E1 2F ED C9	AP 会话的序列号
HMAC OUT	51 16 B2 AF 7D B9 FD 22 14 65 D1 8A 17 A2 DB 98 D8 80 0C 62 8D 60 6B 49 B3 C1 A2 51 51 57 F9 0D	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码、命令码和封装数据做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用封装操作密钥 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) 授权数据

创建封装操作密钥 AP 会话时，需要封装操作密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

d) 封装操作密钥

封装操作密钥采用的是 keyC。

6.36 TCM_Unseal

依赖于：

a) TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c） 存在封装操作密钥。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C3	TCM _ TAG _ RQU _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 38	
3	4	命令码	00 00 80 18	TCM_ORD_Unseal
4	4	解封操作密钥句柄	05 00 00 02	KeyC
5	可变	待解封数据		
6	4	解封操作密钥授权会话句柄	00 00 00 10	
7	32	解封操作密钥授权数据验证码	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 01	也可以是其他任意数据
8	4	封装数据授权会话句柄	00 00 00 2A	
9	32	封装数据授权数据验证码	51 16 B2 AF 7D B9 FD 22 14 65 D1 8A 17 A2 DB 98 D8 80 0C 62 8D 60 6B 49 B3 C1 A2 51 51 57 F9 0D	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 01 0C	
3	4	返回码	00 00 00 00	
4	可变	封装数据块	00 16 00 00 00 00 00 00 00 00 00 D6 04 69 EF 29 4A 63 57 0D DC B4 69 62 1D 87 ED D9 3E A6 D6 CE 98 81 34 F1 E4 CE 71 FB B8 E0 0C 6D 47 CF EF 6C 19 30 61 5E DD 79 51 03 A8 28 DC 40 DA 8E 83 B6 72 E3 32 5C 15 38 CF 3B E8 99 96 EA 02 BA 61 3B C1 96 E4 96 B1 27 3E 64 74 84 A4 89 D8 32 26 38 43 84 90 5F 47 95 5A D7 7B 16 A9 13 C9 E7 8E E5 F5 6D 04 0B E9 44 D2 71 7B 2D 79 32 A9 E8 99 4F FE E3 87 CF 49 D0 20 80 B9 18 D7 CD FC 92 3D 69 5F C7 60 AB 5B 36 79 80 5D 96 F9 F3 15 F8 85 D3 81 86 CB B1 48 06 14 6A EF E7 85 6B ED 27 9E D4 5A C1 49 71 BD AC BF CF 2D 82 47 AF BB CC 41 FC 7F 9D 6E 20 24 E2 BB 73 DC F0 F8 7A D5 6E 53 0C D7 6A 61 DF F2 27 22 C6 4A CE 5F B0 B7 00 C3 8C 43 CC	

序号	长度	名称	值	说明
5	32	授权数据验证码	FE 58 06 FA 3A 20 49 2C 31 B8 A4 9E B2 FF FF 5E A4 F4 EF 26 D0 31 8E 80 55 51 B2 6A AD 61 D9 C6	
		命令码	00 00 80 18	TCM_ORD_Unseal

输入 Blob：

00 C3 00 00 01 38 00 00 80 18 05 00 00 02 00 16 00 00 00 00 00 00 00 00 00 D6 04 69 EF 29 4A 63 57 0D DC B4 69 62 1D 87 ED D9 3E A6 D6 CE 98 81 34 F1 E4 CE 71 FB B8 E0 0C 6D 47 CF EF 6C 19 30 61 5E DD 79 51 03 A8 28 DC 40 DA 8E 83 B6 72 E3 32 5C 15 38 CF 3B E8 99 96 EA 02 BA 61 3B C1 96 E4 96 B1 27 3E 64 74 84 A4 89 D8 32 26 38 43 84 90 5F 47 95 5A D7 7B 16 A9 13 C9 E7 8E E5 F5 6D 04 0B E9 44 D2 71 7B 2D 79 32 A9 E8 99 4F FE E3 87 CF 49 D0 20 80 B9 18 D7 CD FC 92 3D 69 5F C7 60 AB 5B 36 79 80 5D 96 F9 F3 15 F8 85 D3 81 86 CB B1 48 06 14 6A EF E7 85 6B ED 27 9E D4 5A C1 49 71 BD AC BF CF 2D 82 47 AF BB CC 41 FC 7F 9D 6E 20 24 E2 BB 73 DC F0 F8 7A D5 6E 53 0C D7 6A 61 DF F2 27 22 C6 4A CE 5F B0 B7 00 C3 8C 43 CC 00 00 00 2C 10 DC 7D FB 81 05 E2 87 88 25 9B 68 D1 17 EC 16 42 AA DE 7B 6F B3 60 25 23 2C CB 7C AE C4 81 20 00 00 00 2B 31 08 8D A1 15 9C AC 5E 1D 87 77 B9 42 03 10 0F F9 5A 74 27 7F A5 EA 89 48 BB 2B DB F3 F3 72 B1

输出 Blob：

00 C4 00 00 00 0A 00 00 00 01

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 17	命令码
HASH IN 2	0A C4 6B F4 E2 E7 09 B8 AA 52 E5 19 2D D4 5E 0E 7C 85 BA 8D 58 A3 2B 79 82 54 3A B7 84 84 9A E9	加密的授权数据
HASH IN 3	00 00 00 00	PCR 信息长度
HASH IN 4		PCR 信息
HASH IN 5	00 00 00 10	待封装数据长度
HASH IN 6	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 01	待封装数据
HASH OUT	34 6D 13 36 0C 96 06 9C DC 62 95 6A 7C F5 08 58 FA A8 41 26 A0 D5 C1 92 E8 67 AD 37 11 C3 B1 D6	HMAC IN 1
KEY	0F 34 72 9A 84 19 02 DC 61 68 7A 86 15 AC 56 8E 49 B7 0A 32 EB CC 1B DE 38 C4 4E 8D AF E0 AE 68	封装操作密钥 AP 会话的共享秘密数据
HMAC IN 1	34 6D 13 36 0C 96 06 9C DC 62 95 6A 7C F5 08 58 FA A8 41 26 A0 D5 C1 92 E8 67 AD 37 11 C3 B1 D6	HASH OUT
HMAC IN 2	E1 2F ED C9	AP 会话的序列号
HMAC OUT	51 16 B2 AF 7D B9 FD 22 14 65 D1 8A 17 A2 DB 98 D8 80 0C 62 8D 60 6B 49 B3 C1 A2 51 51 57 F9 0D	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码、命令码和封装数据做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为

Owner 创建的 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) 授权数据

创建封装操作密钥 AP 会话时，需要封装操作密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

d) 封装操作密钥

封装操作密钥采用的是 keyC。

6.37 TCM_CreateWrapKey

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 99	
3	4	命令码	00 00 80 1F	TCM_ORD_CreateWrapKey
4	4	保护操作密钥句柄	40 00 00 00	SMK 句柄
5	32	加密的使用授权数据	30 F0 67 6F B1 E7 C0 EC A1 96 B4 DC EA 5C F5 FD 14 0C 15 81 91 C3 37 07 0D 78 30 56 B2 DC 4B E5	KEYAUTH
6	32	加密的迁移授权数据	30 F0 67 6F B1 E7 C0 EC A1 96 B4 DC EA 5C F5 FD 14 0C 15 81 91 C3 37 07 0D 78 30 56 B2 DC 4B E5	KEYAUTH
7	可变	密钥信息	00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00	
8	4	保护操作密钥授权会话句柄	00 00 00 2F	
9	32	保护操作密钥授权数据验证码	63 FB 14 BA 8F A5 1A B9 AA 7B E9 63 F6 0B 10 7C C7 C5 74 BF 76 7F 0C 76 35 94 4B 3F C1 A5 76 81	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 01 22	

序号	长度	名称	值	说明
3	4	返回码	00 00 00 00	
4	可变	创建的密钥	00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 41 04 E0 C4 92 0C 82 91 0B F8 A4 73 00 23 CE 6C F0 22 9E D7 1B 9A 1F D7 8D 09 69 DB 2F A7 91 AF 5A F6 2A AC 7B 7D C5 37 E9 A2 16 08 F5 EE 83 76 49 A7 08 8B 02 31 8A 66 2C 58 B4 47 10 6A 86 B3 39 B0 00 00 00 90 42 99 89 C0 2D 47 CE 95 D9 1B 99 87 B0 79 09 34 64 5B 8E 51 69 C5 9C D6 49 3A 1B DA 60 B5 04 28 83 F2 7A A8 51 96 99 3B D8 13 31 85 66 01 4B 09 B9 20 CD 83 0E 08 9E 32 13 93 01 C3 46 BB 37 8F 2B CB 50 50 EB 84 18 7E D8 B0 C1 37 67 24 B0 41 2C 70 AB 07 6A A7 6D 03 B8 DF BA 00 45 AB 31 B5 90 CF F3 0D 44 5B 48 5F E3 82 63 45 39 36 0A C3 7B 88 A9 74 27 E3 85 2A 94 17 29 E7 6A D1 81 9A 36 BE 82 BC D9 9B 3D 40 0A C1 53 7A 6F C7 B6 5B	
5	32	授权数据验证码	7C C8 9C 78 81 33 0F 8D 85 C6 ED 31 19 A2 D2 22 FA 79 F6 BD 0F 67 94 8A 44 19 AC 72 9F D9 29 1F	
		命令码	00 00 80 1F	TCM_ORD_CreateWrapKey

输入 Blob：

00 C2 00 00 00 99 00 00 80 1F 40 00 00 00 30 F0 67 6F B1 E7 C0 EC A1 96 B4 DC EA 5C F5 FD 14 0C 15 81 91 C3 37 07 0D 78 30 56 B2 DC 4B E5 30 F0 67 6F B1 E7 C0 EC A1 96 B4 DC EA 5C F5 FD 14 0C 15 81 91 C3 37 07 0D 78 30 56 B2 DC 4B E5 00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2F 63 FB 14 BA 8F A5 1A B9 AA 7B E9 63 F6 0B 10 7C C7 C5 74 BF 76 7F 0C 76 35 94 4B 3F C1 A5 76 81

输出 Blob：

00 C5 00 00 01 22 00 00 00 00 00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 41 04 E0 C4 92 0C 82 91 0B F8 A4 73 00 23 CE 6C F0 22 9E D7 1B 9A 1F D7 8D 09 69 DB 2F A7 91 AF 5A F6 2A AC 7B 7D C5 37 E9 A2 16 08 F5 EE 83 76 49 A7 08 8B 02 31 8A 66 2C 58 B4 47 10 6A 86 B3 39 B0 00 00 00 90 42 99 89 C0 2D 47 CE 95 D9 1B 99 87 B0 79 09 34 64 5B 8E 51 69 C5 9C D6 49 3A 1B DA 60 B5 04 28 83 F2 7A A8 51 96 99 3B D8 13 31 85 66 01 4B 09 B9 20 CD 83 0E 08 9E 32 13 93 01 C3 46 BB 37 8F 2B CB 50 50 EB 84 18 7E D8 B0 C1 37 67 24 B0 41 2C 70 AB 07 6A A7 6D 03 B8 DF BA 00 45 AB 31 B5 90 CF F3 0D 44 5B 48 5F E3 82 63 45 39 36 0A C3 7B 88 A9 74 27 E3 85 2A 94 17 29 E7 6A D1 81 9A 36 BE 82 BC D9 9B 3D 40 0A C1 53 7A 6F C7 B6 5B 7C C8 9C 78 81 33 0F 8D 85 C6 ED 31 19 A2 D2 22 FA 79 F6 BD 0F 67 94 8A 44 19 AC 72 9F D9 29 1F

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 1F	命令码
HASH IN 2	30 F0 67 6F B1 E7 C0 EC A1 96 B4 DC EA 5C F5 FD 14 0C 15 81 91 C3 37 07 0D 78 30 56 B2 DC 4B E5	加密的使用授权数据
HASH IN 3	30 F0 67 6F B1 E7 C0 EC A1 96 B4 DC EA 5C F5 FD 14 0C 15 81 91 C3 37 07 0D 78 30 56 B2 DC 4B E5	加密的迁移授权数据
HASH IN 4	00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	密钥信息
HASH OUT	61 CD 54 36 CE 23 B9 52 FC 63 47 68 87 DB 62 4E 72 62 87 5D 0B 4D 88 11 8E B6 D3 14 8A 41 50 07	HMAC IN 1
KEY	BA 8A 44 56 F0 4A 59 88 1A 93 03 72 9C ED 65 1A ED 38 2C 59 8E 6A 93 0F 9E E1 8C 30 19 9E 8E A2	保护操作密钥 AP 会话的共享秘密数据
HMAC IN 1	61 CD 54 36 CE 23 B9 52 FC 63 47 68 87 DB 62 4E 72 62 87 5D 0B 4D 88 11 8E B6 D3 14 8A 41 50 07	HASH OUT
HMAC IN 2	43 5C 2A F0	AP 会话的序列号
HMAC OUT	63 FB 14 BA 8F A5 1A B9 AA 7B E9 63 F6 0B 10 7C C7 C5 74 BF 76 7F 0C 76 35 94 4B 3F C1 A5 76 81	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码、命令码和创建的密钥做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用保护操作密钥创建的 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c） 授权数据

创建保护操作密钥 AP 会话时，需要保护操作密钥的使用授权数据。本标准采用 KEYAUTH 常量值。创建的新密钥的使用授权数据和迁移授权数据都是常量值 KEYAUTH。

6.38 TCM_LoadKey

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c） 已经创建了一个密钥，即 TCM_CreateWrapKey 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 01 2A	
3	4	命令码	00 00 80 EF	TCM_ORD_LoadKey
4	4	保护操作密钥句柄	40 00 00 00	SMK 句柄

序号	长度	名称	值	说明
5	可变	被加载密钥	00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 41 04 59 51 23 3B 37 16 1C FE 3A 9D E8 2C B8 6A 2C AA 4D 2C 80 1E 7F EF EA 5B A7 BA 68 BC E6 52 4B 9B E5 10 13 77 61 3E C9 2D 1A 43 E3 E7 55 B9 7D 2B 38 62 E5 1C DE 4F 0D 17 8D 0B AA F6 52 F4 36 E6 00 00 00 90 42 99 89 C0 2D 47 CE 95 D9 1B 99 87 B0 79 09 34 64 5B 8E 51 69 C5 9C D6 49 3A 1B DA 60 B5 04 28 83 F2 7A A8 51 96 99 3B D8 13 31 85 66 01 4B 09 B9 20 CD 83 0E 08 9E 32 13 93 01 C3 46 BB 37 8F BF B0 45 90 0A 57 4C 6E 49 FD A6 3F C7 8B 46 0C B1 F2 43 10 F4 EC D7 D3 76 31 6E 60 23 E7 64 E0 30 8F CC 4D 5B 4D 85 9B 7A A5 3E 93 E9 5E 1D 13 BE 9C AA F3 21 AD 0B 64 14 8C 38 12 5B BF 7B BA D7 E8 9E 74 69 BC 87 11 A1 A7 D1 5A 63 E9 EE 08	
6	4	保护操作密钥授权会话句柄	00 00 00 31	
7	32	保护操作密钥授权数据验证码	89 51 60 36 3B 25 3F CB 70 F9 EC 74 19 EF ED 5D 20 7A C1 5F F6 AF 79 E5 B7 78 76 22 57 DD 44 E0	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2E	
3	4	返回码	00 00 00 00	
4	4	被加载密钥句柄	05 00 00 05	
5	32	授权数据验证码	D8 14 09 F9 4B B2 FF BB 1C 91 78 6A 89 6D C2 A5 3D 8A B9 50 D6 A8 44 7D 1A 1D 98 16 FC 5D 2E C5	
		命令码	00 00 80 EF	TCM_ORD_LoadKey

输入 Blob：

00 C2 00 00 01 2A 00 00 80 EF 40 00 00 00 00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 00 41 04 59 51 23 3B 37 16 1C FE 3A 9D E8 2C B8 6A 2C AA 4D 2C 80 1E 7F EF EA 5B A7 BA 68 BC E6 52 4B 9B E5 10 13 77 61 3E C9 2D 1A 43 E3 E7 55 B9 7D 2B 38 62 E5 1C DE 4F 0D 17 8D 0B AA F6 52 F4 36 E6 00 00 00 90 42 99 89 C0 2D 47 CE 95 D9 1B 99 87 B0 79 09 34 64 5B 8E 51 69 C5 9C D6 49 3A 1B DA 60 B5 04 28 83 F2 7A A8 51 96 99 3B D8

13 31 85 66 01 4B 09 B9 20 CD 83 0E 08 9E 32 13 93 01 C3 46 BB 37 8F BF B0 45 90 0A 57 4C 6E 49 FD A6 3F C7 8B 46 0C B1 F2 43 10 F4 EC D7 D3 76 31 6E 60 23 E7 64 E0 30 8F CC 4D 5B 4D 85 9B 7A A5 3E 93 E9 5E 1D 13 BE 9C AA F3 21 AD 0B 64 14 8C 38 12 5B BF 7B BA D7 E8 9E 74 69 BC 87 11 A1 A7 D1 5A 63 E9 EE 08 00 00 00 31 89 51 60 36 3B 25 3F CB 70 F9 EC 74 19 EF ED 5D 20 7A C1 5F F6 AF 79 E5 B7 78 76 22 57 DD 44 E0

输出 Blob：

00 C5 00 00 00 2E 00 00 00 00 05 00 00 05 D8 14 09 F9 4B B2 FF BB 1C 91 78 6A 89 6D C2 A5 3D 8A B9 50 D6 A8 44 7D 1A 1D 98 16 FC 5D 2E C5

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 EF	命令码
HASH IN 2	00 15 00 00 00 11 00 00 00 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 41 04 59 51 23 3B 37 16 1C FE 3A 9D E8 2C B8 6A 2C AA 4D 2C 80 1E 7F EF EA 5B A7 BA 68 BC E6 52 4B 9B E5 10 13 77 61 3E C9 2D 1A 43 E3 E7 55 B9 7D 2B 38 62 E5 1C DE 4F 0D 17 8D 0B AA F6 52 F4 36 E6 00 00 00 90 42 99 89 C0 2D 47 CE 95 D9 1B 99 87 B0 79 09 34 64 5B 8E 51 69 C5 9C D6 49 3A 1B DA 60 B5 04 28 83 F2 7A A8 51 96 99 3B D8 13 31 85 66 01 4B 09 B9 20 CD 83 0E 08 9E 32 13 93 01 C3 46 BB 37 8F BF B0 45 90 0A 57 4C 6E 49 FD A6 3F C7 8B 46 0C B1 F2 43 10 F4 EC D7 D3 76 31 6E 60 23 E7 64 E0 30 8F CC 4D 5B 4D 85 9B 7A A5 3E 93 E9 5E 1D 13 BE 9C AA F3 21 AD 0B 64 14 8C 38 12 5B BF 7B BA D7 E8 9E 74 69 BC 87 11 A1 A7 D1 5A 63 E9 EE 08	被加载密钥
HASH OUT	2D 4C 69 A5 16 B2 F6 83 C3 97 C2 39 EA 32 16 81 F3 F8 79 48 61 63 B7 D1 1B D4 B5 C7 10 30 CB 5D	HMAC IN 1
KEY	05 EE F8 3E FD 7C EB 05 3E 34 3B 17 73 CB 3B 9D 05 6D A5 B1 EE AB DB 62 E1 92 FD 49 4A 50 38 5B	保护操作密钥 AP 会话的共享秘密数据
HMAC IN 1	2D 4C 69 A5 16 B2 F6 83 C3 97 C2 39 EA 32 16 81 F3 F8 79 48 61 63 B7 D1 1B D4 B5 C7 10 30 CB 5D	HASH OUT
HMAC IN 2	E7 80 24 E8	AP 会话的序列号
HMAC OUT	63 FB 14 BA 8F A5 1A B9 AA 7B E9 63 F6 0B 10 7C C7 C5 74 BF 76 7F 0C 76 35 94 4B 3F C1 A5 76 81	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码与命令码做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用保护操作密钥创建的 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c） 授权数据

创建保护操作密钥 AP 会话时，需要保护操作密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

6.39 TCM_GetPubKey

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 已经载入了一个密钥，即 TCM_LoadKey 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 32	
3	4	命令码	00 00 80 21	TCM_ORD_GetPubKey
4	4	密钥句柄	05 00 00 03	keyA
5	4	密钥授权会话句柄	00 00 00 32	
6	32	密钥授权数据验证码	D6 C8 D8 F9 DD 81 62 A4 8F EE 3F 7F 82 98 F5 CF 8A 17 6F 39 60 9E DD BB 10 9F DB DC 5E 93 64 20	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 7F	
3	4	返回码	00 00 00 00	
4	可变	密钥公钥部分	00 00 00 0B 00 06 00 01 00 00 00 04 00 00 00 00 00 00 00 41 04 35 DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72	
5	32	密钥授权数据验证码	07 AE 55 3B DA DD 75 C3 41 DA A4 50 46 B4 55 7C 0F 77 7D 87 6F 4F 54 D3 44 73 B5 06 B8 F0 9C E4	
		命令码	00 00 80 21	TCM_ORD_GetPubKey

输入 Blob：

00 C2 00 00 00 32 00 00 80 21 05 00 00 03 00 00 00 32 D6 C8 D8 F9 DD 81 62 A4 8F EE 3F 7F 82 98 F5 CF 8A 17 6F 39 60 9E DD BB 10 9F DB DC 5E 93 64 20

输出 Blob：

00 C5 00 00 00 7F 00 00 00 00 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 00 00 00 00 00 41 04 35

DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72 07 AE 55 3B DA DD 75 C3 41 DA A4 50 46 B4 55 7C 0F 77 7D 87 6F 4F 54 D3 44 73 B5 06 B8 F0 9C E4

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 21	命令码
HASH OUT	66 B5 90 83 44 00 68 17 AE 21 3C B9 8E 54 36 5B A2 1A D4 5A 86 E7 C2 FD 51 F5 7B 78 30 D7 24 C0	HMAC IN 1
KEY	8B B8 AC A5 39 A6 A1 5B A3 DC AF 3E C9 72 37 54 FA E4 D0 53 87 B5 CC E7 11 A1 84 9F 91 0D F2 43	密钥 AP 会话的共享秘密数据
HMAC IN 1	66 B5 90 83 44 00 68 17 AE 21 3C B9 8E 54 36 5B A2 1A D4 5A 86 E7 C2 FD 51 F5 7B 78 30 D7 24 C0	HASH OUT
HMAC IN 2	B3 E1 78 CA	AP 会话的序列号
HMAC OUT	D6 C8 D8 F9 DD 81 62 A4 8F EE 3F 7F 82 98 F5 CF 8A 17 6F 39 60 9E DD BB 10 9F DB DC 5E 93 64 20	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码、命令码和密钥公钥部分做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用该密钥创建的 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c） 授权数据

创建该密钥 AP 会话时，需要该密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

6.40 TCM_WrapKey

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c） 已经载入了一个密钥，由于本向量采用的是 SMK 作为保护操作密钥，所以不需要 TCM_LoadKey 的执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 01 5F	
3	4	命令码	00 00 80 BD	TCM_ORD_WrapKey
4	4	保护操作密钥句柄	40 00 00 00	SMK

序号	长度	名称	值	说明
5	32	使用授权数据	EA AB A4 C3 E6 A6 ED 82 5E 55 C8 26 07 D6 6B F9 EB 2E 87 19 0B A1 3C 34 17 13 F0 5A 6B 6B 97 54	KEYAUTH
6	32	迁移授权数据	EA AB A4 C3 E6 A6 ED 82 5E 55 C8 26 07 D6 6B F9 EB 2E 87 19 0B A1 3C 34 17 13 F0 5A 6B 6B 97 54	KEYAUTH
7	可变	密钥信息	00 15 00 00 00 14 00 00 00 02 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 41 04 35 DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72 00 00 00 85 01 0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50 0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50 44 9D C2 7B AD 1F 49 5B 69 FF E7 66 C9 38 D9 E9 38 CB CC 61 76 50 C4 32 F9 C7 73 90 3B 96 1E A1 00 00 00 20 4F E0 6B CE 0C A3 A8 AF 92 18 C5 A2 EC 0E B5 1F 6A DD 7B 03 01 D9 F4 13 BC A1 02 85 C1 C6 31 9D	
8	4	保护操作密钥授权会话句柄	00 00 00 34	
9	32	保护操作密钥授权数据验证码	AE B8 40 43 15 53 BB 8F 0C 98 AD E3 D2 DA DE E7 71 AB 59 5E 7B A8 AE 81 3B 37 BD 6F B2 5E 75 8A	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 01 22	
3	4	返回码	00 00 00 00	

序号	长度	名称	值	说明
4	可变	密钥信息	00 15 00 00 00 14 00 00 00 02 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 41 04 35 DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72 00 00 00 90 42 99 89 C0 2D 47 CE 95 D9 1B 99 87 B0 79 09 34 64 5B 8E 51 69 C5 9C D6 49 3A 1B DA 60 B5 04 28 3F F8 CF B6 87 FE C2 0F 0D 39 EF 5F 17 A0 1C 21 28 C4 32 23 C5 D8 CA F0 8C 4E E5 AB 7C 98 4B 16 60 20 DF E9 A5 35 BC 93 BA BA 63 B3 92 DB 96 96 51 D6 48 87 E1 63 64 52 DD EA 79 F8 DF F9 29 CA 2A 78 C3 1E 96 49 37 C5 4F 5E 57 A5 17 B8 A7 CA C3 E7 48 3D 5E ED D7 5A 6B 6F F4 3F 3D 27 F0 3B D7 A5 F1 1F 20 94 8B B4 90 F1 2C 0F 4A AC 89 25	
5	32	保护操作密钥授权数据验证码	B2 2E 23 9B 76 B3 FE 29 76 EC F2 BA 9D C9 D3 E6 5D C9 5D ED 91 1B 38 43 C7 6F C5 18 7E D4 D1 E5	
		命令码	00 00 80 BD	TCM_ORD_WrapKey

输入 Blob：

00 C2 00 00 01 5F 00 00 80 BD 40 00 00 00 EA AB A4 C3 E6 A6 ED 82 5E 55 C8 26 07 D6 6B F9 EB 2E 87 19 0B A1 3C 34 17 13 F0 5A 6B 6B 97 54 EA AB A4 C3 E6 A6 ED 82 5E 55 C8 26 07 D6 6B F9 EB 2E 87 19 0B A1 3C 34 17 13 F0 5A 6B 6B 97 54 00 15 00 00 00 14 00 00 00 02 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 41 04 35 DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72 00 00 00 85 01 0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50 0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50 44 9D C2 7B AD 1F 49 5B 69 FF E7 66 C9 38 D9 E9 38 CB CC 61 76 50 C4 32 F9 C7 73 90 3B 96 1E A1 00 00 00 20 4F E0 6B CE 0C A3 A8 AF 92 18 C5 A2 EC 0E B5 1F 6A DD 7B 03 01 D9 F4 13 BC A1 02 85 C1 C6 31 9D 00 00 00 34 AE B8 40 43 15 53 BB 8F 0C 98 AD E3 D2 DA DE E7 71 AB 59 5E 7B A8 AE 81 3B 37 BD 6F B2 5E 75 8A

输出 Blob：

00 C5 00 00 01 22 00 00 00 00 00 15 00 00 00 14 00 00 00 02 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 41 04 35 DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72 00 00 00 90 42 99 89 C0 2D 47 CE 95 D9 1B 99 87 B0 79 09 34 64 5B 8E 51 69 C5 9C D6 49 3A 1B DA 60 B5 04 28 3F F8 CF B6 87 FE C2 0F 0D 39 EF 5F

17 A0 1C 21 28 C4 32 23 C5 D8 CA F0 8C 4E E5 AB 7C 98 4B 16 60 20 DF E9 A5 35 BC 93 BA BA 63 B3 92 DB 96 96 51 D6 48 87 E1 63 64 52 DD EA 79 F8 DF F9 29 CA 2A 78 C3 1E 96 49 37 C5 4F 5E 57 A5 17 B8 A7 CA C3 E7 48 3D 5E ED D7 5A 6B 6F F4 3F 3D 27 F0 3B D7 A5 F1 1F 20 94 8B B4 90 F1 2C 0F 4A AC 89 25 B2 2E 23 9B 76 B3 FE 29 76 EC F2 BA 9D C9 D3 E6 5D C9 5D ED 91 1B 38 43 C7 6F C5 18 7E D4 D1 E5

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 BD	命令码
HASH IN 2	EA AB A4 C3 E6 A6 ED 82 5E 55 C8 26 07 D6 6B F9 EB 2E 87 19 0B A1 3C 34 17 13 F0 5A 6B 6B 97 54	使用授权数据
HASH IN 3	EA AB A4 C3 E6 A6 ED 82 5E 55 C8 26 07 D6 6B F9 EB 2E 87 19 0B A1 3C 34 17 13 F0 5A 6B 6B 97 54	迁移授权数据
HASH IN 4	00 15 00 00 00 14 00 00 00 02 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 41 04 35 DE E8 1F 15 32 18 F1 A4 96 CD 10 30 FA BF E6 AB 50 D3 E7 B3 C1 DA 3E 35 99 BD FF 27 C3 2F 3D 07 2C D1 E3 72 CD 31 85 55 B3 46 E9 FE E9 4E 5C 1F B8 E1 4F 76 C4 78 1F F9 EA 13 12 26 47 8A 72 00 00 00 85 01 0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50 0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50 44 9D C2 7B AD 1F 49 5B 69 FF E7 66 C9 38 D9 E9 38 CB CC 61 76 50 C4 32 F9 C7 73 90 3B 96 1E A1 00 00 00 20 4F E0 6B CE 0C A3 A8 AF 92 18 C5 A2 EC 0E B5 1F 6A DD 7B 03 01 D9 F4 13 BC A1 02 85 C1 C6 31 9D	密钥信息
HASH OUT	82 93 72 0B 13 E7 3E 6E F4 0B C5 AC 39 69 EA 20 AD 4A 44 D0 F3 87 89 5F 39 C2 4D 95 2E 1A C5 9D	HMAC IN 1
KEY	09 C3 6E 9A A6 B8 8E 84 A6 C3 8D 2A 9E 4E B3 44 06 60 7F BD 41 B7 B6 E3 14 98 6B 9D 5D D9 56 61	保护操作密钥 AP 会话的共享秘密数据
HMAC IN 1	82 93 72 0B 13 E7 3E 6E F4 0B C5 AC 39 69 EA 20 AD 4A 44 D0 F3 87 89 5F 39 C2 4D 95 2E 1A C5 9D	HASH OUT
HMAC IN 2	1B 82 62 F5	AP 会话的序列号
HMAC OUT	AE B8 40 43 15 53 BB 8F 0C 98 AD E3 D2 DA DE E7 71 AB 59 5E 7B A8 AE 81 3B 37 BD 6F B2 5E 75 8A	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码、命令码和密钥信息做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用保护操作密钥创建的 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) 授权数据

创建保护操作密钥 AP 会话时，需要保护操作密钥的使用授权数据。本标准采用 KEYAUTH 常量值。对于新产生的密钥，其使用授权数据和迁移授权数据也都采用了 KEYAUTH 的常量值。

6.41 TCM_CertifyKey

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 已经载入了两个密钥，需要 TCM_LoadKey 的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM _ TAG _ RQU _ AUTH _COMMAND
2	4	数据长度	00 00 00 32	
3	4	命令码	00 00 80 32	TCM_ORD_CertifyKey
4	4	验证密钥句柄	05 00 00 05	
5	4	待验证密钥句柄	05 00 00 06	
6	32	抗重放数据	20 F8 DE 9E 8A 47 62 B8 28 F9 1A 22 4D 12 B3 6D 84 56 0F 5B C2 B7 86 92 04 44 1B 90 7B 50 09 06	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM _ TAG _ RSP _ AUTH _COMMAND
2	4	数据长度	00 00 00 AE	
3	4	返回码	00 00 00 00	
4	可变	验证信息	01 00 00 00 00 10 00 00 00 02 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 16 6A E2 17 2B 8C A9 83 A3 FD 38 FC ED A9 39 58 C2 5E E0 22 B6 D2 E0 3E 3A 98 CD EF B5 FA 8B 59 20 F8 DE 9E 8A 47 62 B8 28 F9 1A 22 4D 12 B3 6D 84 56 0F 5B C2 B7 86 92 04 44 1B 90 7B 50 09 06 00 00 00 00 00	
5	4	验证信息签名的长度	00 00 00 40	
6	可变	验证信息的签名	52 DA C4 85 43 27 4C 63 AF 02 82 34 47 DB 02 F0 C7 26 1E 5C 2C CD B8 B4 8C 55 20 D7 E0 73 24 5B E6 B6 6C 21 5F 50 48 AA 96 AC C6 0D 67 BB BA 4A A0 61 1C FD A9 55 06 4D A8 05 71 9E 7C 5C 54 0B	
		命令码	00 00 80 32	TCM_ORD_CertifyKey

输入 Blob：

00 C1 00 00 00 32 00 00 80 32 05 00 00 05 05 00 00 06 20 F8 DE 9E 8A 47 62 B8 28 F9 1A 22 4D

12 B3 6D 84 56 0F 5B C2 B7 86 92 04 44 1B 90 7B 50 09 06

输出 Blob：

00 C4 00 00 00 AE 00 00 00 00 01 00 00 00 00 10 00 00 00 02 00 00 00 00 0B 00 04 00 05 00 00 00 04 00 00 01 00 16 6A E2 17 2B 8C A9 83 A3 FD 38 FC ED A9 39 58 C2 5E E0 22 B6 D2 E0 3E 3A 98 CD EF B5 FA 8B 59 20 F8 DE 9E 8A 47 62 B8 28 F9 1A 22 4D 12 B3 6D 84 56 0F 5B C2 B7 86 92 04 44 1B 90 7B 50 09 06 00 00 00 00 00 00 00 00 40 52 DA C4 85 43 27 4C 63 AF 02 82 34 47 DB 02 F0 C7 26 1E 5C 2C CD B8 B4 8C 55 20 D7 E0 73 24 5B E6 B6 6C 21 5F 50 48 AA 96 AC C6 0D 67 BB BA 4A A0 61 1C FD A9 55 06 4D A8 05 71 9E 7C 5C 54 0B

6.42 TCM_AuthorizeMigrationKey

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 85	
3	4	命令码	00 00 80 C3	TCM _ ORD _ AuthorizeMigrationKey
4	2	迁移模式	00 01	TCM_MS_MIGRATE
5	可变	迁移密钥公钥	00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 D1 95 F4 50 E3 33 57 C4 27 8F DA 92 31 25 F0 C1 BE 32 8D AD	
6	4	Owner 授权句柄	F0 62 B9 C9	
7	32	Owner 授权会话校验码	BD FA 31 59 9E 38 6E 06 91 05 04 F8 39 DC 6B 01 3E DB AC 84 4D E2 47 4D F0 82 7E 85 78 C4 B0 E0	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 A1	
3	4	返回码	00 00 00 00	

序号	长度	名称	值	说明
4	可变	迁移认证数据	00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 D1 95 F4 50 E3 33 57 C4 27 8F DA 92 31 25 F0 C1 BE 32 8D AD F0 62 B9 C9 BD FA 31 59 9E 38 6E 06 91 05 04 F8 39 DC 6B 01 3E DB AC 84 4D E2 47 4D F0 82 7E 85 78 C4 B0 E0 B5 F8 09 22 C4 F2 64 08 00 01 35 02 05 9C 9E C9 44 D5 A5 9E 5F 85 7E AB 77 04 E0 50 0A C2 7D 47 DD 10 3A 4E 0C 21 CE 38 E0 3C	
5	32	Owner 授权会话校验码	13 69 AC AC CB B4 73 C6 61 FE 99 DF 58 71 53 9C D0 35 10 08 2A F9 84 A2 C5 30 8A 6B FB DF 9F 52	
		命令码	00 00 80 C3	TCM _ ORD _ AuthorizeMigrationKey

输入 Blob：

00 C2 00 00 00 85 00 00 80 C3 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 D1 95 F4 50 E3 33 57 C4 27 8F DA 92 31 25 F0 C1 BE 32 8D AD F0 62 B9 C9 BD FA 31 59 9E 38 6E 06 91 05 04 F8 39 DC 6B 01 3E DB AC 84 4D E2 47 4D F0 82 7E 85 78 C4 B0 E0 B5 F8 09 22 C4 F2 64 08 00 00 00 7D 7F A7 03 D9 04 60 34 F7 4A 8F 79 79 E1 BB 1C 88 A3 77 73 D2 75 9B 56 EA F3 1D 9F F0 C2 03 0F EC

输出 Blob：

00 C5 00 00 00 A1 00 00 00 00 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 D1 95 F4 50 E3 33 57 C4 27 8F DA 92 31 25 F0 C1 BE 32 8D AD F0 62 B9 C9 BD FA 31 59 9E 38 6E 06 91 05 04 F8 39 DC 6B 01 3E DB AC 84 4D E2 47 4D F0 82 7E 85 78 C4 B0 E0 B5 F8 09 22 C4 F2 64 08 00 01 35 02 05 9C 9E C9 44 D5 A5 9E 5F 85 7E AB 77 04 E0 50 0A C2 7D 47 DD 10 3A 4E 0C 21 CE 38 E0 3C 13 69 AC AC CB B4 73 C6 61 FE 99 DF 58 71 53 9C D0 35 10 08 2A F9 84 A2 C5 30 8A 6B FB DF 9F 52

6.43 TCM_CreateMigratedBlob

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) TCM_AuthorizeMigrationKey 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C3	TCM _ TAG _ RQU _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 B9	
3	4	命令码	00 00 80 C1	TCM_ORD_CreateMigratedBlob

序号	长度	名称	值	说明
4	4	待迁移密钥父密钥句柄	05 00 00 03	
5	2	迁移模式	00 01	TCM_MS_MIGRATE
6	可变	迁移密钥认证数据	00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 D1 95 F4 50 E3 33 57 C4 27 8F DA 92 31 25 F0 C1 BE 32 8D AD F0 62 B9 C9 BD FA 31 59 9E 38 6E 06 91 05 04 F8 39 DC 6B 01 3E DB AC 84 4D E2 47 4D F0 82 7E 85 78 C4 B0 E0 B5 F8 09 22 C4 F2 64 08 00 01 35 02 05 9C 9E C9 44 D5 A5 9E 5F 85 7E AB 77 04 E0 50 0A C2 7D 47 DD 10 3A 4E 0C 21 CE 38 E0 3C	
7	4	待迁移的密钥数据长度	00 00 00 E6	
8	可变	待迁移的密钥数据	04 29 0B BD F2 D8 53 57 B3 2B 81 93 AF FC 20 A8 C5 BC E8 D0 90 01 2F 22 79 54 12 E5 73 A2 68 97 43 62 11 D2 5F FC 5A A6 D3 93 10 3E B1 FE 84 46 93 CE 05 05 A0 C5 6B A0 AE 89 82 A1 93 DD 4C 92 AD 83 68 5E B6 69 9A 43 43 11 26 C2 F6 DA 78 56 F4 27 5D 84 EF 88 7C 3D 26 00 4A F0 10 62 76 DC 9E F2 01 F8 79 B7 8C 92 E7 52 7C D7 80 48 BE 37 FA CB 04 C9 60 8E 7C 24 09 90 7F 57 F6 68 BD C0 60 72 58 5F 69 93 32 BB CA 15 E8 AF 38 5B 76 8C 63 9E E7 47 B6 36 D1 0E 06 D6 DB 84 71 03 21 EC 45 DA 83 FD 3B CE 46 A8 71 6B 97 95 4F 18 E7 0E 06 C5 29 A6 32 41 05 6A A7 62 B2 48 E9 8B 4E 41 E5 30 88 DF 12 6F 04 53 41 54 18 66 8F C4 69 E2 FA 15 B7 7C 8F F3 26 64 B8 3B 41 B4 33 37 C8 1C 28 8F 4F 3D 44 19	
9	4	待迁移密钥父密钥授权会话句柄	00 00 00 7E	
10	32	待迁移密钥父密钥授权会话校验码	FF 8A 02 01 C5 DF F1 50 71 D2 CF E8 C8 DF 0D 0A B0 5F F9 D3 31 89 95 D6 18 D2 03 38 AA 51 DE D9	
11	4	待迁移密钥迁移授权会话句柄	00 00 00 7F	
12	32	待迁移密钥迁移授权会话验证码	4C 97 91 E8 06 6B 34 48 C9 A3 D0 24 0E A5 2F E7 D9 30 23 46 0F B7 6D C6 AD FC E6 34 62 11 61 BF	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C6	TCM _ TAG _ RSP _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 D5	
3	4	返回码	00 00 00 00	
4	4	用对称密钥加密的待迁移密钥大小	00 00 00 F3	
5	可变	用对称密钥加密的待迁移密钥	04 AD A5 8F 4C 04 C6 4A 90 52 CE BC 9A 57 BD 1C FA E5 AE 14 EE 12 CC 63 A4 CA C5 E6 E0 4E 69 02 9A 64 FF 06 35 AA 63 EC 9F B7 A8 78 EE FC 00 49 CA 7A DE A5 38 EA 5C DA A1 62 68 30 1D 5B 53 97 A9 6E 29 AD 34 8D 08 AD F1 B4 3D ED B6 BE DA F2 EE 2B 9C 9B 70 6F 4C 44 6F 16 44 7B 4B EE 11 DF 94 7B 07 98 5D D8 32 5A 65 E2 16 2C 8F 43 12 6C 75 29 2A 79 C3 89 52 68 D7 9A 0F FE 69 25 F5 E6 9C 27 EC B2 95 8E 39 75 A2 44 74 FD 02 E9 6F CE 61 CF 70 48 49 0D 7D A3 DE 70 B8 01 F2 5F 0B 0D F8 10 95 DF 47 F7 24 1F 70 24 AE 12 E3 E4 53 B3 21 A2 EF 98 EC D0 11 2D B2 3F 83 8D D9 3E A1 AE A3 82 1F BC EA 1F 17 ED 87 11 A2 5B E8 27 2F F4 7D FC 12 86 D6 02 6E 65 15 E6 CB 38 7A 1D 52 BC 2A 96 D5 37 0D D4 20 7C 7D F9 69 45 3F 25 73 29 58 0C C4	
6	4	用迁移公钥加密的数据大小	00 00 00 90	
7	可变	用迁移公钥加密的数据	4E D6 57 6C 08 EF 2A 9C 54 8F 0F 90 4D 52 3E CA 59 D3 5E C1 7F 9D DA E0 C3 E2 42 3B 90 BD 9D 19 58 C9 73 1F 97 40 4D E2 6C 9B E2 48 FA B6 58 39 FE 49 4C 04 C3 06 08 27 23 2E 66 2D 6A B9 7D 0C 13 00 B6 D9 66 C8 5A 72 B9 CB FA 3E F7 11 BA 79 46 D9 3E 14 26 AF 72 D6 31 2B EA D5 DA 47 CF 65 4D 09 F1 69 95 13 E0 87 34 22 B7 C9 3D 7D 56 3D BA 8D 04 20 67 A7 B9 98 0C 6A 37 E1 86 58 10 CD AA 28 34 87 EF 7C 98 41 9B 8F 66 53 99 7A 81 31	
8	32	待迁移密钥父密钥授权会话验证码	4E E3 61 AA A1 10 6C 3D 79 BE AB CE E1 0A A7 BD 1F 8C 54 89 56 CF 9C 92 0C EB 3F 37 91 8D 3A 9B	

序号	长度	名称	值	说明
9	32	待迁移密钥迁移授权会话验证码	16 45 E4 29 9B CE 84 BE 2A C4 B5 12 65 B9 2C 3C DA E2 49 76 46 BA 05 87 B0 2C 2C 72 F2 6F 0B 13	
		命令码	00 00 80 C1	TCM_ORD_CreateMigratedBlob

输入 Blob：

00 C3 00 00 01 B9 00 00 80 C1 05 00 00 03 00 01 00 00 00 0B 00 06 00 01 00 00 00 04 00 00 01 00 00 00 00 41 04 D1 95 F4 50 E3 33 57 C4 27 8F DA 92 31 25 F0 C1 BE 32 8D AD F0 62 B9 C9 BD FA 31 59 9E 38 6E 06 91 05 04 F8 39 DC 6B 01 3E DB AC 84 4D E2 47 4D F0 82 7E 85 78 C4 B0 E0 B5 F8 09 22 C4 F2 64 08 00 01 35 02 05 9C 9E C9 44 D5 A5 9E 5F 85 7E AB 77 04 E0 50 0A C2 7D 47 DD 10 3A 4E 0C 21 CE 38 E0 3C 00 00 00 E6 04 29 0B BD F2 D8 53 57 B3 2B 81 93 AF FC 20 A8 C5 BC E8 D0 90 01 2F 22 79 54 12 E5 73 A2 68 97 43 62 11 D2 5F FC 5A A6 D3 93 10 3E B1 FE 84 46 93 CE 05 05 A0 C5 6B A0 AE 89 82 A1 93 DD 4C 92 AD 83 68 5E B6 69 9A 43 43 11 26 C2 F6 DA 78 56 F4 27 5D 84 EF 88 7C 3D 26 00 4A F0 10 62 76 DC 9E F2 01 F8 79 B7 8C 92 E7 52 7C D7 80 48 BE 37 FA CB 04 C9 60 8E 7C 24 09 90 7F 57 F6 68 BD C0 60 72 58 5F 69 93 32 BB CA 15 E8 AF 38 5B 76 8C 63 9E E7 47 B6 36 D1 0E 06 D6 DB 84 71 03 21 EC 45 DA 83 FD 3B CE 46 A8 71 6B 97 95 4F 18 E7 0E 06 C5 29 A6 32 41 05 6A A7 62 B2 48 E9 8B 4E 41 E5 30 88 DF 12 6F 04 53 41 54 18 66 8F C4 69 E2 FA 15 B7 7C 8F F3 26 64 B8 3B 41 B4 33 37 C8 1C 28 8F 4F 3D 44 19 00 00 00 7E FF 8A 02 01 C5 DF F1 50 71 D2 CF E8 C8 DF 0D 0A B0 5F F9 D3 31 89 95 D6 18 D2 03 38 AA 51 DE D9 00 00 00 7F 4C 97 91 E8 06 6B 34 48 C9 A3 D0 24 0E A5 2F E7 D9 30 23 46 0F B7 6D C6 AD FC E6 34 62 11 61 BF

输出 Blob：

00 C6 00 00 01 D5 00 00 00 00 00 00 00 F3 04 AD A5 8F 4C 04 C6 4A 90 52 CE BC 9A 57 BD 1C FA E5 AE 14 EE 12 CC 63 A4 CA C5 E6 E0 4E 69 02 9A 64 FF 06 35 AA 63 EC 9F B7 A8 78 EE FC 00 49 CA 7A DE A5 38 EA 5C DA A1 62 68 30 1D 5B 53 97 A9 6E 29 AD 34 8D 08 AD F1 B4 3D ED B6 BE DA F2 EE 2B 9C 9B 70 6F 4C 44 6F 16 44 7B 4B EE 11 DF 94 7B 07 98 5D D8 32 5A 65 E2 16 2C 8F 43 12 6C 75 29 2A 79 C3 89 52 68 D7 9A 0F FE 69 25 F5 E6 9C 27 EC B2 95 8E 39 75 A2 44 74 FD 02 E9 6F CE 61 CF 70 48 49 0D 7D A3 DE 70 B8 01 F2 5F 0B 0D F8 10 95 DF 47 F7 24 1F 70 24 AE 12 E3 E4 53 B3 21 A2 EF 98 EC D0 11 2D B2 3F 83 8D D9 3E A1 AE A3 82 1F BC EA 1F 17 ED 87 11 A2 5B E8 27 2F F4 7D FC 12 86 D6 02 6E 65 15 E6 CB 38 7A 1D 52 BC 2A 96 D5 37 0D D4 20 7C 7D F9 69 45 3F 25 73 29 58 0C C4 00 00 00 90 4E D6 57 6C 08 EF 2A 9C 54 8F 0F 90 4D 52 3E CA 59 D3 5E C1 7F 9D DA E0 C3 E2 42 3B 90 BD 9D 19 58 C9 73 1F 97 40 4D E2 6C 9B E2 48 FA B6 58 39 FE 49 4C 04 C3 06 08 27 23 2E 66 2D 6A B9 7D 0C 13 00 B6 D9 66 C8 5A 72 B9 CB FA 3E F7 11 BA 79 46 D9 3E 14 26 AF 72 D6 31 2B EA D5 DA 47 CF 65 4D 09 F1 69 95 13 E0 87 34 22 B7 C9 3D 7D 56 3D BA 8D 04 20 67 A7 B9 98 0C 6A 37 E1 86 58 10 CD AA 28 34 87 EF 7C 98 41 9B 8F 66 53 99 7A 81 31 4E E3 61 AA A1 10 6C 3D 79 BE AB CE E1 0A A7 BD 1F 8C 54 89 56 CF 9C 92 0C EB 3F 37 91 8D 3A 9B 16 45 E4 29 9B CE 84 BE 2A C4 B5 12 65 B9 2C 3C DA E2 49 76 46 BA 05 87 B0 2C 2C 72 F2 6F 0B 13

6.44 TCM_ConvertMigratedBlob

依赖于：

a) TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c） TCM_AuthorizeMigrationKey 命令的成功执行。

d） TCM_CreateMigratedBlob 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C3	TCM _ TAG _ RQU _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 E5	
3	4	命令码	00 00 80 C2	TCM_ORD_ConvertMigrationBlob
4	4	迁移密钥句柄	05 00 00 03	
5	4	迁移目标父密钥句柄	05 00 00 04	
6	4	用对称密钥加密的待迁移密钥大小	00 00 00 F3	
7	可变	用对称密钥加密的待迁移密钥	04 AD A5 8F 4C 04 C6 4A 90 52 CE BC 9A 57 BD 1C FA E5 AE 14 EE 12 CC 63 A4 CA C5 E6 E0 4E 69 02 9A 64 FF 06 35 AA 63 EC 9F B7 A8 78 EE FC 00 49 CA 7A DE A5 38 EA 5C DA A1 62 68 30 1D 5B 53 97 A9 6E 29 AD 34 8D 08 AD F1 B4 3D ED B6 BE DA F2 EE 2B 9C 9B 70 6F 4C 44 6F 16 44 7B 4B EE 11 DF 94 7B 07 98 5D D8 32 5A 65 E2 16 2C 8F 43 12 6C 75 29 2A 79 C3 89 52 68 D7 9A 0F FE 69 25 F5 E6 9C 27 EC B2 95 8E 39 75 A2 44 74 FD 02 E9 6F CE 61 CF 70 48 49 0D 7D A3 DE 70 B8 01 F2 5F 0B 0D F8 10 95 DF 47 F7 24 1F 70 24 AE 12 E3 E4 53 B3 21 A2 EF 98 EC D0 11 2D B2 3F 83 8D D9 3E A1 AE A3 82 1F BC EA 1F 17 ED 87 11 A2 5B E8 27 2F F4 7D FC 12 86 D6 02 6E 65 15 E6 CB 38 7A 1D 52 BC 2A 96 D5 37 0D D4 20 7C 7D F9 69 45 3F 25 73 29 58 0C C4	
8	4	用迁移公钥加密的数据大小	00 00 00 90	
9	可变	用迁移公钥加密的数据	4E D6 57 6C 08 EF 2A 9C 54 8F 0F 90 4D 52 3E CA 59 D3 5E C1 7F 9D DA E0 C3 E2 42 3B 90 BD 9D 19 58 C9 73 1F 97 40 4D E2 6C 9B E2 48 FA B6 58 39 FE 49 4C 04 C3 06 08 27 23 2E 66 2D 6A B9 7D 0C 13 00 B6 D9 66 C8 5A 72 B9 CB FA 3E F7 11 BA 79 46 D9 3E 14 26 AF 72 D6 31 2B EA D5 DA 47 CF 65 4D 09 F1 69 95 13 E0 87 34 22 B7 C9 3D 7D 56 3D BA 8D 04 20 67 A7 B9 98 0C 6A 37 E1 86 58 10 CD AA 28 34 87 EF 7C 98 41 9B 8F 66 53 99 7A 81 31	

序号	长度	名称	值	说明
10	4	迁移密钥授权会话句柄	00 00 00 80	
11	32	迁移密钥授权会话校验码	64 88 8E 75 15 94 6E 26 66 96 7D A6 1B 77 3C 7B A7 0A 96 C8 90 FB FE B1 6A 1B E6 B3 3F FA 8A B4	
12	4	迁移目标父密钥授权会话句柄	00 00 00 81	
13	32	迁移目标父密钥授权会话验证码	2D BE 12 FF EF 3C 62 C7 D7 93 51 66 B3 71 43 99 17 11 C2 6B F7 B2 50 A5 2C 8F 68 D5 64 47 A7 A2	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C6	TCM _ TAG _ RSP _ AUTH2 _COMMAND
2	4	数据长度	00 00 01 34	
3	4	返回码	00 00 00 00	
4	4	加密的私钥或对称密钥大小	00 00 00 E6	
5	可变	加密的私钥或对称密钥	04 2D 3C 23 9D E6 86 0E B1 49 3F B4 05 27 7D 28 5B 6A A6 87 9F 21 79 B4 DE 64 08 D2 4A 1E A0 D9 50 6A 93 B1 A6 7F 07 B4 E0 12 05 E2 E5 9C 12 A0 DC 22 B2 A8 02 E0 E6 05 FC 9D DF 95 2A 5B 7E D9 AB 22 BE 0C 3F F1 02 73 08 26 B7 41 AD 87 70 B7 2B 69 6C FD 4D F9 32 D0 55 B6 BD E2 DE 4E 55 50 AC 3A 4B E6 37 3F D2 5D 7C F4 8D 1A 8F 9D 79 60 D7 9F 96 01 23 D4 DB BE A0 5C 98 11 22 24 23 06 EF 98 C3 67 7E 7C C2 D9 84 33 F5 30 A2 74 04 45 1F E5 C3 5F A1 70 F4 E7 D5 08 D1 BB A5 02 49 7F 69 D1 EF E6 95 02 8F 7C 25 BF F1 E6 D1 0E 7F C4 18 B8 BC 01 42 9A 10 3F 65 B3 0A 4C D0 EE E0 F6 71 3C 15 22 22 39 F4 AE 3A 56 4A A7 FB EF E0 92 25 51 E0 A2 3B EE E3 15 AE EF 0D 3C 0C A1 40 7C E9 09 2D 0D 91 EE	
6	32	迁移密钥授权会话验证码	9D 1D 1E CA AB 9D 74 8F A6 57 CB 2A 1C 8B E2 6A E6 FD F3 FD 85 91 43 41 D9 C4 12 4B 33 DE 31 09	

序号	长度	名称	值	说明
7	32	迁移目标父密钥授权会话验证码	DB 10 54 BC B3 4B 06 4E AC 4A FA 0A 95 F6 77 37 1C A4 CA 79 95 EE 38 D8 58 22 CC 50 66 2A 77 B2	
		命令码	00 00 80 C2	TCM_ORD_ConvertMigration-Blob

输入 Blob：

00 C3 00 00 01 E5 00 00 80 C2 05 00 00 03 05 00 00 04 00 00 00 F3 04 AD A5 8F 4C 04 C6 4A 90 52 CE BC 9A 57 BD 1C FA E5 AE 14 EE 12 CC 63 A4 CA C5 E6 E0 4E 69 02 9A 64 FF 06 35 AA 63 EC 9F B7 A8 78 EE FC 00 49 CA 7A DE A5 38 EA 5C DA A1 62 68 30 1D 5B 53 97 A9 6E 29 AD 34 8D 08 AD F1 B4 3D ED B6 BE DA F2 EE 2B 9C 9B 70 6F 4C 44 6F 16 44 7B 4B EE 11 DF 94 7B 07 98 5D D8 32 5A 65 E2 16 2C 8F 43 12 6C 75 29 2A 79 C3 89 52 68 D7 9A 0F FE 69 25 F5 E6 9C 27 EC B2 95 8E 39 75 A2 44 74 FD 02 E9 6F CE 61 CF 70 48 49 0D 7D A3 DE 70 B8 01 F2 5F 0B 0D F8 10 95 DF 47 F7 24 1F 70 24 AE 12 E3 E4 53 B3 21 A2 EF 98 EC D0 11 2D B2 3F 83 8D D9 3E A1 AE A3 82 1F BC EA 1F 17 ED 87 11 A2 5B E8 27 2F F4 7D FC 12 86 D6 02 6E 65 15 E6 CB 38 7A 1D 52 BC 2A 96 D5 37 0D D4 20 7C 7D F9 69 45 3F 25 73 29 58 0C C4 00 00 00 90 4E D6 57 6C 08 EF 2A 9C 54 8F 0F 90 4D 52 3E CA 59 D3 5E C1 7F 9D DA E0 C3 E2 42 3B 90 BD 9D 19 58 C9 73 1F 97 40 4D E2 6C 9B E2 48 FA B6 58 39 FE 49 4C 04 C3 06 08 27 23 2E 66 2D 6A B9 7D 0C 13 00 B6 D9 66 C8 5A 72 B9 CB FA 3E F7 11 BA 79 46 D9 3E 14 26 AF 72 D6 31 2B EA D5 DA 47 CF 65 4D 09 F1 69 95 13 E0 87 34 22 B7 C9 3D 7D 56 3D BA 8D 04 20 67 A7 B9 98 0C 6A 37 E1 86 58 10 CD AA 28 34 87 EF 7C 98 41 9B 8F 66 53 99 7A 81 31 00 00 00 80 64 88 8E 75 15 94 6E 26 66 96 7D A6 1B 77 3C 7B A7 0A 96 C8 90 FB FE B1 6A 1B E6 B3 3F FA 8A B4 00 00 00 81 2D BE 12 FF EF 3C 62 C7 D7 93 51 66 B3 71 43 99 17 11 C2 6B F7 B2 50 A5 2C 8F 68 D5 64 47 A7 A2

输出 Blob：

00 C6 00 00 01 34 00 00 00 00 00 00 00 E6 04 2D 3C 23 9D E6 86 0E B1 49 3F B4 05 27 7D 28 5B 6A A6 87 9F 21 79 B4 DE 64 08 D2 4A 1E A0 D9 50 6A 93 B1 A6 7F 07 B4 E0 12 05 E2 E5 9C 12 A0 DC 22 B2 A8 02 E0 E6 05 FC 9D DF 95 2A 5B 7E D9 AB 22 BE 0C 3F F1 02 73 08 26 B7 41 AD 87 70 B7 2B 69 6C FD 4D F9 32 D0 55 B6 BD E2 DE 4E 55 50 AC 3A 4B E6 37 3F D2 5D 7C F4 8D 1A 8F 9D 79 60 D7 9F 96 01 23 D4 DB BE A0 5C 98 11 22 24 23 06 EF 98 C3 67 7E 7C C2 D9 84 33 F5 30 A2 74 04 45 1F E5 C3 5F A1 70 F4 E7 D5 08 D1 BB A5 02 49 7F 69 D1 EF E6 95 02 8F 7C 25 BF F1 E6 D1 0E 7F C4 18 B8 BC 01 42 9A 10 3F 65 B3 0A 4C D0 EE E0 F6 71 3C 15 22 22 39 F4 AE 3A 56 4A A7 FB EF E0 92 25 51 E0 A2 3B EE E3 15 AE EF 0D 3C 0C A1 40 7C E9 09 2D 0D 91 EE 9D 1D 1E CA AB 9D 74 8F A6 57 CB 2A 1C 8B E2 6A E6 FD F3 FD 85 91 43 41 D9 C4 12 4B 33 DE 31 09 DB 10 54 BC B3 4B 06 4E AC 4A FA 0A 95 F6 77 37 1C A4 CA 79 95 EE 38 D8 58 22 CC 50 66 2A 77 B2

6.45 TCM_SCHStart

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 EA	TCM_ORD_SCHStart

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0E	
3	4	返回码	00 00 00 00	
4	4	可以发给 TCM_SCHUpdate 的最大比特数	00 00 02 00	
		命令码	00 00 80 EA	TCM_ORD_SCHStart

输入 Blob：

00 C1 00 00 00 0A 00 00 80 EA

输出 Blob：

00 C4 00 00 00 0E 00 00 00 00 00 00 02 00

6.46 TCM_SCHUpdate

依赖于：

a） TCM_Startup 命令的成功执行。

b） TCM_SCHStart 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 2F	
3	4	命令码	00 00 80 EB	TCM_ORD_SCHUpdate
4	4	数据块大小	00 00 00 21	
5	可变	数据块	61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6A 68 69 6A 6B 69	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 EB	TCM_ORD_SCHUpdate

输入 Blob：

00 C1 00 00 00 2F 00 00 80 EB 00 00 00 21 61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6A 68 69 6A 6B 69

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

说明：

做 SCH 运算的数据选自[FIPS-180-1]的附录 B 中 hash 运算的例子。

6.47 TCM_SCHComplete

依赖于：

a) TCM_Startup 命令的成功执行。

b) TCM_SCHStart 命令的成功执行。

c) TCM_SCHUpdate 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 25	
3	4	命令码	00 00 80 EC	TCM_ORD_SCHComplete
4	4	数据块大小	00 00 00 17	
5	可变	数据块	6A 6B 6C 6A 6B 6C 6D 6B 6C 6D 6E 6C 6D 6E 6F 6D 6E 6F 70 6E 6F 70 71	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	Hash 结果	63 9B 6C C5 E6 4D 9E 37 A3 90 B1 92 DF 4F A1 EA 07 20 AB 74 7F F6 92 B9 F3 8C 4E 66 AD 7B 8C 05	
		命令码	00 00 80 EC	TCM_ORD_SCHComplete

输入 Blob：

00 C1 00 00 00 25 00 00 80 EC 00 00 00 17 6A 6B 6C 6A 6B 6C 6D 6B 6C 6D 6E 6C 6D 6E 6F 6D 6E 6F 70 6E 6F 70 71

输出 Blob：

00 C4 00 00 00 2A 00 00 00 00 63 9B 6C C5 E6 4D 9E 37 A3 90 B1 92 DF 4F A1 EA 07 20 AB 74 7F F6 92 B9 F3 8C 4E 66 AD 7B 8C 05

说明：

做 SCH 运算的数据选自[FIPS-180-1]的附录 B 中 hash 运算的例子。

6.48 TCM_SCHCompleteExtend

依赖于：

TCM_Startup 命令的成功执行。

TCM_SCHStart 命令的成功执行。

TCM_SCHUpdate 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 29	
3	4	命令码	00 00 80 ED	TCM _ ORD _ SCHCompleteExtend
4	4	指定的 PCR	00 00 00 0C	
5	4	数据块大小	00 00 00 17	
6	可变	数据块	6A 6B 6C 6A 6B 6C 6D 6B 6C 6D 6E 6C 6D 6E 6F 6D 6E 6F 70 6E 6F 70 71	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 4A	
3	4	返回码	00 00 00 00	
4	32	Hash 结果	63 9B 6C C5 E6 4D 9E 37 A3 90 B1 92 DF 4F A1 EA 07 20 AB 74 7F F6 92 B9 F3 8C 4E 66 AD 7B 8C 05	
5	32	PCR 结果	9C E8 92 FF E9 C2 E7 F0 00 9A 5E E4 05 65 B5 91 54 29 BD B9 D1 7B 0A 00 36 19 48 26 C5 8C 8E E1	
		命令码	00 00 80 ED	TCM _ ORD _ SCHCompleteExtend

输入 Blob：

00 C1 00 00 00 29 00 00 80 ED 00 00 00 0C 00 00 00 17 6A 6B 6C 6A 6B 6C 6D 6B 6C 6D 6E 6C 6D 6E 6F 6D 6E 6F 70 6E 6F 70 71

输出 Blob：

00 C4 00 00 00 4A 00 00 00 00 63 9B 6C C5 E6 4D 9E 37 A3 90 B1 92 DF 4F A1 EA 07 20 AB 74 7F F6 92 B9 F3 8C 4E 66 AD 7B 8C 05 9C E8 92 FF E9 C2 E7 F0 00 9A 5E E4 05 65 B5 91 54 29 BD B9 D1 7B 0A 00 36 19 48 26 C5 8C 8E E1

说明：

做 SCH 运算的数据选自[FIPS-180-1]的附录 B 中 hash 运算的例子。

6.49 TCM_Sign

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c） 存在已加载的签名密钥，即 TCM_LoadKey 的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 56	
3	4	命令码	00 00 80 3C	TCM_ORD_Sign
4	4	签名密钥句柄	05 00 00 06	KeyB
5	4	待签名摘要数据长度	00 00 00 20	
6	32	待签名摘要数据	90 90 90 90 90 90 90 90 90 87 78 89 89 78 76 78 90 90 90 90 90 90 90 90 90 87 78 89 89 78 76 78	
7	4	签名密钥授权会话句柄	00 00 00 4E	
8	32	签名密钥授权数据验证码	F7 D8 A2 78 B8 A0 56 65 CB 68 22 4F B7 0C DC 7F 53 C1 61 5B 58 8D 00 F5 03 4B 0A C5 0F 56 E2 A9	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 6E	
3	4	返回码	00 00 00 00	
4	4	签名数据长度	00 00 00 40	
5	可变	签名数据	AD B5 72 F0 C1 2B E7 00 59 D6 C4 F6 E7 2F F7 EF 97 81 A4 9D 00 B9 99 09 8B 25 80 AA E9 C6 68 BF A1 43 80 92 BF 3F 99 33 89 1C D3 70 73 C4 10 2D 92 F5 5F BB 4F B5 C6 80 FC 8B 36 14 05 BE 70 27	
6	32	签名密钥授权数据验证码	0A 46 39 F0 24 8F FB 64 8F EC 5A 5D 6C 0B 84 41 88 F5 42 13 33 3A BF DF A0 F2 DC 27 BE C1 F3 D6	
		命令码	00 00 80 3C	TCM_ORD_Sign

输入 Blob：

00 C2 00 00 00 56 00 00 80 3C 05 00 00 06 00 00 00 20 90 90 90 90 90 90 90 90 90 87 78 89 89 78 76 78 90 90 90 90 90 90 90 90 90 87 78 89 89 78 76 78 00 00 00 4E F7 D8 A2 78 B8 A0 56 65 CB 68 22 4F B7 0C DC 7F 53 C1 61 5B 58 8D 00 F5 03 4B 0A C5 0F 56 E2 A9

输出 Blob：

00 C5 00 00 00 6E 00 00 00 00 00 00 00 40 AD B5 72 F0 C1 2B E7 00 59 D6 C4 F6 E7 2F F7 EF 97 81 A4 9D 00 B9 99 09 8B 25 80 AA E9 C6 68 BF A1 43 80 92 BF 3F 99 33 89 1C D3 70 73 C4 10 2D 92 F5 5F BB 4F B5 C6 80 FC 8B 36 14 05 BE 70 27 0A 46 39 F0 24 8F FB 64 8F EC 5A 5D 6C 0B 84 41 88 F5 42 13 33 3A BF DF A0 F2 DC 27 BE C1 F3 D6

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 3C	命令码
HASH IN 2	00 00 00 20	待签名摘要数据长度
HASH IN 3	90 90 90 90 90 90 90 90 87 78 89 89 78 76 78 90 90 90 90 90 90 90 90 90 87 78 89 89 78 76 78	待签名摘要数据
HASH OUT	BB 4C 64 EE 1C 92 D0 D8 EB 92 5F AF 42 3F F3 78 80 6C 07 F2 92 4E FC 0E A4 AB C1 7D FF 39 1A 1D	HMAC IN 1
KEY	D4 B2 83 2A 52 E2 4E A2 C2 63 A2 04 B7 95 4F 95 04 F6 36 EE C6 41 2A 06 F0 FB 86 07 97 35 0E 07	签名密钥 AP 会话的共享秘密数据
HMAC IN 1	BB 4C 64 EE 1C 92 D0 D8 EB 92 5F AF 42 3F F3 78 80 6C 07 F2 92 4E FC 0E A4 AB C1 7D FF 39 1A 1D	HASH OUT
HMAC IN 2	09 4D 9C DF	AP 会话的序列号
HMAC OUT	F7 D8 A2 78 B8 A0 56 65 CB 68 22 4F B7 0C DC 7F 53 C1 61 5B 58 8D 00 F5 03 4B 0A C5 0F 56 E2 A9	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码、命令码、签名数据长度和签名做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用签名密钥 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) 授权数据

创建签名密钥 AP 会话时，需要封装操作密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

d) 签名密钥

签名密钥采用的是 keyB。

6.50 TCM_SMS4Encrypt

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 已经载入了一个对称加密密钥，即 TCM_LoadKey 的执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 50	
3	4	命令码	00 00 80 C5	TCM_ORD_SMS4Encrypt
4	4	密钥句柄	05 00 00 01	keyE
5	16	CBC 模式使用的 IV	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
6	4	待加密数据长度	00 00 00 0A	
7	可变	待加密数据	01 01 01 01 01 01 01 01 01 01	也可以是其他数据
8	4	加密密钥授权会话句柄	00 00 00 38	
9	32	加密密钥授权数据验证码	3F B7 17 36 B1 0D 6C 0F EC ED 08 AA 96 F7 75 92 80 91 A6 89 E0 57 1A 3D 56 38 16 42 FF C1 B4 27	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 3E	
3	4	返回码	00 00 00 00	
4	4	已加密数据长度	00 00 00 10	
5	可变	已加密数据	B7 18 11 5E 69 29 00 93 B0 5E BE 14 F8 6F 8C 09	
5	32	加密密钥授权数据验证码	F6 53 D7 E3 4B 12 19 75 35 B3 2B 81 FF 9A BE 4B 3C D0 6F 30 E7 E3 B6 D1 3D 6A 5F 00 20 6D 73 6C	
		命令码	00 00 80 C5	TCM_ORD_SMS4Encrypt

输入 Blob：

00 C2 00 00 00 50 00 00 80 C5 05 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A 01 01 01 01 01 01 01 01 01 01 00 00 00 38 3F B7 17 36 B1 0D 6C 0F EC ED 08 AA 96 F7 75 92 80 91 A6 89 E0 57 1A 3D 56 38 16 42 FF C1 B4 27

输出 Blob：

00 C5 00 00 00 3E 00 00 00 00 00 00 00 10 B7 18 11 5E 69 29 00 93 B0 5E BE 14 F8 6F 8C 09 F6 53 D7 E3 4B 12 19 75 35 B3 2B 81 FF 9A BE 4B 3C D0 6F 30 E7 E3 B6 D1 3D 6A 5F 00 20 6D 73 6C

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 C5	命令码
HASH IN 2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	CBC 模式使用的 IV
HASH IN 3	00 00 00 0A	待加密的数据长度
HASH IN 4	01 01 01 01 01 01 01 01 01 01	待加密数据
HASH OUT	BF 4B 02 0A 76 86 40 F9 9F 26 B6 FF 6D 26 E0 48 00 49 14 42 A7 C1 1E 1F AE 7A 3E E2 D3 67 3D 8B	HMAC IN 1
KEY	8F F2 CC CA 4E 50 BD 17 76 47 90 07 0D BA AA 1E 28 90 A8 BF B8 6F 29 43 E7 CD C9 E9 59 3B 64 74	加密密钥 AP 会话的共享秘密数据
HMAC IN 1	BF 4B 02 0A 76 86 40 F9 9F 26 B6 FF 6D 26 E0 48 00 49 14 42 A7 C1 1E 1F AE 7A 3E E2 D3 67 3D 8B	HASH OUT
HMAC IN 2	7F 18 9D E7	AP 会话的序列号
HMAC OUT	3F B7 17 36 B1 0D 6C 0F EC ED 08 AA 96 F7 75 92 80 91 A6 89 E0 57 1A 3D 56 38 16 42 FF C1 B4 27	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码、命令码、已加密数据的长度和已加密数据做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用加密密钥创建的 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) 授权数据

创建加密密钥 AP 会话时，需要加密密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

6.51 TCM_SMS4Decrypt

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 已经载入了一个对称解密密钥，即 TCM_LoadKey 的执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 56	
3	4	命令码	00 00 80 C6	TCM_ORD_SMS4Decrypt
4	4	密钥句柄	05 00 00 01	keyE
5	16	CBC 模式使用的 IV	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
6	4	待解密数据长度	00 00 00 10	

序号	长度	名称	值	说明
7	可变	待解密数据	B7 18 11 5E 69 29 00 93 B0 5E BE 14 F8 6F 8C 09	来自 TCM_SMS4Encrypt 命令执行结果
8	4	解密密钥授权会话句柄	00 00 00 39	
9	32	解密密钥授权数据验证码	EF 54 FD C4 95 9B 81 1D 1F 9F 23 9E 76 0B 8A 7F 23 E6 44 B6 2D 54 E2 19 78 E7 65 5E CB 76 63 41	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 38	
3	4	返回码	00 00 00 00	
4	4	输出数据长度	00 00 00 0A	
5	可变	解密后数据	01 01 01 01 01 01 01 01 01 01	
5	32	解密密钥授权数据验证码	59 8A 3A 6A A0 A0 DC 88 67 B8 3C 3C A2 47 8A 2A F2 78 8D B9 A6 41 17 E5 25 6E 25 7C 16 58 62 F0	
		命令码	00 00 80 C6	TCM_ORD_SMS4Decrypt

输入 Blob：

00 C2 00 00 00 56 00 00 80 C6 05 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 B7 18 11 5E 69 29 00 93 B0 5E BE 14 F8 6F 8C 09 00 00 00 39 EF 54 FD C4 95 9B 81 1D 1F 9F 23 9E 76 0B 8A 7F 23 E6 44 B6 2D 54 E2 19 78 E7 65 5E CB 76 63 41

输出 Blob：

00 C5 00 00 00 38 00 00 00 00 00 00 00 0A 01 01 01 01 01 01 01 01 01 01 59 8A 3A 6A A0 A0 DC 88 67 B8 3C 3C A2 47 8A 2A F2 78 8D B9 A6 41 17 E5 25 6E 25 7C 16 58 62 F0

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 C6	命令码
HASH IN 2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	CBC 模式使用的 IV
HASH IN 3	00 00 00 10	待解密数据长度
HASH IN 4	B7 18 11 5E 69 29 00 93 B0 5E BE 14 F8 6F 8C 09	待解密数据
HASH OUT	1A 59 6E 43 A3 35 31 AE 78 63 4A 49 32 8F BE 4B B4 E4 B0 88 24 32 EB 1C 65 7E 1D 07 FD 92 27 33	HMAC IN 1
KEY	5D 1D 5E 9B D9 CE 10 B0 37 6C 33 49 62 4C 76 DF 7D BC 17 F1 47 E2 C1 BD C4 DA 33 70 3E AD EA 86	解密密钥 AP 会话的共享秘密数据

输入域	输入域授权数据验证码	说明
HMAC IN 1	1A 59 6E 43 A3 35 31 AE 78 63 4A 49 32 8F BE 4B B4 E4 B0 88 24 32 EB 1C 65 7E 1D 07 FD 92 27 33	HASH OUT
HMAC IN 2	D3 C0 33 C5	AP 会话的序列号
HMAC OUT	EF 54 FD C4 95 9B 81 1D 1F 9F 23 9E 76 0B 8A 7F 23 E6 44 B6 2D 54 E2 19 78 E7 65 5E CB 76 63 41	输入域授权数据验证码

b) 输出域授权数据验证码的计算过程

返回码、命令码、输出数据的长度和解密后数据做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用解密密钥创建的 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) 授权数据

创建解密密钥 AP 会话时，需要解密密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

6.52 TCM_EccDecrypt

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 已经载入了一个非对称解密密钥，即 TCM_LoadKey 的执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 9B	
3	4	命令码	00 00 80 EE	TCM_ORD_EccDecrypt
4	4	密钥句柄	05 00 00 08	keyA
5	4	待解密数据长度	00 00 00 65	
6	可变	待解密数据	04 77 8E 09 8B 01 11 36 51 5D E5 9B 9F 6C FD 53 75 92 83 6F 40 22 1F 62 1C F2 27 52 A2 83 74 9D F7 5D 47 0C 74 0D EC 71 CD A6 6E C3 7F 96 0D B5 62 C4 D5 0B DB 10 F6 32 BA 8B 14 BF 10 4E A4 20 15 DF C4 0A 54 96 2A 07 4D BD DF 13 9A B5 83 39 55 A0 66 68 E6 5E 17 76 D9 80 F8 39 BD 27 A7 1B 9E EF FC EF 07	来自外部用 keyA 公钥加密后的结果
7	4	解密密钥授权会话句柄	00 00 00 3B	
8	32	解密密钥授权数据验证码	60 B2 DB 5E DA 46 5D 6F 44 F9 39 C2 7E C8 69 3A 6C 5E A4 DB 65 17 05 8B E2 80 12 6A 4A F9 12 6E	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 32	
3	4	返回码	00 00 00 00	
4	4	解密后数据长度	00 00 00 04	
5	可变	解密后数据	19 90 90 90	
5	32	解密密钥授权数据验证码	76 BD 57 C5 A2 4D C9 51 F6 16 A9 95 D3 FE 40 AA 8E DB 9F 02 68 8E 4B 6D E9 F3 98 C7 03 89 07 0D	
		命令码	00 00 80 EE	TCM_ORD_EccDecrypt

输入 Blob：

00 C2 00 00 00 9B 00 00 80 EE 05 00 00 08 00 00 00 65 04 77 8E 09 8B 01 11 36 51 5D E5 9B 9F 6C FD 53 75 92 83 6F 40 22 1F 62 1C F2 27 52 A2 83 74 9D F7 5D 47 0C 74 0D EC 71 CD A6 6E C3 7F 96 0D B5 62 C4 D5 0B DB 10 F6 32 BA 8B 14 BF 10 4E A4 20 15 DF C4 0A 54 96 2A 07 4D BD DF 13 9A B5 83 39 55 A0 66 68 E6 5E 17 76 D9 80 F8 39 BD 27 A7 1B 9E EF FC EF 07 00 00 00 3B 60 B2 DB 5E DA 46 5D 6F 44 F9 39 C2 7E C8 69 3A 6C 5E A4 DB 65 17 05 8B E2 80 12 6A 4A F9 12 6E

输出 Blob：

00 C5 00 00 00 32 00 00 00 00 00 00 00 04 19 90 90 90 76 BD 57 C5 A2 4D C9 51 F6 16 A9 95 D3 FE 40 AA 8E DB 9F 02 68 8E 4B 6D E9 F3 98 C7 03 89 07 0D

说明：

a) 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 EE	命令码
HASH IN 2	00 00 00 65	待解密数据长度
HASH IN 3	04 77 8E 09 8B 01 11 36 51 5D E5 9B 9F 6C FD 53 75 92 83 6F 40 22 1F 62 1C F2 27 52 A2 83 74 9D F7 5D 47 0C 74 0D EC 71 CD A6 6E C3 7F 96 0D B5 62 C4 D5 0B DB 10 F6 32 BA 8B 14 BF 10 4E A4 20 15 DF C4 0A 54 96 2A 07 4D BD DF 13 9A B5 83 39 55 A0 66 68 E6 5E 17 76 D9 80 F8 39 BD 27 A7 1B 9E EF FC EF 07	待解密数据
HASH OUT	68 33 B0 15 3E 63 EB 06 CC CD 98 EF 0E AC 79 FB BC 3B 81 F1 87 43 12 DF EB 9F D9 F2 DF 7E 18 67	HMAC IN 1
KEY	4C C0 12 72 C4 BB 69 DE 52 74 51 BB A5 37 67 7C 22 14 19 6F EC 61 EA 6B 14 DE 37 75 CA C0 33 CC	解密密钥 AP 会话的共享秘密数据
HMAC IN 1	68 33 B0 15 3E 63 EB 06 CC CD 98 EF 0E AC 79 FB BC 3B 81 F1 87 43 12 DF EB 9F D9 F2 DF 7E 18 67	HASH OUT
HMAC IN 2	45 05 86 E3	AP 会话的序列号
HMAC OUT	60 B2 DB 5E DA 46 5D 6F 44 F9 39 C2 7E C8 69 3A 6C 5E A4 DB 65 17 05 8B E2 80 12 6A 4A F9 12 6E	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码、命令码、解密后数据的长度和解密后数据做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用解密密钥创建的 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c） 授权数据

创建解密密钥 AP 会话时，需要解密密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

6.53 TCM_GetRandom

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0E	
3	4	命令码	00 00 80 46	TCM_ORD_GetRandom
4	4	随机数据长度	00 00 00 10	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 1E	
3	4	返回码	00 00 00 00	
4	4	随机数据长度	00 00 00 10	
5	可变	随机数据	2F 7E 88 F6 C9 90 5E A8 48 9A C3 39 DA 96 2A D5	
		命令码	00 00 80 46	TCM_ORD_GetRandom

输入 Blob：

00 C1 00 00 00 0E 00 00 80 46 00 00 00 10

输出 Blob：

00 C4 00 00 00 1E 00 00 00 00 00 00 00 10 2F 7E 88 F6 C9 90 5E A8 48 9A C3 39 DA 96 2A D5

6.54 TCM_APCreate

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有授权实体或者是 TCM_ET_NONE。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 50	
3	4	命令码	00 00 80 BF	TCM_ORD_APCreate
4	2	实体类型	00 12	也可以是其他实体类型，参看 GM/T BBBB 中创建授权协议会话 TCM_APCreate 命令的描述
5	4	实体值	00 00 00 00	实体值，参看 GM/T BBBB 的描述。
6	32	调用者 nonce	C4 D3 C1 E9 6B F4 4C B4 5C A1 3F 62 26 0E 6D 77 23 A5 D1 1D BB 2B 9D 6D B3 0E 01 C5 2C 32 5B 4E	
7	32	授权数据验证码	50 7E FE 12 31 32 E5 81 96 6D 10 CF D5 A6 41 E1 5D 67 A9 55 44 F0 E4 C3 BB 41 59 FF DB D9 18 AC	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 52	
3	4	返回码	00 00 00 00	
4	4	授权会话句柄	00 00 00 42	
5	32	TCM nonce	91 BC 4E FE E4 5C 29 59 74 A6 BC 36 63 37 4B 0A 7E 40 3A FF 3A E5 42 56 15 AD 3C 56 99 1A BB D4	
6	4	序列号	55 91 FD CF	
7	32	实体授权数据校验码	B1 84 15 02 2B 8E BB BE 08 EC B2 AC C0 05 9A 65 66 A4 A2 D5 CF D0 48 EC 62 41 B6 1B DF 00 05 EB	
		命令码	00 00 80 BF	TCM_ORD_APCreate

输入 Blob：

00 C2 00 00 00 50 00 00 80 BF 00 12 00 00 00 00 C4 D3 C1 E9 6B F4 4C B4 5C A1 3F 62 26 0E 6D 77 23 A5 D1 1D BB 2B 9D 6D B3 0E 01 C5 2C 32 5B 4E 50 7E FE 12 31 32 E5 81 96 6D 10 CF D5 A6 41 E1 5D 67 A9 55 44 F0 E4 C3 BB 41 59 FF DB D9 18 AC

输出 Blob：

00 C5 00 00 00 52 00 00 00 00 00 00 00 42 91 BC 4E FE E4 5C 29 59 74 A6 BC 36 63 37 4B 0A 7E 40 3A FF 3A E5 42 56 15 AD 3C 56 99 1A BB D4 55 91 FD CF B1 84 15 02 2B 8E BB BE 08 EC B2 AC C0 05 9A 65 66 A4 A2 D5 CF D0 48 EC 62 41 B6 1B DF 00 05 EB

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 BF	命令码
HASH IN 2	00 12	实体类型
HASH OUT	95 64 12 34 48 44 B6 9F 90 C7 E0 A4 10 08 E8 08 F9 32 25 1E 55 AD 6C 08 A1 99 83 11 E3 39 37 12	HMAC IN 1
KEY	8E 51 7E C5 46 0B A1 CD 4D 83 68 8D 60 B7 79 8D 0B 75 62 96 21 CF 93 D0 CF 1A 06 5F 17 1E 32 7B	实体授权数据
HMAC IN 1	95 64 12 34 48 44 B6 9F 90 C7 E0 A4 10 08 E8 08 F9 32 25 1E 55 AD 6C 08 A1 99 83 11 E3 39 37 12	HASH OUT
HMAC IN 2	C4 D3 C1 E9 6B F4 4C B4 5C A1 3F 62 26 0E 6D 77 23 A5 D1 1D BB 2B 9D 6D B3 0E 01 C5 2C 32 5B 4E	调用者 nonce
HMAC OUT	50 7E FE 12 31 32 E5 81 96 6D 10 CF D5 A6 41 E1 5D 67 A9 55 44 F0 E4 C3 BB 41 59 FF DB D9 18 AC	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码、命令码和 TCM nonce 做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为 AP 会话的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

6.55 TCM_APTerminate

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有授权实体或者是 TCM_ET_NONE。

c） TCM_APCreate 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 2E	
3	4	命令码	00 00 80 C0	TCM_ORD_APTerminate
4	4	实体授权会话句柄	00 00 00 43	
5	32	授权数据验证码	F3 4E 59 C6 72 08 AD 17 A8 D7 2A C1 0D B6 DB B1 9B 3E 56 DB 3F 71 C8 A1 0A 65 F2 9B 50 16 E4 1A	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM _ TAG _ RSP _ AUTH _COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 C0	TCM_ORD_APTerminate

输入 Blob：

00 C2 00 00 00 2E 00 00 80 C0 00 00 00 43 F3 4E 59 C6 72 08 AD 17 A8 D7 2A C1 0D B6 DB B1 9B 3E 56 DB 3F 71 C8 A1 0A 65 F2 9B 50 16 E4 1A

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

说明：

输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 C0	命令码
HASH OUT	32 64 12 34 48 44 B6 80 90 C7 E0 A4 10 08 E8 08 F9 32 25 1E 55 AD 6C 08 54 66 83 11 E3 39 37 69	HMAC IN 1
KEY	86 51 7F C9 46 0B A5 CD 4D 83 68 8D 60 B7 79 8D 0B 75 62 96 21 CF 93 D9 CF 15 06 5F 17 1E 32 7B	TCM_APCreate 中生成的共享秘密数据
HMAC IN 1	32 64 12 34 48 44 B6 80 90 C7 E0 A4 10 08 E8 08 F9 32 25 1E 55 AD 6C 08 54 66 83 11 E3 39 37 69	HASH OUT
HMAC IN 2	E5 83 AD BF	序列号
HMAC OUT	F3 4E 59 C6 72 08 AD 17 A8 D7 2A C1 0D B6 DB B1 9B 3E 56 DB 3F 71 C8 A1 0A 65 F2 9B 50 16 E4 1A	输入域授权数据验证码

6.56 TCM_Extend

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 2E	
3	4	命令码	00 00 80 14	TCM_ORD_Extend
4	4	PCR 索引	00 00 00 01	也可以是其他 PCR，具体参看 GM/T BBBB 中的描述
5	32	输入摘要值	0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	新的度量值	40 95 8C 70 72 02 0B 6F 92 48 7F 0A 27 84 69 8B 84 EA 55 43 EB B7 24 E2 FB 31 84 66 3B EB F9 F8	
		命令码	00 00 80 14	TCM_ORD_Extend

输入 Blob：

00 C1 00 00 00 2E 00 00 80 14 00 00 00 01 0F D8 55 A9 D1 E9 6C EF 0E A7 45 1B ED 1B 29 A9 5F 7A 60 EA 8C FB 20 F4 77 46 CE 65 FD 1E 69 50

输出 Blob：

00 C4 00 00 00 2A 00 00 00 00 40 95 8C 70 72 02 0B 6F 92 48 7F 0A 27 84 69 8B 84 EA 55 43 EB B7 24 E2 FB 31 84 66 3B EB F9 F8

6.57 TCM_PCRRead

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0E	
3	4	命令码	00 00 80 15	TCM_ORD_PCRRead
4	4	PCR 索引	00 00 00 01	也可以是其他 PCR，具体参看 GM/T BBBB 中的描述

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 2A	
3	4	返回码	00 00 00 00	
4	32	PCR 值	40 95 8C 70 72 02 0B 6F 92 48 7F 0A 27 84 69 8B 84 EA 55 43 EB B7 24 E2 FB 31 84 66 3B EB F9 F8	
		命令码	00 00 80 15	TCM_ORD_PCRRead

输入 Blob：

00 C1 00 00 00 0E 00 00 80 15 00 00 00 01

输出 Blob：

00 C4 00 00 00 2A 00 00 00 00 40 95 8C 70 72 02 0B 6F 92 48 7F 0A 27 84 69 8B 84 EA 55 43 EB B7 24 E2 FB 31 84 66 3B EB F9 F8

6.58 TCM_Quote

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) 存在已加载的签名密钥，即 TCM_LoadKey 的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C2	TCM _ TAG _ RQU _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 56	
3	4	命令码	00 00 80 16	TCM_ORD_Quote
4	4	密钥句柄	05 00 00 06	KeyB
5	32	防重放攻击数据	02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02	
6	可变	目标 PCR	00 02 00 11	
7	4	授权会话句柄	00 00 00 4F	
8	32	授权数据验证码	7B 21 1A 5F B6 73 06 22 DC 26 9F 29 EE 31 66 DC 4B 80 32 A1 EC 45 DA AC 51 23 AD 21 C7 0A 33 7C	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C5	TCM _ TAG _ RSP _ AUTH1 _COMMAND
2	4	数据长度	00 00 00 B6	
3	4	返回码	00 00 00 00	
4	可变	PCR 数据	00 02 00 11 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9C E8 92 FF E9 C2 E7 F0 00 9A 5E E4 05 65 B5 91 54 29 BD B9 D1 7B 0A 00 36 19 48 26 C5 8C 8E E1	
5	4	签名数据长度	00 00 00 40	

序号	长度	名称	值	说明
6	可变	签名数据	BF FA B5 A2 76 0B CD CB 2B B8 32 B1 B6 B9 C5 B4 C8 C5 5E 60 B7 F9 62 FC B6 68 CE C2 58 BB 94 7A 86 3D DD 0E A1 34 76 E0 49 86 A0 1F 78 34 9A 22 7D 99 DF 1F 19 A1 E3 53 D4 30 9A DB A0 0D 4B B1	
7	32	签名密钥授权数据验证码	90 31 C0 71 6F 3A BF 54 1D CE E3 8B B5 FF 89 57 89 75 A1 20 93 AD 5F 59 A9 14 B2 DE 76 F4 5F 2F	
		命令码	00 00 80 16	TCM_ORD_Quote

输入 Blob：

00 C2 00 00 00 56 00 00 80 16 05 00 00 06 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 00 02 00 11 00 00 00 4F 7B 21 1A 5F B6 73 06 22 DC 26 9F 29 EE 31 66 DC 4B 80 32 A1 EC 45 DA AC 51 23 AD 21 C7 0A 33 7C

输出 Blob：

00 C5 00 00 00 B6 00 00 00 00 00 02 00 11 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9C E8 92 FF E9 C2 E7 F0 00 9A 5E E4 05 65 B5 91 54 29 BD B9 D1 7B 0A 00 36 19 48 26 C5 8C 8E E1 00 00 00 40 BF FA B5 A2 76 0B CD CB 2B B8 32 B1 B6 B9 C5 B4 C8 C5 5E 60 B7 F9 62 FC B6 68 CE C2 58 BB 94 7A 86 3D DD 0E A1 34 76 E0 49 86 A0 1F 78 34 9A 22 7D 99 DF 1F 19 A1 E3 53 D4 30 9A DB A0 0D 4B B1 90 31 C0 71 6F 3A BF 54 1D CE E3 8B B5 FF 89 57 89 75 A1 20 93 AD 5F 59 A9 14 B2 DE 76 F4 5F 2F

说明：

a） 输入域授权数据验证码的计算过程

输入域	输入域授权数据验证码	说明
HASH IN 1	00 00 80 16	命令码
HASH IN 2	02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02	防重放攻击数据
HASH IN 3	00 02 00 11	目标 PCR
HASH OUT	F7 28 2D 46 84 EC CA 44 42 99 B0 95 22 B8 E1 FA 4F 92 BE C9 26 58 76 67 3D 11 AE 15 05 8A 65 3E	HMAC IN 1
KEY	A0 10 56 78 F7 DC CC A0 76 F2 33 F6 A6 C6 F1 1C 85 F0 04 1B 1E BE 70 FB BA 27 03 5D D9 2D 25 29	签名密钥 AP 会话的共享秘密数据
HMAC IN 1	F7 28 2D 46 84 EC CA 44 42 99 B0 95 22 B8 E1 FA 4F 92 BE C9 26 58 76 67 3D 11 AE 15 05 8A 65 3E	HASH OUT
HMAC IN 2	3D 8B 64 EF	AP 会话的序列号
HMAC OUT	7B 21 1A 5F B6 73 06 22 DC 26 9F 29 EE 31 66 DC 4B 80 32 A1 EC 45 DA AC 51 23 AD 21 C7 0A 33 7C	输入域授权数据验证码

b） 输出域授权数据验证码的计算过程

返回码、命令码、PCR 数据和签名数据做哈希计算，其结果再与序列号做 HMAC 计算，HMAC 的密钥为使用签名密钥 AP 会话产生的共享秘密数据。

建议厂商给出 TCM 运算时的中间值，使用户在 TCM 的符合性测试状态下能够获得更多符合性测试的信息。同时厂商可以将符合性测试状态下的 AP 授权会话句柄也固定下来，有助于整个符合性测试的展现。

c) 授权数据

创建签名密钥 AP 会话时，需要封装操作密钥的使用授权数据。本标准采用 KEYAUTH 常量值。

d) 签名密钥

签名密钥采用的是 keyB。

6.59 TCM_PCR_Reset

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0F	
3	4	命令码	00 00 80 C8	TCM_ORD_PCR_Reset
4	可变	目标 PCR	00 03 00 00 80	也可以是其他 PCR，具体参看 GM/T BBBB 中的描述

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 C8	TCM_ORD_PCR_Reset

输入 Blob：

00 C1 00 00 00 0F 00 00 80 C8 00 03 00 00 80

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

7 脚本向量

对于需要执行一个命令序列才能测试的命令，需要根据所涉及命令的测试向量组成测试脚本来进行符合性测试。对于与厂商实现相关的命令，则需要厂商提供测试脚本来进行符合性测试。通过测试脚本方式进行检测的 TCM 命令如下所示：

7.1 TCM_SaveState

依赖于：

TCM_Startup 命令的成功执行。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 0A	
3	4	命令码	00 00 80 98	TCM_ORD_SaveState

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	参数长度	00 00 00 0A	
3	4	返回码	00 00 00 00	
		命令码	00 00 80 98	TCM_ORD_SaveState

输入 Blob：

00 C1 00 00 00 0A 00 00 80 98

输出 Blob：

00 C4 00 00 00 0A 00 00 00 00

7.2 TCM_SaveContext

依赖于：

a) TCM_Startup 命令的成功执行。

b) 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c) KeyA 的存在。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 00 22	
3	4	命令码	00 00 80 B8	TCM_ORD_SaveContext
4	4	资源句柄	05 00 00 06	KeyA 的 Handle，也可以是其他资源句柄
5	4	资源类型	00 00 00 01	TCM_RT_KEY，也可以是 TCM_RT_AUTH 或者 TCM_RT_TRANS
6	16	标签	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01	

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 02 CA	
3	4	返回码	00 00 00 00	

序号	长度	名称	值	说明
4	4	输出的要保存数据长度	00 00 02 BC	
5	可变	输出的要保存数据	00 01 00 00 00 01 05 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 21 77 75 DC EC 12 54 73 9E B8 82 5B 29 3D F4 32 D9 78 AA 7C EE 4B E6 10 A9 7A 8E 71 28 02 C2 C0 00 00 00 36 00 38 00 00 00 10 55 DA F1 E6 AB E9 B4 97 36 3E 89 BF CF F5 C2 CF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 40 34 1F 3F 5E 86 D6 30 D5 C4 EE 59 AA 20 D0 9C E2 03 16 C4 16 3C ED 1B 31 51 83 A6 C3 B7 0C 36 81 5B CF 1B E3 4B 2F 85 54 25 42 F5 E1 E6 6A B7 5C 8F 82 B8 D0 D4 5B 06 B3 22 3E 46 EE 7B 8B 06 F2 B3 3B B4 34 5F 6A D7 4E 76 2C 88 00 E5 56 4A 5C CE D0 FB DF 6D A9 65 56 73 FA EB 96 7B B7 42 0C 6C C1 ED AD C0 32 F5 FC 35 6B 6D F7 12 43 E3 98 FF 48 9C DC E7 3E 49 0C FC 47 B1 CC 94 57 B0 33 B2 0E CD 9D BA B1 1D 8D A4 06 B1 91 25 9A AE 16 D4 9C 06 DE 57 D4 9D 0C C4 BF B4 2F 59 8D 2A F1 D7 1A 44 7B 0D A0 4E 76 CC 3D 95 0E DD 44 A2 67 BA 93 C3 C8 7B 9F 18 4F ED F1 53 D8 DE 41 D8 5F 39 35 48 09 49 B9 03 84 53 65 AE A7 FC 29 59 3C 7B 76 3F 1C A6 32 B5 9E C1 5B F6 1F B3 CE B5 C2 91 27 09 CC 0A 46 CF 98 59 AB 31 6B CD 21 5A 3D 15 BE 7A EC 72 D5 35 D1 9F 8F 37 AE 97 69 08 76 3E 7F CF 14 B1 93 4A 9E 3D F8 5D B8 19 F3 56 AE 36 7F B2 D2 D3 0C 22 0F 05 76 A9 D9 6A ED 25 96 18 80 9B A6 40 42 C7 16 3A 34 17 2F C3 AA DE 19 CD 7F E7 CF 3E A6 A7 55 94 5F CB B7 BB 9A CE C7 2F FD C9 7A 63 EC 6D 24 F8 FC AA 6E 0E F9 DC D2 B2 F7 3F 82 F6 83 80 0A B7 A7 30 09 A7 F2 15 3B 9E C7 7F 90 93 6E 39 80 12 18 F3 79 51 AA BE 55 34 75 F3 96 EB 43 F6 13 91 EF 1E 8D F6 97 45 B4 5C 55 EF BB BD 03 BB B8 B3 14 8F BF EA 82 E3 39 04 F6 6D D7 69 54 38 DE EE D7 A7 77 95 17 A8 65 23 C6 D2 99 A5 32 56 E6 D2 B9 9B 91 F4 BC F3 B3 60 A7 18 C4 C6 1B B0 02 E1 00 70 1B 87 39 E6 BC 13 BB 7B 98	

序号	长度	名称	值	说明
			71 35 30 E6 F3 F1 D0 F1 44 DB ED 4E 08 34 CB 97 D3 11 EB 42 98 12 E9 72 47 57 B2 55 18 0B E7 FB 27 8E 9C 19 D5 CD F5 F7 B3 B1 AE 5F E3 46 51 F7 BC 02 EB 35 0B 3C F7 69 91 A8 D4 A3 4E 2A 2F 8E D6 EA E2 FF 48 3F A0 03 31 B0 B3 E3 13 D2 E1 44 4A 35 18 50 50 2E C7 D9 C2 40 04 51 79 01 12 CC 5E B6 A9 03 41 42 4A 1B FA 66 B3 2A 20 FF FA E2 37 41 73 72 3A A8 58 E8 F9 12 C4 0D	
		命令码	00 00 80 B8	TCM_ORD_SaveContext

输入 Blob：

00 C1 00 00 00 22 00 00 80 B8 05 00 00 06 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

输出 Blob：

00 C4 00 00 02 CA 00 00 00 00 00 00 02 BC 00 01 00 00 00 01 05 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 21 77 75 DC EC 12 54 73 9E B8 82 5B 29 3D F4 32 D9 78 AA 7C EE 4B E6 10 A9 7A 8E 71 28 02 C2 C0 00 00 00 36 00 38 00 00 00 10 55 DA F1 E6 AB E9 B4 97 36 3E 89 BF CF F5 C2 CF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 40 34 1F 3F 5E 86 D6 30 D5 C4 EE 59 AA 20 D0 9C E2 03 16 C4 16 3C ED 1B 31 51 83 A6 C3 B7 0C 36 81 5B CF 1B E3 4B 2F 85 54 25 42 F5 E1 E6 6A B7 5C 8F 82 B8 D0 D4 5B 06 B3 22 3E 46 EE 7B 8B 06 F2 B3 3B B4 34 5F 6A D7 4E 76 2C 88 00 E5 56 4A 5C CE D0 FB DF 6D A9 65 56 73 FA EB 96 7B B7 42 0C 6C C1 ED AD C0 32 F5 FC 35 6B 6D F7 12 43 E3 98 FF 48 9C DC E7 3E 49 0C FC 47 B1 CC 94 57 B0 33 B2 0E CD 9D BA B1 1D 8D A4 06 B1 91 25 9A AE 16 D4 9C 06 DE 57 D4 9D 0C C4 BF B4 2F 59 8D 2A F1 D7 1A 44 7B 0D A0 4E 76 CC 3D 95 0E DD 44 A2 67 BA 93 C3 C8 7B 9F 18 4F ED F1 53 D8 DE 41 D8 5F 39 35 48 09 49 B9 03 84 53 65 AE A7 FC 29 59 3C 7B 76 3F 1C A6 32 B5 9E C1 5B F6 1F B3 CE B5 C2 91 27 09 CC 0A 46 CF 98 59 AB 31 6B CD 21 5A 3D 15 BE 7A EC 72 D5 35 D1 9F 8F 37 AE 97 69 08 76 3E 7F CF 14 B1 93 4A 9E 3D F8 5D B8 19 F3 56 AE 36 7F B2 D2 D3 0C 22 0F 05 76 A9 D9 6A ED 25 96 18 80 9B A6 40 42 C7 16 3A 34 17 2F C3 AA DE 19 CD 7F E7 CF 3E A6 A7 55 94 5F CB B7 BB 9A CE C7 2F FD C9 7A 63 EC 6D 24 F8 FC AA 6E 0E F9 DC D2 B2 F7 3F 82 F6 83 80 0A B7 A7 30 09 A7 F2 15 3B 9E C7 7F 90 93 6E 39 80 12 18 F3 79 51 AA BE 55 34 75 F3 96 EB 43 F6 13 91 EF 1E 8D F6 97 45 B4 5C 55 EF BB BD 03 BB B8 B3 14 8F BF EA 82 E3 39 04 F6 6D D7 69 54 38 DE EE D7 A7 77 95 17 A8 65 23 C6 D2 99 A5 32 56 E6 D2 B9 9B 91 F4 BC F3 B3 60 A7 18 C4 C6 1B B0 02 E1 00 70 1B 87 39 E6 BC 13 BB 7B 98 71 35 30 E6 F3 F1 D0 F1 44 DB ED 4E 08 34 CB 97 D3 11 EB 42 98 12 E9 72 47 57 B2 55 18 0B E7 FB 27 8E 9C 19 D5 CD F5 F7 B3 B1 AE 5F E3 46 51 F7 BC 02 EB 35 0B 3C F7 69 91 A8 D4 A3 4E 2A 2F 8E D6 EA E2 FF 48 3F A0 03 31 B0 B3 E3 13 D2 E1 44 4A 35 18 50 50 2E C7 D9 C2 40 04 51 79 01 12 CC 5E B6 A9 03 41 42 4A 1B FA 66 B3 2A 20 FF FA E2 37 41 73 72 3A A8 58 E8 F9 12 C4 0D

7.3 TCM_LoadContext

依赖于：

a） TCM_Startup 命令的成功执行。

b） 有所有者，即 TCM_TakeOwnership 命令的成功执行。

c） keyA 的存在。

输入域：

序号	长度	名称	值	说明
1	2	标识	00 C1	TCM_TAG_RQU_COMMAND
2	4	数据长度	00 00 02 CF	
3	4	命令码	00 00 80 B9	TCM_ORD_LoadContext
4	4	实体句柄	00 00 00 21	新的 AP 会话句柄
5	1	保存句柄	00	也可以是 01
6	4	以前保存的数据长度	00 00 02 BC	
7	可变	以前保存的数据	00 01 00 00 00 01 05 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 54 50 E0 66 1D 05 30 1F F1 6E 89 1A 16 2D 1F C8 E7 B2 97 A9 B2 D9 2A B2 18 24 B4 2F 34 89 97 0A 00 00 00 36 00 38 00 00 00 10 61 75 A2 12 6D 07 D9 B4 4C 62 07 61 8D 78 FE DC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 40 7C 3F 15 B0 FD 96 45 DD 45 A2 B9 8A 78 DE 12 11 AD 1F 13 E1 FF A8 EF 99 B0 AC 9A 42 0E CB AF 2F 87 F7 48 BC C8 50 0F D9 23 6A 77 07 E7 DB 21 BA 81 1B 34 56 09 58 A8 37 BF AC 16 D2 97 14 24 A9 B1 17 C7 0C 82 6E 55 90 51 D0 8A 2E 70 E7 46 44 F2 00 B3 0F 13 1F C3 93 FF 7C 2A D7 7A 11 A4 12 43 3D 9C 02 67 19 74 DB 29 63 5D 8A 0D B1 CD 0A 0B 19 27 9E F8 07 CE 33 FC 80 F1 7B CE 1E C6 2A 1B 5E D1 23 02 6D 63 9A 85 D2 D7 06 74 C9 7A D6 66 4F D5 47 E1 48 0D 95 8F B7 62 21 69 8E DB 9E 1A AE 78 24 83 67 E2 C1 9F C3 D5 ED A6 A0 36 24 82 89 45 67 AB A3 D3 60 2C C1 EF A7 EC FE 2E 82 EB A6 1C B7 A4 D8 B6 46 6E A0 46 5B F1 91 1C F6 85 95 3B B7 D7 2D A9 A2 21 18 14 31 71 EC 3C E0 67 EA E7 47 2D 33 33 64 03 43 1D 5A 30 0D F4 C2 D1 07 4E D4 1D 62 B5 59 BA 79 47 F7 E6 FF 5C D5 FB 47 22 78 58 2B C6 58 D1 2E E0 E6 C1 2B B9 A2 E7 6F 93 56 1E 90 F0 26 22 AD FA F7 EA 4E 26 35 98 C7 4A 37 16 36 49 51 0A 33 2E 08 73 65 B4 72 34 3E 76 CE 17 A2 AB 03 45 33 25 D2 E3 E7 C2 6E E0	

序号	长度	名称	值	说明
			9B 48 CE 02 05 09 76 C9 36 B8 AB C7 59 69 47 61 85 D7 8A 10 25 EF C8 B8 B0 7F 92 3F A0 6C 55 DA 9B 19 A6 1C 94 A5 80 69 1E 40 79 6A D1 FF 75 0F 97 D6 E1 CE CC E6 0E 31 B7 CE 04 28 E6 0B 09 C0 83 8A E9 0F A6 C4 39 A1 DF 1C A7 C1 1F 49 F1 0F 26 3D EB DD 09 D6 68 E1 6F 6F 29 45 E9 F5 2D B4 BE E0 31 A2 A5 DA D0 06 DE 54 16 C4 F4 ED F0 E7 63 B3 61 40 30 23 9E 06 10 42 55 20 C7 DA C6 9A C5 09 04 E7 F4 87 2B 89 50 F1 F1 CD 80 55 15 AB 33 14 A5 0E B4 9D 5F 53 B6 E3 9A 09 0E 03 29 A9 7E 32 D5 C5 F5 0A DA 86 6E F9 41 37 7A 44 7C 1F 0A 62 B5 3B 8E 82 F2 7A CE 81 92 B8 8B 24 F6 D2 84 6E BA 92 B1 1A 4C BC 55 37 5C 04 30 0E DC 9D D2 83 B1 97 99 5D FB 3F 28 48 FB 08 71 B6 EA 94 B3 7A 25 29 19 B6 8F 0B 84 50 0A 2F 9D B2 05 C7 23 D2 77 5A 79 9A A7 75 6A B1 2F B2 F4 00 35	TCM_SaveContext 命令保存载入的 keyA 的输出数据，也可以是其他预先保存的数据。

输出域：

序号	长度	名称	值	说明
1	2	标识	00 C4	TCM_TAG_RSP_COMMAND
2	4	数据长度	00 00 00 0E	
3	4	返回码	00 00 00 00	
4	4	资源句柄	05 00 00 02	新的 keyA 的句柄
		命令码	00 00 80 B9	TCM_ORD_LoadContext

输入 Blob：

00 C1 00 00 02 CF 00 00 80 B9 00 00 00 21 00 00 00 02 BC 00 01 00 00 00 01 05 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 54 50 E0 66 1D 05 30 1F F1 6E 89 1A 16 2D 1F C8 E7 B2 97 A9 B2 D9 2A B2 18 24 B4 2F 34 89 97 0A 00 00 00 36 00 38 00 00 00 10 61 75 A2 12 6D 07 D9 B4 4C 62 07 61 8D 78 FE DC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 40 7C 3F 15 B0 FD 96 45 DD 45 A2 B9 8A 78 DE 12 11 AD 1F 13 E1 FF A8 EF 99 B0 AC 9A 42 0E CB AF 2F 87 F7 48 BC C8 50 0F D9 23 6A 77 07 E7 DB 21 BA 81 1B 34 56 09 58 A8 37 BF AC 16 D2 97 14 24 A9 B1 17 C7 0C 82 6E 55 90 51 D0 8A 2E 70 E7 46 44 F2 00 B3 0F 13 1F C3 93 FF 7C 2A D7 7A 11 A4 12 43 3D 9C 02 67 19 74 DB 29 63 5D 8A 0D B1 CD 0A 0B 19 27 9E F8 07 CE 33 FC 80 F1 7B CE 1E C6 2A 1B 5E D1 23 02 6D 63 9A 85 D2 D7 06 74 C9 7A D6 66 4F D5 47 E1 48 0D 95 8F B7 62 21 69 8E DB 9E 1A AE 78 24 83 67 E2 C1 9F C3 D5 ED A6 A0 36 24 82 89 45 67 AB A3 D3 60 2C C1 EF A7 EC FE 2E 82 EB A6 1C B7 A4 D8 B6 46 6E A0 46 5B F1 91 1C F6 85 95 3B B7 D7 2D A9 A2 21 18 14 31 71 EC 3C E0 67 EA E7 47 2D 33 33 64 03 43 1D 5A 30 0D F4 C2 D1 07 4E D4 1D 62 B5 59 BA 79 47 F7 E6 FF 5C D5 FB 47 22 78 58 2B C6 58 D1 2E E0 E6

C1 2B B9 A2 E7 6F 93 56 1E 90 F0 26 22 AD FA F7 EA 4E 26 35 98 C7 4A 37 16 36 49 51 0A 33 2E 08 73 65 B4 72 34 3E 76 CE 17 A2 AB 03 45 33 25 D2 E3 E7 C2 6E E0 9B 48 CE 02 05 09 76 C9 36 B8 AB C7 59 69 47 61 85 D7 8A 10 25 EF C8 B8 B0 7F 92 3F A0 6C 55 DA 9B 19 A6 1C 94 A5 80 69 1E 40 79 6A D1 FF 75 0F 97 D6 E1 CE CC E6 0E 31 B7 CE 04 28 E6 0B 09 C0 83 8A E9 0F A6 C4 39 A1 DF 1C A7 C1 1F 49 F1 0F 26 3D EB DD 09 D6 68 E1 6F 6F 29 45 E9 F5 2D B4 BE E0 31 A2 A5 DA D0 06 DE 54 16 C4 F4 ED F0 E7 63 B3 61 40 30 23 9E 06 10 42 55 20 C7 DA C6 9A C5 09 04 E7 F4 87 2B 89 50 F1 F1 CD 80 55 15 AB 33 14 A5 0E B4 9D 5F 53 B6 E3 9A 09 0E 03 29 A9 7E 32 D5 C5 F5 0A DA 86 6E F9 41 37 7A 44 7C 1F 0A 62 B5 3B 8E 82 F2 7A CE 81 92 B8 8B 24 F6 D2 84 6E BA 92 B1 1A 4C BC 55 37 5C 04 30 0E DC 9D D2 83 B1 97 99 5D FB 3F 28 48 FB 08 71 B6 EA 94 B3 7A 25 29 19 B6 8F 0B 84 50 0A 2F 9D B2 05 C7 23 D2 77 5A 79 9A A7 75 6A B1 2F B2 F4 00 35

输出 Blob：

00 C4 00 00 00 0E 00 00 00 00 05 00 00 02

7.4 TCM_FiledUpgrade

该命令用于固件升级，为可选命令，厂商可以自行决定实现方式。因此，符合性测试将采用厂商自己编写的脚本测试。测试必须能够证明其实现遵循以下原则：

a) TCM 的升级机制不能依靠 TCM 保持一个全局的秘密值来实现。全局秘密的定义不能够被多个 TCM 共享。

b) 不能使用 EK 用于升级过程的鉴别与加密。

c) 可以使用预生成的公钥来验证升级包。

d) 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 PCR 信息等。

e) 当所有者不存在，则需要物理现场操作。所有者存在时必须有所有者授权。

参 考 文 献

[1] Trusted Computing Group. TPM Main Specification:Design Principles V1. 2. 2007. http://www. trustedcomputinggroup. org.

[2] Atmel Corporation. AT97SC3201 Security Target. Version 2. 3. 21. 2005.

[3] Atmel Corporation. Trusted Platform Module AT97SC3201 Summary. Version 1. 2. 2005.

[4] Ahmad-Reza Sadeghi, Marcel Selhorst, Christian Stüble, Christian Wachsmann, and Marcel Winandy. TCG Inside? - A Note on TPM Specification Compliance. Proceedings of the First ACM Workshop on Scalable Trusted Computing. Network:ACM Press, 2006:47-56.

[5] Danilo Bruschi, Lorenzo Cavallaro, Andrea Lanzi, and Mattia Monga. Replay Attack in TCG Specificaion and Solution. 21th Annual Computer Security Application Conference. Tucson: IEEE Press, 2005:127-137.

[6] Boris Beizer. Black-Box Testing: Techniques for Functional Testing of Software and Systems. New York:John Wiley & Sons Press, 1995.