ICS 35.240.60
P 07

中华人民共和国国家标准

GB/T 33242—2016

数字城市智能卡应用技术要求

Technical requirements for application of smart card in digital cities

2016-12-13 发布　　2017-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中华人民共和国住房和城乡建设部提出。

本标准由全国智能建筑及居住区数字化标准化技术委员会(SAC/TC 426)归口。

本标准起草单位:住房和城乡建设部 IC 卡应用服务中心、中外建设信息有限责任公司、深圳德诚信用咭制造有限公司、深圳市华旭科技开发有限公司、天津市通卡公用网络系统有限公司、深圳市德卡科技有限公司、深圳市旺龙智能科技有限公司、东信和平科技股份有限公司、北京亿速码数据处理有限责任公司、上海华虹集成电路有限责任公司、上海复旦微电子集团股份有限公司、聚辰半导体(上海)有限公司、航天信息股份有限公司、广东楚天龙智能卡有限公司、上海浦江智能卡系统有限公司、中山达华智能科技股份有限公司、山东华冠智能卡有限公司、天津环球磁卡股份有限公司、福建索天信息科技股份有限公司、新开普电子股份有限公司、陕西煤航安全印务有限公司、福州兆科智能卡有限公司、江西省洪城一卡通投资有限公司、西安城市一卡通有限责任公司、国网电力科学研究院通信与用电技术分公司。

本标准主要起草人:王辉、马虹、申绯斐、张永刚、徐科、周欣、苑朋朋、尚治宇、殷骏、尚小航、马健、范琳琳、周斌、徐睿、陈勇、周亮、王晓雨、李标彬、王小军、李强、孙旭、朱伟平、徐钦鸿、娄亚华、刘振禹、蔡文成、林晟、张振京、何庆卿、陈为明、涂勇涛、吕岩巍、申德周。

数字城市智能卡应用技术要求

1 范围

本标准规定了数字城市智能卡卡片(以下简称“卡片”)体系架构、生命周期模型、通用平台(GP)运行环境、安全域、卡片和应用管理、安全通信、应用协议数据单元(APDU)命令和相应的定义、符号等。

本标准适用于智能卡的设计、制造、管理、发行和应用等领域。

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 16649.4 识别卡 带触点的集成电路卡 第4部分:用于交换的行业间命令

GB/T 16649.6—2001 识别卡 带触点的集成电路卡 第6部分:行业间数据元

ISO/IEC 7812 识别卡 发行方识别(Identification cards—Identification of issuers)

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字城市智能卡 smart card in digital cities

可承载多应用的开放式平台,带有中央处理器、存储单元(包括随机存储器、程序存储器、用户数据存储器)、芯片操作系统。

3.2

基本逻辑通道 basic logical channel

卡片和卡外实体之间的永久性接口,其编号为0。

3.3

卡片会话 card session

卡片与卡外建立的某种通信链路。

注1:接触式卡片开始于卡片复位或者卡片上电,结束于卡片其后再次复位或者卡片下电。

注2:非接触式卡片开始于卡片激活或者卡片上电,结束于卡片释放或者卡片下电。

3.4

当前安全级别 current security level

在根据安全通信协议进行安全消息传送时,应用于当前命令/响应的安全级别。

3.5

数据鉴权模式块 DAP block

加载文件中用来验证加载文件数据块的部分。

3.6

数据鉴权验证 DAP verification

安全域对加载文件数据块的可信性进行验证的机制。

3.7

委托管理　delegated management

由经过认证的应用提供方对卡片内容进行预先授权的改变。

3.8

数字签名　digital signature

一种特殊的加密算法，数据接收者能够借此确认数据的来源和完整性，避免数据被第三方篡改，数据发送者也可以借此确保数据不会被接收者篡改。

3.9

可执行加载文件　executable load file

实际存在于卡片上的包含一个或多个应用的可执行代码包（可执行模块），它既可以驻留在只读存储器中，也可以作为加载文件数据块的映像在可变存储器中生成。

3.10

可执行模块　executable module

可执行加载文件中包含的一个单独应用的可执行代码。

3.11

主机　host

支持本文件功能实现的后台系统。

注：主机执行的功能包括授权与认证、管理、发布后的应用代码与数据下载、事务处理等。

3.12

主控安全域　issuer security domain

发卡方安全域

对卡片管理者（通常是发卡方）的控制、安全、通信需求进行支持的卡片首要空间单元。

3.13

生命周期　life cycle

卡片内容的不同存在阶段，也可以指卡片本身不同的存在阶段。

3.14

生命周期状态　life cycle state

卡片或卡片内容在生命周期中的某个特定状态。

3.15

加载文件　load file

传送加载到符合卡片上的文件，该卡片包含了加载文件数据块，并有可能包含一个或者多个数据鉴权模式块。

3.16

加载文件数据块　load file data block

加载文件中包含一个或多个应用（或库），以及平台所需应用支持信息的部分。

3.17

加载文件数据块散列值　load file data block hash

加载文件数据块经由哈希函数计算出的散列值，用于确保加载文件数据块的一致性。

3.18

可变存储器　mutable persistent memory

可以对其存储的内容进行改写的存储器。

3.19

收条 receipt

卡片根据发卡方要求出具的一个加密值，用来作为一个委托管理操作已经发生的证据。

3.20

运行环境 runtime environment

卡片运行期间的核心功能，为卡上的多个应用运行提供了一个安全的环境。

3.21

安全通道 secure channel

为一个卡外实体或者卡外和卡片之间的信息交换提供某种安全保障的通信机制。

3.22

安全通道协议 secure channel protocol

安全通信协议和相关安全服务的统称。

3.23

安全通道会话 secure channel session

在应用会话期间建立的另外一种会话机制，开始于安全通道的初始化，结束于安全通道的终结或者应用会话或卡片会话的终结。

3.24

安全域 security domain

负责对某个卡外实体(例如发卡方、应用提供方、授权管理者)的控制、安全、通信需求进行支持的卡内空间区域。

3.25

会话安全级别 session security level

在进行安全消息交换的安全通信协议中，用于确保命令安全所需的最低安全级别，在安全通道会话初始化时以特指或默认的方式建立。

3.26

辅助逻辑通道 supplementary logical channel

补充逻辑通道

卡片和卡外实体之间除了基本逻辑通道之外的其他接口，最多可有19个，辅助逻辑通道的编号在1和19之间，且编号不可重复。

3.27

辅助安全域 supplementary security domain

补充安全域

主控安全域之外的其他安全域。

3.28

令牌 token

发卡方出具的一个加密值，用来作为一个委托管理操作已经被授权的证据。

4 缩略语

下列缩略语适用于本文件。

AID：应用程序标识符(Application Identifier)

AP：应用提供方(Application Provider)

APDU：应用协议数据单元(Application Protocol Data Unit)

API:应用程序接口(Application Programming Interface)
CA:授权管理(Controlling Authority)
CBC:密码块链(Cipher Block Chaining)
CC:密码校验码(Cryptographic Checksum)
CCT:加密校验模板(Cryptographic Checksum Template)
CIN:卡片映像编号(Card Image Number / Card Identification Number)
CL:非接触式(Contactless)
CLF:非接触式前端接口(Contactless Front-end interface)
CPL:命令包长度(Command Packet Length)
CREL:非接触式注册事件监听(Contactless Registry Event Listener)
CRS:非接触式注册服务(Contactless Registry Services)
CT:保密模板(Confidential Template)
CVM:卡持有者身份验证方法(Cardholder Verification Method)
DAP:数据鉴权模式(Data Authentication Pattern)
DGI:数据分组索引(Data Group Index)
DS:数字签名(Digital Signature)
GP:通用平台(Global Platform)
IIN:发卡方标识编号(Issuer Identification Number)
ISD:发卡方安全域(Security Domain of the Issuer)
MAC:消息认证码(Message Authentication Code)
NFC:近场通信(Near Field Communication)
OCE:卡外实体(Off-Card Entity)
PK:非对称密钥对中的公钥(Public Key of an asymmetric key pair)
RAM:远程应用管理(Remote Applet Management)
RTE:运行环境(Runtime Environment)
R-MAC:MAC 响应值(Response MAC)
SD:安全域(Security Domain)
SIN:安全域提供方标识编号(Security Identification Number)
TLV:标签、长度、值(Tag, Length, Value)

5 卡片体系架构

5.1 技术架构

智能卡应以多应用为目标,引入虚拟机、GP 运行环境等多类应用的运行环境构成跨领域业务平台,实现多个维度的“一卡多应用”,并完成政府与公共事业、通信、金融等多类应用并存的业务需求。智能卡运行平台技术架构见图 1。

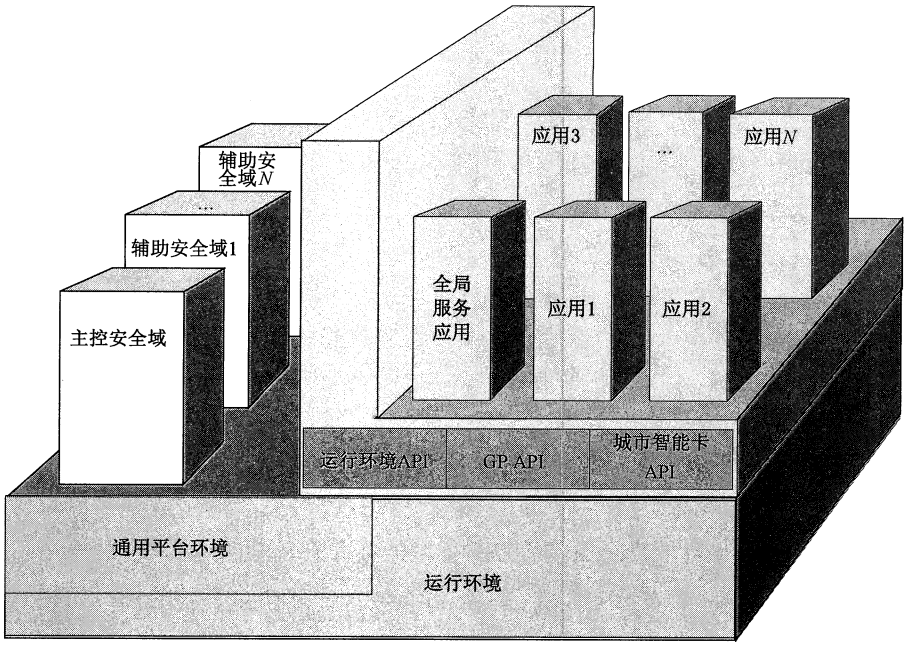


图 1 智能卡运行平台技术架构图

5.2 安全域

5.2.1 分类要求

依据卡外实体的不同授权，安全域应包含以下三类：

a) 主控安全域；

b) 辅助安全域；

c) 授权管理者安全域。

5.2.2 功能要求

安全域应提供至少下列安全服务：

a) 密钥管理；

b) 加密解密；

c) 数字签名的生成与验证。

5.3 GP 环境

5.3.1 功能要求

GP 环境的主要功能应包括向应用提供 API、指令分发、应用选择、逻辑通道管理、卡片内容管理、应用代码的加载和存储器管理。

5.3.2 注册表

GP 环境可使用一个内部的 GP 注册表作为卡片内容管理的信息源。该 GP 注册表应包含卡片、可执行加载文件、应用、关联安全域和权限等内容的信息。

5.4 全局服务应用

卡上可存在若干全局服务应用向卡片的其他应用提供服务。

5.5 卡片内容

5.5.1 存在方式

卡片内容应以可执行加载文件的形式存在，包括以下存在方式：

a) 只读存储器：内容是在卡片制造阶段加载的，除了禁用操作外，不能对其做任何修改；

b) 可变存储器：内容是卡片个人化前和卡片个人化后都可被加载或删除的。

5.5.2 卡片内容关系

当安装应用时，可变存储器应生成一个应用，包含可执行模块或者应用数据。所有的应用及其相关数据在安全条件下可被删除。当可执行模块存在时，卡片内容关系见图 2。

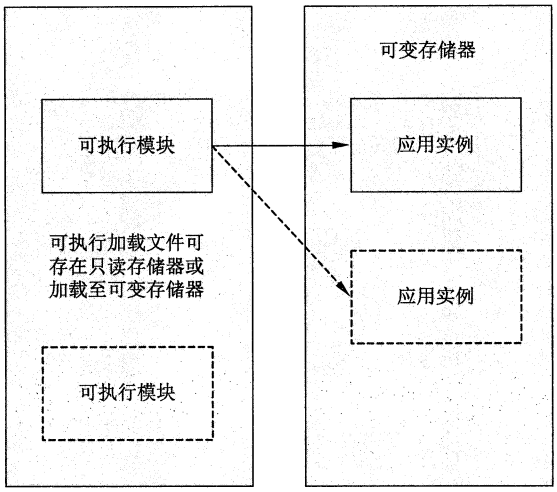


图 2 卡片内容关系图

5.6 智能卡 API

智能卡可向上层应用提供运行环境 API、GP API、支持国密算法的 API、支持获取安全认证识别码的 API 等。安全认证识别码应与智能卡应用一起下载到安全域中。智能卡 API 在卡片逻辑架构中所处的层次，见图 3。智能卡逻辑架构应包括：

a) 硬件层是指芯片硬件，包括密码算法协处理；

b) 驱动层包括各硬件接口驱动，以及和密码算法协处理器配套的算法库；

c) 片上操作系统层是支持多应用运行环境的片上操作系统，向应用层提供各种 API 接口；

d) 应用层包括各种用户应用。

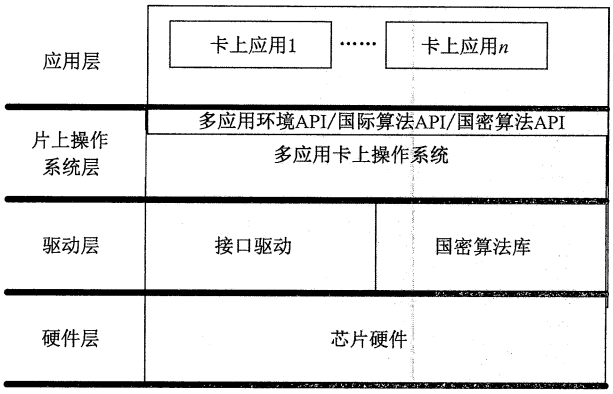


图 3　智能卡逻辑架构

6　生命周期模型

6.1　卡片生命周期

6.1.1　管理要求

GP 环境应负责维护卡片及其内容的安全及管理。GP 环境的生命周期应等同于卡片的生命周期。从 GP 的角度看，卡片生命周期应开始于 GP 的准备状态，结束于终结状态。

6.1.2　卡片生命周期状态

6.1.2.1　准备状态

6.1.2.1.1　卡内实体

卡片处于准备状态时，运行环境应就位，主控安全域作为已经被选择的应用，应做好接收、处理、响应 APDU 命令的准备。当卡片处于准备状态时，应符合以下要求：

a）　运行环境应完成执行的准备；

b）　GP 环境应完成执行的准备；

c）　对于所有的卡片界面，主控安全域应处于隐式已选择状态；

d）　驻留在只读存储器中的可执行加载文件应已注册至 GP 注册表；

e）　主控安全域中应具有可用的初始密钥。

6.1.2.1.2　卡外实体

卡外实体可在卡片处于准备状态时执行以下操作：

a）　加载或安装辅助安全域；

b）　安装辅助安全域密钥。

6.1.2.2　初始化状态

初始化状态应表明某些初始化信息（如主控安全域的密钥及数据）已载入到卡片上，此时卡片不应发行给持卡人。从准备状态到初始化状态的迁移应是不可逆的。

6.1.2.3 安全状态

安全状态在卡片生命周期中应是发卡个人化结束后的一个状态，并应符合以下要求：

a) 安全域和应用可利用此状态执行安全策略；

b) 从初始化状态到安全状态的迁移应是不可逆的；

c) 主控安全域应包含所必需的密钥及满足完备功能的安全因素。

6.1.2.4 锁定状态

锁定状态不应对卡片上的安全域和应用进行选择，并应符合以下要求：

a) 从安全状态到卡锁定状态的迁移应是可逆的；

b) 只有具备“最后应用权限”的应用才可在此状态下被选中；

c) 对卡片内容的任何改变应是不允许的；

d) GP 环境本身及具备“卡片锁定权限”的安全域或应用，可启动从安全到锁定状态的迁移。

6.1.2.5 终结状态

终结状态应是卡片生命周期的结束，并应符合以下要求：

a) 从任何其他状态到终结状态的迁移都应是不可逆的；

b) 当发现卡片遭受严重威胁或者已经过期时，某个应用可在逻辑意义上“销毁”卡片，并应符合以下要求：

   1) 如果此时某个安全域具备“最终应用权限”，则只有 GET DATA 命令应被处理，其他命令都应被禁止，且返回为一个错误；

   2) 如果此时某个应用具备“最终应用权限”，则其对命令的处理策略应由发卡方定义。

c) GP 环境本身及具备“卡片终结权限”的安全域或应用，可启动从任何其他状态到终结状态的迁移。

6.1.3 卡片生命周期状态的迁移

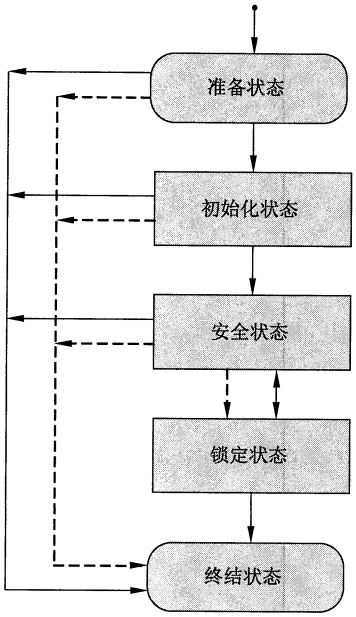
卡片生命周期状态迁移，见图 4。并应符合以下要求：

a) 准备状态和初始化状态应适用于卡片生命周期中的个人化结束前阶段；

b) 安全状态、锁定状态和终结状态应适用于个人化结束后的阶段；

c) 在卡片生命周期的任何时刻可使卡片进入终结状态；

d) 状态迁移可出现反向迁移或状态跳跃。



图例：
具有特权的安全域———
特权应用 - - - -

图 4 卡片生命周期状态迁移

6.2 可执行加载文件/可执行模块生命周期

6.2.1 可执行加载文件生命周期

6.2.1.1 状态

可执行加载文件的生命周期应只有已加载一个状态，并应符合以下要求：

a) GP 环境应确定卡上所有可执行加载文件都处在已加载状态；
b) 通过加载过程成功载入卡片后生成的可执行加载文件，应注册为 GP 注册表中的一个条目；
c) 只读存储器中的可执行加载文件应自动注册为 GP 注册表的条目，且从注册时起就关联到主控安全域。

6.2.1.2 文件删除

GP 环境收到删除可执行加载文件的请求后，应符合以下要求：

a) 回收可执行加载文件驻留的存储器空间，并重新利用，GP 注册表中该可执行加载文件及其包含的每个可执行模块对应的条目应设为不可访问；
b) GP 环境无需对已删除的可执行加载文件或可执行模块保留其曾经存在过的记录；
c) 当删除请求同时要求对可执行加载文件中的可执行模块下的应用也进行删除时，每个被删除应用的要求见 6.3.2.5 或 6.3.4.6。

6.2.2 可执行模块生命周期

可执行模块的生命周期应与可执行加载文件的生命周期一致。

6.3 应用与安全域生命周期

6.3.1 管理要求

应用或安全域的生命周期应从可执行模块实例化成功开始，其生命周期反映了 GP 环境管理的状态和自身管理的状态，并应符合下列要求：

a) 在应用或安全域安装过程中，应用注册为 GP 注册表的条目，其生命周期状态应被 GP 环境设置为已安装；当安装过程中收到了选择该应用的请求，且该应用是可选择的，则 GP 环境应将该应用的生命周期状态设为可选择；

b) 当应用或安全域是可选择的，则开始管理其自身的生命周期，生命周期状态的迁移应由应用或安全域定义；

c) 在应用或安全域生命周期的任何时刻，GP 环境都可将应用或安全域的生命周期状态设置为已锁定，并应具有从卡片上删除应用的能力。

6.3.2 应用生命周期状态

6.3.2.1 状态分类

应用生命周期状态应包括：

a) 已安装状态；

b) 可选择状态；

c) 已锁定状态。

6.3.2.2 已安装状态

当应用处于已安装状态时，应用的可执行代码应已正确链接，并完成了所有必需的存储器分配。该应用在卡片注册表中应注册为一个条目，经过与该应用关联的安全域认证后的卡外实体可对该条目进行访问，该应用此时应不能被选择。安装过程无需与应用个人化相关，个人化操作可单独完成。

6.3.2.3 可选择状态

当应用处于可选择状态时，可接收来自卡外实体的命令。从已安装状态到可选择状态的迁移应是不可逆的。在设置为可选择状态前，应用应已经正确安装且功能正常。应用的生命周期从已安装状态迁移到可选择状态，可同应用的安装一起进行。

6.3.2.4 已锁定状态

已锁定状态应符合下列要求：

a) GP 环境、应用及其关联的安全域、具备“全局锁定权限”的应用及安全域，都可利用已锁定状态作为安全管控的手段，以阻止该应用的选定与执行；

b) 当卡外实体受到安全的原因，需要将卡上的某个特定应用进行锁定，可借助 GP 环境来启动应用生命周期状态的迁移；

c) 当处于已锁定状态，只有与应用关联的安全域、具备“全局锁定权限”的应用及安全域，才可对应用进行解锁。GP 环境应确保应用生命周期能够恢复到锁定前的状态。

6.3.2.5 应用删除

GP 环境可在应用生命周期的任何时刻，收到删除某个应用的请求。被删除应用的存储器空间应被回收并可供重新利用，GP 注册表中该应用对应的条目应设为不可访问，GP 环境也无需对已删除的

应用保留其存在记录。

6.3.3 应用自定义的生命周期状态

GP 环境不应对应用自定义的生命周期状态之间的迁移进行任何控制。

6.3.4 安全域生命周期状态

6.3.4.1 状态分类

安全域生命周期状态如下：

a) 已安装状态；
b) 可选择状态；
c) 已个人化状态；
d) 已锁定状态。

6.3.4.2 已安装状态

当安全域处于已安装状态时，该安全域应注册为 GP 注册表中的一个条目，经过关联的安全域认证后的卡外实体可对该条目进行访问。该状态下安全域应不能被选择，且该安全域不能与可执行加载文件或应用相关联，应用不可使用该安全域提供的安全域服务。

6.3.4.3 可选择状态

安全域处于可选择状态时，该安全域可接收来自卡外实体的命令(特别是个人化命令)。安全域不可与可执行加载文件或应用关联，应用不可使用该安全域提供的安全域服务。从已安装状态到可选择状态的迁移应是不可逆的，安全域的生命周期从已安装状态迁移到可选择状态，可与安全域的安装一起进行。

6.3.4.4 已个人化状态

安全域应确定迁移到已个人化状态需要的操作。该状态下的安全域应拥有所有的个人化数据和密钥，并可同应用相关联，使其能向关联的应用提供服务。从可选择状态到已个人化状态的迁移应是不可逆的。

6.3.4.5 已锁定状态

已锁定状态应符合下列要求：

a) GP 环境、安全域及其关联的其他安全域、具备“全局锁定权限”的应用及安全域，都可利用已锁定状态作为安全管控的手段，以阻止该安全域的选定；
b) 当卡外实体受到安全威胁时，可通过 GP 环境来启动安全域生命周期状态的迁移，将卡上的某个特定安全域应用进行锁定；
c) 当安全域处于已锁定状态时，应拒绝所有接收到的命令；
d) 当安全域处于已锁定状态时，只有与该安全域关联的其他安全域、具备“全局锁定权限”的应用及安全域，才可对安全域进行解锁。GP 环境应确保安全域生命周期能够恢复到锁定前的状态。

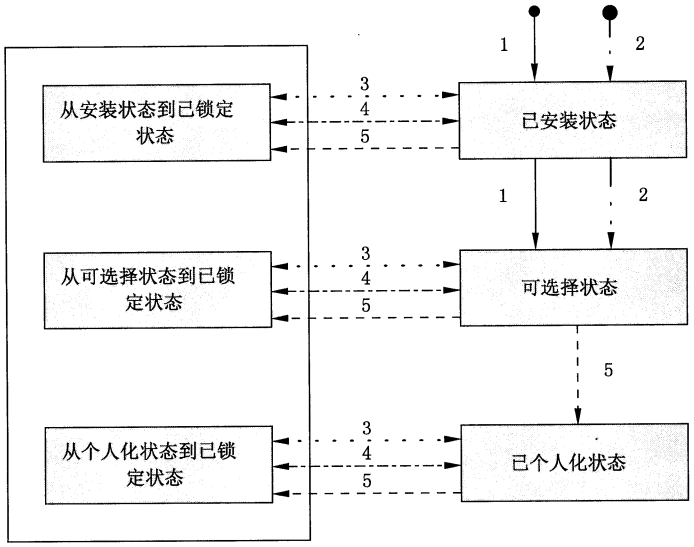
6.3.4.6 安全域删除

GP 环境可在安全域生命周期的任何时刻，收到删除某个安全域的请求。被删除安全域的存储器

空间应被回收并可供重新利用，GP 注册表中该应用对应的条目应设为不可访问，GP 环境也无需对已删除的安全域保留存在记录。

6.3.5 安全域生命周期状态迁移

安全域生命周期状态迁移应是顺序过程，可出现反向变迁或状态跳跃。安全域生命周期的状态迁移见图 5。



图例：

1.授权安全域

2.委托安全域

3.相关联的安全域

4.拥有全局锁特权的安全域或者应用

5.安全域本身

图 5 安全域生命周期状态迁移图

6.4 生命周期示例

生命周期示例参见附录 A。

7 通用平台(GP)运行环境

7.1 功能要求

GP 环境架构可被视作建立在 GP 注册表之上的系统功能集合。GP 注册表应是支持不同 GP 系统功能的数据集合，GP 环境应支持以下功能：

a) 命令分发。具体包括：

1) 应用和安全域的选择；

2) 逻辑通道的管理；

3) 命令的分发。

b) 卡片内容管理。具体包括：

1) 内容验证；

2） 内容加载；
3） 内容安装；
4） 内容删除；
5） 卡片内容管理的访问控制规则。

c） 安全管理。具体包括：
1） 安全域的锁定和解锁；
2） 应用的锁定和解锁；
3） 卡片的锁定和解锁；
4） 卡片终结；
5） 权限的使用；
6） 安全域权限的使用；
7） 跟踪和事件日志。

d） GP 可信任框架。

7.2 GP 环境服务

应用和安全域应能访问或修改 GP 环境的某些内容。根据发起请求的实体相关权限，GP 环境应提供以下服务：

a） 获取 GP 环境保存在 GP 注册表中应用自身的生命周期状态；
b） 获取卡片的生命周期状态；
c） 获得访问与应用相关联的安全域所提供服务的途径；
d） 将卡片的生命周期状态置为已锁定状态；
e） 对卡片设置历史字节；
f） 对 GP 环境保存在 GP 注册表中应用自身的生命周期状态进行迁移；
g） 将卡片的生命周期状态置为终结状态；
h） 获得访问 GP 注册表信息的途径。

7.3 命令分发

7.3.1 处理方式

卡片收到的命令应由 GP 环境处理或分发到被选定应用来处理。

7.3.2 GP 环境处理

GP 环境处理应符合下列要求：

a） 对于所有的命令而言，如果命令中指定了一个不能打开的逻辑通道，其处理方式应符合以下要求：
1） 如果卡片无法识别逻辑通道，那么该命令应分发到被选定的应用进行处理；
2） 如果卡片能识别逻辑通道，则 GP 环境应进行“错误”响应。

b） SELECT [by name]命令应由 GP 环境处理。主控安全域成为被选定应用的方法应符合以下要求：
1） 在 SELECT 命令中指定主控安全域的应用标识符(AID)；
2） 卡外实体应在 SELECT 命令对应的响应中得到主控安全域的 AID。

c） MANAGE CHANNEL 命令的处理应取决于卡片的能力，并应包含以下情况：
1） 如果卡片能识别逻辑通道但只支持基本逻辑通道，则 GP 环境应进行“错误”响应；

2) 如果卡片能识别逻辑通道且能够支持至少一个辅助逻辑通道，则 GP 环境应对该命令进行处理；
3) 如果卡片无法识别逻辑通道，那么该命令应分发到被选定的应用进行处理。

7.3.3 被选定应用处理

被选定应用处理应符合以下要求：

a) 除 SELECT [by name]、MANAGE CHANNEL 之外的其他类型命令应分发到当前被选定的应用进行处理；
b) 命令既可通过基本逻辑通道(逻辑通道编号为 0)，也可通过附属逻辑通道(逻辑通道编号不为 0)进行收取；
c) 为了与符合 GB/T 16649.4 的接触式卡相兼容，应在 APDU 命令头的命令消息类型标识字节中指定逻辑通道的信息。支持多个逻辑通道的卡片主控安全域不应存在多重选定方面的限制。

7.4 逻辑通道和应用选择

7.4.1 隐式选择分配

7.4.1.1 分配原则

应用的隐式选择分配应符合以下原则：

a) 主控安全域应作为卡片所有 I/O 接口上的所有逻辑通道默认的隐式可选择应用。
b) 当卡片 I/O 接口某个逻辑通道的隐式可选择应用被删除时，主控安全域应成为该接口的该逻辑通道的隐式可选择应用。

7.4.1.2 运行行为

GP 环境应通过每个应用的隐式选择注册信息控制下列运行行为：

a) 在卡片复位或激活时，应识别卡片当前 I/O 接口的基本逻辑通道上的隐式可选择应用；
b) 在卡片当前 I/O 接口上通过基本逻辑通道打开一个新的附属逻辑通道时，应识别该附属逻辑通道上的隐式可选择应用。

7.4.2 基本逻辑通道

7.4.2.1 管理要求

卡片的基本逻辑通道应为永久性可用接口，并应被 GP 环境所支持。GP 环境也可对附加选择过程进行处理。GP 环境应支持基于非完整 AID 的应用选择。GP 环境应借助以下两种方式来处理基本逻辑通道上的应用选择：

a) 卡片复位或者卡片激活之后的隐式选择；
b) 通过 SELECT [by name]命令进行的显式选择。

7.4.2.2 应用选择

7.4.2.2.1 隐式选择

当卡片会话已经建立且第一个命令发送到卡片之前，卡片对应的 I/O 接口的基本逻辑通道上定义的隐式可选择应用应成为该接口基本逻辑通道上的已选择应用。GP 环境对隐式应用选择的处理应符合下列要求：

a) 如果卡片在生命周期中处于已锁定状态或终结状态，具备“最终应用权限”的应用应是基本逻辑通道上的已选定应用，GP 环境不应尝试辨识隐式可选择应用；

b) 在其他情况下，GP 环境应搜索 GP 注册表以找出当前卡片 I/O 接口的基本逻辑通道上标记为隐式可选择的应用，并应符合下列要求：

1) 如果该应用的生命周期状态不是已锁定状态，就应是该基本逻辑通道的已选定应用；

2) 如果该应用的生命周期状态是已锁定状态，则具备“最终应用权限”的应用是基本逻辑通道上的已选定应用。

7.4.2.2.2 显式选择

7.4.2.2.2.1 选择条件

某个应用成为基本逻辑通道上的已选定应用应符合以下要求：

a) 命令请求的 AID(完全或部分地)与该应用的 AID 相匹配；

b) 被选定的该应用处于正确的生命周期状态；

c) 该应用没有多重选择上的约束，且支持当前的卡片接口。

7.4.2.2.2.2 运行行为

当在基本逻辑通道上进行应用的显式选择时，GP 环境的运行行为(以下要求不适用于终结状态)应符合下列要求：

a) 当卡片的生命周期状态设置成已锁定状态时，应符合下列要求：

1) 当选择的应用具备“最终应用权限”时，则该应用又重新被选定，并给卡外实体返回警告；

2) 当选择其他应用时，则具备“最终应用权限”的应用继续被选定，并给卡外实体返回错误。

b) 当收到的 SELECT [by name] [first or only occurrence]命令或是 SELECT [by name] [next occurrence]命令消息没有数据域时，则主控安全域应成为当前的已选定应用，且 SELECT 命令被分发到主控安全域。

c) 当收到 SELECT [by name] [first or only occurrence]命令时，应从 GP 注册表的起始条目进行搜索。

d) 当收到 SELECT [by name] [next occurrence]命令时，应从该基本逻辑通道上已选定应用在 GP 注册表中的下一个条目开始搜索。

e) 当搜索到完全或部分匹配的应用，且其生命周期状态为已安装状态时，继续通过 GP 注册表搜索下一个完全或部分匹配的应用。如未搜索到，则 GP 环境应给卡外实体返回错误。

f) 当搜索到完全或部分匹配的应用，且其生命周期状态为已锁定状态时，继续通过 GP 注册表搜索下一个完全或部分匹配的应用。如果发现该锁定的应用是基本逻辑通道上的已选定应用，则 GP 环境应中止其对应的应用会话。如未搜索到，则 GP 环境应给卡外实体返回错误。

g) 当搜索到完全或部分匹配的应用，且其因为对多重选择的限制或该应用拒绝被选择(如它不支持当前的卡片接口)时，继续通过 GP 注册表搜索下一个完全或部分匹配的应用。如未搜索到，则 GP 环境应给卡外实体返回错误。

h) 当搜索到完全或部分匹配的应用，且该应用为可选择的(正处于正确的生命周期状态，且没有多重选择的限制)，则该应用应成为基本逻辑通道上的当前已选定应用，接收到的 SELECT [by name]命令，无论其参数是[first or only occurrence]还是[next occurrence]，都应由运行环境进行处理。

i) 当搜索不到完全或部分匹配的应用，则基本逻辑通道上的当前已选定应用保持不变，并应符合下列要求：

1) 如果 SELECT [by name]命令的参数设置为[first or only occurrence]，则该 SELECT 命令被分发到该应用；
2) 如果 SELECT [by name]命令的参数设置为[next occurrence]，则 GP 环境应给卡外实体返回错误。

j) 当前应用会话已经终结且搜索不到完全或部分匹配的应用，则 GP 环境应尝试将当前卡片接口基本逻辑通道上标记为隐式可选择的应用选择为已选定应用。

7.4.2.3 逻辑通道管理

7.4.2.3.1 基本要求

逻辑通道管理应符合下列要求：

a) 当能够识别逻辑通道的卡片收到 MANAGE CHANNEL [open]命令时，应符合下列要求：
1) 如果某个应用被预设为当前卡片接口的新附属逻辑通道上的隐式可选择应用，则该应用会在打开新的附属逻辑通道时，被隐式选择为当前应用，且会发生相应的运行行为；
2) 如果没有应用被预设为当前卡片接口的新附属逻辑通道上的隐式可选择应用，则已被预设为当前卡片接口的基本逻辑通道上的隐式可选择应用应作为新的附属逻辑通道上的隐式可选择应用，且会发生相应的运行行为。

b) 当能够识别逻辑通道的卡片收到 MANAGE CHANNEL [close]命令时，应符合下列要求：
1) 终结命令中指定的附属逻辑通道上的当前已选定应用会话，并关闭该逻辑通道；
2) 如果命令中指定的是基本逻辑通道，则该逻辑通道不会被关闭。

7.4.2.3.2 运行行为

当 GP 环境收到 MANAGE CHANNEL [open]命令时，运行行为应符合下列要求：

a) 如果卡片生命周期状态为已锁定状态或终结状态，则返回适当的错误；
b) 如果 GP 环境支持的逻辑通道数量不足以支持打开新的附属逻辑通道，则返回错误；
c) GP 环境应搜索 GP 注册表以查找当前支持卡片接口且标记为新附属逻辑通道上隐式可选择的应用，并应符合下列要求：
1) 如果找到应用的生命周期状态为已锁定状态，则具备“最终应用权限”的应用应成为该附属逻辑通道上的已选定应用；
2) 如果找到应用限制进行多重选择，则不能打开新逻辑通道且 GP 环境应返回错误；
3) 在其他情况下，会打开新附属逻辑通道，且找到的应用应成为该附属逻辑通道上的已选定应用。

7.4.2.4 应用命令分发

当某个应用成为基本逻辑通道上的已选定应用，后续命令的分发应由 GP 环境来控制。在能够识别逻辑通道的卡片上，MANAGE CHANNEL 命令应仅由 GP 环境处理，其他所有命令应立即分发到基本逻辑通道的当前已选定应用。

7.4.3 附属逻辑通道

7.4.3.1 管理要求

GP 环境应在附属逻辑通道上支持基于非完整 AID 的应用选择。在一个可用的附属逻辑通道上，GP 环境应通过下列途径支持应用选择：

a) 成功处理 MANAGE CHANNEL [open]命令后的隐式选择；

b) 通过 SELECT [by name]命令进行的显式选择。

7.4.3.2 应用选择

7.4.3.2.1 隐式选择

附属逻辑通道应由基本逻辑通道或者另一个附属逻辑通道打开,其应用的隐式选择表现可不同。

7.4.3.2.2 显式选择

7.4.3.2.2.1 选择条件

某个应用成为附属逻辑通道上的已选定应用应符合下列要求:

a) 命令请求的 AID(完全或部分地)与该应用的 AID 相匹配;

b) 被选定的该应用处于正确的生命周期状态;

c) 该应用没有多重选择上的约束,且支持当前的卡片接口。

7.4.3.2.2.2 运行行为

当在附属逻辑通道上进行应用的显式选择时,GP 环境的运行行为应符合下列要求:

a) 当卡片的生命周期状态设置成已锁定状态或终结状态时,关闭打开的附属逻辑通道,并给卡外实体返回错误响应。

b) 当收到的 SELECT [by name] [first or only occurrence]命令或是 SELECT [by name] [next occurrence]命令消息没有数据域时,则主控安全域应成为当前的已选定应用,且 SELECT 命令应被分发到主控安全域。

c) 当收到 SELECT [by name] [first or only occurrence]命令时,应从 GP 注册表起始条目进行搜索。

d) 当收到 SELECT [by name] [next occurrence]命令时,应从该附属逻辑通道上已选定应用在 GP 注册表中的下一个条目开始搜索。

e) 当搜索到完全或部分匹配的应用,且其生命周期状态为已安装状态时,应继续通过 GP 注册表搜索下一个完全或部分匹配的应用。如未搜索到,则 GP 环境应给卡外实体返回错误。

f) 当搜索到完全或部分匹配的应用,且其生命周期状态为已锁定状态时,应继续通过 GP 注册表搜索下一个完全或部分匹配的应用。如发现该锁定的应用是附属逻辑通道上的已选定应用,则 GP 环境应中止其对应的应用会话。如未搜索到,则 GP 环境应给卡外实体返回错误。

g) 当搜索到完全或部分匹配的应用,且其因为对多重选择的限制或该应用拒绝被选择时,应继续通过 GP 注册表搜索下一个完全或部分匹配的应用。如未搜索到,则 GP 环境应给卡外实体返回错误。

h) 当搜索到完全或部分匹配的应用,且该应用为可选择的,则该应用应成为附属逻辑通道上的当前已选定应用,接收到的 SELECT [by name]命令,无论其参数是[first or only occurrence]还是[next occurrence],都应由运行环境进行处理。

i) 当搜索不到完全或部分匹配的应用,则附属逻辑通道上的当前已选定应用保持不变,并应符合下列要求:

   1) 如 SELECT [by name]命令的参数设置为[first or only occurrence],则该 SELECT 命令被分发到该应用;

   2) 如 SELECT [by name]命令的参数设置为[next occurrence],则 GP 环境应给卡外实体返回错误。

7.4.3.3 逻辑通道管理

7.4.3.3.1 基本要求

GP 环境可在附属逻辑通道上收到打开或关闭一个附属逻辑通道的请求，并应符合下列要求：

a) 当收到 MANAGE CHANNEL [open]命令时，若原先的附属逻辑通道上的已选定应用对多重选择没有限制，则该应用应在打开新的附属逻辑通道时，成为新逻辑通道的当前已选定应用；

b) 当卡片收到 MANAGE CHANNEL [close]命令时，终结命令中指定的附属逻辑通道上的当前已选定应用会话，并关闭该逻辑通道。

7.4.3.3.2 运行行为

收到 MANAGE CHANNEL [open]命令时，运行行为应符合下列要求：

a) 如果卡片生命周期状态为已锁定状态或终结状态，则返回适当的错误；

b) 如果 GP 环境支持的逻辑通道数量不足以支持打开新的附属逻辑通道，则返回错误；

c) 如果原先附属逻辑通道上的当前已选定应用在新的附属逻辑通道上限制进行多重选择，则不能打开新逻辑通道，且 GP 环境应返回错误；

d) 在其他情况下，命令中指定的附属逻辑通道会被打开，原先的附属逻辑通道上的已选定应用应成为新逻辑通道的当前已选定应用。

7.4.3.4 应用命令分发

当某个应用成为附属逻辑通道上的已选定应用时，后续命令的应由 GP 环境来控制。MANAGE CHANNEL 命令应由 GP 环境处理，其他所有命令应立即分发到附属逻辑通道的当前已选定应用。

7.5 GP 注册表

7.5.1 应用范围和更新操作

应用、安全域、可执行加载文件都应为 GP 注册表中的条目，GP 注册表的内容应根据内置 GP 环境、授权应用发起的操作而更新。GP 注册表应用于：

a) 保存卡片管理信息；

b) 保存相关的应用管理信息；

c) 支持卡片资源管理数据；

d) 保存应用生命周期信息；

e) 保存卡片生命周期信息；

f) 跟踪与日志关联的计数器。

7.5.2 应用/可执行加载文件/可执行模块等数据元素

7.5.2.1 AID

AID 应符合下列要求：

a) 每个可执行加载文件或可执行模块应与卡片上某个唯一的 AID 相关联；

b) 每个应用的 AID 可与可执行模块的 AID 相同，但不可以与可执行加载文件或者另一个 GP 注册表中已经存在应用的 AID 相同；

c) 可在 SELECT 命令中指定应用的 AID，不可选择可执行加载文件或可执行模块。

7.5.2.2 生命周期

应用生命周期状态数据元素应包含应用、可执行加载文件、可执行模块的当前生命周期状态。

7.5.2.3 存储器资源管理参数

资源管理数据元素应包括一个应用可以分配的存储器资源等信息，具体数值应与具体的卡片系统有关。GP 环境可利用作为管理存储器分配的一种控制机制。当某个应用请求更多的资源时，GP 环境应利用保存在 GP 注册表中的该数据元素来查验这个请求。

7.5.2.4 权限

权限数据元素应表明每个应用具备的权限。

7.5.2.5 隐式应用选择参数

隐式应用选择参数应表明应用在某接口的某逻辑通道上是否为隐式可选择的。

7.5.2.6 关联安全域的 AID

可执行加载文件和应用应与某个安全域相关联，安全域的 AID 应注册在 GP 注册表中。安全域也可与其他安全域相关联，被关联的安全域既可是另一个安全域，也可是发起关联的安全域本身。

7.5.2.7 应用提供方 ID

GP 注册表应保存作为应用和可执行加载文件所有者的应用提供方标识，该标识应在加载和安装过程中明确指定。卡内实体可利用此信息来贯彻安全策略。

7.5.3 卡片级数据

卡片生命周期状态应保存在 GP 注册表中，任何对 GP 环境卡片管理功能的限制都应保存在 GP 注册表中。

7.6 权限

7.6.1 权限定义

安全域和应用的权限定义应符合表 1 的要求。

表 1 权限定义

编号	权限名	描述
0	安全域权限	拥有此权限的应用是一个安全域
1	DAP 验证权限	拥有此权限的应用能够进行 DAP 验证；该应用也应拥有安全域权限
2	委托管理权限	拥有此权限的应用能够对卡片内容进行委托管理；该应用也应拥有安全域权限
3	卡片锁定权限	拥有此权限的应用能够对卡片进行锁定
4	卡片终结权限	拥有此权限的应用能够对卡片进行终结
5	卡片复位权限	拥有此权限的应用能够修改一个或多个卡片接口的历史字节
6	CVM 管理权限	拥有此权限的应用能够对一个需要 CVM 验证的应用进行 CVM(持卡人验证方法)管理

表 1（续）

编号	权限名	描述
7	强制 DAP 验证权限	拥有此权限的应用要求对所有的加载操作进行 DAP 验证；该应用也应拥有安全域权限和 DAP 验证权限
8	可信路径权限	拥有此权限的应用是应用间通信的一条可信路径
9	授权管理权限	拥有此权限的应用能够管理卡片内容；该应用也应拥有安全域权限
10	令牌验证权限	拥有此权限的应用能够对卡片内容委托管理操作所需的令牌进行验证
11	全局删除权限	拥有此权限的应用能够删除卡片上的任何内容
12	全局锁定权限	拥有此权限的应用能够锁定或解锁任何应用
13	全局注册表权限	拥有此权限的应用能够访问 GP 注册表的任何条目
14	最终应用权限	拥有此权限的应用是卡片状态为已锁定状态或终结状态时唯一可访问的应用
15	全局服务权限	拥有此权限的应用能够向卡片上的其他应用提供服务
16	收条创建权限	拥有此权限的应用能够为卡片内容委托管理操作创建
17	加密文件数据块	安全域要求相关的装载文件被加密装载
18	非接激活	在非接触式接口下应用可以激活或停用其他应用
19	非接自我激活	在没有非接触特权应用请求激活的优先请求条件下，应用可以在非接触接口下自激活

7.6.2 权限分配

权限分配应符合下列要求：

a) 在某个卡片接口上，卡片在任意时刻只有一个应用或安全域可设置成拥有“卡片复位权限”；

b) 当某个应用被分配了“卡片复位权限”之后，可通过删除该应用或撤销这个分配的权限的方式，将“卡片复位权限”分配给新的应用；

c) “卡片复位权限”在缺省的情况下应分配给主控安全域。只有当主控安全域具备了“卡片复位权限”时，才能重新分配该权限；

d) 当拥有“卡片复位权限”的应用被删除时，则该权限重新被分配给主控安全域；

e) “最终应用权限”在缺省的情况下应分配给主控安全域。只有当主控安全域具备了“最终应用权限”时，才能重新分配该权限；

f) 卡片在任意时刻只有一个应用或安全域可设置成拥有“最终应用权限”；

g) 当某个应用被分配了“最终应用权限”之后，可通过删除该应用或撤销这个分配的权限的方式，将“最终应用权限”分配给新的应用；

h) 当拥有“卡片复位权限”的应用被删除时，则该权限重新被分配给主控安全域；

i) “授权管理权限”和“委托管理权限”应互斥，“令牌验证权限”和“委托管理权限”应互斥，“收条创建权限”和“委托管理权限”应互斥，其他权限不应互斥。

7.6.3 权限集

当卡片生命周期状态为准备状态时，主控安全域应初始化为拥有以下权限集：

a) 安全域权限；

b） 授权管理权限；
c） 全局注册表权限；
d） 全局锁定权限；
e） 全局删除权限；
f） 令牌验证权限；
g） 卡片锁定权限；
h） 卡片终结权限；
i） 可信路径权限；
j） CVM 管理权限；
k） 卡片复位权限；
l） 最终应用权限；
m） 收条创建权限。

7.6.4 缺省权限

权限可在应用或安全域的生命周期中添加或收回。为了同只支持 0～7 号权限的卡片向后兼容，缺省权限应符合表 2 的要求。

表 2 缺省权限

权限编号	权限名	主控安全域	辅助安全域	其他应用
8	可信路径权限	是	是	否
9	授权管理权限	是	否	否
10	令牌验证权限	是	否	否
11	全局删除权限	是	否	否
12	全局锁定权限	是	否	否
13	全局注册表权限	是	否	否
14	最终应用权限	是	否	否
15	全局服务权限	否	否	否
16	收条创建权限	是	否	否
17	加密文件数据块	否	否	否
18	非接激活	否	否	否
19	非接自激活	否	否	否

7.6.5 权限管理

GP 环境应运用权限的数据元素和每个应用的隐式选择参数，控制检查修改历史字节的请求合法性，对双界面卡来说，此修改应针对卡片接口上的历史字节进行，且该卡片接口已被正在请求的卡上应用注册为隐式可选择，卡片宜仅支持基本逻辑通道。GP 环境应运用权限的数据元素和应用的关联层次来控制下列运行行为：

a) 在需要时确保令牌的验证；
b) 在需要时确保收条的创建；
c) 在需要时确保 DAP 验证的进行；
d) 检查加载、安装、迁移、注册表更新或是删除等改变卡片内容的请求合法性；
e) 检查锁定或解锁卡片的请求合法性；
f) 检查锁定或解锁应用和安全域的请求合法性；
g) 检查终结卡片的请求合法性；
h) 检查与另一个卡片应用进行通信的请求合法性；
i) 检查访问另一个应用或安全域在 GP 注册表中条目的请求合法性；
j) 当卡片处于已锁定状态或终结状态时，辨识出具备“最终应用权限”的应用，使其成为缺省的已选定应用。

7.7 GP 可信任框架

当应用的安全域作为接收实体收到 APDU 命令后，在将其发给 GP 可信任框架之前，应对该命令进行解包操作。目标应用可通过安全域建立的安全会话通道来使用安全域可用的加解密服务。GP 可信任框架应进行下列检查：

a) 接收实体具备“可信任路径权限”；
b) 接收实体是一个安全域；
c) 目标应用在 GP 注册表中有对应的条目，且激活了“过程数据”的访问入口；
d) 如果目标应用已在另一条逻辑通道上成为已选定应用，则该应用没有多重选择限制；
e) 目标应用关联到作为当前接收实体的安全域。

8 安全域

8.1 管理要求

支持多个安全域的卡应允许应用提供方通过自身的安全域管理其应用，并使用安全域密钥向应用提供加解密服务，各安全域应负责管理其密钥。安全域的密钥和加密算法应包括如下用途：

a) 个人化支持：在应用提供者的应用进行个人化过程中提供安全通信支持；
b) 运行消息的支持：为没有安全消息密钥的应用提供运行安全通信支持。

8.2 主控安全域特征

主控安全域除了具有安全域的共有特征之外，还具备以下特征：

a) 安装在卡片上的第一个应用，在 GP 注册表中被视为一个应用；
b) 直接继承卡片的生命周期状态，不同于普通安全域的生命周期状态；
c) 当具备“卡片复位权限”的应用被删除后，主控安全域将具有该权限；
d) 当与主控安全域在同一个卡片 I/O 接口的同一个逻辑通道上的隐式可选择应用被删除后，主控安全域将成为该 I/O 接口上的该逻辑通道上的隐式已选定应用；
e) 当卡片 I/O 接口的逻辑通道上的隐式可选择应用被删除后，主控安全域将成为该卡片接口的该逻辑通道上的隐式已选定应用；
f) 主控安全域可通过不带命令数据域的 SELECT 命令进行选择；
g) 当具备“最终应用权限”的应用被删除后，主控安全域将获得该权限。

8.3 安全域的关联

主控安全域应关联到自身，安全域可通过迁移操作关联到自身。卡片上可存在一个或多个安全域关联层次，每个关联层次的根是一个关联到自身的安全域，图 6 展示了两个关联层次。安全域与应用的关联应为直接关联，上一层安全域与这个应用的关联应为间接关联。安全域关联内容应包括其自身、与其在同关联层次中的所有应用和可执行加载文件。

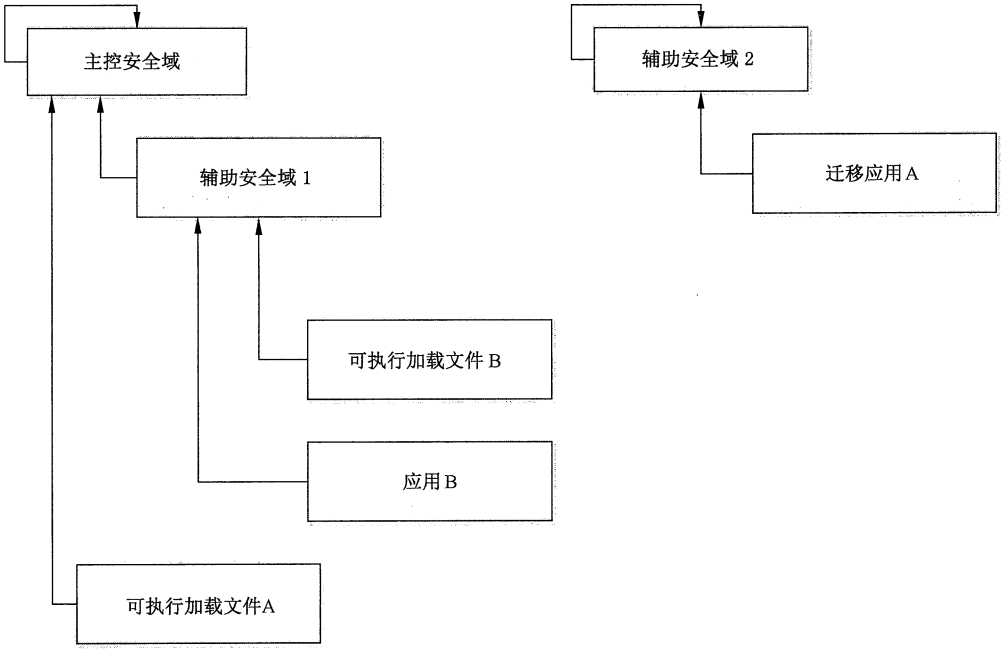


图 6 安全域层级示例

8.4 安全域服务

8.4.1 应用访问安全域服务

8.4.1.1 服务内容

应用应能通过其关联安全域提供的服务，依靠安全域的加密支持来保证个人化和运行的机密性和完整性，并应包含如下内容：

a) 通过验证卡外实体，初始化安全通道会话；
b) 通过验证命令的完整性和/或解密被加密的数据，对在安全通道会话中接收的命令进行解包；
c) 控制 APDU 命令序列；
d) 对私密数据块进行解密；
e) 设定适用于下一条接收的命令和/或发出的响应的安全级别，包括完整性和机密性；
f) 根据请求关闭安全通道会话，并销毁任何与该安全通道会话相关的机密信息；
g) 根据支持的特定安全通道协议，安全域还可能包括如下服务：
   1) 通过添加完整性处理和/或进行加密，对在安全通道会话中发送的响应进行打包；
   2) 加密私密数据块；
   3) 控制 APDU 响应序列。

8.4.1.2 多安全通道会话处理要求

安全域可支持多个并发的安全通道会话，或者仅管理一个安全通道会话，并应符合下列要求：

a) 当安全域支持管理多个并发的安全通道会话，则该安全域应能区分不同的安全通道会话及其各自的逻辑通道；

b) 当安全域不支持管理多个并发的安全通道会话，则在当前安全通道会话相关的逻辑通道之外的其他逻辑通道上打开新的安全通道会话时，该安全域应拒绝该请求；

c) 当某个应用请求其关联的安全域，在已经打开的安全通道会话相关的逻辑通道之外的其他逻辑通道上申请服务时，该安全域应拒绝该请求。

8.4.2 安全域访问应用服务

安全域访问应用服务应符合下列要求：

a) 安全域应拥有接收 STORE DATA 命令的单元，用以关联到该安全域的一个应用；

b) 安全域在将该命令转发到应用之前，应根据当前安全级别，对该命令进行解包处理；

c) 命令应通过 GP 可信任框架发送给应用，可信任框架负责处理安全域和应用之间的相互通信。

8.4.3 个人化支持

8.4.3.1 支持方式

应用的个人化数据应包括密钥及持卡方的特定数据等。应用可利用其关联的安全域提供的安全通道和密钥解密服务管理这些数据的安全加载，并应符合下列方式：

a) 利用运行消息传送的支持；

b) 利用安全域访问应用的能力。

8.4.3.2 处理实现

应用关联的安全域接受数据完成个人化的示例见图 7。处理实现应符合下列要求：

a) 在收到 INSTALL [for personalization]命令和后续的 STORE DATA 命令时，执行应用个人化的安全域应符合下列要求：

1) 运用自己的安全通信策略；

2) 验证卡外实体为合法的应用提供方；

3) 在将 STORE DATA 命令转发到目标应用之前，应根据当前安全级别，对该命令进行预处理。

b) 在收到转发命令给应用的请求时，GP 环境应符合下列要求：

1) 确认卡片生命周期状态不应是已锁定状态或终结状态；

2) 确认 GP 环境和发起请求的卡内实体没有对个人化进行限制；

3) 运用可信任框架运行的要求。

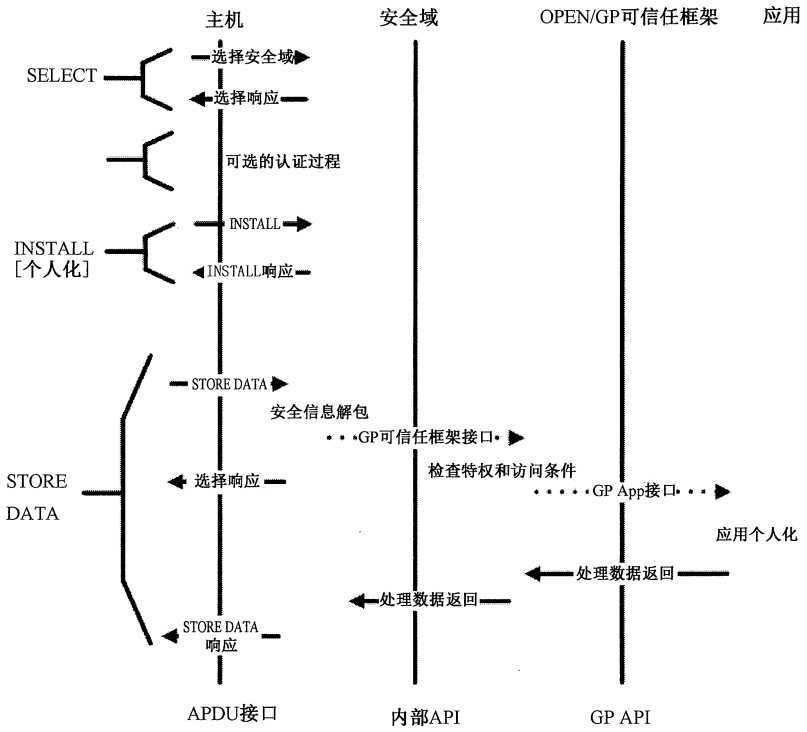


图 7　通过关联的安全域实现应用个人化

8.4.4　运行消息支持

安全域可向其直接关联的应用提供安全通信的运行支持，以替代向应用中加载附加通信密钥，运行消息流程见图 8。应用提供方可选择在应用的整个生命周期，利用该应用关联的安全域提供的服务来支持所有的应用通信。

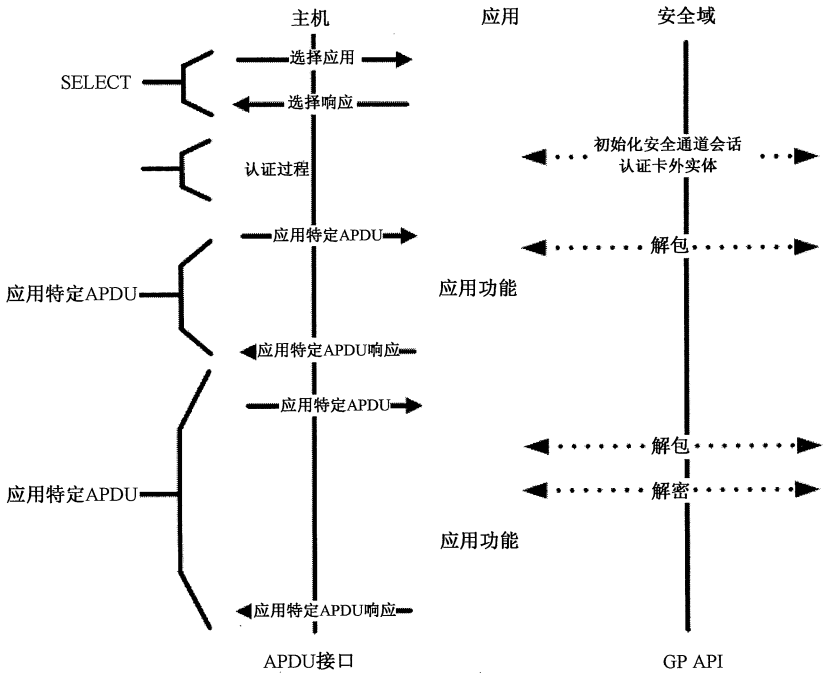


图 8　运行消息流程

8.5 安全域数据

8.5.1 主控安全域

8.5.1.1 控制内容

主控安全域应能够控制以下数据：

a) 主控标识编号(IIN)；
b) 卡片映像编号(CIN)；
c) 卡片标识数据；
d) 其他卡发行者的私有数据。

8.5.1.2 主控标识编号

IIN 可被卡外实体用来关联卡片和特定的卡片管理系统。典型的 IIN 应包含了符合 ISO/IEC 7812 定义的主控标识，并由符合 GB/T 16649.6—2001 中标记号“42”的数据模板持有。IIN 数据元素的长度应是可变的。

8.5.1.3 卡片映像编号

CIN 可被卡片管理系统用来在它的卡片数据库中唯一标识某张卡片，由符合 GB/T 16649.6—2001 中标记号为“45”的数据模板持有，并由发卡方(通过 IIN 进行标识)分配。CIN 数据元素的长度应是可变的。

8.5.1.4 卡片标识数据

卡片管理系统在能够与卡片交互之前，应得到卡片的信息，包括卡片类型和能够支持何种安全通道协议等。卡片标识数据作为一种能够提供卡片信息的机制，应能避免反复尝试现象的发生。卡片标识数据应被包含在 GB/T 16649.6—2001 的标记号为“73”的数据模板中。卡片数据可利用 GET DATA 命令得到。除额外的动态数据对象外，卡片标识数据在卡上的动态更新应没有特殊要求。

注：卡片标识数据提供的信息应足够开启与卡片的通信，而不必借助反复尝试，对完成此目的无必要的信息，应在接下来系统与卡片的交互过程中提供。

8.5.2 辅助安全域

8.5.2.1 控制内容

辅助安全域可控制的标识数据包括：

a) 安全域提供方标识编号(SIN)；
b) 安全域映像编号；
c) 安全域管理数据；
d) 其他的应用提供方私有数据。

8.5.2.2 安全域提供方标识编号

SIN 可被卡外实体用来关联安全域和特定的卡片管理系统，且应是一个 IIN，包含了符合 ISO 7812 中定义的安全域提供方标识，并应由符合 GB/T 16649.6—2001 中标记号为“42”的数据模板持有。SIN 数据元素的长度应是可变的。

8.5.2.3 安全域映像编号

安全域映象编号可被应用管理系统用来唯一标识卡片上某个安全域的实例，应由符合 GB/T 16649.6—2001 中标记号为“45”的数据模板持有，其值是唯一的。

8.5.2.4 安全域管理数据

安全域管理数据提供的信息应足够开启与卡片的通信，应能够避免反复尝试现象，并应符合下列要求：

a) 利用 SELECT 命令的响应返回的安全域管理数据应被包含在 GB/T 16649.6—2001 的标记号为“73”的数据模板中；

b) 利用 GET DATA 命令的响应返回的安全域管理数据应被包含在 GB/T 16649.6—2001 的标记号为“66”的数据模板中。

8.6 安全域密钥

8.6.1 密钥信息

8.6.1.1 属性

密钥应具有下列属性：

a) 密钥标识：用来标识卡内实体的每个密钥。每个密钥可能包含一个或多个组件。每个密钥的所用密钥组件共享同一个密钥标识。卡内实体不同的密钥标识应用来区分各个密钥及其用法和功能。在分配密钥标识，包括同一实体的非连续密钥标识的时候，不必遵循任何约束或是预定义的顺序；

b) 密钥版本号：某个卡内实体的不同密钥版本号可用来标识同一密钥的不同实例或不同版本。在分配密钥版本号时，不必遵循任何约束或是预定义的顺序；

c) 加密算法：每个特定的密钥只能与一种加密算法相关联；

d) 长度：每种加密算法会对应若干个密钥长度；

e) 访问条件：用来控制和分割对密钥的访问。

8.6.1.2 管理要求

卡外实体可通过 GET DATA 命令来获取安全域信息内标记号为“E0”的数据模板中包含的密钥。安全域对密钥的管理应符合下列要求：

a) 密钥标识和密钥版本号唯一指向某卡内实体的某个密钥，每个密钥标识和密钥版本号的组合标识了卡内实体唯一的密钥；

b) 添加一个密钥，相当于分配新的密钥值、密钥标识或密钥版本号；

c) 更换密钥的操作应使用新的密钥值及关联的新密钥版本号来进行更新，而密钥标识保持不变，之前的密钥将不复存在。

8.6.2 密钥访问

8.6.2.1 访问条件

安全域密钥的访问条件应满足下列条件之一：

a) 密钥所有者，即安全域本身；

b) 密钥所有者之外的授权用户；

c) 所有的授权用户，包括作为密钥所有者的安全域本身。

8.6.2.2 编码格式

安全域密钥访问条件编码格式应符合下列条件：

a) “00”：所有授权用户，包括密钥所有者都能访问，当没有在 PUT KEY 命令中指明时，此访问条件是安全通道协议所用密钥的默认访问条件；
b) “01”：只有密钥所有者能访问，当没有在 PUT KEY 命令中指明时，此访问条件是令牌和 DAP 所用密钥的默认访问条件；
c) “02”：密钥所有者之外的授权用户，都能访问；
d) “03”到“7F”：保留为将来用途；
e) “80”到“FE”：保留为私有用途；
f) “FF”：不能访问。

8.6.2.3 访问要求

对安全域密钥的访问应符合下列要求：

a) GP 环境应识别出应用关联的安全域，并提供该安全域对应的安全通道接口的引用给发起请求的应用；
b) 应用可通过安全通道接口向安全域请求加密服务。

8.7 数据和密钥管理

数据和密钥管理应符合下列要求：

a) 当收到数据和密钥管理的请求时，对应的安全域应按照自身的访问控制规则管理该数据和密钥，卡片生命周期状态不应设为已锁定状态或终结状态；
b) 当收到 DELETE[key]、PUT KEY 或 STORE DATA 命令时，执行数据和密钥管理的安全域应实施自身的安全通信策略；
c) 安全域提供方可就密钥的删除实施自身的密钥管理策略。

9 卡片和应用管理

9.1 卡片内容管理

9.1.1 管理要求

卡片的内容管理应包括对卡片内容进行加载、安装、迁移、注册表更新、删除等操作。卡片内容的改变应由卡片上分配了不同权限的各个安全域进行许可。发卡方可将卡片内容管理委托给应用提供方，并应符合下列要求：

a) 发卡方可授权某个应用提供方来执行所有的卡片内容管理操作；
b) 发卡方可授权某个应用提供方对发卡方的卡片内容进行完全的控制；
c) 发卡方可授权某个应用提供方将其自身的安全域和应用与其他应用提供方（尤其是发卡方自身）隔离。

9.1.2 对 GP 环境的要求

GP 环境应负责执行物理上的加载和安全操作，不应进行以下操作：

a) 多个卡片内容管理操作的并行；

b) 当卡片生命周期状态为已锁定状态或终结状态时进行的卡片内容管理操作。

9.1.3 对安全域的要求

9.1.3.1 具备“令牌验证权限”的安全域

该权限应允许安全域提供方，对卡片内容管理操作进行授权。具备“令牌验证权限”的安全域应掌握该令牌的密钥及算法。

注：具备该权限并不意味着具备卡片内容管理的能力。

9.1.3.2 具备“授权管理权限”的安全域

该权限应允许安全域提供方在卡外实体被合法认证为该安全域的所有者(即安全域提供方)时，无需授权(即不用令牌)就可执行卡片内容管理。此时“令牌验证权限”不应是必需的。当卡外实体被认证为非安全域提供方的合法实体时，令牌应是必需的。

9.1.3.3 具备“委托管理权限”的安全域

该权限应允许应用提供方在授权后对卡片内容进行管理。具备“令牌验证权限”的安全域应负责对授权操作进行控制。该权限应允许应用提供方的安全域执行下列操作：

a) 委托加载；
b) 委托安装和可选择化；
c) 委托迁移；
d) 委托更新 GP 注册表；
e) 委托删除。

9.1.3.4 具备“全局删除权限”的安全域

该安全域应能从卡片上删除可执行加载文件或应用，即使该可执行加载文件或应用并不属于该安全域。不具备“全局删除权限”但又能进行卡片内容管理的安全域，应只能删除与自身直接或间接关联的可执行加载文件或应用。

9.1.3.5 具备“全局锁定权限”的安全域

该权限应提供独立于安全域关联层次而对卡片上的应用进行锁定和解锁的权力，同时还应提供对 GP 环境的卡片内容管理功能进行限制的能力。

9.1.3.6 具备“收条创建权限”的安全域

该权限应允许安全域提供方对已经执行的卡片内容管理操作进行确认，并应符合下列要求：

a) 具备“收条创建权限”的安全域应掌握创建收条所需的密钥和算法；
b) 该安全域应跟踪确认计数器，该计数器会在每次创建一个收条时自动增加，当确认计数器达到最大值时，不得归零，卡片支持的该计数器的最大值为 32 767；
c) 每个卡片上应只允许一个安全域具备“收条创建权限”。

9.2 卡片内容的授权和管理

9.2.1 数据鉴别(DAP)模式验证

应用提供方可要求对其加载到卡片的应用代码进行完整性和真实性的验证。授权管理者可要求对所有加载到卡片的应用代码进行完整性和真实性的验证。具备“强制 DAP 验证权限”的授权管理者安

全域，应代表授权管理者提供这种验证服务。

9.2.2 加载文件数据块的散列值

加载文件数据块的散列值应是整个加载文件数据块传送到卡片时进行完整性验证的方法，是 INSTALL [for load]命令的一个数据域。如果加载文件中存在加载文件数据块的散列值，则应对该散列值进行验证。

9.2.3 令牌

令牌应专门用于委托管理，或是卡外实体不是安全域提供方时的授权管理。在执行内容管理功能的过程中，该令牌应被卡片上具备“令牌验证权限”的安全域所验证。

9.3 卡片内容的加载、安装和可选择化

9.3.1 卡片内容加载和安装管理要求

卡片内容加载和安装过程中两个可能的阶段见图 9。卡片内容加载和安装应符合下列要求：

a) 卡片内容加载过程应设计为在卡片的可变存储器中添加代码；

b) 卡片内容安装过程应设计为允许发卡方将先前加载到卡片上的应用代码设置为可执行状态；

c) 卡片内容加载和安装过程应包括可执行代码的特殊链接和实际验证的实现；

d) 当成功完成卡片内容的加载后，可执行加载文件应存在于卡片之中，GP 环境应在 GP 注册表中为该可执行加载文件及其包含的每个可执行模块创建一个条目。

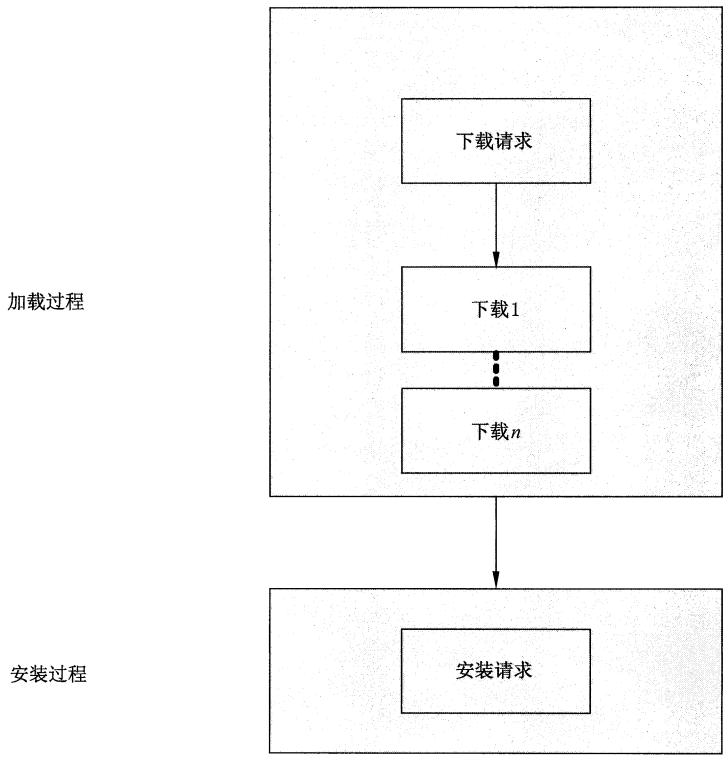


图 9 加载和安装过程

9.3.2 卡片内容的加载

9.3.2.1 加载条件

卡片内容的加载条件应符合下列要求：

a) 当GP环境请求加载卡片内容时，具备“令牌验证权限”的安全域应验证加载文件从卡外实体传输到卡片操作的合法性；

b) 具备对应权限的安全域在GP环境将新内容提交给存储器之前，应验证加载文件数据块的完整性；

c) 具备“授权管理权限”或者“委托管理权限”的安全域可加载可执行加载文件到任何安全域。该可执行加载文件是否能被安全域接受应取决于该安全域自身的要求。

9.3.2.2 加载过程概述

卡片内容的加载过程应符合下列基本要求：

a) 加载过程应由一个INSTALL [for load]命令以及一个或多个LOAD命令构成，所有命令都应由安全域处理；

b) 安全域应将加载请求连同加载文件传给GP环境，以进行额外的验证和处理；

c) 加载过程令牌应允许GP环境借助具备“令牌验证权限”的安全域，确保令牌发放者对加载过程和加载文件数据块的内容加载操作进行授权；

d) 加载文件数据块的散列值应将令牌和有效的加载文件数据块进行关联；

e) 当加载过程完全结束后，应返回给执行委托管理操作的安全域一个可选的收条，且收条应被该安全域发送到卡外实体。

9.3.3 卡片内容的安装

9.3.3.1 安装条件

具备“授权管理权限”或者“委托管理权限”的安全域可将应用安装到对应的可执行加载文件关联的安全域。当执行安装操作的安全域不是可执行加载文件关联的安全域时，此现象应被称为“应用的隐式迁移”。

9.3.3.2 安装过程概述

卡片内容的安装过程应符合下列基本要求：

a) 安装过程应由一条安全域处理的INSTALL [for install]命令构成；

b) 安全域应将安装请求传给GP环境，以进行额外的验证和处理；

c) 安装过程令牌应允许GP环境借助具备“令牌验证权限”的安全域，确保发卡方对安装过程进行授权；

d) 当安装过程完全结束后，应返回给执行委托管理操作的安全域一个可选的收条，且收条应被该安全域发送到卡外实体。

9.3.4 卡片内容的加载、安装和可选择化联合操作

9.3.4.1 联合操作条件

联合操作条件应符合下列要求：

a) 当GP环境请求对卡片内容进行加载、安装和可选择化联合操作时，具备“令牌验证权限”的安全域应验证加载文件从卡外实体传输到卡片操作的合法性；
b) 具备对应权限的安全域在GP环境将新内容提交给存储器之前，宜验证加载文件数据块的完整性；
c) 具备“授权管理权限”或者“委托管理权限”的安全域可加载可执行加载文件到任何安全域，应由该可执行加载文件安装一个应用，并使得该应用是可选择的。

9.3.4.2 联合操作过程概述

联合操作过程应符合下列基本要求：
a) 加载、安装和可选择化联合操作过程应由一条初始的INSTALL [for load, install and make selectable]命令，一条或多条LOAD命令，以及一条最后的INSTALL [for load, install and make selectable]命令构成，这些命令都应由安全域处理；
b) 加载、安装和可选择化联合操作过程令牌应允许GP环境借助具备“令牌验证权限”的安全域，确保令牌发放者对加载过程和加载文件数据块的内容加载操作，以及从该可执行加载文件安装一个应用的操作，都进行了授权；
c) 当加载和安装过程完全结束后，应返回给执行委托管理操作的安全域一个可选的收条，且收条应被该安全域发送到卡外实体。

9.3.5 卡片内容的加载过程

9.3.5.1 命令序列

加载的APDU命令序列应符合下列要求：
a) 一条INSTALL [for load]命令用于发起加载的请求，数据域细化对加载文件的要求；
b) 根据文件大小和卡片通信缓冲区大小对加载文件进行分块，多条LOAD命令用来将分块后的加载文件传输到卡片；
c) 每条INSTALL或LOAD命令在加载请求转发给GP环境处理前，应先由接收该命令的安全域进行处理。

9.3.5.2 运行行为

内容加载过程的运行行为应符合下列要求：
a) 当收到INSTALL [for load]命令后，执行加载操作的安全域应遵循以下规则：
   1) 实施该安全域自身的安全通信策略；
   2) 实施该安全域自身的安全策略，如检查其生命周期状态是否为已个人化状态；
   3) 如果INSTALL [for load]中存在加载文件数据块的散列值，则请求GP环境开始对后续的加载文件数据块验证其散列值；
   4) 如果执行加载操作的安全域具备“委托管理权限”，则检查INSTALL [for load]中是否存在一个加载过程令牌；
   5) 如果执行加载操作的安全域具备“授权管理权限”，且发起加载请求的卡外实体没能被认证为对应的安全域提供方，则检查INSTALL [for load]中是否存在一个加载过程令牌；
   6) 如果INSTALL [for load]中存在一个加载过程令牌，则请求GP环境返回该加载过程令牌的验证结果；
   7) 如果加载请求中存在应用提供方标识符，则请求GP环境在GP注册表为该可执行加载

文件保存该应用提供方标识符。

b) 当收到加载请求时，GP 环境应符合以下规则：

1) 检查卡片生命周期状态不是已锁定状态或者终结状态；

2) 检查 GP 环境和发起请求的卡内实体对加载操作没有限制；

3) 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；

4) 检查加载文件的 AID 没有在 GP 注册表中注册为可执行加载文件或者应用；

5) 如果请求中存在关联的安全域的 AID，则检查该 AID 是否在 GP 注册表中并且以“安全域权限”进行了注册。如果执行加载操作的安全域并未直接或间接与关联的安全域相关联，则检查关联的安全域是否接受此迁移。如果没有关联的 AID 被指定，则执行加载操作的安全域就成为默认的关联安全域；

6) 当收到执行加载操作的安全域的请求时，GP 环境会请求具备“令牌验证权限”的安全域对加载操作进行授权（即对加载过程令牌进行验证）。

c) 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应对加载过程令牌进行验证。

d) 当收到 GP 环境的请求时，接收隐式迁移的安全域应进行如下操作：

1) 实施安全域提供方的策略来决定是否认可该隐式迁移；

2) 实施自身的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

e) 当收到 LOAD 命令时，执行加载操作的安全域应符合以下规则：

1) 实施该安全域自身的安全通信策略；

2) 查找是否存在任何具备“强制 DAP 验证权限”的安全域，如存在，确保加载文件中含有需要的认证数据（鉴别该安全域的 DAP 数据块）；

3) 查找是否存在任何具备“DAP 验证权限”的安全域，如存在，确保加载文件中含有需要的认证数据（鉴别该安全域的 DAP 数据块）；

4) 当加载文件中含有认证数据（一个或多个 DAP 数据块）时，则应确保加载请求过程中收到加载文件数据块的散列值，并从加载文件中提取认证数据（一个或多个 DAP 数据块）；对于加载文件的每个 DAP 数据块，请求 GP 环境返回 DAP 数据块中指定安全域进行的 DAP 验证结果。

f) 当收到加载文件后，GP 环境应符合以下规则：

1) 对加载文件资源需求进行验证并确认卡片资源是充分可用的；

2) 检查执行加载操作的安全域发出的每个 DAP 验证请求，是否与 GP 注册表中注册的具备“DAP 验证权限”或“强制 DAP 验证权限”的安全域有关系；如有关联，则返回 DAP 验证的结果；

3) 当被要求验证某个 DAP 数据块或加载过程令牌时，计算加载文件数据块的散列值。

g) 当收到 GP 环境请求时，进行 DAP 验证的安全域应验证 DAP 与加载文件数据块散列值是否匹配。

h) 当收到最后一条 LOAD 命令时，执行加载操作的安全域应进行如下操作：

1) 实施自身的安全通信策略；

2) 请求 GP 环境返回一个加载过程收条。

i) 当加载过程结束时，GP 环境应符合以下规则：

1) 当收到执行加载操作的安全域请求时，验证加载请求中的加载文件数据块的散列值；

2) 查找 GP 注册表中是否存在任何具备“强制 DAP 验证权限”的安全域，如存在，确保该安全域已经成功地进行了一次 DAP 验证；

3) 查找 GP 注册表中是否存在任何具备“DAP 验证权限”的安全域，如存在，确保该安全域已经成功地进行了一次 DAP 验证；
4) 当执行了一个或多个 DAP 验证时，验证加载请求中的加载文件数据块的散列值；
5) 当安全域具备“委托管理权限”时，则确保具备“令牌验证权限”的安全域已经成功验证了相应的加载过程令牌；
6) 当执行了加载过程令牌的验证时，则验证加载请求中的加载文件数据块的散列值；
7) 利用加载文件数据块来创建一个可执行加载文件；
8) 在 GP 注册表中为该可执行加载文件创建一个条目并指明其关联的安全域；
9) 在 GP 注册表中为该可执行加载文件包含的每个可执行模块创建一个条目，该条目应包含安全域的加载请求中指明的应用提供方标识符。每个可执行模块关联的安全域与该可执行加载文件关联的安全域应是同一个安全域；
10) 当收到执行加载操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建一个加载过程收条。

j) 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应决定是否创建一个加载过程收条。

9.3.6 卡片内容的安装过程

9.3.6.1 管理要求

接收到 INSTALL [for install]命令的安全域在安装请求转发到 GP 环境之前，应对其进行处理。安装的内部处理过程应包括实例的创建和应用数据所需存储器的分配。可执行加载文件中的所有应用应关联到该可执行加载文件所关联的安全域，这些应用也可被迁移至其他安全域。

9.3.6.2 运行行为

内容安装过程中的运行行为应符合下列要求：

a) 当收到 INSTALL [for install]命令时，执行安装操作的安全域应执行以下规则：
1) 实施自身的安全通信策略；
2) 实施该安全域自身的安全策略，如检查其生命周期状态是否为已个人化状态；
3) 如执行安装操作的安全域具备“授权管理权限”，且发起安装请求的卡外实体没能被认证为对应的安全域提供方，则检查 INSTALL [for install]命令中是否存在一个安装过程令牌；
4) 如 INSTALL [for install]命令中存在一个安装过程令牌，则请求 GP 环境返回该安装过程令牌的验证结果；
5) 如安装请求中存在应用提供方标识符，则请求 GP 环境在 GP 注册表中为该应用保存对应的应用提供方标识符；
6) 请求 GP 环境返回安装过程收条。

b) 当收到安装请求时，GP 环境应执行以下规则：
1) 检查卡片生命周期状态不应为已锁定状态或者终结状态；
2) 检查 GP 环境和发起请求的卡内实体对安装操作没有限制；
3) 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；
4) 检查可执行模块的 AID 是否已经在 GP 注册表中进行了注册；
5) 检查应用的 AID 没有在 GP 注册表中注册为可执行加载文件或者应用；
6) 检查执行安装操作的安全域是否为用作应用安装来源的可执行模块所关联的安全域；如

执行安装操作的安全域没有直接或间接地与用作应用安装来源的可执行模块相关联，则应检查与该可执行模块关联的安全域是否接受此安装操作；

7) 当收到执行安装操作的安全域的请求时，GP 环境应请求具备“令牌验证权限”的安全域对安装操作进行授权；

8) 对加载文件资源需求进行验证，并确认卡片资源是充分可用的；

9) 按照底层的运行环境的要求，执行应用的安装操作；

10) 如执行安装操作的安全域具备“委托管理权限”，则应确保具备“令牌验证权限”的安全域对安装过程令牌进行成功的验证；

11) 从可执行模块创建一个应用；

12) 依据底层的运行环境的不同，确保安装的应用知道自身的 AID、权限以及安装参数；

13) 在 GP 注册表中为安装的应用创建条目并指明其关联的安全域、生命周期状态、权限，如安装请求中存在隐式选择、服务以及存储器资源的参数，应将其内容包含在该条目中；如安全域在安装请求中指定了应用提供方的标识符，应将其包含在该条目中；

14) 当收到执行安装操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建安装过程收条。

c) 当收到 GP 环境的请求时，相关的安全域应执行以下规则：

1) 实施安全域提供方的策略以决定接受或拒绝安装操作；

2) 实施自身的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

d) 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应对安装过程令牌进行验证。

e) 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应决定是否创建安装过程收条。

9.3.7 卡片内容的可选择化过程

9.3.7.1 管理要求

接收到 INSTALL[for make selectable]命令的安全域在该可选择化请求转发到 GP 环境之前，应对其进行处理。进行操作时，GP 环境应在 GP 注册表中注册附加信息。

9.3.7.2 运行行为

内容可选择化过程中的运行行为应符合下列要求：

a) 当收到 INSTALL [for make selectable]命令时，执行可选择化操作的安全域应执行以下规则：

1) 实施自身的安全通信策略；

2) 实施该安全域自身的安全策略，如检查其生命周期状态是否为已个人化状态；

3) 如执行可选择化操作的安全域具备“授权管理权限”，且发起可选择化请求的卡外实体没能被认证为对应的安全域提供方，则应检查 INSTALL [for make selectable]中是否存在一个可选择化过程令牌；

4) 如 INSTALL [for make selectable]中存在一个可选择化过程令牌，则应请求 GP 环境返回该可选择化过程令牌的验证结果；

5) 如可选择化请求中存在应用提供方标识符，则应请求 GP 环境在 GP 注册表中为该应用保存对应的应用提供方标识符；

6) 请求 GP 环境返回可选择化过程收条。

b) 当收到可选择化请求时，GP 环境应执行以下规则：

1) 检查卡片生命周期状态不应为已锁定状态或者终结状态；
2) 检查 GP 环境和发起请求的卡内实体对可选择化操作没有限制；
3) 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；
4) 检查可执行模块的 AID 是否已在 GP 注册表中进行了注册；
5) 检查执行可选择化操作的安全域是否直接或间接地与应用相关联；
6) 当收到执行可选择化操作的安全域的请求时，GP 环境应请求具备“令牌验证权限”的安全域对可选择化操作进行授权；
7) 按照底层的运行环境的要求，执行应用的可选择化操作；
8) 如执行可选择化操作的安全域具备“委托管理权限”，则应确保具备“令牌验证权限”的安全域对可选择化过程令牌进行了成功的验证；
9) 更新 GP 注册表中应用所对应的条目(权限和隐式选择参数等)；
10) 当收到执行可选择化操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建可选择化过程收条。

c) 当收到 GP 环境的请求时，相关的安全域应执行以下规则：
1) 实施安全域提供方的策略以决定接受或拒绝可选择化操作；
2) 实施自身的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

d) 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应对可选择化过程令牌进行验证。

e) 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应决定是否创建可选择化过程收条。

9.3.8 卡片内容的加载、安装和可选择化联合操作过程

9.3.8.1 命令序列

APDU 命令序列应符合下列要求：

a) INSTALL [for load, install and make selectable]命令应用于发起加载和安装的联合操作请求，该命令的数据域细化对加载文件的要求；

b) 根据文件和卡片通信缓冲区大小，多条 LOAD 命令应用于将加载文件进行分块后传输到卡片；

c) INSTALL [for load, install and make selectable]命令应用于完成加载和安装的联合操作过程，该命令的数据域细化对加载文件的要求；

d) 每条 INSTALL 或 LOAD 命令在加载请求或加载文件数据块被转发给 GP 环境处理前，应先由接收该命令的安全域进行处理。

9.3.8.2 运行行为

联合操作过程的运行行为应符合下列要求：

a) 当收到 INSTALL [for load, install and make selectable]命令后，执行加载和安装联合操作的安全域应执行以下规则：
1) 实施该安全域自身的安全通信策略；
2) 实施该安全域自身的安全策略，如检查其生命周期状态是否为已个人化状态；
3) 如 INSTALL [for load, install and make selectable]中存在加载文件数据块的散列值，则应请求 GP 环境对后续的加载文件数据块验证其散列值；
4) 如加载请求中存在应用提供方标识符，则应请求 GP 环境在 GP 注册表为该可执行加载文件保存该应用提供方标识符。

b) 当收到联合操作请求时，GP 环境应执行以下规则：

1) 检查卡片生命周期状态不应为已锁定状态或者终结状态；
2) 检查 GP 环境和发起请求的卡内实体对加载、安装和可选择化联合操作没有限制；
3) 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；
4) 检查加载文件的 AID 没有在 GP 注册表中注册为可执行加载文件或者应用；
5) 如请求中存在关联的安全域的 AID，则检查该 AID 是否在 GP 注册表中并且以“安全域权限”进行了注册。如执行联合操作的安全域并未直接或间接与关联的安全域相关联，则检查关联的安全域是否接受此迁移。如没有关联的 AID 被指定，则执行加载操作的安全域就成为默认的关联安全域。

c) 当收到 GP 环境的请求时，相关的安全域应执行以下规则：

1) 实施安全域提供方的策略以决定接受或拒绝加载、安装和可选择化联合操作；
2) 实施自身的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

d) 当收到 GP 环境的请求时，接收隐式迁移的安全域应符合下列要求：

1) 实施安全域提供方的策略来决定是否认可该隐式迁移；
2) 实施自身的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

e) 当收到 LOAD 命令时，执行加载操作的安全域应执行以下规则：

1) 实施该安全域自身的安全通信策略；
2) 查找是否存在任何具备“强制 DAP 验证权限”的安全域，如存在，确保加载文件中含有需要的认证数据（鉴别该安全域的 DAP 数据块）；
3) 查找是否存在任何具备“DAP 验证权限”的安全域，如存在，确保加载文件中含有需要的认证数据（鉴别该安全域的 DAP 数据块）；
4) 如加载文件中含有认证数据（一个或多个 DAP 数据块），则应确保加载、安装和可选择化联合操作过程中收到一个加载文件数据块的散列值；从加载文件中提取认证数据（一个或多个 DAP 数据块）；对于加载文件的每个 DAP 数据块，应请求 GP 环境返回 DAP 数据块中指定的安全域进行的 DAP 验证的结果。

f) 当收到加载文件后，GP 环境应执行以下规则：

1) 对加载文件资源需求进行验证，并确认卡片资源是充分可用的；
2) 检查执行加载操作的安全域发出的每个 DAP 验证请求，是否与 GP 注册表中注册的具备“DAP 验证权限”或“强制 DAP 验证权限”的安全域有关系；如果有，则应返回 DAP 验证的结果；
3) 当被要求验证某个 DAP 数据块或加载过程令牌时，应计算加载文件数据块的散列值。

g) 当收到 GP 环境的请求时，进行 DAP 验证的安全域应验证 DAP 与加载文件数据块的散列值是否匹配。

h) 当加载过程结束时，GP 环境应执行以下规则：

1) 当收到执行加载、安装和可选择化联合操作的安全域的请求时，则应验证加载、安装和可选择化联合操作请求中的加载文件数据块的散列值；
2) 查找 GP 注册表中是否存在任何具备“强制 DAP 验证权限”的安全域，如存在，确保该安全域已经成功地进行了一次 DAP 验证；
3) 查找 GP 注册表中是否存在任何具备“DAP 验证权限”的安全域，如存在，确保该安全域已经成功地进行了一次 DAP 验证；
4) 当执行了一个或多个 DAP 验证时，应验证加载请求中的加载文件数据块的散列值。

i) 当收到 INSTALL [for load, install and make selectable]命令时,执行加载和安装联合操作的安全域应执行以下规则:
   1) 实施自身的安全通信策略;
   2) 如执行安装操作的安全域具备"授权管理权限",且发起安装请求的卡外实体没能被认证为对应的安全域提供方,则应检查 INSTALL [for load, install and make selectable]中是否存在一个加载、安装和可选择化联合操作过程令牌;
   3) 如 INSTALL [for load, install and make selectable]中存在一个加载、安装和可选择化联合操作过程令牌,则应请求 GP 环境返回该令牌的验证结果;
   4) 如加载、安装和可选择化联合操作请求中存在应用提供方标识符,则应请求 GP 环境在 GP 注册表中为操作中的可执行加载文件和应用保存对应的应用提供方标识符;
   5) 请求 GP 环境返回一个加载、安装和可选择化联合操作过程收条。
j) 当加载、安装和可选择化联合操作过程结束时,GP 环境应执行以下规则:
   1) 如执行加载、安装和可选择化联合操作的安全域具备"委托管理权限",应确保具备"令牌验证权限"的安全域成功对令牌进行了验证;
   2) 利用加载文件数据块来创建一个可执行加载文件;
   3) 在 GP 注册表中,应为该可执行加载文件创建一个条目并指明其关联的安全域;
   4) 在 GP 注册表中。应为该可执行加载文件包含的每个可执行模块创建一个条目,该条目应包含安全域的加载请求中指明的应用提供方标识符。每个可执行模块关联的安全域与该可执行加载文件关联的安全域应是同一个安全域;
   5) 检查应用的 AID 没有在 GP 注册表中注册为可执行加载文件或者应用;
   6) 按照底层的运行环境的要求,执行应用的安装操作;
   7) 从可执行模块创建一个应用;
   8) 依据底层的运行环境的不同,确保安装的应用掌握自身的 AID、权限以及安装参数;
   9) 在 GP 注册表中为安装的应用创建一个条目,并指明其关联的安全域、生命周期状态、权限,如加载、安装和可选择化联合操作请求中存在,还应指明其隐式选择、服务以及存储器资源的参数等;
   10) 如安全域在加载、安装和可选择化联合操作请求中指定了应用提供方的标识符,应将其包含在该条目中;
   11) 验证应用资源请求,以保证可用的卡片资源充足。
k) 当收到 GP 环境的请求时,具备"令牌验证权限"的安全域应对加载、安装和可选择化联合操作过程令牌进行验证;
l) 当收到 GP 环境的请求时,具备"收条创建权限"的安全域应决定是否创建联合操作过程收条。

9.3.9 加载与安装流程示例

9.3.9.1 加载与安装流程

在 GP 平台卡片上以一个具有授权管理权限的安全域为例,执行应用的加载与安装,见图 10。

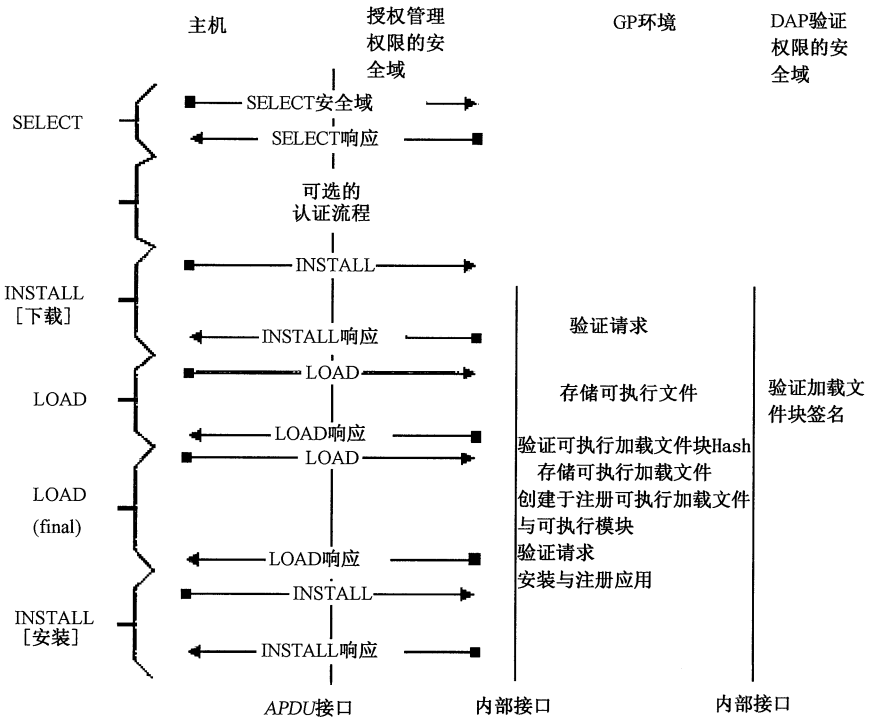


图 10　加载安装流程图

9.3.9.2　加载流程

在 GP 平台卡片上以一个具有授权管理权限的安全域为例，执行应用的加载，见图 11。

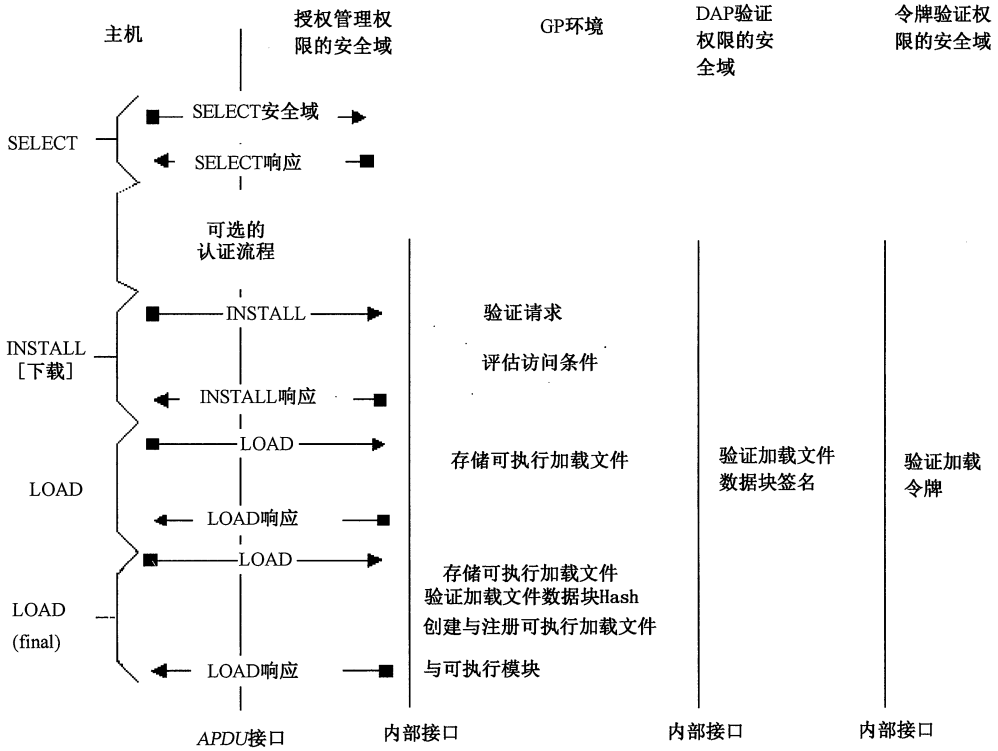


图 11　加载流程图

9.3.9.3 安装流程

在GP平台上以一个具有授权管理权限的安全域为例，当智能卡上已经存在可执行加载文件时，执行该可执行加载文件的应用安装，见图12。

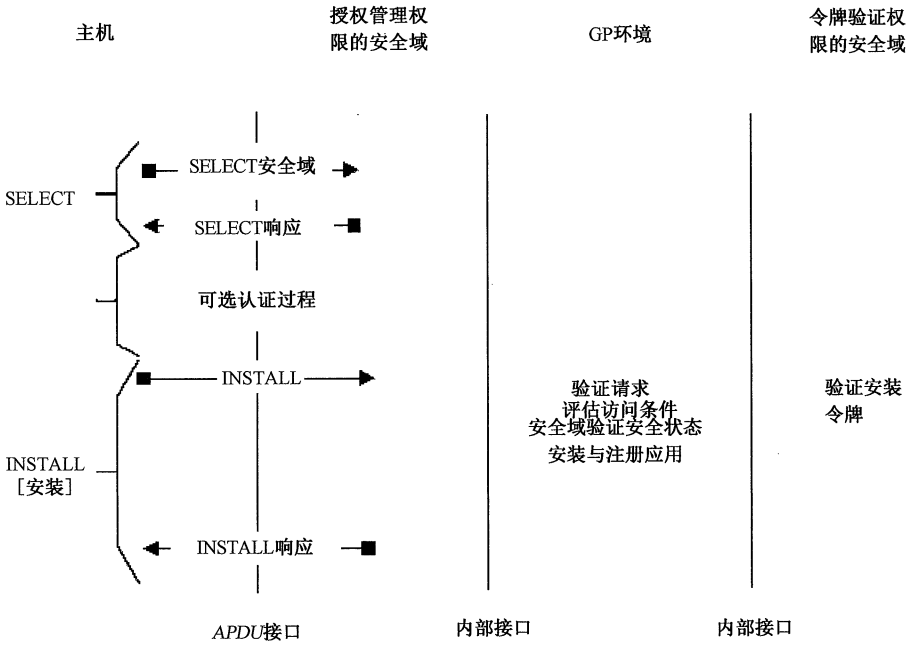


图12 安装流程图

9.4 内容的迁移和注册表的更新

9.4.1 内容的迁移

9.4.1.1 管理要求

内容迁移应符合下列管理要求：

a) 卡片内容迁移过程应允许先前安装的应用或先前加载的可执行加载文件关联到另一个安全域；

b) 迁移操作可在应用生命周期的任何时候进行，任何处于已个人化状态的安全域，或者既不处于已锁定状态也不处于终结状态的主控安全域，都能够接受被迁移的应用；

c) 迁移过程应由安全域处理的INSTALL [for extradition]命令构成，安全域应将迁移请求传给GP环境，以进行额外的验证和处理；

d) 迁移过程令牌应允许GP环境借助具备“令牌验证权限”的安全域，确保发卡方对迁移过程进行授权；

e) 当迁移过程结束后，应返回给执行委托管理操作的安全域一个可选的收条，且应被该安全域发送到卡外实体。

9.4.1.2 运行行为

内容迁移过程中的运行行为应符合下列要求：

a) 当收到INSTALL [for extradition]命令时，执行迁移操作的安全域应执行以下规则：

1) 实施该安全域自身的安全通信策略；

2） 实施该安全域自身的安全策略，如检查其生命周期状态是否为已个人化状态；
3） 如执行迁移操作的安全域具备“授权管理权限”，且发起迁移请求的卡外实体没能被认证为对应的安全域提供方，则应检查 INSTALL [for extradition]命令中是否存在一个迁移过程令牌；
4） 如 INSTALL [for extradition]命令中存在一个迁移过程令牌，则应请求 GP 环境返回该迁移过程令牌的验证结果；
5） 请求 GP 环境返回一个迁移过程收条。

b） 当收到迁移请求时，GP 环境应：
1） 检查卡片生命周期状态不应为已锁定状态或者终结状态；
2） 检查 GP 环境和发起请求的卡内实体对迁移操作没有限制；
3） 检查被迁移的应用或可执行加载文件是否已经在 GP 注册表中进行了注册；
4） 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；
5） 检查执行迁移操作的安全域是否直接或间接地与被迁移的应用或可执行加载文件相关联；
6） 检查 AID 与应用或可执行加载文件被迁移后将要关联到安全域相同的卡内实体，是否已经在 GP 注册表中进行了注册，并且具备“安全域权限”；
7） 如执行迁移操作的安全域没有直接或间接地与应用或可执行加载文件被迁移后将要关联到安全域相关联，则应检查后一个安全域是否接受此迁移操作；
8） 如执行迁移操作的安全域具备“委托管理权限”，则应确保具备“令牌验证权限”的安全域对迁移过程令牌进行了成功的验证；
9） 更新 GP 注册表中被迁移的应用和可执行加载文件对应的条目；
10） 当收到执行迁移操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建迁移过程收条。

c） 当收到 GP 环境的请求时，相关的安全域应执行以下规则：
1） 实施安全域提供方的策略以决定接受或拒绝迁移请求；
2） 实施自身的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

d） 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应对迁移过程令牌进行验证。

e） 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应决定是否创建迁移过程收条。

f） 当收到 GP 环境的请求时，接受显式迁移的安全域应符合下列要求：
1） 实施安全域提供方的策略，以决定是否接受还是拒绝迁移操作；
2） 实施该安全域自身的安全策略，如检查其生命周期状态是否为已个人化状态。

9.4.1.3 授权迁移流程

安全域请求迁移不需要关联被迁移的加载文件或应用，最初关联应用的安全域可配置是否接受迁移。授权迁移流程示例见图 13。

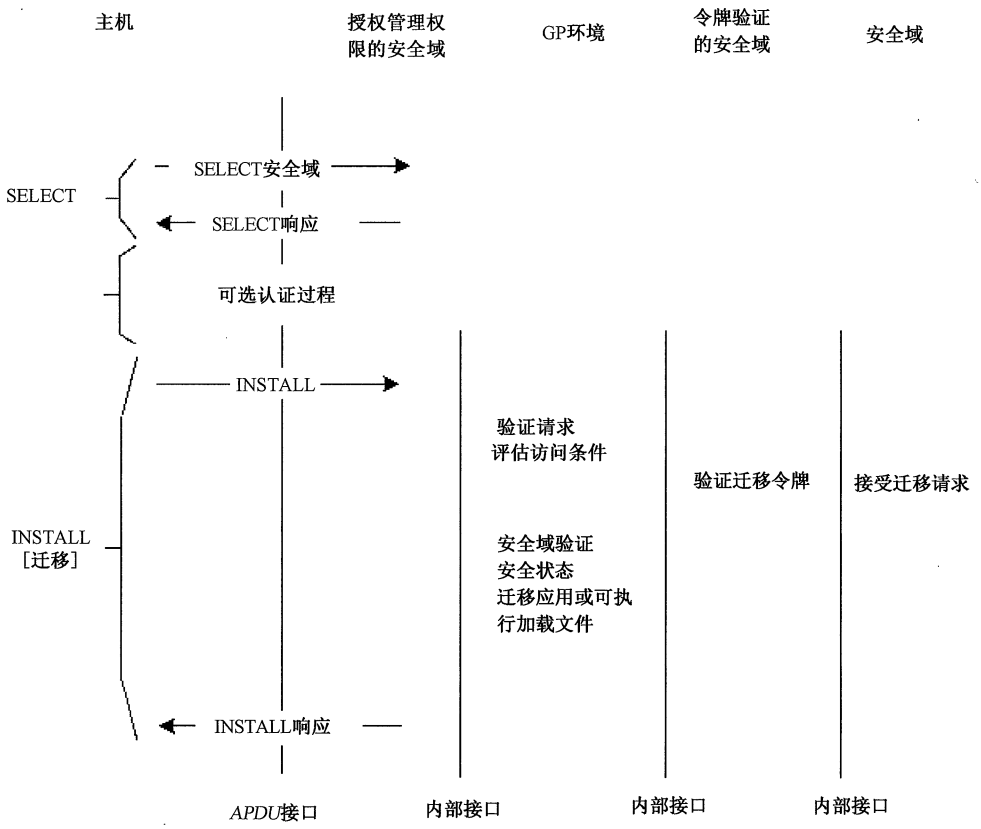


图 13　授权迁移流程图

9.4.2　注册表的更新

9.4.2.1　普通的注册表更新

9.4.2.1.1　管理要求

注册表更新应符合下列管理要求：

a) 注册表更新过程应允许对 GP 注册表中与应用关联的数据进行修改，该过程应允许对特定安全域甚至 GP 环境自身的卡片内容管理功能进行限制。

b) 注册表更新过程可在应用生命周期的任何时候，以及卡片生命周期的任何时候（卡锁定状态或终结状态除外）进行。

c) 注册表更新过程应由一条或多条 INSTALL [for registry update]命令构成，这些命令应由进行接收的安全域来处理。

d) 如要对 GP 环境的卡片管理功能进行限制，则不应在 INSTALL [for registry update]命令中指定 AID。安全域将注册表更新请求传给 GP 环境，以进行额外的验证和处理。

e) 注册表更新过程令牌允许 GP 环境借助具备“令牌验证权限”的安全域，确保发卡方对注册表更新过程进行授权。

f) 当注册表更新过程结束后，一个可选的收条被返回给执行委托管理操作的安全域，且应被该安全域发送到卡外实体。

9.4.2.1.2　运行行为

内容注册表更新过程中的运行行为应符合下列要求：

a) 当收到 INSTALL [for registry update]命令时，执行注册表更新操作的安全域应执行以下规则：
   1) 实施该安全域自身的安全通信策略；
   2) 实施该安全域自身的安全策略，比如检查其生命周期状态是否为已个人化状态；
   3) 如执行注册表更新操作的安全域具备“授权管理权限”，且发起注册表更新请求的卡外实体未被认证为对应的安全域提供方，则应检查 INSTALL [for registry update]命令中是否存在一个注册表更新过程令牌；
   4) 如 INSTALL [for registry update]命令中存在一个注册表更新过程令牌，则应请求 GP 环境返回该注册表更新过程令牌的验证结果；
   5) 请求 GP 环境返回一个注册表更新过程收条。
b) 当收到注册表更新请求时，GP 环境应执行以下规则：
   1) 检查卡片生命周期状态不应为卡锁定状态或者终结状态；
   2) 检查 GP 环境和发起请求的卡内实体对注册表更新操作没有限制；
   3) 检查其注册表信息被更新的应用是否已经在 GP 注册表中进行了注册；
   4) 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；
   5) 当对 GP 环境功能进行限制时，检查发起请求的卡内实体是否为具备“全局锁定权限”的安全域；
   6) 检查发起注册表更新请求的安全域是否直接或间接与其注册表信息被更新的应用相关联；
   7) 如执行注册表更新操作的安全域具备“委托管理权限”，则应确保具备“令牌验证权限”的安全域对注册表更新过程令牌进行了成功的验证；
   8) 更新 GP 注册表中其信息被更新的应用所对应的条目；
   9) 当收到执行注册表更新操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建一个注册表更新过程收条。
c) 当收到 GP 环境的请求时，相关的安全域应当执行以下规则：
   1) 实施安全域提供方的策略以决定接受或拒绝注册表更新；
   2) 实施自身的安全策略，比如检查自身的安全域生命周期状态是否为已个人化状态。
d) 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应对注册表更新过程令牌进行验证。
e) 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应实施发卡方的策略，以决定是否创建一个注册表更新过程收条。

9.4.2.2 注册表更新中的迁移操作

迁移操作可利用注册表更新过程完成，通过特定格式 INSTALL [for registry update]命令可同时完成迁移操作和注册表更新操作。当注册表更新操作需要令牌时，应使用注册表更新过程令牌；当注册表更新操作需要收条时，应使用注册表更新过程收条。

9.4.3 内容的删除

9.4.3.1 删除过程

内容的删除过程应通过对应用和/或可执行加载文件的删除。只有未被其他卡内实体引用的代码和数据才可被删除，并应符合下列要求：

a) DELETE 命令应允许对可变存储器上内容的物理删除和对只读存储器上内容的逻辑删除。DELETE 命令应先由接收到该命令的安全域先处理，再将该请求转发到 GP 环境处理。

b) 根据被删除的应用和可执行加载文件在存储器中存储位置不同，GP 环境应执行不同的动作。应用或可执行加载文件被删除后，其在存储器中的内容应被设置为不可访问。

c) 具备“全局删除权限”的安全域能够从卡片上删除任何应用或可执行加载文件，而不用考虑被删除的应用或可执行加载文件关联的安全域。

d) 应用提供方可指示 GP 环境删除自身关联的应用和可执行加载文件。根据发卡方的策略，GP 环境可能需要获得发卡方的预先授权。

e) 对 DELETE 命令的响应标志着删除过程的结束。当删除过程完全结束后，一个可选的收条应被返回给执行委托管理操作的安全域，且应被该安全域发送到卡外实体。

f) 应用提供方应将删除过程收条转发给其他相应的卡外实体，以作为删除过程已经成功执行的证据。

9.4.3.2 删除流程

应用和/或可执行加载文件的删除流程见图 14。

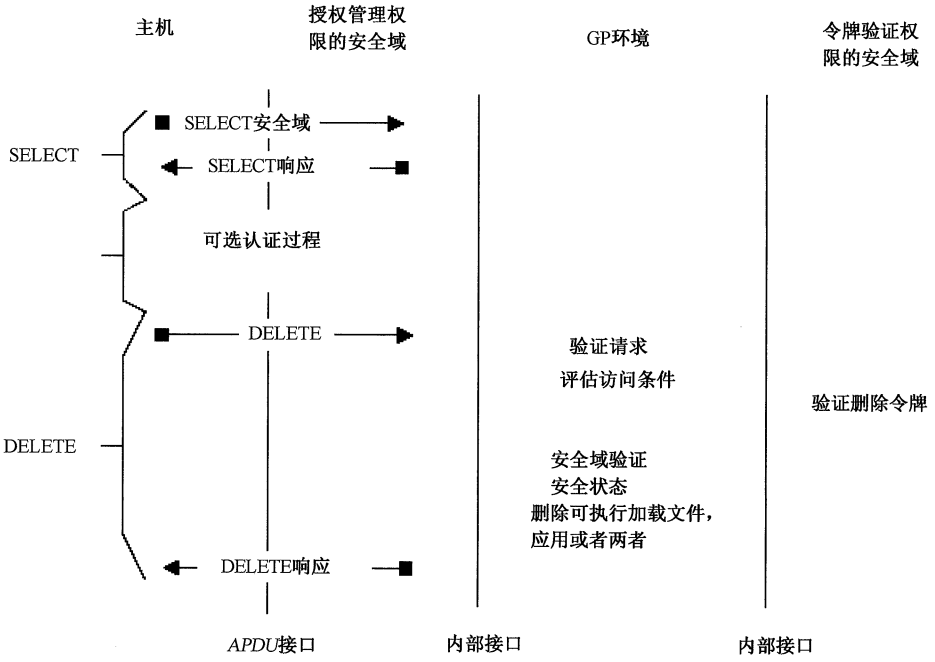


图 14 内容删除流程图

9.4.4 应用删除

9.4.4.1 管理要求

应用删除应包括应用实例的删除，以及与应用相关联的任何应用数据的删除。

9.4.4.2 运行行为

应用删除过程中的运行行为应符合下列要求：

a) 当收到删除应用的请求时，执行删除操作的安全域应执行以下规则：

1) 实施该安全域自己的安全通信策略；

2) 实施该安全域自己的安全策略，比如检查其生命周期状态是否为已个人化状态；

3) 如执行删除操作的安全域具备“授权管理权限”，且发起删除请求的卡外实体未被认证为

对应的安全域提供方，则应检查 DELETE 命令中是否存在一个删除过程令牌；

4） 如 DELETE 命令中存在一个删除过程令牌，则应请求 GP 环境返回该删除过程令牌验证结果；

5） 请求 GP 环境返回一个删除过程收条。

b） 当收到删除应用的请求时，GP 环境应执行以下规则：

1） 检查卡片生命周期状态不应为卡锁定状态或者终结状态；

2） 检查 GP 环境和发起请求的卡内实体对删除操作没有限制；

3） 检查被删除的应用是否已经在 GP 注册表中进行了注册；

4） 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；

5） 检查执行删除操作的安全域是否为与被删除应用直接或间接相关联的安全域，或者是否具备“全局删除权限”；如执行删除操作的安全域没有直接或间接地与被删除应用相关联，或者不具备“全局删除权限”，则应检查与该应用关联的安全域是否接受此删除操作；

6） 当收到执行删除操作的安全域的请求时，GP 环境应请求具备“令牌验证权限”的安全域对删除过程令牌进行验证；

7） 判断被删除的应用并非其他逻辑通道上的已选择应用；

8） 判断卡片上没有其他应用引用了被删除应用；

9） 判断卡片上没有其他应用引用了被删除应用内的任何数据；

10） 如删除的是一个安全域，判断卡片上没有任何引用或可执行加载文件与该安全域相关联；

11） 如执行删除操作的安全域具备“委托管理权限”，则应确保具备“令牌验证权限”的安全域对删除过程令牌进行了成功的验证；

12） 删除 GP 注册表中被删除应用所对应的条目；

13） 根据“权限分配”的定义，应将被删除应用的可再分配的权限，重新分配给主控安全域；

14） 根据“隐式选择的分派”的定义，如被删除应用是隐式可选择的，则应重新将主控安全域设为隐式已选定应用；

15） 如卡片支持的话，释放被删除应用占用的可变存储器，将其标记为可用的，并执行“存储器资源管理”中描述的存储器资源管理规则；

16） 当收到执行删除操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建一个删除过程收条。

c） 当收到 GP 环境的请求时，相关的安全域应执行以下规则：

1） 实施安全域提供方的策略以决定接受或拒绝该应用的删除；

2） 实施自己的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

d） 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应实施发卡方的策略，以决定是否接受或是拒绝没有删除过程令牌的删除授权请求；或者对删除过程令牌进行验证。

e） 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应实施发卡方的策略，以决定是否创建一个删除过程收条。

9.4.5 可执行加载文件的删除

9.4.5.1 管理要求

可执行加载文件的删除应符合下列要求：

a） 删除操作应针对整个可执行加载文件；

b） 可变存储器应执行物理删除；

c) 只读存储器应执行逻辑删除。

9.4.5.2 运行行为

可执行加载文件删除过程中的运行行为应符合下列要求：

a) 当收到删除可执行加载文件的请求时，执行删除操作的安全域应执行以下规则：
   1) 实施该安全域自己的安全通信策略；
   2) 实施该安全域自己的安全策略，如检查其生命周期状态是否为已个人化状态；
   3) 如执行删除操作的安全域具备“授权管理权限”，且发起删除请求的卡外实体未被认证为对应的安全域提供方，则应检查 DELETE 命令中是否存在一个删除过程令牌；
   4) 如 DELETE 命令中存在一个删除过程令牌，则应请求 GP 环境返回该删除过程令牌验证结果；
   5) 请求 GP 环境返回一个删除过程收条。
b) 当收到删除可执行加载文件的请求时，GP 环境应执行以下规则：
   1) 检查卡片生命周期状态不应为卡锁定状态或者终结状态；
   2) 检查 GP 环境和发起请求的卡内实体对删除操作没有限制；
   3) 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；
   4) 检查执行删除操作的安全域是否为与被删除的可执行加载文件直接或间接相关联的安全域，或者是否具备“全局删除权限”；如执行删除操作的安全域没有直接或间接地与被删除的可执行加载文件相关联，或者不具备“全局删除权限”，则应检查与该可执行加载文件关联的安全域是否接受此删除操作；
   5) 当收到执行删除操作的安全域的请求时，GP 环境应请求具备“令牌验证权限”的安全域对删除过程令牌进行验证；
   6) 判断被删除的可执行加载文件是否已经在 GP 注册表中进行了注册；
   7) 判断卡片上没有其他应用或可执行加载文件引用了被删除的可执行加载文件；
   8) 如执行删除操作的安全域具备“委托管理权限”，则应确保具备“令牌验证权限”的安全域对删除过程令牌进行了成功的验证；
   9) 删除 GP 注册表中被删除的可执行加载文件所对应的条目，以及该可执行加载文件中的所有可执行模块所对应的条目；
   10) 如卡片支持的话，释放被删除的可执行加载文件占用的可变存储器，将其标记为可用的，并执行存储器资源管理规则；
   11) 当收到执行删除操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建一个删除过程收条。
c) 当收到 GP 环境的请求时，相关的安全域应当执行以下规则：
   1) 实施安全域提供方的策略以决定接受或拒绝该可执行文件的删除；
   2) 实施自己的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。
d) 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应实施发卡方的策略，以决定是否接受或是拒绝没有删除过程令牌的删除授权请求；或者对删除过程令牌进行验证。
e) 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应实施发卡方的策略，以决定是否创建一个删除过程收条。

9.4.6 可执行加载文件和相关应用的删除

9.4.6.1 管理要求

可执行加载文件应包含可执行模块，应用应通过相关的可执行模块安装，并应符合下列要求：

a) 可执行加载文件的删除可能伴随着相关应用的删除；
b) 可变存储器应执行物理删除；
c) 只读存储器应执行逻辑删除。

9.4.6.2 运行行为

可执行加载文件和相关应用的删除过程中的运行行为应符合下列要求：

a) 当收到删除可执行加载文件的请求时，执行删除操作的安全域应执行以下规则：
   1) 实施该安全域自身的安全通信策略；
   2) 实施该安全域自身的安全策略，如检查其生命周期状态是否为已个人化状态；
   3) 如执行删除操作的安全域具备“授权管理权限”，且发起删除请求的卡外实体未被认证为对应的安全域提供方，则应检查 DELETE 命令中是否存在一个删除过程令牌；
   4) 如 DELETE 命令中存在一个删除过程令牌，则应请求 GP 环境返回该删除过程令牌验证结果；
   5) 请求 GP 环境返回一个删除过程收条。
b) 当收到删除可执行加载文件和相关应用的请求时，GP 环境应执行以下规则：
   1) 检查卡片生命周期状态不应为卡锁定状态或者终结状态；
   2) 检查 GP 环境和发起请求的卡内实体对删除操作没有限制；
   3) 检查发起请求的卡内实体是否为具备“委托管理权限”或者“授权管理权限”的安全域；
   4) 检查执行删除操作的安全域是否为与每个被删除应用直接或间接相关联的安全域，或者是否具备“全局删除权限”；如执行删除操作的安全域没有直接或间接地与一个或多个被删除应用相关联，或者不具备“全局删除权限”，则应检查与该应用关联的安全域是否接受此删除操作；
   5) 检查执行删除操作的安全域是否为与被删除的可执行加载文件直接或间接相关联的安全域，或者是否具备“全局删除权限”；如执行删除操作的安全域没有直接或间接与被删除的可执行加载文件相关联，或者不具备“全局删除权限”，则应检查与该可执行加载文件关联的安全域是否接受此删除操作；
   6) 当收到执行删除操作的安全域的请求时，GP 环境应请求具备“令牌验证权限”的安全域对删除过程令牌进行验证；
   7) 如执行删除操作的安全域具备“委托管理权限”，则应确保具备“令牌验证权限”的安全域对删除过程令牌进行了成功的验证；
   8) 判断被删除的可执行加载文件和相关应用是否已经在 GP 注册表中进行了注册；
   9) 查找以可执行加载文件包含的可执行模块作为安装来源的每个应用，且应判断被删除应用并非为查找到的应用其他逻辑通道上的已选择应用；判断卡片上没有其他应用引用了被删除应用；判断卡片上没有其他应用引用了被删除应用内的任何数据；如被删除的是一个安全域，判断卡片上没有任何引用或可执行加载文件与该安全域相关联；
   10) 判断卡片上没有其他应用或可执行加载文件引用了被删除的可执行加载文件；
   11) 删除 GP 注册表中被删除的可执行加载文件所对应的条目，以及该可执行加载文件中的所有可执行模块所对应的条目；
   12) 删除 GP 注册表中被删除的相关应用所对应的条目；
   13) 根据“权限分配”的定义，将被删除相关应用的可再分配权限，重新分配给主控安全域；
   14) 根据“隐式选择的分派”的定义，如被删除的相关应用是隐式可选择的，则应重新将主控安全域设为隐式已选定应用；
   15) 如卡片支持的话，释放被删除的可执行加载文件占用的可变存储器，将其标记为可用

的，并执行存储器资源管理规则；

16） 当收到执行删除操作的安全域的请求时，GP 环境应请求具备“收条创建权限”的安全域创建一系列的删除过程收条，一个用于可执行加载文件的删除，另一个用于每个相关应用的删除。

c） 当收到 GP 环境的请求时，相关的安全域应执行以下规则：

1） 实施安全域提供方的策略以决定接受或拒绝该可执行文件及其相关应用的删除；

2） 实施自己的安全策略，如检查自己的安全域生命周期状态是否为已个人化状态。

d） 当收到 GP 环境的请求时，具备“令牌验证权限”的安全域应实施发卡方的策略，以决定是否接受没有删除过程令牌的删除授权请求；或者对删除过程令牌进行验证。

e） 当收到 GP 环境的请求时，具备“收条创建权限”的安全域应实施发卡方的策略，以决定是否创建一个删除过程收条。

9.5 安全管理

9.5.1 生命周期管理

用于管理卡内实体生命周期的服务集应至少包括：

a） 应用的锁定和解锁；

b） 卡片的锁定和解锁；

c） 卡片的终结；

d） 应用生命周期的查询；

e） 卡片生命周期的查询。

生命周期管理服务流程见图 15。

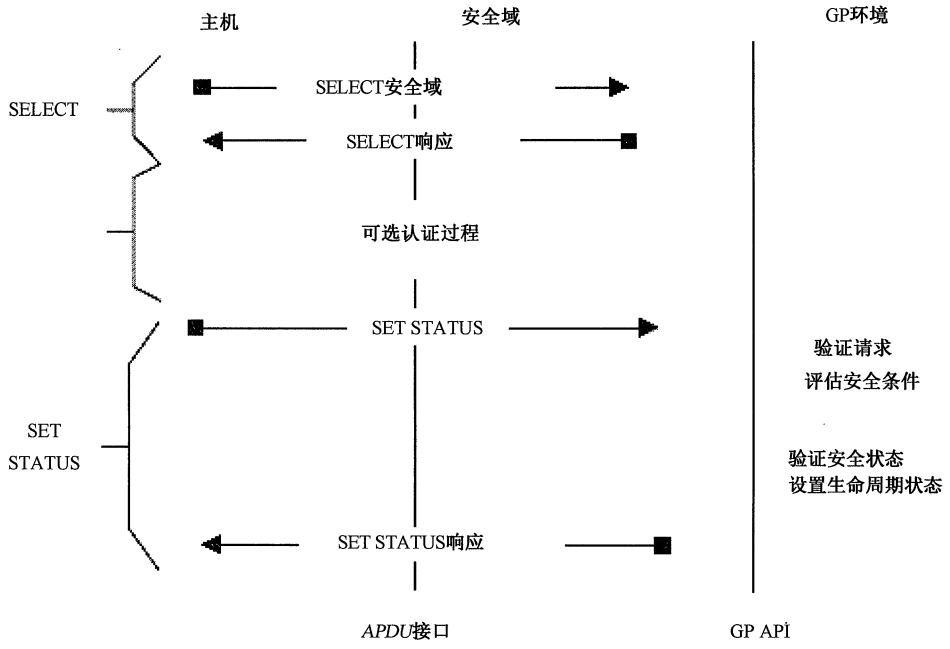


图 15 生命周期管理流程图

9.5.2 应用的锁定和解锁

可对应用进行锁定的卡内实体应包括具备“全局锁定权限”的应用、将要被锁定的应用、与其直接或

间接关联的安全域。可对被锁定的应用进行解锁的卡内实体应包括具备“全局锁定权限”的应用、与被锁定的应用直接或间接关联的安全域。并符合下列要求：

a) 当收到 SET STATUS 命令时，执行生命周期管理的安全域应执行以下规则：
   1) 实施该安全域自身的安全通信策略；
   2) 检查确认发起锁定或解锁请求的卡外实体可被认证为应用提供方或是目标应用的安全域提供方。
b) 当收到锁定或解锁应用的请求时，GP 环境应执行以下规则：
   1) 检查确认发起请求的卡内实体就是被锁定或解锁的应用自身，与其直接或间接关联的安全域，或者具备“全局锁定权限”的应用；
   2) 检查确认发起解锁操作的卡内实体不是被执行解锁操作的应用自身；
   3) 检查确认被锁定或解锁的应用已在 GP 注册表中进行了注册，且不具备“最终应用权限”；
   4) 对于锁定操作，应将应用的生命周期状态设置为已锁定状态；
   5) 对于解锁操作，应将应用的生命周期状态设置为其被锁定前的状态；
   6) 对于锁定操作，应将应用被锁定前的生命周期状态记录下来，以确保将来可以且只可以向后迁移到该状态。

9.5.3 卡片的锁定和解锁

9.5.3.1 管理要求

当卡片的生命周期状态被设为已锁定状态，则只有具备“最终应用权限”的应用可对其进行操作。卡片的锁定操作应通过适当的安全机制和授权执行。

9.5.3.2 锁定请求来源

卡片锁定请求有以下两个来源：

a) 卡内来源：GP 环境、主控安全域或者授权的应用都可从卡片内部发起卡片锁定请求。这些内部请求有可能是对卡片的某种运行状况的响应；
b) 卡外来源：显式的卡片锁定请求可由发卡方向主控安全域，或是某个授权的代理向某个具备“卡片锁定权限”的应用，发出 APDU 命令来发起。

9.5.3.3 执行操作

卡片锁定和解锁应符合下列要求：

a) 当收到 SET STATUS 命令时，执行生命周期管理的安全域应执行以下规则：
   1) 实施该安全域自身的安全通信策略；
   2) 检查确认发起锁定或解锁请求的卡外实体可被认证为安全域提供方。
b) 当收到锁定卡片的请求时，GP 环境应执行以下规则：
   1) 检查确认发起请求的卡内实体具备“卡片锁定权限”的应用；
   2) 检查确认卡片的生命周期状态为安全状态；
   3) 将卡片的生命周期状态设为已锁定状态。
c) 当收到解锁卡片的请求时，GP 环境应执行以下规则：
   1) 检查确认发起请求的卡内实体具备“卡片锁定权限”的应用；
   2) 将卡片的生命周期状态设置为安全状态。

9.5.4 卡片终结

9.5.4.1 管理要求

当卡片生命周期状态为终结状态时，所有发送到卡片的通信应直接分派到具备“最终应用权限”的应用。卡片终结操作应通过适当的安全机制和授权来执行。

9.5.4.2 终结操作

卡片终结操作应满足下列情况之一：

a) 卡内来源：GP 环境、主控安全域或者授权的应用都可从卡片内部发起卡片终结请求；

b) 卡外来源：显式的卡片锁定请求，可由发卡方向主控安全域，或是某个授权的代理向某个具备“卡片终结权限”的应用，发出 APDU 命令来发起。

9.5.4.3 执行操作

卡片的终结应符合下列要求：

a) 当收到 SET STATUS 命令时，执行生命周期管理的安全域应执行以下规则：

1) 实施该安全域自身的安全通信策略；

2) 检查确认发起终结请求的卡外实体可被认证为安全域提供方。

b) 当收到终结卡片的请求时，GP 环境应执行以下规则：

1) 检查确认发起请求的卡内实体具备“卡片终结权限”；

2) 将卡片的生命周期状态设置为终结状态。

9.5.5 应用状况查询

应用(或安全域)的状况，如生命周期状态、权限以及其他在 GP 注册表中注册的参数等，可被适当授权的实体所访问。当收到 GET STATUS 命令时，执行生命周期查询的安全域应执行以下规则：

a) 实施该安全域自身的安全通信策略；

b) 检查确认发起查询请求的卡外实体可认证为被查询应用的应用提供方或安全域提供方。

9.5.6 卡片状况查询

卡片和主控安全域的状况可被适当授权的实体所访问。当收到 GET STATUS 命令时，执行生命周期查询的安全域应执行以下规则：

a) 实施该安全域自身的安全通信策略；

b) 检查确认发起查询请求的卡外实体为已认证的安全域提供方。

9.5.7 操作频度检测

9.5.7.1 检测范围

GP 环境应实现频度检测安全机制，频度检测应是对卡片上的安全敏感活动的主动监控、处理和控制，并应至少包括：

a) 内容安装；

b) 卡片异常；

c) 应用异常。

9.5.7.2 内容加载和安装

GP 环境可跟踪尝试加载和安装一个特定应用的连续失败次数，或者所有应用尝试失败总次数。防御性措施应包括锁定或终结卡片。

9.5.7.3 异常

当 GP 环境创建异常时，也可实现频度检测。跟踪用的缓冲区和事件日志可用来作为频度检测的补充。

9.5.8 跟踪和事件日志

卡片上可允许跟踪和事件日志功能，但应根据发卡方安全策略的要求来实现。

9.6 存储器资源管理

存储器资源管理数据元素描应包括可变存储器和只读存储器的使用需求，以及对每种存储对象（代码和数据）的使用需求，并应符合下列要求：

a) 当卡片支持存储器资源管理时，GP 环境应根据对应的存储器资源管理数据元素的描述，来分配每种可用的存储器资源。存储器资源的分配应执行以下规则：
   1) 为可执行加载文件分配最小存储器，不得减少卡片上当前的可用存储器；
   2) 为应用分配存储器配额，不得减少卡片上当前的可用存储器；
   3) 分配给应用的存储器配额的数量，不得小于该应用的保留存储器；
   4) 为可执行加载文件和应用分配其保留存储器。

b) 当卡片支持存储器资源管理时，GP 环境应执行以下规则：
   1) 当加载请求到达时，卡片应满足最小可用存储器的要求；
   2) 当成功加载了一个可执行加载文件（即执行了最后一条 LOAD 命令）后，分配给该可执行加载文件的有效存储器应先从其保留存储器划拨。如没有保留存储器分配给该可执行加载文件，则卡片的当前可用存储器资源的数量应相应减少；
   3) 当某个应用的安装请求到达时，分配给该应用的有效存储器应先从其保留存储器划拨，直到保留存储器完全耗尽。如保留存储器已经耗尽，则其余分配给该应用的存储器应先从其存储器配额划拨，且卡片的当前可用存储器资源的数量应相应减少。如该应用的存储器配额或卡片的当前可用存储器资源已耗尽，则该应用的安装失败；
   4) 成功删除可执行加载文件或者应用，应通过有效释放该可执行加载文件或应用的保留存储器，来增加卡片的当前可用存储器资源；
   5) 当某个应用创建数据时，分配给该应用的有效存储器应先从其保留存储器划拨，直到保留存储器完全耗尽。如果保留存储器已耗尽，则其余分配给该应用的存储器应先从其存储器配额划拨，且卡片的当前可用存储器资源的数量应相应减少。如该应用的存储器配额或卡片的当前可用存储器资源已耗尽，则该存储器资源分配失败；
   6) 对存储器资源的报告结果与具体的实现有关；
   7) 当某个应用删除数据后，其释放的存储器应重新分配为该应用的保留存储器和存储器配额。如没有保留存储器分配给该应用，则卡片可用的存储器资源大小应增加。

10 安全通信

10.1 管理要求

GP 的安全通信特性应包括安全传送 APDU 命令，在多数流程中都隐含可选的认证过程，创建安全通道的能力，应用能够使用安全域的服务等。安全通信协议应为安全域和应用与卡外实体之间的通信提供安全的环境。

10.2 安全通道

安全通道应在应用会话期间为卡片和卡外实体提供安全的通信路径。安全通道会话可划分为以下三个连续阶段：

a) 安全通道发起：卡内应用和卡外实体已交换具备加密功能所需的信息。安全通道会话的发起应包含卡上应用对卡外实体的认证；

b) 安全通道运行：卡内应用和卡外实体应利用安全通道会话提供的加密保护进行数据交换。根据安全通道协议的不同，安全通道服务可能有所不同；

c) 安全通道终止：当卡内应用或卡外实体的某一方判断出没有必要继续进行通信时，该通道就会被终止。

10.3 显式和隐式安全通道

10.3.1 管理要求

安全通道会话在成功发起后应被打开，并包括卡内应用对卡外实体的认证过程。在同一安全信道会话成功结束最后一次通信后，安全通道会话应被终止。

10.3.2 显式安全通道开启

显式安全通道的开启应通过卡外实体发送 APDU 命令，或卡内应用调用 API 来开启安全通道会话。卡外实体可采用 APDU 命令在当前安全通道会话中，指定所采用的安全级别(完整性和机密性)，并使得卡外实体可选择要用到的密钥。

10.3.3 隐式安全通道开启

当卡片在收到第一个包含加密保护的 APDU 命令时，由安全通道协议处理器直接或调用 API 的方式，初始化安全通道会话。安全通信协议处理器应默认安全级别和密钥，或是在发起安全通道会话前，由卡外实体通过 APDU 命令指定密钥。

10.3.4 安全通道终止

10.3.4.1 管理要求

安全通道会话的终止应通过卡内应用调用 API 或是卡外实体发送 APDU 命令实现。当新的安全通道会话在其他逻辑通道上建立时，现有逻辑通道上的安全通道会话不会被终止。当安全通道会话终止时，所有的会话数据应被重置，完整性检测向量和会话密钥应被删除。

10.3.4.2 正常终止

安全通道会话在以下情况发生时应终止：

a) 卡片应用会话被终止；

b) 相关逻辑通道的显式关闭；

c) 卡片被复位或掉电。

10.3.4.3 异常中止

当安全通道会话异常中止时，则开启安全级别应设置为 NO_SECURITY，会话安全级别不应被复位，错误条件应保持至安全通道会话被终止。安全通道会话在以下情况发生时应异常中止：

a) 卡片应用收到包含错误的加密保护的 APDU 命令；

b) 卡片应用收到的 APDU 命令缺乏安全通道会话期间建立的加密保护。

10.4 安全通道协议的直接/间接处理

卡片应用通过两种方式处理安全通道协议：

a) 直接处理：应用拥有自身的整套安全通道密钥且完全实现了安全通道协议；

b) 间接处理：应用调用安全域服务来处理安全通道协议，利用这些服务可允许独立于卡片支持的安全通道协议的应用被编码。

10.5 实体认证

10.5.1 对称加密算法下的认证

当使用对称加密的安全通道协议时，可信的卡外实体应拥有开启安全通道会话所需密钥的实体。卡片应无法区分安全域实际的提供方和拥有其安全通道密钥的代理方。卡片应无法区分安全域提供方和安全域某个关联应用的提供方。

10.5.2 非对称加密下的认证

当使用非对称加密的安全通道协议时，应获得一个对其公钥进行签名的证书的卡外实体，并能够被安全域认证成功。卡片应能够区分安全域提供方、安全域某个关联应用提供方或其他卡外实体，三者不必是同一实体。每个卡内实体的应用提供方 ID 在该实体的加载和安装过程中，应注册到 GP 全局注册表，且不应被改变。

10.6 安全的消息传送

在发送消息到接收实体之前，应允许发送实体向 APDU 消息中添加机密性和/或完整性及可信性数据作为其组成部分，并应符合下列要求：

a) 发送给卡片的 APDU 命令应具备完整性、机密性；

b) 通过安全通道会话发送给卡片的 APDU 命令序列应具备完整性；

c) 根据采用的安全通道协议，卡片发送的 APDU 响应应具备机密性、完整性。

10.7 安全级别

在整个会话或单独命令响应期间，安全级别应建立对消息发送的最低安全保护。当前安全级别的编码应符合表 3 的规定。安全通道协议的运作应依据已建立的安全级别，包括以下两种情形：

a) 在安全通道会话开启时，明确或隐含地设置强制性安全级别；

b) 针对某个独立的命令或响应，设置安全级别。

表 3 当前安全级别编码

b8	b7	b6	b5	b4	b3	b2	b1	描述
1	0	—	—	—	—	—	—	AUTHENTICATED
0	1	—	—	—	—	—	—	ANY_AUTHENTICATED
—	—	—	—	—	—	1	—	C_DECRYPTION
—	—	—	—	—	—	—	1	C_MAC
—	—	1	—	—	—	—	—	R_ENCRYPTION
—	—	—	1	—	—	—	—	R_MAC
—	—	—	—	X	X	—	—	RFU
0	0	0	0	0	0	0	0	NO_SECURITY_LEVEL

注：当前安全级别不能同时设置成 AUTHENTICATED 指示器和 ANY_AUTHENTICATED 指示器。

10.8 安全通道协议标识符

安全通道协议标识符应标志着在安全域中实现具体的安全通信协议和安全服务。下列内容可作为安全通道协议标识符：

a) “00”不可用；

b) “01”～“7F”保留 GP 将来使用，其中包含如下规定：

1) “01”为安全通道协议 1；

2) “02”为安全通道协议 2；

3) “10”为安全通道协议 10；

c) “80”～“EF”保留用于 GP 注册的个人用途，其中“80”为安全通道协议 80；

d) “F0”～“FF”保留用于未被 GP 注册的个人用途。

11 应用协议数据单元(APDU)命令

11.1 命令范围和安全级别

11.1.1 命令范围

GP APDU 命令应用于实现卡片生命周期状态转换与查询、包括密钥在内的卡片数据的装载与删除、安全通道的建立以及逻辑通道管理等，具体的指令包括：

a) DELETE 命令：用于删除卡上安全域的密钥、应用实例、包；

b) GET DATA 命令：用于获取卡上非敏感数据的数据内容；

c) GET STATUS 命令：用于获取卡片目前的生命周期状态；

d) INSTALL 命令：用于包下载的开启、应用实例的安装；

e) LOAD 命令：用于包的安装；

f) MANAGE CHANNEL 命令：用于逻辑通道的开启与关闭；

g) PUT KEY 命令：用于安全域密钥的加载；

h) SELECT 命令：用于应用实例的选择；

i) SET STATUS 命令：用于卡片生命周期的设置；

j) STORE DATA 命令：用于卡片数据的装载；

k) INITIALIZE UPDATE:用于初始化安全通道;

l) EXTERNAL AUTHENTICATE:结合 INITIALIZE UPDATE,用于外部认证并建立安全通道。

指令的具体要求可参考 GP 规范最新版本。对这些指令在不同的生命周期及安全级别下的执行条件见表 4。

表 4 每个卡生命周期状态被认证的 GP 命令

命令	准备			初始化			安全			卡锁定		终结	
	AM SD	DM SD	SD	AM SD	DM SD	SD	AM SD	DM SD	SD	FA SD	SD	FA SD	SD
DELETE Executable Load File	—	—	~	—	—	~	—	—	~	~	~	~	~
DELETE Executable Load File and related Application(s)	—	—	~	—	—	~	—	—	~	~	~	~	~
DELETE Application	√	—	~	√	—	~	√	—	~	~	~	~	~
DELETE Key	—	—	—	—	—	—	—	—	—	~	~	~	~
GET DATA	√	√	√	√	√	√	√	√	√	√	~	√	~
GET STATUS	√	—	—	√	—	—	√	—	—	√	~	~	~
INSTALL [for load]	—	—	~	—	—	~	—	—	~	~	~	~	~
INSTALL [for install]	—	—	~	—	—	~	—	—	~	~	~	~	~
INSTALL [for load, install and make selectable]	—	—	~	—	—	~	—	—	~	~	~	~	~
INSTALL [for install and make selectable]	√	√	~	√	√	~	√	√	~	~	~	~	~
INSTALL [for make selectable]	—	—	~	—	—	~	—	—	~	~	~	~	~
INSTALL [for extradition]	—	—	~	—	—	~	—	—	~	~	~	~	~
INSTALL [for registry update]	—	—	~	—	—	~	—	—	~	~	~	~	~
INSTALL [for personalization]	—	—	—	—	—	—	—	—	—	~	~	~	~
LOAD	—	—	~	—	—	~	—	—	~	~	~	~	~
PUT KEY	√	—	—	√	—	—	√	—	—	~	~	~	~
SELECT	√	√	√	√	√	√	√	√	√	√	~	~	~

表 4（续）

命令	准备			初始化			安全			卡锁定		终结	
	AM SD	DM SD	SD	AM SD	DM SD	SD	AM SD	DM SD	SD	FA SD	SD	FA SD	SD
SET STATUS	√	—	—	√	—	—	√	—	—	√	～	～	～
STORE DATA	√	—	—	√	—	—	√	—	—	～	～	～	～

表中符号含义如下：
AM SD：授权管理者安全域；
DM SD：带有委托管理权限的应用提供者安全域；
FA SD：带有最终应用权限的安全域；
SD：其他安全域；
√：必备；
～：可选；
—：禁止。

11.1.2 命令最小安全级别

APDU 命令的最小安全级别要求见表 5。

表 5 GP 命令的最小安全级别

命令	最小安全级别
DELETE	安全通道的开启或数字签名验证
GET DATA	无
GET STATUS	安全通道的开启
INSTALL	安全通道的开启或数字签名验证
LOAD	安全通道的开启或数字签名验证
MANAGE CHANNEL	不适用
PUT KEY	安全通道的开启
SELECT	不适用
SET STATUS	安全通道的开启
STORE DATA	安全通道的开启

11.2 编码规则

11.2.1 生命周期编码

可执行的装载文件的生命周期被编码见表 6 所描述的一个字节。

表 6　可执行装载文件的生命周期编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	1	已加载

应用的生命周期被编码见表 7 所描述的一个字节。

表 7　应用的生命周期编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	1	1	已安装
0	0	0	0	0	1	1	1	可选择
0	X	X	X	X	1	1	1	应用特定状态
1	—	—	—	—	—	1	1	卡锁定
应用可以自由使用 4～7 位，并且这些位的编码应超出本标准的范围。								

安全域的生命周期被编码见表 8 所描述的一个字节。

表 8　安全域的生命周期编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	1	1	已安装
0	0	0	0	0	1	1	1	可选择
0	0	0	0	1	1	1	1	已个人化
1	0	0	0	X	X	1	1	卡锁定

发行者安全域继承卡的生命周期状态编码见表 9。

表 9　发行者安全域的生命周期编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	1	准备
0	0	0	0	0	1	1	1	初始化
0	0	0	0	1	1	1	1	安全
0	1	1	1	1	1	1	1	卡锁定
1	1	1	1	1	1	1	1	终结

11.2.2　应用权限编码

应用的权限被编码见表 10～表 12，一个应用可以有一个或多个权限。

表 10 权限(字节 1)

b8	b7	b6	b5	b4	b3	b2	b1	含义	特权序号
1	—	—	—	—	—	—	—	安全域	0
1	1	—	—	—	—	—	0	DAP 验证	1
1	—	1	—	—	—	—	—	委托管理	2
—	—	—	1	—	—	—	—	卡锁定	3
—	—	—	—	1	—	—	—	卡终止	4
—	—	—	—	—	1	—	—	缺省选定	5
—	—	—	—	—	—	1	—	CVM 管理	6
1	1	—	—	—	—	—	1	强制 DAP 验证	7

表 11 权限(字节 2)

b8	b7	b6	b5	b4	b3	b2	b1	含义	特权序号
1	—	—	—	—	—	—	—	可信路径	8
—	1	—	—	—	—	—	—	授权管理	9
—	—	1	—	—	—	—	—	令牌管理	10
—	—	—	1	—	—	—	—	全局删除	11
—	—	—	—	1	—	—	—	全局锁定	12
—	—	—	—	—	1	—	—	全局注册	13
—	—	—	—	—	—	1	—	最终应用	14
—	—	—	—	—	—	—	1	全局服务	15

表 12 权限(字节 3)

b8	b7	b6	b5	b4	b3	b2	b1	含义	特权序号
1	—	—	—	—	—	—	—	Receipt Generation	16
—	X	X	X	X	X	X	X	RFU	—

11.2.3 一般性错误代码

可以被任何命令返回的错误代码描述详见表 13。

表 13 一般错误代码

SW1	SW2	含义
“64”	“00”	未指定
“67”	“00”	Lc 中错误的长度
“68”	“81”	逻辑通道不支持或没有激活

表 13（续）

SW1	SW2	含义
“69”	“82”	安全状态不满足
“69”	“85”	使用条件不满足
“6A”	“86”	P1、P2 不正确
“6D”	“00”	无效的指令(INS)
“6E”	“00”	无效的类(CLA)

11.2.4 CLASS 字节编码

所有 GP 命令中的类字节将符合 GB/T 16649.4 的要求，命令中在使用基本逻辑通道 0 和逻辑通道 1～3 时，将采用表 14 的编码格式；命令中使用更多的逻辑通道 4～19 时，将采用表 15 的编码格式。

表 14 CLA 字节编码(0,1～3)

b8	b7	b6	b5	b4	b3	b2	b1	描述
0	0	0	0	—	—	—	—	GB/T 16649.4
1	0	0	0	—	—	—	—	GP 命令
—	0	0	0	0	0	—	—	无安全报文
—	0	0	0	0	1	—	—	安全报文——GP 专用
—	0	0	0	1	0	—	—	安全报文——GB/T 16649.4 命令头不处理(no C-MAC)
—	0	0	0	1	1	—	—	安全报文——GB/T 16649.4 命令头验证(C-MAC)
—	0	0	0	—	—	X	X	逻辑通道序号

表 15 CLA 字节编码(4～19)

b8	b7	b6	b5	b4	b3	b2	b1	描述
0	1	—	0	—	—	—	—	GB/T 16649.4
1	1	—	0	—	—	—	—	GP 命令
—	1	0	0	—	—	—	—	无安全报文
—	1	1	0	—	—	—	—	安全报文—— GB/T 16649.4 或 GP 专用
—	0	0	0	X	X	X	X	逻辑通道序号

11.2.5 APDU 命令和数据长度

所有 GP 命令都符合 GB/T 16649.4 的要求，也就是 Lc 字节被编码为 1 字节。

所有 GP 命令消息(包括 APDU 头)在长度上都被限制到 255 字节。

11.2.6 APDU 命令响应数据中带确认信息的结构

响应数据的按照 BER-TLV 格式编码，结构如表 16 所示。

表 16 响应数据结构

长度	数据项	卡片支持
1～2	数据的长度(“00”—“7F”或“81 80”—“81—FF”)	必选
0～n	数据	有条件的
5～n	验证数据	必选

验证数据的结构如表 17 所示。

表 17 验证数据结构

长度	数据项	卡片支持
1	验证计数器数据的长度	必选
2	验证计数器数据	必选
1	卡唯一性数据的长度	必选
1～n	卡唯一性数据	必选
1	令牌标识符的长度	可选
0～n	令牌标识符	可选
1	令牌签名数据的长度	有条件的
0～n	令牌签名数据	可选
注：卡的唯一性数据由卡的 IIN 和 CIN 连接组成。		

11.2.7 隐性选择参数编码

指定一个应用为一个或多个逻辑通道在一个或多个通信方式下的隐性选择。该参数一个字节的编码如表 18 所示，其中 b8 和 b7 都置“0”表示本应用只能通过 select 指令选择，同时逻辑通道序号无效。

表 18 隐性选择参数编码

b8	b7	b6	b5	b4	b3	b2	b1	描述
1	—	—	—	—	—	—	—	非接触方式
—	1	—	—	—	—	—	—	接触方式
—	—	X	—	—	—	—	—	RFU
—	—	—	X	X	X	X	X	逻辑通道序号

11.2.8 密钥类型编码

密钥类型编码的长度可以是 1 个或 2 个字节，当长度是 2 字节时，第 1 个字节应设置成“FF”，第 2 个字节的编码和长度与 1 个字节时的编码一致，如表 19 所示。

表 19　密钥类型编码

值	含义
“00”～“7F”	保留为私用
“80”	DES - mode (EBC/CBC) implicitly known
“81”	保留(TDES)
“82”	CBC 模式的 TDES
“83”	ECB 模式的 DES
“84”	CBC 模式的 DES
“85”～“9F”	RFU(对称算法)
XX	SM X
“A0”	RSA 公钥-E(明文)
“A1”	RSA 公钥-N(明文)
“A2”	RSA 私钥-N
“A3”	RSA 私钥-D
“A4”	RSA 私钥-P (余数定理)
“A5”	RSA 私钥-Q (余数定理)
“A6”	RSA 私钥-PQ (余数定理)
“A7”	RSA 私钥-DP1 (余数定理)
“A8”	RSA 私钥-DQ1 (余数定理)
“A9”～“FE”	RFU(非对称算法)
“FF”	扩展格式

11.2.9　密钥用途编码

密钥用途的编码如表 20 所示。

表 20　密钥用途编码

b8	b7	b6	b5	b4	b3	b2	b1	描述
1	—	—	—	—	—	—	—	验证(DST, CCT, CAT),加密(CT)
—	1	—	—	—	—	—	—	计算(DST, CCT, CAT),解密(CT)
—	—	1	—	—	—	—	—	安全报文-响应数据域(CT,CCT)
—	—	—	1	—	—	—	—	安全报文-命令数据域(CT,CCT)
—	—	—	—	1	—	—	—	机密(CT)
—	—	—	—	—	1	—	—	密码校验(CCT)
—	—	—	—	—	—	1	—	数字签名(DST)
—	—	—	—	—	—		1	加密授权(CAT)

GP 中使用的值：

a) C−MAC = “14”, R−MAC = “24”, C−MAC + R−MAC = “34”;
b) C−ENC =“18”, R−ENC = “28”, C−ENC + R−ENC = “38”;
c) C−DEK = “48”, R−DEK = “88”, C−DEK + R−DEK = “C8”;
d) PK_SD_AUT = “82”;
e) SK_SD_AUT = “42”;
f) Token = “81”;
g) Receipt = “44”;
h) DAP = “84”;
i) PK_SD_AUT + Token = “83”;
j) SK_SD_AUT + Receipt = “43”;
k) PK_SD_AUT + DAP = “86”;
l) PK_SD_AUT + Token + DAP = “87”。

11.2.10 密钥访问编码

密钥访问参数的值如表 21 所示。

表 21 密钥访问编码

值	描述
“00”	密钥可以被安全域和任何应用使用
“01”	密钥只能被安全域使用
“02”	密钥可以被和安全域相关的任何应用使用,安全域自身不能使用
“03”−“1F”	RFU
“20”~“FE”	专用
“FF”	不可使用

11.2.11 Tag 编码

GP 中对安全域的 Tag 编码规则如下:

a) “00”~“7E”:保留给 ISO/IEC;
b) “80”~“9E“和“A0”~“BE”:保留给相关内容;
c) “C0”~“DD”和“E0”~“FD”:保留给 GP 或通过 GP 注册的个别方案,其中“CA”和“EA”:保留给 ETSI TS 102 226 规范;
d) “DE”和“FE”:保留给专用的和未经 GP 注册的;
e) “1F 1F”~“7F 7F”:保留给 ISO/IEC;
f) “9F 1F”~“9F 7F”和“BF 1F”~“BF 7F”:保留给相关内容;
g) “DF 1F”~“DF 7F”和“FF 1F”~“FF 7F”:保留给 GP 或通过 GP 注册的个别方案,其中“FF 1F”~“FF 3F”保留给 ETSI TS 102 226 规范。

附 录 A
（资料性附录）
生命周期示例说明

本附录举例说明了 GP 卡片和从它创建到终结的生命周期的迁移过程，同时也展示了若干可执行加载文件、可执行模块和应用的状态以及它们和卡片生命周期的相互关系。

图 A.1 说明了这些生命周期状态：

a) 应用 A：该应用的代码以可执行模块的形式随着可执行加载文件在卡片制造期间驻留于可变存储器中，并以一种与特定的实现相关的方式进行了安装。除了卡片处于已锁定状态之外，它在卡片的整个生命周期中都是可用的。

b) 应用 B：该应用的代码以可执行模块的形式随着可执行加载文件在芯片制造期间驻留于只读存储器中，并在卡片初始化之前进行了安装。它随着某个可执行加载文件在卡片终结前的某个生命周期的时刻，从卡片上删除。由于该应用对应的可执行加载文件驻留在只读存储器中，因此不能在物理上将其从卡片删除。

c) 应用 C：该应用的代码以可执行模块的形式随着可执行加载文件以一种与特定的实现相关的方式加载到卡片上，并在发卡后阶段当卡片处于安全状态时，进行了安装。该应用使用了一段时间后在卡片终结以前随着可执行加载文件而删除。由于该应用和对应的可执行加载文件，以及所有对应的可执行模块都驻留在可变存储器中，因此被彻底从卡片的可变存储器中清除干净，其占用的存储器空间被回收以便重新利用。

d) 应用 D：该应用的代码以可执行模块的形式随着可执行加载文件以一种与特定的实现相关的方式加载到卡片上。除了卡片处于已锁定状态之外，它在卡片的整个生命周期中都是可用的，直至卡片终结。

e) 应用 E：该应用的代码以可执行模块的形式随着可执行加载文件出现，在发卡后阶段当卡片处于安全状态时，以一种与特定的实现相关的方式加载并安装到卡片上。除了卡片处于已锁定状态之外，它在卡片的整个生命周期中都是可用的，直至卡片终结。

f) 应用 F：该应用的代码以可执行模块的形式与应用 E 共存于同一可执行加载文件中，它在发卡后阶段且卡片处于安全状态时，加载并安装到卡片上，并在卡片终结前的某个时刻，从卡片上删除。

注：图 A.1 示例的说明并不能用于全面阐明在每个卡片生命周期状态时可执行的全部操作。

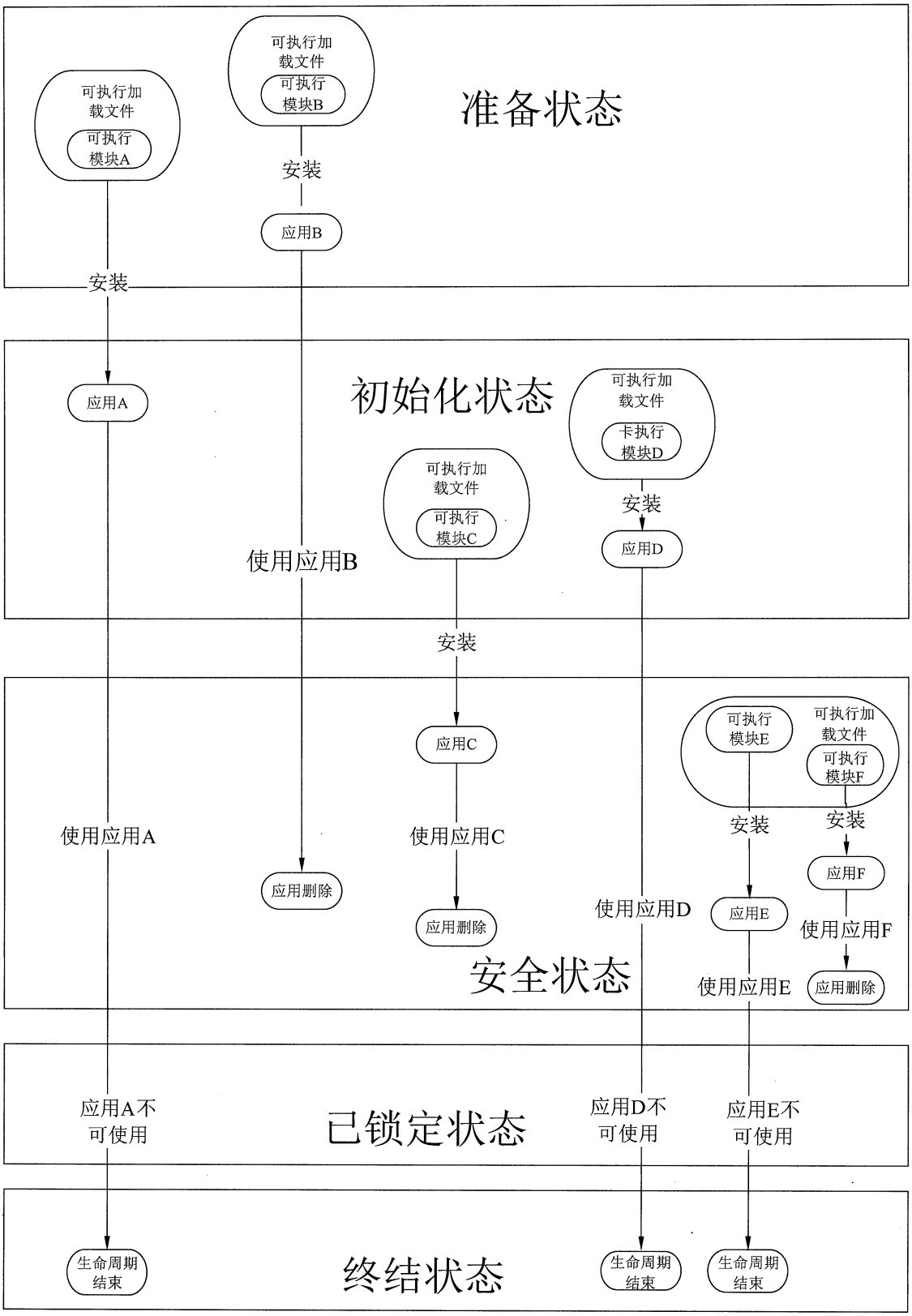


图 A.1　卡片生命周期和应用生命周期

参 考 文 献

[1] GlobalPlatform Card Specification V2.2.1
[2] GlobalPlatform Card Specification V2.1.1
[3] GlobalPlatform Card Contactless Services Card Specification V2.2.1-Amendment C V1.0
[4] Smart Cards; Remote APDU structure for UICC based application(ETSI 102.226)