



中华人民共和国国家标准

GB/T 16649.13—2013/ISO/IEC 7816-13:2007

识别卡 集成电路卡 第13部分:在多 应用环境中的应用管理命令

Identification cards—Integrated circuit cards—Part 13: Commands for
application management in a multi-application environment

(ISO/IEC 7816-13:2007, IDT)

2013-11-12 发布

2014-05-01 实施



中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目次

前言 Ⅲ

引言 Ⅳ

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语和符号 1

5 多应用环境和应用的生命周期 2

 5.1 多应用环境 2

 5.2 应用生命周期 2

 5.3 用于互用性的存储资源分配数据对象 4

6 卡管理服务识别 5

 6.1 卡管理服务模板 5

 6.2 卡管理服务模板获取 6

7 应用管理命令 6

 7.1 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令 6

 7.2 加载应用(LOAD APPLICATION)命令 7

 7.3 删除应用(REMOVE APPLICATION)命令 8

 7.4 应用管理的考虑 9

附录 A (资料性附录) 与发卡者和应用提供者无关模型的卡应用管理实例 10

附录 B (资料性附录) 卡应用管理的实例 12

附录 C (资料性附录) 卡应用管理的更多实例 15

附录 D (资料性附录) 卡应用管理的更多实例 18

参考文献 20

前 言

GB/T 16649《识别卡 集成电路卡》已经或计划发布以下部分：

- 第1部分：带触点的卡 物理特性；
- 第2部分：带触点的卡 触点的尺寸和位置；
- 第3部分：带触点的卡 电信号和传输协议；
- 第4部分：用于交换的结构、安全和命令；
- 第5部分：应用标识符的国家编号体系和注册规程；
- 第6部分：行业间数据元；
- 第7部分：用于结构化卡查询语言(SCQL)的行业间命令；
- 第8部分：与安全相关的行业间命令；
- 第9部分：用于卡管理的命令；
- 第10部分：带触点的卡 同步卡的电信号和复位应答；
- 第11部分：通过生物特征识别方法的个人验证(制定中)；
- 第12部分：带触点的卡 USB 电气接口和操作规程；
- 第13部分：在多应用环境中的应用管理命令；
- 第15部分：密码信息应用。

本部分为 GB/T 16649 的第13部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用 ISO/IEC 7816-13:2007《识别卡 集成电路卡 第13部分：在多应用环境中的应用管理命令》。

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。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：中国电子技术标准化研究院、北京华大智宝电子系统有限公司、东信和平智能卡股份有限公司、深圳市特种证件研究制作中心、航天信息股份有限公司北京航天金卡分公司、北京握奇智能科技有限公司。

本部分主要起草人：耿力、杨海波、赵子渊、冯敬、金倩、赵继红、张咏江、王文峰、牛争科、乔申杰。

引 言

GB/T 16649 是规定集成电路卡的参数和交换中集成电路卡的使用的国家标准。集成电路卡是用于信息交换(该信息交换由外界和卡上集成电路之间商定)的识别卡。作为信息交换的结果,卡传送信息(计算结果、存储的数据),和/或更改其内容(数据存储、结果记忆)。

——有 5 个部分规定了带触点的卡,其中有 3 部分还规定了电气接口:

- GB/T 16649.1 规定了带触点的卡的物理特性;
- GB/T 16649.2 规定了触点的尺寸和位置;
- GB/T 16649.3 规定了异步卡的电信号和传输协议;
- GB/T 16649.10 规定了同步卡的电信号和复位应答;
- GB/T 16649.12 规定了 USB 卡的电气接口和操作规程。

——所有其他部分均独立于物理接口技术,它们适用于通过触点和/或射频访问的卡:

- GB/T 16649.4 规定了用于交换的结构、安全和命令;
- GB/T 16649.5 规定了应用提供者的注册;
- GB/T 16649.6 规定了用于交换的行业间数据元;
- GB/T 16649.7 规定了结构化卡查询语言的命令;
- GB/T 16649.8 规定了用于安全操作的命令;
- GB/T 16649.9 规定了用于卡管理的命令;
- GB/T 16649.11 规定了通过生物识别方法的身份认证;
- GB/T 16649.13 规定了在多应用环境中的应用管理命令;
- GB/T 16649.15 规定了密码信息应用。

附录 A~附录 D 为实施 GB/T 16649 的本部分提供了应用实例。

识别卡 集成电路卡 第 13 部分:在多应用环境中的应用管理命令

1 范围

GB/T 16649 的本部分规定了多应用环境中的应用管理命令。这些命令覆盖了多应用集成电路卡中的整个应用生命周期。这些命令可以在卡发行到持卡者之前和之后使用。本部分不包括卡内部和/或卡外部的实现。

2 规范性引用文件

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

GB/T 16263.1—2006 信息技术 ASN.1 编码规则 第 1 部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范(ISO/IEC 8825-1:2002, IDT)

GB/T 16649.4—2010 识别卡 集成电路卡 第 4 部分:用于交换的结构、安全和命令(ISO/IEC 7816-4:2005, IDT)

GB/T 16649.9—2010 识别卡 集成电路卡 第 9 部分:用于卡管理的命令(ISO/IEC 7816-9:2004, IDT)

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用 application

为满足特定功能所需的数据结构、数据元和程序模块。

[GB/T 16649.4—2010]

3.2

应用提供者 application provider

提供卡上应用的组成部分的实体。

[GB/T 16649.4—2010]

3.3

卡平台 card platform

负责基本卡功能的卡上组件。

3.4

卡管理应用 card manager application

提供卡应用管理功能和指导卡资源分配的卡应用。

4 缩略语和符号

AID 应用标识符(application identifier)

- APP 应用 (application)
- DF 专用文件 (dedicated file)
- DO 数据对象 (data object)
- ICC 集成电路卡 (integrated circuit card)
- P1-P2 参数字节(短划线无意义,为清楚而插入)(parameter bytes)
- RID 注册的应用提供者标识符 (registered application provider identifier)

5 多应用环境和应用的生命周期

5.1 多应用环境

本部分上下文的多应用环境具有以下特点:

- a) 应用是多应用卡上唯一可寻址的功能组,它提供数据存储和计算服务;
- b) 在卡发给持卡者之前或者之后,可以给卡添加应用;
- c) 可以给卡添加多个应用;
- d) 卡平台提供资源管理机制,如存储管理;
- e) 卡平台给每个应用提供安全边界机制,以防止来自卡上任何其他应用未授权的互操作和安全侵害;
- f) 应用提供者是使用卡应用向持卡者提供服务并对应用行为负责的实体;
- g) 卡应用的应用提供者可以不是发卡者;
- h) 应用的生命周期与同一卡上的任何其他应用的生命周期无关;
- i) 如 GB/T 16649.9—2010 所定义,除了当卡处于终止状态时,应用的生命周期与卡的生命周期无关;
- j) 如 GB/T 16649.4—2010 所定义,所有应用至少应该可通过 SELECT 命令的以 AID 为 DF 名称的选择方式被选中;
- k) 通过 SELECT 命令的 AID 选择方式选择,卡管理应用应存在且唯一和可被选择。其他卡上的应用可以提供应用管理功能;
- l) 卡管理应用的默认 AID 是“E8 28 BD 08 0D”。

图 1 为多应用 IC 卡可能结构的概念性表示。

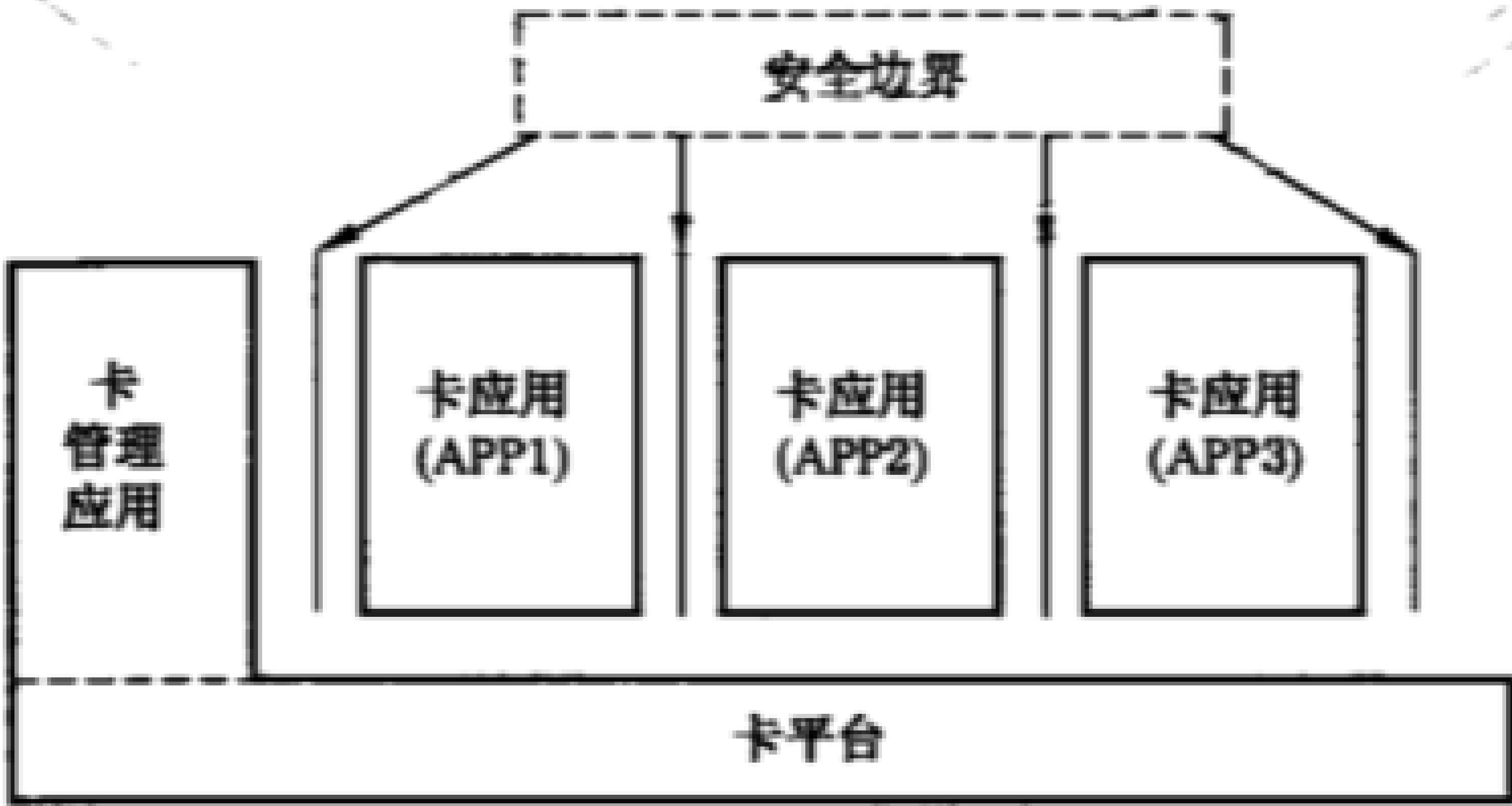


图 1 多应用 IC 卡结构的概念性表示

5.2 应用生命周期

生命周期状态应与每个应用关联。应用可以使用与其安全属性结合的生命周期状态,以确保其执行的任何操作与该应用的安全策略一致。卡管理应用应提供生命周期从不存在到操作激活状态的转换途径。

- 以下命令启动生命周期状态的转换：
- 应用管理请求(APPLICATION MANAGEMENT REQUEST)；
 - 加载应用(LOAD APPLICATION)；
 - 删除应用(REMOVE APPLICATION)。

图 2 为生命周期状态的概念性表示以及调用每个状态转换的命令。该图仅示出一个应用在生命周期转换完成时能达到的稳定(永久)状态。其他状态和中间状态可以在生命周期转换期间存在(例如,从不存在到创建状态),但是当程序中断时不保持。

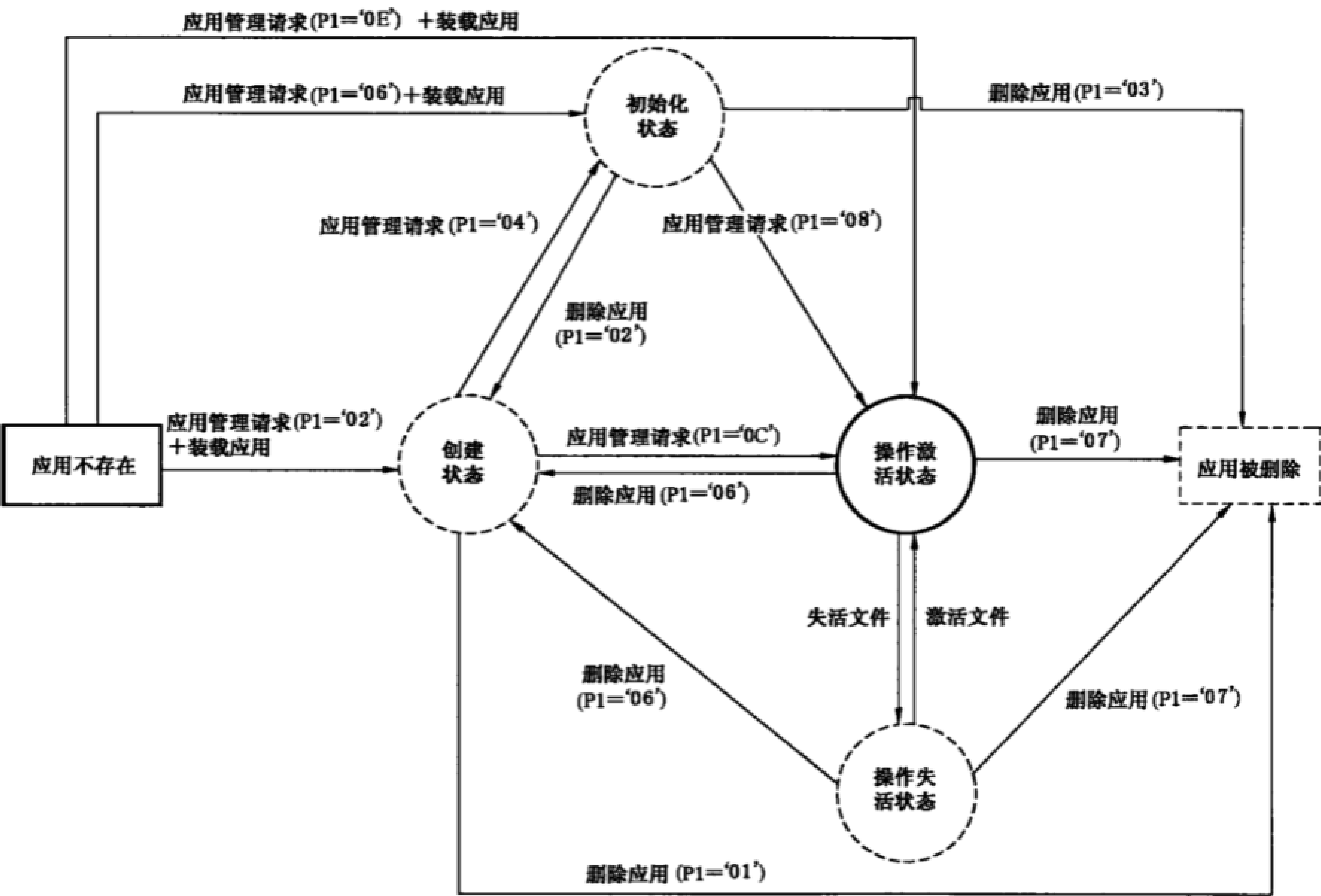


图 2 应用生命周期图

- 注 1：该图表按照以下方式理解：例如，执行了 APPLICATION MANAGEMENT REQUEST (P1 = “0E”) 和 LOAD APPLICATION 命令后，应用处于操作激活生命周期状态，即可执行和可选择。
- 注 2：方框代表卡存储的状态，圆形代表应用生命周期状态。虚线圆代表可选的应用生命周期状态。
- 注 3：在 GB/T 16649.9—2010 中定义了 ACTIVATE FILE 和 DEACTIVATE FILE 命令。

应用生命周期状态如表 1 定义。

应用生命周期状态的编码应与 GB/T 16649.4—2010 中定义的生命周期状态位(LCS 位)的编码一致。

表 1 应用生命周期状态

应用不存在	从卡管理应用的角度看,应用不存在
创建状态	从卡管理应用的角度看,应用存在,不可执行和不可选择
初始状态	应用存在,可执行有限的功能,并且不可选择
操作激活状态	应用存在,可执行和可选择
操作失活状态	应用存在,可执行有限的功能,并且 SELECT 命令返回应用是失活的警告
应用删除	应用不存在,不可执行和不可选择。可能只有部分以前分配的存储资源被释放并再次使用
<p>——一些卡平台可以具有另外的生命周期特定状态。另外的状态超出本部分的范围。如果卡支持另外的生命周期状态和状态转换,它们不应影响图 2 中的生命周期状态和状态转换。</p> <p>——斜体的状态表示卡存储状态,普通字符的状态表示应用生命周期状态。</p>	

5.3 用于互用性的存储资源分配数据对象

描述将存储资源分配给应用的存储资源分配模板(标记符“7F56”)可以与每个应用关联。

表 2 规定了用于每种存储类型的存储资源分配数据对象:持久的或者易失性存储器,其中:

- 保留存储是唯一分配给应用的存储数量;
- 存储配额是允许应用请求的最大存储数量。

存储资源分配数据对象代表以字节计算的存储资源量,编码为整数值,见 GB/T 16263.1—2006。

表 2 存储资源分配数据对象

标记符	描 述	要求
“80”	在持久存储器中用于应用代码的保留存储数量; 如果不要代码和数据之间的分隔,则“80”应该用于表示应用代码和数据两者的持久存储器存储的保留量	必选
“81”	在应用选择应用数据时的保留易失性存储数量	可选
“82”	用于应用数据的保留持久存储器存储数量; 如果“82”不存在,则“80”表示用于应用代码和数据两者的持久存储器存储的和	可选
“83”	用于应用代码的持久存储器存储的存储配额数量; 如果不要代码和数据之间的分隔,则“83”应该用于表示应用代码和数据两者的持久存储器存储的存储配额	可选
“84”	在应用选择应用数据时的易失性存储的存储配额数量	可选
“85”	用于应用数据的持久存储器的存储配额数量; 如果“85”不存在,则“83”表示用于应用代码和数据两者的持久存储器存储的和	可选
在此上下文中,ISO/IEC JTC 1/SC 17 保留上下文特定类的任何其他数据对象(第一字节从“80”到“BF”)。		

在使用存储资源分配数据对象的值时,应用以下规则:

- 保留存储分配给应用减少卡上其他应用可用的存储资源;
- 存储配额分配给应用不减少卡上其他应用可用的存储资源;
- 存储配额的值大于或者等于保留存储的值;
- 在成功创建应用时(例如,从不存在到操作激活状态的转换),分配给该应用的存储数量首先满

- 足分配给该应用的保留存储,直到全部用完。当应用的保留存储用完时,分配的存储数量减少卡上其他应用可用的存储资源,只要它不超过该应用的存储配额。当任一存储配额超出或者卡上目前可用的存储资源用完时,应用创建失败;
- 在成功删除应用时(即,转换到应用删除),卡上其他应用可用的存储资源以存储实际释放量增加,保留存储的任何未使用部分被重新分配给卡上其他应用可用的存储资源。

6 卡管理服务识别

6.1 卡管理服务模板

卡管理服务模板(标记符“7F64”)应存在。表 3 定义了卡管理服务模板的内容。

表 3 卡管理服务数据对象

标记符	长度/格式	描 述	要求
“80”	2 字节	卡支持的卡管理能力;该值是表 4 和表 5 中定义的位的组合	必选
“81”	可变	卡管理配置名称和版本;指明配置名称和版本(主要的和次要的)的对象标识符值(见 GB/T 16263.1—2006),用于管理卡和其应用	必选
“82”	可变	卡识别过程指示器;指明用于唯一标识卡的过程的对象标识符值(见 GB/T 16263.1—2006)。其定义了如何访问卡上的本地标识符,例如,ICC 序列号,以及该标识符是否是全球唯一的	可选
“4F”	可变	卡管理应用 AID;当与“E8 28 BD 08 0D”不同时,选择卡管理应用的应用识别符	可选
在本部分中,ISO/IEC JTC 1/SC 17 保留上下文特定类的任何其他数据对象(第一字节从“80”到“BF”)。			

表 4 卡管理能力:第一字节

b8	b7	b6	b5	b4	b3	b2	b1	支持生命周期状态转换的值
—	—	—	—	—	—	—	1	不存在到创建
—	—	—	—	—	—	1	—	创建到初始化
—	—	—	—	—	1	—	—	初始化到操作激活
—	—	—	—	1	—	—	—	创建到操作激活
—	—	—	1	—	—	—	—	不存在到操作激活
—	—	1	—	—	—	—	—	操作激活到操作失活
—	1	—	—	—	—	—	—	操作失活到操作激活
1	—	—	—	—	—	—	—	操作激活到应用删除

表 5 卡管理能力:第二字节

b8	b7	b6	b5	b4	b3	b2	b1	支持生命周期状态转换的值
0	0	0	—	—	—	—	1	创建到应用删除
0	0	0	—	—	—	1	—	初始化到应用删除
0	0	0	—	—	1	—	—	初始化到创建
0	0	0	—	1	—	—	—	操作激活到创建
0	0	0	1	—	—	—	—	操作失活到应用删除
任何其他值保留用于 ISO/IEC JTC 1/SC 17 未来使用。								

6.2 卡管理服务模板获取

获取卡管理服务模板采用 GB/T 16649.4—2010 定义的与应用无关的卡服务。

本条定义的尝试不同获取流程的顺序不在本部分中定义。如果在此描述的所有流程不能返回卡管理服务模板,则卡与本部分不一致。

当选择 MF 或者隐式选择应用 DF 时,可以通过两个流程获取卡管理服务模板:

- 读取 EF.ATR,其中可包含“7F64”数据对象;
- GET DATA 命令,P1-P2 设为“7F 64”,可以在其响应数据字段中返回卡管理服务模板。

另一个流程也可获得:选择 AID 为“E8 28 BD 08 0D”的应用,后跟 P1-P2 设为“7F 64”的 GET DATA 命令,在 GET DATA 的响应数据字段中返回卡管理服务模板。

7 应用管理命令

在选择了卡管理应用和可选的认证程序后,卡应用的管理过程由使用以下三个命令中的一个或者多个产生:

- 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令;
- 加载应用(LOAD APPLICATION)命令;
- 删除应用(REMOVE APPLICATION)命令。

卡管理应用应至少支持前两个命令。

如果卡管理应用支持本条款规定的命令,则应支持至少一个命令选项。

仅当安全状态满足卡管理应用规定的安全条件时,可以执行应用管理命令。

7.1 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令

应用管理请求命令启动应用的管理程序,见表 6。卡管理应用验证命令数据字段中的应用管理请求信息。该命令后面可以跟 7.2 中描述的加载应用命令。如果支持存储资源管理,存储资源分配模板(标记符“7F65”)中描述的应用存储资源分配应与 5.3 中规定的规则一致。

表 6 应用管理请求命令—响应对

CLA	如 GB/T 16649.4—2010 中定义
INS	“40”或“41”
P1	根据表 7 的应用生命周期状态控制
P2	根据表 8 的应用管理控制
Lc 字段	命令数据字段中的字节数
数据字段	卡管理应用(INS=“40”)知道其格式和内容的应用管理请求信息,或在下面的数据对象(INS=“41”)中编码: 目标应用的 AID(标记符“4F”)(必选); 存储资源分配(标记符“7F65”); 一个或者多个数字签名块(标记符“7F3D”),包含数字签名 DO(标记符“9E”)和可能更多的 DO,例如,具有应用的代码散列值(标记符“90”)
Le 字段	编码 N _c =0 时,不存在;编码 N _c >0 时,存在
数据字段	附加信息或不存在
SW1-SW2	见 GB/T 16649.4—2010 的表 5 和表 6 中相关部分,例如“6982”、“6985”
——应用管理请求信息可以包含其他数据对象,例如,发卡者识别号(标记符“42”),文件引用(标记符“51”),或者自由选择的数据(标记符“53”或者“73”)。 ——数字签名块(标记符“7F3D”)的编码超出本部分的范围。	

表 7 P1 中的应用生命周期目标状态控制

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0	0	0	0	未给出信息
0	0	0	0	0	0	1	0	从不存在状态到创建状态的转换
0	0	0	0	0	1	0	0	从创建状态到初始化状态的转换
0	0	0	0	0	1	1	0	从不存在状态到初始化状态的转换
0	0	0	0	1	0	0	0	从初始化状态到操作激活状态的转换
0	0	0	0	1	1	0	0	从创建状态到操作激活状态的转换
0	0	0	0	1	1	1	0	从不存在状态到操作激活状态的转换
任何其他值保留用于 ISO/IEC JTC 1/SC 17 未来使用。								

表 8 P2 中的应用管理控制

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0	0	0	0	未给出信息
0	0	0	0	0	0	0	1	验证应用管理请求
0	0	0	0	0	0	1	0	提交应用管理请求
0	0	0	0	0	0	1	1	验证和提交应用管理请求
任何其他值保留用于 ISO/IEC JTC 1/SC 17 未来使用。								

7.2 加载应用 (LOAD APPLICATION) 命令

加载应用命令将应用传输到卡上,见表 9。应用可以划分为多个部分,每个部分可以划分为多个程序块用于向卡的传输。每个加载应用命令向卡传输一个程序块。该命令之前可以是应用管理请求命令,见 7.1。

如果加载应用命令之前是应用管理请求命令,则存储资源分配通过前面的应用管理请求命令实现。成功执行该系列命令完成在前面的应用管理请求命令中指明的生命周期转换。

如果加载应用命令之前不是应用管理请求命令,则基于加载应用命令系列提供的信息,分配存储资源并将应用生命周期状态设定为适当值。

如果支持存储资源管理,分配给成功创建应用的存储数量应与 5.3 中规定的规则一致。

表 9 加载应用命令—响应对

CLA	如 GB/T 16649.4—2010 中定义
INS	“EA”或“EB”
P1-P2	见表 10
Lc 字段	命令数据字段中的字节数
数据字段	应用组件,卡管理应用 (INS=“EA”)知道其格式和内容,或者编码为单独的数据对象 (INS=“EB”)
Le 字段	编码 $N_e=0$ 时,不存在;编码 $N_e>0$ 时,存在
数据字段	附加信息或不存在
SW1-SW2	见 GB/T 16649.4—2010 的表 5 和表 6 中相关部分,例如“6982”、“6985”

表 10 P1 和 P2 中序列号或偏移量

P1								P2	含 义
b8	b7	b6	b5	b4	b3	b2	b1		
0	0	0	0	0	0	0	0	00	未给出信息
—	×	×	×	×	×	×	×	×	序列号或偏移量
—	0	×	×	×	×	×	×	×	—偏移量
—	1	×	×	×	×	×	×	×	—序列号
0	—	—	—	—	—	—	—	—	更多的块
1	—	—	—	—	—	—	—	—	最后的块
<div>——如果 P1 的 b7 设为 0,则其余的 P1-P2(14 位)编码为从 0 到 16383 的偏移量,如果 P1 的 b7 设为 1,则其余的 P1-P2(14 位)编码为命令的序列号。</div> <div>——如果 P1 的 b8 设为 0,则预计有后续块,如果 P1 的 b8 设为 1,则该命令包含最后的块。</div> <div>——偏移量从应用传输开始以字节计算。</div> <div>——序列号从应用传输开始每个块增加 1。</div>									

7.3 删除应用(REMOVE APPLICATION)命令

删除应用命令删除一个应用并且可能收回分配给该应用的存储资源,见表 11。

当在命令数据字段中存在时,卡管理应用验证应用删除信息。

如果支持存储资源管理,根据 5.3 中规定的规则,成功删除应用应增加卡上应用可使用的存储资源。

表 11 删除应用(REMOVE APPLICATION)命令—响应对

CLA INS P1 P2	如 GB/T 16649.4—2010 中定义 “EC”或“ED” 根据表 12 删除状态控制 “00”未给出信息 (任何其他值保留用于 ISO/IEC JTC 1/SC 17 未来使用)
Lc 字段	不存在或者命令数据字段中的字节数
数据字段	不存在或卡管理应用(INS=“EC”)知道其格式和内容的应用删除信息, 或者在下面的数据对象(INS=“ED”)中编码的应用删除信息: 目标应用的 AID(标记符“4F”)(必选); 一个或者多个数字签名块(标记符“7F3D”),包含数字签名 DO(标记符“9E”)
Le 字段	编码 N _e =0 时,不存在;编码 N _e >0 时,存在
数据字段	附加信息或不存在
SW1-SW2	见 GB/T 16649.4—2010 的表 5 和表 6 中相关部分,例如“6982”、“6985”
<div>——应用删除信息可以包含其他数据对象,例如,自由选择的数据(标记符“53”或“73”)。</div> <div>——数字签名块(标记符“7F3D”)的编码超出本部分的范围。</div>	

表 12 P1 中删除状态控制

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0	0	0	0	未给出信息
0	0	0	0	0	0	0	1	从创建状态到应用删除的转换
0	0	0	0	0	0	1	0	从初始化状态到创建状态的转换
0	0	0	0	0	0	1	1	从初始化状态到应用删除的转换
0	0	0	0	0	1	1	0	从操作(激活或失活)状态到创建状态的转换
0	0	0	0	0	1	1	1	从操作(激活或失活)状态到应用删除的转换
任何其他值保留用于 ISO/IEC JTC 1/SC 17 未来使用。								

7.4 应用管理的考虑

卡管理方案和/或发卡者政策规定了被要求签名的类型和数量,例如:

- 发卡者签名;
- 应用提供者签名;
- 卡管理方案授权签名。

卡应能强制这些策略并且处理相应的签名验证密钥。

发卡者和应用提供者之间的应用管理策略及其实现超出本部分的范围。

附录 A
(资料性附录)
与发卡者和应用提供者无关模型的卡应用管理实例

A.1 引言

本实例示出如何管理与发卡者和应用提供者无关模型的卡的应用。进行以下假定：
——在发卡后，可以由无关的应用提供者添加应用到卡上，该模型在图 A.1 中示出；
——可以通过联网和脱机两种方式发放应用创建证书。
注：下一代 IC 卡系统研究组(NICSS)使用此模型。

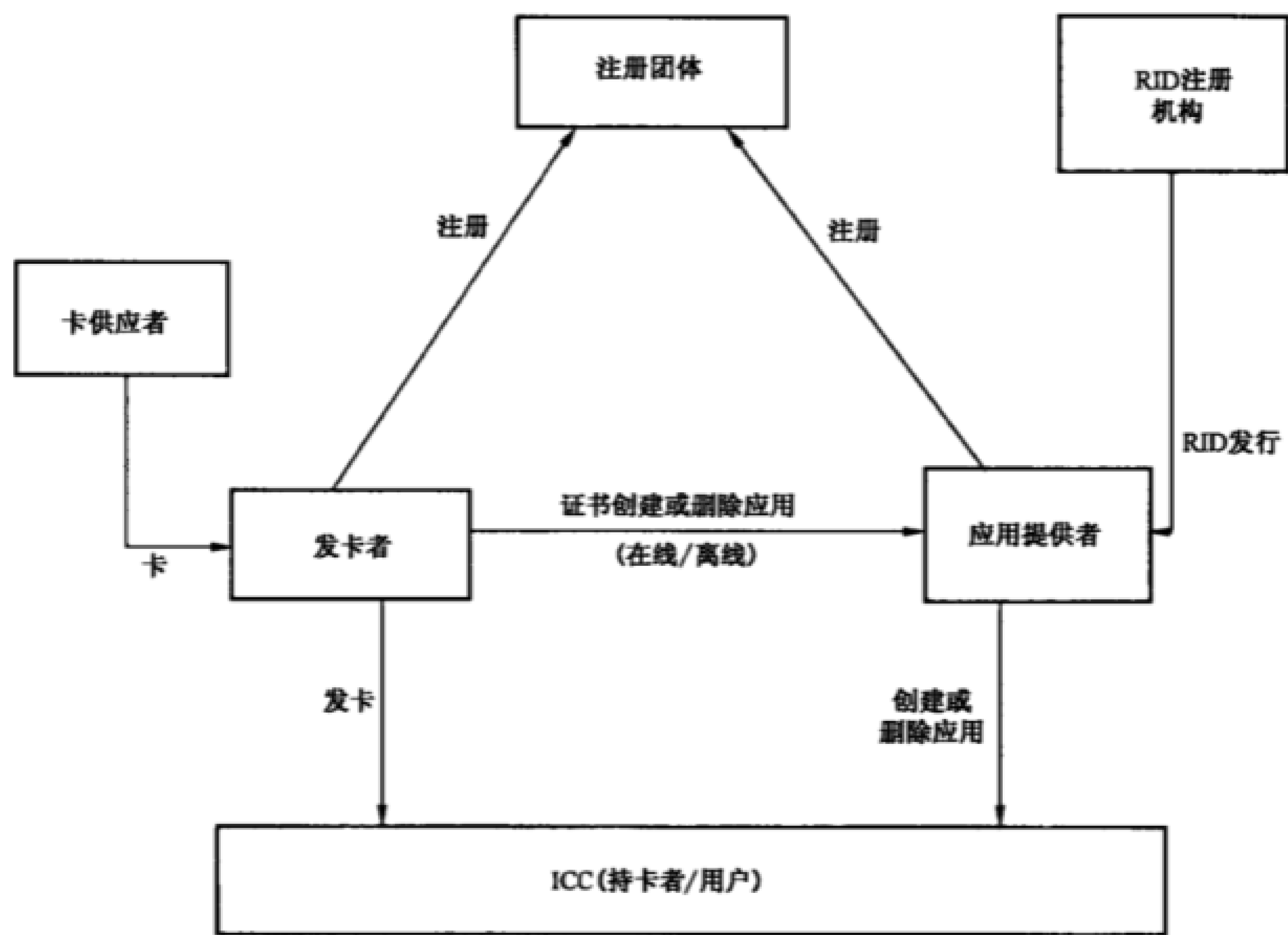


图 A.1 与发卡者和应用提供者无关的模型

A.2 应用管理过程的例子

A.2.1 与 CI（远程 CD）无关的 APR 的例子：加载前验证证书

- a) 用 AID “E8 28 BD 08 0D”选择(SELECT)应用；
- b) 用 GET DATA 获取卡管理服务模板(标记符“7F64”)；
- c) 用卡管理服务模板中指定的 AID(标记符“4F”)选择(SELECT)卡管理应用；
- d) 相互授权；
- e) 从发卡者(在线/离线)获得应用创建证书。该证书可以包含 AID、应用的散列值、核准的 ID、卡 ID 和发卡者的数字签名；
- f) 带证书的 APPLICATION MANAGEMENT REQUEST；

g) 通过 LOAD APPLICATION 加载应用。

A.2.2 远程 CI 的例子:加载后验证证书

- a) 用 AID “E8 28 BD 08 0D”选择(SELECT)应用;
- b) 用 GET DATA 获取卡管理服务模板(标记符“7F64”);
- c) 用卡管理服务模板中指明的 AID(标记符“4F”)选择(SELECT)卡管理应用;
- d) 相互授权;
- e) 从发卡者获得应用创建证书;
- f) 无证书分配给存储的 APPLICATION MANAGEMENT REQUEST;
- g) 通过 LOAD APPLICATION 加载应用;
- h) 带证书的 APPLICATION MANAGEMENT REQUEST。

A.3 删除程序的例子

A.3.1 远程 CI 的例子:删除期间验证证书

- a) 用 AID “E8 28 BD 08 0D”选择(SELECT)应用;
- b) 用 GET DATA 获取卡管理服务模板(标记符“7F64”);
- c) 用卡管理服务模板中指明的 AID(标记符“4F”)选择(SELECT)卡管理应用;
- d) 相互授权;
- e) 从发卡者获得应用删除证书(在线/离线)。该证书可以包含 AID、核准的 ID、卡 ID 和发卡者的数字签名;
- f) 带证书的 REMOVE APPLICATION。

A.3.2 远程 CI 的例子:删除前验证证书

- a) 用 AID “E8 28 BD 08 0D”选择(SELECT)应用;
- b) 用 GET DATA 获取卡管理服务模板(标记符“7F64”);
- c) 用卡管理服务模板中指明的 AID(标记符“4F”)选择(SELECT)卡管理应用;
- d) 相互授权;
- e) 从发卡者获得应用删除证书;
- f) 带证书的 APPLICATION MANAGEMENT REQUEST;
- g) 无证书的 REMOVE APPLICATION。

附录 B
(资料性附录)
卡应用管理的实例

B.1 引言

本实例示出应用创建和激活的两步模型：首先加载应用代码，然后安装和激活应用实例。

注：GlobalPlatform(GP)使用此模型。

应用包括应用代码和应用数据。使用加载对象(Load Object)将应用代码(但不是应用数据)加载到卡上。应用的安装从加载对象和可能的一些应用数据创建实例。

在此实例中，创建和激活应用另外需要：

- 卡应用管理系统(CAMS)的预先认证；
- 通过安全信息保护命令及响应；
- 验证发卡者的证书。

B.2 用于应用管理的命令

B.2.1 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令

发送应用管理请求命令来启动和执行各种步骤，这些步骤是加载一个加载对象以及安装和激活应用实例所必需的，见表 B.1。

表 B.1 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义
INS	“40”
P1	应用生命周期目标状态控制：见表 B.2
P2	应用管理控制：见表 B.3
Lc 字段	命令数据字段中的字节数
数据字段	应用管理请求信息
Le 字段	编码 $N_c=0$ 时，不存在；编码 $N_c>0$ 时，存在
数据字段	不存在或应用管理确认信息
SW1-SW2	见 GB/T 16649.4—2010 的表 5 和表 6 中相关部分，例如“6982”、“6985”

应用管理请求命令的参数 P1 描述了命令的作用并且根据表 B.2 编码。

表 B.2 P1 中的应用生命周期目标状态控制

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	1	1	0	0	从创建状态到操作激活状态的转换
0	0	0	0	1	0	0	0	从初始化状态到操作激活状态的转换
0	0	0	0	0	1	0	0	从创建状态到初始化状态的转换
0	0	0	0	0	0	1	0	从不存在状态到创建状态的转换
×	×	×	×	—	—	—	—	RFU

b4=1 表示激活命令数据字段中标识的应用。这适用于仅创建(目前的生命周期状态=创建)或者已经初始化(目前的生命周期状态=初始化)的应用。

b3=1 表示命令数据字段中标识的应用的初始化(目前的生命周期状态=创建)。

b2=1 表示命令数据字段中标识的应用的创建(目前的生命周期状态=不存在)。

表 B.3 P2 中的应用管理控制

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0	0	0	1	验证应用管理请求
0	0	0	0	0	0	1	1	验证和提交应用管理请求

在本实例中,应用管理请求命令发送两次。

——参数 P1 中的 b2=1,P2 设为“01”,以启动对应用代码的加载(加载对象)。命令数据字段包含加载对象标识、应用提供者标识、加载对象存储资源分配信息、加载对象散列和发卡者发行的应用创建证书。在响应消息中不返回响应数据字段。紧跟一个或者多个 LOAD APPLICATION 命令。成功执行最后一个 LOAD APPLICATION 命令时,创建应用管理请求隐含提交,并且应用生命周期状态设为创建。

——参数 P1 中的 b4=1 同时 b3=1,P2 设为“03”,来同时安装和激活应用实例。命令数据字段包含已经加载的加载对象标识、应用实例标识、应用实例的存储资源分配信息和发卡者发行的应用初始化和激活证书。成功执行命令时,应用生命周期状态从创建转换到操作激活。在响应消息中可能返回响应数据字段。当存在时,响应数据字段的内容包含长度(根据 GB/T 16263.1—2006 中规定的 ASN.1 规则进行编码)及应用初始化和激活确认的值。

B.2.2 加载应用(LOAD APPLICATION)命令

加载对象分为多个块:用于传输到卡的加载块。加载应用命令启动向卡传输的加载块,见表 B.4。可以请求多个加载应用命令向卡传输加载对象。

表 B.4 加载应用(LOAD APPLICATION)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义
INS	“EA”
P1	加载块序列号的最高有效字节,见表 B.5
P2	加载块序列号的最低有效字节,见表 B.6
Lc 字段	命令数据字段中的字节数
数据字段	加载块
Le 字段	编码 $N_c=0$ 时,不存在;编码 $N_c>0$ 时,存在
数据字段	不存在或应用创建确认信息
SW1-SW2	见 GB/T 16649.4—2010 的表 5 和表 6 中相关部分,例如“6581”、“6A84”

加载应用命令的参数 P1 和 P2 描述了加载块的顺序并根据表 B.5 和表 B.6 编码。

表 B.5 P1 中的序列号最高有效字节

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	1	×	×	×	×	×	×	更多块,序列号最高有效字节
1	1	×	×	×	×	×	×	最后一个块,序列号最高有效字节

- b8=0 表示预计有更多加载块。
- b8=1 表示序列中的最后的加载块。
- b7=1 表示从 0 到 16383 的第 14 位编码的加载块序列号。

表 B.6 P2 中的序列号最低有效字节

b8	b7	b6	b5	b4	b3	b2	b1	含 义
×	×	×	×	×	×	×	×	序列号最低有效字节位

第一个 LOAD APPLICATION 命令之前是用于创建命令的 APPLICATION MANAGEMENT REQUEST(P1 的 b2 设为 1)。

加载块序列号(P1-P2 的低 14 位)从 0 开始。加载块编号严格按照顺序并且递增 1。卡收到加载对象最后块的通知(LOAD APPLICATION 命令中 P1 的 b8 设为 1)。

响应数据字段可以在响应消息中返回。当存在时,响应数据字段的内容包括长度(根据 GB/T 16263.1—2006 中规定的 ASN.1 规则进行编码)及应用创建确认值。它仅存在于传输最后加载块(P1 的 b8 设为 1)的 LOAD APPLICATION 命令的响应数据字段中。

对于除了传输最后加载块(P1 的 b8 设为 1)的最后 LOAD APPLICATION 命令之外的 LOAD APPLICATION 命令,没有响应数据字段。

B.3 应用管理序列

- 该模型中用于创建和激活应用的典型应用管理序列如下：
- a) 用 AID “E8 28 BD 08 0D”选择(SELECT)应用；
 - b) 用 GET DATA 获取卡管理服务模板(标记符“7F64”)；
 - c) 用卡管理服务模板中指明的 AID(标记符“4F”)选择(SELECT)卡管理应用；
 - d) 用于创建的 APPLICATION MANAGEMENT REQUEST,其中 P1=“02”和 P2=“01”；
 - e) 第一个 LOAD APPLICATION,其中 P1=“40”和 P2=“00”；
 - f) 多个 LOAD APPLICATION 命令,其中顺序增加 P1-P2；
 - g) 最后的 LOAD APPLICATION,其中 P1=“Cx”和 P2=“yz”,“xyz”是最后加载块的序列号(假设“xyz”小于 4095)；
 - h) 用于初始化和激活的 APPLICATION MANAGEMENT REQUEST,其中 P1=“0C”和 P2=“03”。

附录 C
(资料性附录)
卡应用管理的更多实例

C.1 引言

本实例示出应用创建和激活的三步模型：分配卡资源、加载应用代码和数据以及进行操作激活。
注：MULTOS 使用本模型。

最初的应用管理请求命令确保卡资源可用，并准备好该卡对后续卡内容管理的请求。然后用加载应用命令将应用加载到卡。应用包括应用代码和应用数据、默认的文件控制信息、目录文件输入、数字签名和密钥转换单元。所有都作为应用加载单元加载到卡上。第二和最后的应用管理请求命令最后确定应用创建和激活过程，包括检查应用加载单元的发卡者授权和应用服务提供者的数字签名。

C.2 用于应用管理的命令

C.2.1 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令

发送应用管理请求命令来启动和最后确定应用加载过程，见表 C.1。

表 C.1 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义
INS	“40”
P1	应用管理请求的作用：见表 C.2
P2	应用管理请求的作用：见表 C.3
Lc 字段	命令数据字段中的字节数
数据字段	应用加载证书
Le 字段	编码 $N_c=0$ 时，不存在；编码 $N_c>0$ 时，存在
数据字段	不存在或卡公钥证书
SW1-SW2	见 GB/T 16649.4—2010 的表 5 和表 6 中相关部分，例如“6982”、“6985”

应用管理请求命令的参数 P1 描述了命令的目的并根据表 C.2 编码。

表 C.2 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令中 P1 的编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	1	1	1	0	从不存在状态到操作激活状态的转换

应用管理请求命令的参数 P2 描述了命令的目的并根据表 C.3 编码。

表 C.3 应用管理请求(APPLICATION MANAGEMENT REQUEST)命令的 P2 编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	1	验证应用管理请求
0	0	0	0	0	0	1	1	验证和提交应用管理请求

C.2.2 加载应用(LOAD APPLICATION)命令

应用加载单元分为用于向卡传输的更小的组件,见表 C.4。加载应用命令启动该组件向卡传输。可以使用多个加载应用命令向卡传输应用加载单元。

表 C.4 加载应用(LOAD APPLICATION)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义
INS	“EA”
P1	加载块序列号最高有效字节,见表 C.5
P2	加载块序列号最低有效字节,见表 C.6
Lc 字段	命令数据字段中的字节数
数据字段	加载块
Le 字段	编码 $N_c=0$ 时,不存在;编码 $N_c>0$ 时,存在
数据字段	不存在
SW1-SW2	见 GB/T 16649.4—2010 的表 5 和表 6 中相关部分,例如“6581”、“6A84”

加载应用命令的参数 P1 和 P2 描述了组件序列号,并根据表 C.5 和表 C.6 编码。

表 C.5 加载应用(LOAD APPLICATION)命令的 P1 编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	1	×	×	×	×	×	×	更多块,序列号最高有效字节
1	1	×	×	×	×	×	×	最后块,序列号最高有效字节

- b8=0 表示预计有更多加载块。
- b8=1 表示序列中的最后加载块。
- b7=1 表示从 0 到 16383,14 位上编码的加载块序列号。

表 C.6 加载应用(LOAD APPLICATION)命令的 P2 编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
×	×	×	×	×	×	×	×	序列号最低有效字节

第一个加载应用命令之前是应用管理请求命令。
加载块序列号(P1-P2 的低 14 位)从 0 开始。加载块编号严格按照顺序并且递增 1。卡收到加载对象最后块的通知(P1 的 b8 设为 1)。

C.3 应用管理序列

该模型中用于创建和激活应用的典型应用管理序列如下：

- a) 用 AID “E8 28 BD 08 0D”选择(SELECT)应用；
- b) 用 GET DATA 获取卡管理服务模板(标记符“7F64”)；
- c) 选择(SELECT)卡管理应用；
- d) 用于操作激活请求验证的 APPLICATION MANAGEMENT REQUEST,其中 P1=“0E”和 P2=“01”；
- e) 第一个 LOAD APPLICATION,其中 P1=“40”和 P2=“00”；
- f) 多个 LOAD APPLICATION 命令,其中顺序增加 P1-P2；
- g) 最后的 LOAD APPLICATION,其中 P1=“Cx”和 P2=“yz”,“xyz”是最后加载块的序列号；
- h) 用于操作激活的 APPLICATION MANAGEMENT REQUEST,其中 P1=“0E”和 P2=“03”。

附录 D
(资料性附录)
卡应用管理的更多实例

本实例示出了作为应用安装命令包的 LOAD APPLICATION 命令的使用,见表 D.1~表 D.4。其允许通过 LOAD APPLICATION 命令的单个接入规则控制整个加载顺序。例如,需要具有安全消息密钥协议的外部认证。该认证过程可以通过卡应用管理系统(CAMS)执行。

- 注 1: 命令顺序可以与安全消息一同发送。
注 2: 将命令数据字段中待执行的命令进行编码而没有安全消息。

表 D.1 加载应用(LOAD APPLICATION)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义,第 5 位设为 1 表示该命令不是系列命令的最后一个
INS	“EB”
P1-P2	“0000”
Lc 字段	命令数据字段中的字节数
数据字段	待执行命令(标记符“52”): “52”-L-...[创建文件 CREATE FILE(DF)命令]
Le 字段	不存在
数据字段	不存在
SW1-SW2	“9000”或者特定状态位

表 D.2 加载应用(LOAD APPLICATION)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义,第 5 位设为 1 表示该命令不是系列命令的最后一个
INS	“EB”
P1-P2	“0000”
Lc 字段	命令数据字段中的字节数
数据字段	待执行命令(标记符“52”): “52”-L-...[创建文件(CREATE FILE)(EF)命令]
Le 字段	不存在
数据字段	不存在
SW1-SW2	“9000”或者特定状态位

表 D.3 加载应用(Load Application)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义，第 5 位设为 1 表示该命令不是系列命令的最后一个
INS	“EB”
P1-P2	“0000”
Lc 字段	命令数据字段中的字节数
数据字段	待执行命令(标记符“52”)： “52”-L-…[更新二进位(UPDATE BINARY)命令]
Le 字段	不存在
数据字段	不存在
SW1-SW2	“9000”或者特定状态位

表 D.4 加载应用(Load Application)命令—响应对

CLA	如 GB/T 16649.4—2010 中定义，第 5 位设为 1 表示该命令不是系列命令的最后一个
INS	“EB”
P1-P2	“0000”
Lc 字段	命令数据字段中的字节数
数据字段	待执行命令(标记符“52”)： “52”-L-…[激活文件(ACTIVATE FILE)(DF)命令]
Le 字段	不存在
数据字段	不存在
SW1-SW2	“9000”或者特定状态位

参 考 文 献

- [1] GB/T 16649(所有部分) 识别卡 集成电路卡
 - [2] Global Platform Card specification V2. 1. 1 或更高版本, <http://www.globalplatform.org/>
 - [3] NICSS Prerequisites Version 1. 20, 下一代 IC 卡系统研究组, 2001 年 4 月 24 日, <http://www.nicss.or.jp/>
 - [4] 装载和删除应用指南, MAO-DOC-REF-008, MAOSCO, <http://www.multos.com/>
 - [5] 生成应用装载单元指南, MAO-DOC-REF-009, MAOSCO, <http://www.multos.com/>
-

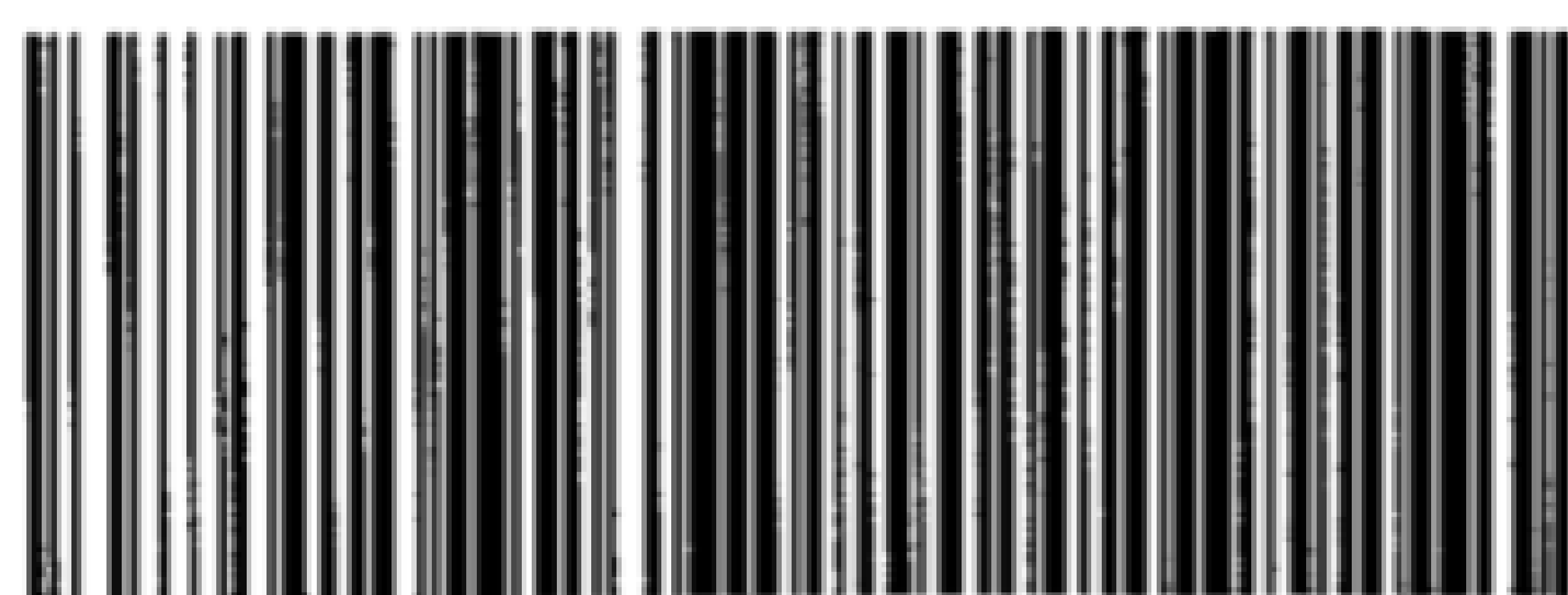
中 华 人 民 共 和 国
国 家 标 准
识别卡 集成电路卡 第 13 部分：在多
应用环境中的应用管理命令
GB/T 16649.13—2013/ISO/IEC 7816-13:2007

*
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 1.75 字数 42 千字
2014 年 3 月第一版 2014 年 3 月第一次印刷

*
书号: 155066 • 1-47931 定价 27.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GB/T 16649.13-2013