ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0136—2016

金融IC卡行业一卡多应用规范

Specification for financial IC card extend multi-applications

2016－06－27 发布　　2016－06－27 实施

中国人民银行　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国人民银行科技司提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、中国金融电子化公司、中金国盛认证中心、中国银联、中钞信用卡产业发展有限公司、中国工商银行、中国建设银行、银行卡检测中心、东信和平智能卡股份有限公司、武汉天喻信息产业股份有限公司、银联数据服务有限公司。

本标准主要起草人：王永红、陆书春、邬向阳、李兴锋、杨倩、魏猛、汤沁莹、张栋、唐守勤、孟秋霞、王永吉、李志远、周新衡、胡瑞璟、张策、尚可、杨卓炯、丁吉、平庆瑞、胡玮。

金融IC卡行业一卡多应用规范

1 范围

本标准规定了金融IC卡行业一卡多应用的框架结构、行业管理及安全部分等方面的技术要求。

本标准适用于金融IC卡在行业多应用领域中卡片平台、受理终端、应用的设计、开发及选型参考。

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，仅所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。

GM/T 0002-2012 SM4分组密码算法

GM/T 0003.2-2012 SM2椭圆曲线公钥密码算法

GM/T 0004-2012 SM3密码杂凑算法

JR/T 0025 中国金融集成电路(IC)卡规范

JR/T 0088.1-2012 中国金融移动支付 应用基础 第1部分：术语

JR/T 0093.6-2012 中国金融移动支付 远程支付应用 第6部分：基于安全单元（SE）的安全服务技术规范

JR/T 0098.4-2012 中国金融移动支付 检测规范 第4部分：安全单元（SE）应用管理终端

JR/T 0098.5-2012 中国金融移动支付 检测规范 第5部分：安全单元（SE）嵌入式软件安全

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融IC卡多应用 financial IC card extend multi-applications

经过合规申请并分发、存储在同一张卡片的多个应用，多个应用能够被各受理环境识别并加载。

3.2

应用提供方 application provider

金融IC卡上应用的提供方。

3.3

应用可信保障方 application trusted guarantor

保障行业应用在进入金融IC卡多应用平台过程中的防伪冒、防篡改等综合可信性的主体。

3.4

应用管理方 application manager

为行业应用提供一个可信的发布平台并提供可信的应用发布服务的主体。

3.5

应用发行方 application issuer

受应用管理方委托或授权完成发布服务，确保持卡人获得有效的行业应用服务的主体。

3.6

卡片发行方 card issuer

为用户提供金融IC卡发行服务的主体。

3.7

行业方 industry user

应用发行方的集合。

3.8

金融IC卡多应用平台 financial IC card extend multi-applications platform

对行业应用管理的系统平台，负责卡片行业应用的管理。

3.9

多应用卡片平台 multi-applications card platform

具备多应用加载的卡片内部的操作系统平台。

3.10

应用标识 application identifier

由注册的应用提供商标识（RID）以及专用应用标识符扩展(PIX)组成。

3.11

应用协议数据单元 application protocol data unit（APDU）

读卡器和SE之间的标准通信消息协议。

3.12

安全域 security domain

负责对某个SE外实体（例如SE卡发行方、应用提供方、授权管理者）的管理、安全、通信需求进行支持的SE内实体。

3.13

多应用平台卡 multi-applications platform card

支持应用的动态下载、安装、删除等操作的IC卡。

3.14

静态卡 static card

不支持应用的动态下载、安装、删除等操作的IC卡。

4 缩略语

下列符号和缩略语适用于本文件。

AID 应用标识符(Application Identifier)

SE 安全单元（Secure Element）

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

PSE 接触式金融支付系统环境(Payment System Environment)

PPSE 非接触式金融近距离支付系统环境(Proximity Payment System Environment)

5 金融 IC 卡行业多应用框架概述

5.1 总体框架

应用提供方将某行业应用提交到应用管理方，应用管理方负责管理，同时应用可信保障方保障本应用的可信性；应用管理方授权或委托应用发行方完成行业应用加载到金融IC卡。

金融IC卡多应用的各方参与者及其相互关系见图1所示：

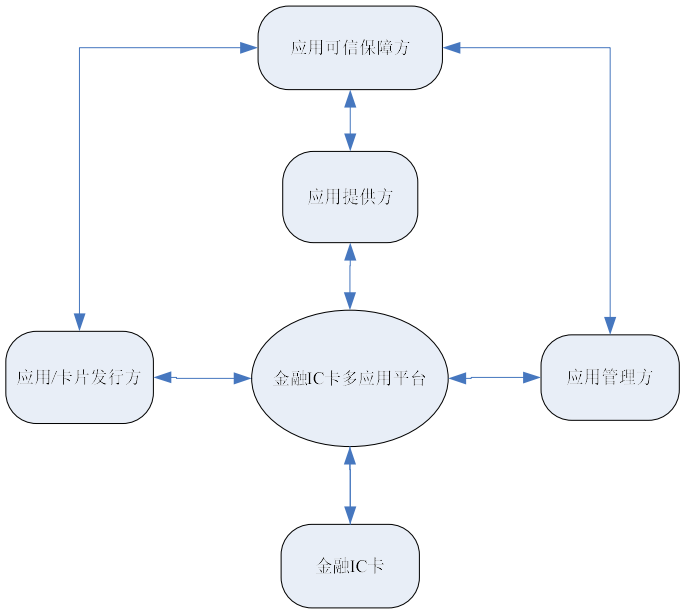

图 1 总体框架

各参与方之间的关系说明如下：

——应用/卡片发行方通过金融 IC 卡多应用平台完成应用/卡片的发行；

——应用管理方通过金融 IC 卡多应用平台进行应用的管理；

——应用提供方将其应用提交到金融 IC 卡多应用平台；

——金融 IC 卡多应用平台进行金融 IC 卡的管理；

——应用提供方通过应用可信保障方确认应用的可信性；

——应用发行方通过应用可信保障方确认应用的可信性；

——应用管理方通过应用可信保障方确认应用的可信性。

5.2 各方职能要求

5.2.1 应用提供方

应用提供方同时是行业应用的使用者和拥有者。无论此应用为何种状态，此应用的归属权均属于应用提供方。其职能要求包括：

——作为应用的提供者应保障此应用的合法性；

——作为应用的提供者应向应用管理方提供真实可靠的应用；

——作为应用的服务者有责任保障加载此应用的金融 IC 卡得到有效的服务。

5.2.2 应用可信保障方

应用可信保障方应保障行业应用在进入金融IC卡多应用平台过程中的防伪冒、防篡改等综合可信性。其职能要求包括：

——为应用提供者添加其应用的可信信息，保障其应用的可信性；

——为应用管理方提供其应用的可信支持；

——为应用/卡片发行方提供其应用的可信支持。

5.2.3 应用管理方

应用管理方为行业应用提供一个可信的发布平台并提供可信的应用发布服务。其职能要求包括：

——受理行业应用的管理申请；

——为行业应用提供注册、存储、发布，并完成行业应用的生命周期管理服务；

——授权或委托发行方完成行业应用加载到金融 IC 卡上的发布服务；

——为持卡人提供应用查询、添加、删除服务。

5.2.4 应用发行方

应用发行方的功能是完成金融IC卡行业应用的加载、预个人化和应用数据个人化工作，确保持卡人获得有效的行业应用服务。

5.2.5 卡片发行方

卡片发行方的卡片可以下载应用发行方发行的各类应用。

5.3 金融 IC 卡框架

5.3.1 卡片系统架构

本条主要描述卡片系统层次架构及其内部的模块构成，见图2。

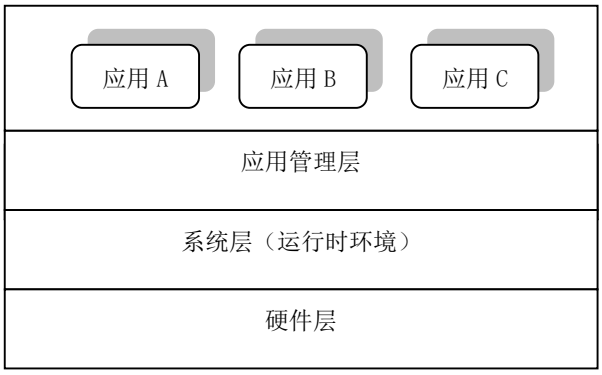

图 2 卡片系统架构

卡片系统各层含义及功能描述如下：

——硬件层指 IC 卡芯片硬件。

——系统层负责驱动 IC 卡芯片所提供的各类硬件协处理器，一般包括硬件加密算法协处理器、通信协处理器等。

——应用管理层负责卡内多应用的管理功能，包括应用程序的下载、删除，应用实例的创建、删除，以及各应用间的防火墙保护。对于不支持发行后下载新应用程序的金融 IC 卡，应用管理层将只负责各应用实例间的防火墙保护。

卡片架构中，以金融IC卡加载某行业应用为例，应用A、应用B、应用C为共存于卡片上的多个应用环境。应用A为金融应用、应用B为某行业应用、应用C为其他应用，其卡内应用结构见图3：

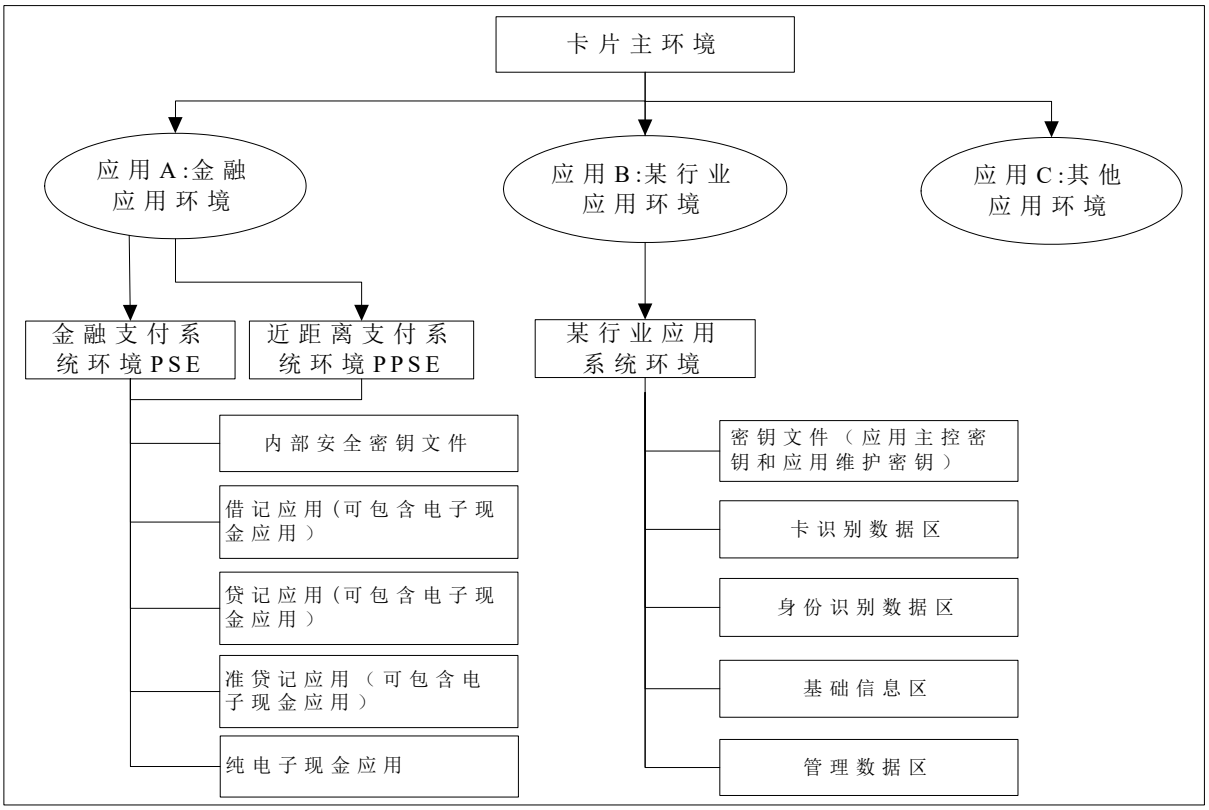

图3　金融IC卡加载某行业应用的卡内文件结构图

在图3中，金融IC卡为多应用平台卡，依据金融应用和某行业应用需求，卡片应建立PSE、PPSE（可选）和某行业应用系统环境，金融、行业的数据文件和密钥文件分别建立在各自环境下，独立管理，互不影响，终端通过选择PSE、PPSE进入金融应用环境，通过选择行业应用环境进入行业应用环境。

PSE与PPSE共用同一套金融应用数据文件和密钥文件。在接触式接口下，终端通过选择PSE进入金融应用；在非接触接口下，终端通过选择PPSE进入金融应用。进入金融应用后，相关指令、交易流程、安全机制应遵循JR/T 0025的要求。

在非接触接口下，终端通过选择行业系统环境进入行业应用。进入行业应用后，相关指令、交易流程、安全机制遵循行业卡技术规范的要求，但物理层应与金融IC卡保持兼容。

5.3.2　生命周期

生命周期包括卡片生命周期、应用生命周期和安全域生命周期三部分。

5.3.2.1 卡片生命周期

卡片生命周期状态及其状态转换关系见图4：

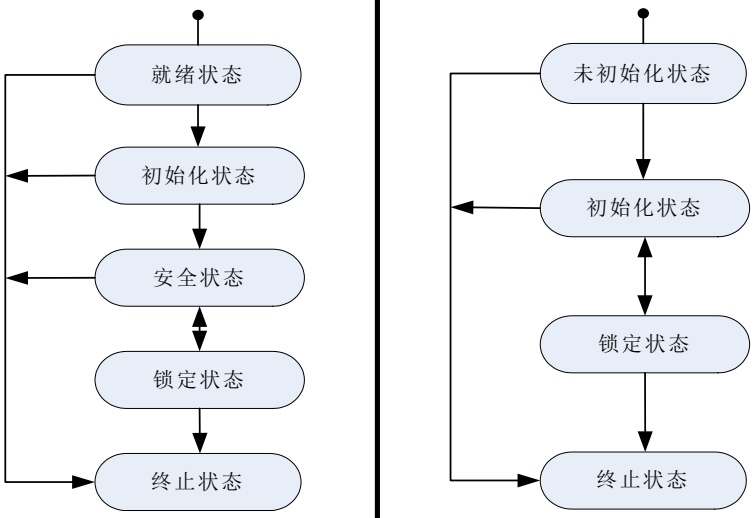

图 4 卡片生命周期状态转换图

对于多应用平台卡，卡片管理器负责卡片及其内容的安全和管理职能，因此其生命周期可以看作是卡片的生命周期。卡片生命周期包括如下状态：

——就绪状态：表示运行时环境已经可以使用，卡片管理器（发行者安全域）作为当前被选定的应用，可以接收、执行和响应 APDU 命令的状态。

——初始化状态：是一个可管理的卡状态。从就绪状态到初始化状态的转换是不可逆的。此状态表示一些初始的数据已经组装（例如：发行者安全域密钥/数据），但是该卡还不能发给卡持有者。

——安全状态：是卡发行后能够进行操作的卡片生命周期状态。此状态用于执行发行后卡行为相关的安全策略，如：应用的装载、安装、激活。从初始化状态到安全状态的转换是不可逆的。

——锁定状态：为卡发行者提供了禁止安全域和应用功能的能力。从安全状态到锁定状态的卡生命周期状态的转换是可逆的。

——卡终止状态：表明卡片生命周期的终止。从任何其他状态到终止状态的转换都是不可逆的。在终止状态下，所有 APDU 命令将被发送给发行者安全域，发行者安全域只对 GET DATA 命令进行响应。

对于静态卡，卡片生命周期即卡片操作系统（COS）的生命周期，其生命周期状态由 COS 开发者完成定义，但必须包括以下四个生命周期状态：

——未初始化状态：表示卡片操作系统 COS 已下载到 IC 卡硬件内，由于没有初始化数据的支持而不能正常使用的状态。

——初始化状态：表示卡操作系统 COS 及其执行所需要的数据已经完成了设置，从而使 IC 卡可以进行使用的状态。从未初始化状态到初始化状态的转换是不可逆的。

——锁定状态：表示 IC 卡的功能被锁定，而不能完全响应外部 APDU 请求的状态。从初始化状态到锁定状态的转换是可逆的。

——终止状态：表示 IC 卡生命周期的结束，其不能再进行回收利用的状态。从任何其他状态到终

止状态的转换都是不可逆的。

5.3.2.2 应用生命周期

应用生命周期状态及其状态转换见图5：

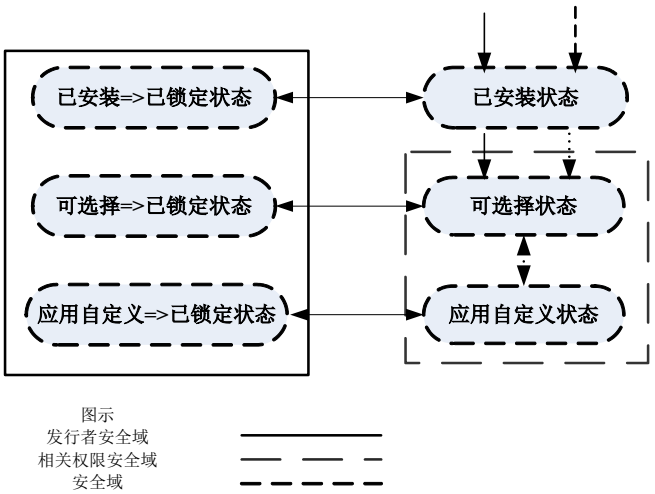

图 5 多应用平台卡应用生命周期状态转换图

对于多应用平台卡，其应用生命周期状态包括：

——已安装状态：应用已安装状态表示应用可执行代码的链接和任何必要的内存分配已经完成，应用已经在卡内应用注册表中完成注册，经过与该应用关联的安全域认证后的卡外实体可以对该注册信息进行访问，但该应用还不是可选的。

——可选择状态：应用可选择状态表示应用能够从卡外实体接收命令。从应用已安装状态到应用可选择状态的转换是不可逆的。在设置成应用可选择状态前，应用必须已经正确安装且功能正常。转换到应用可选择状态可以同应用的安装一起进行。

——已锁定状态：卡片管理器、应用自身、应用关联的安全域、具备“全局锁定权限”的应用以及具备“全局锁定权限”的安全域，都可以利用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。一旦应用处于已锁定状态，只有应用关联的安全域、具备“全局锁定权限”的应用以及具备“全局锁定权限”的安全域，才能够对应用进行解锁。卡片管理器必须确保应用生命周期能够恢复到锁定前的状态。

——应用自定义状态：除了以上的应用生命周期状态，应用还可定义自己的生命周期状态。一旦应用处于可选择状态，就由其自己来维护自定义的生命周期状态。应用可以使用任何自定义状态，只要与本规范定义的状态不冲突即可。应用自定义状态的转换由应用自身进行控制。

对于静态卡，其应用生命周期状态由卡片实现者完成定义，但必须包括以下两个生命周期状态：

——可使用状态：表示应用所需要的数据已经完成了装载，应用处于可以正常使用的状态。

——锁定状态：表示应用功能被锁定，不能完全响应外部 APDU 命令的请求。从可使用状态到锁定状态的转换是可逆的。

5.3.2.3 安全域（密钥）生命周期

安全域（密钥）生命周期状态及其转换见图 6：

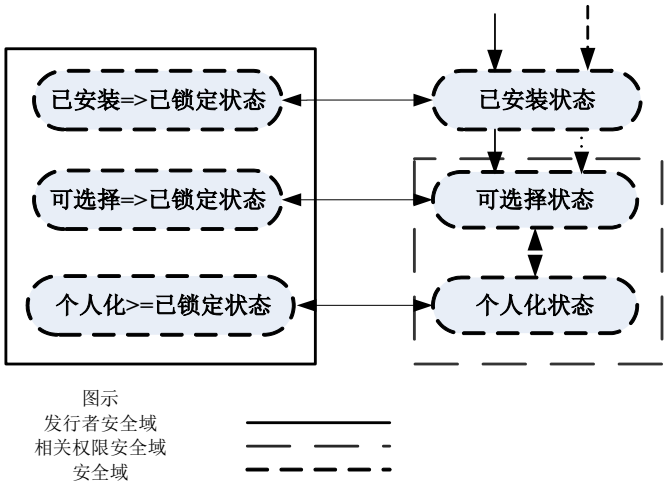

图 6　多应用平台卡的安全域生命周期状态转换图

对于多应用平台卡，安全域（密钥）生命周期状态包括：

——已安装状态：表示安全域已经成为卡片平台应用注册表中的一项，并且经过认证的卡外实体可以访问这项内容。但还不能和应用相关联，因此安全域的服务不能被应用使用。

——可选择状态：表示安全域能够接收来自卡外实体的命令。由于其还没有密钥，不能被应用关联，因此，当在这个状态时，其服务还不能被应用使用。从已安装状态到可选择状态的转换是不可逆的。已安装状态到可选择状态的转换可以与安全域的安装过程一起完成。

——个人化状态：表示安全域已经具有了运行时所需的个人化数据和密钥。从可选择状态到个人化状态的转换是不可逆的。在个人化状态下，安全域可以被应用关联，并且其服务也可被相关联的应用使用。

——已锁定状态：表示安全域被锁定，此状态下，安全域将不能与应用相关联，并且禁止应用访问这个安全域的服务。安全域处于已锁定状态，只允许发行者安全域解锁此安全域。在安全域生命周期的任何状态，卡片管理者都可以接收一个请求来删除一个安全域。

对于静态卡，不存在安全域的概念，此类卡片的安全性由卡内密钥进行保证，因此定义卡内密钥的生命周期状态。具体卡内密钥的生命周期状态由卡片操作系统(COS)实现者完成定义，但密钥生命周期状态必须包括以下两个：

——有效状态：表示密钥的数据已完成设置，而使密钥可以使用的状态；

——无效状态：表示密钥的使用条件已不满足，而使密钥不可再被使用的状态。

从有效状态到无效状态的转换是可逆的。

5.3.3　应用密钥管理

5.3.3.1　密钥装载

密钥装载应符合如下要求：

——应用密钥的装载必须保障密钥数据和密钥属性的完整性要求；

——应用密钥的装载过程必须符合其行业应用规范的要求；

——应用密钥的装载不能泄露卡片及其内部其他应用的安全信息；
——应用密钥的装载必须保证密钥的原子性要求：在存储过程中，卡片掉电不影响此密钥的完整性和安全性。

5.3.3.2 密钥更新

密钥更新应符合如下要求：
——应用密钥的更新必须保障密钥数据和密钥属性的完整性要求；
——应用密钥的更新过程必须保证原卡内其他信息的一致性和完整性；
——应用密钥的更新不能泄露卡片及其内部其他应用的安全信息。

5.3.3.3 密钥存储

密钥存储应符合如下要求：
——应用密钥的存储必须以一种安全的形式存放在卡片的非易失性存储器中；
——应用密钥的存储不能泄露卡片及其内部其他应用的安全信息。

5.3.3.4 密钥销毁

密钥销毁应符合如下要求：
——应用密钥销毁应将密钥数据及其属性从卡片内的非易失性存储器中删除；
——应用密钥销毁不能泄露卡片及其内部其他应用的安全信息。

5.4 系统侧框架

5.4.1 系统侧框架组成及其关系

系统侧框架主要包括：
——应用管理模块；
——卡片管理模块；
——多应用发布模块；
——应用可信验证模块；
——多应用密钥管理模块。
各模块相互关系见图 7。

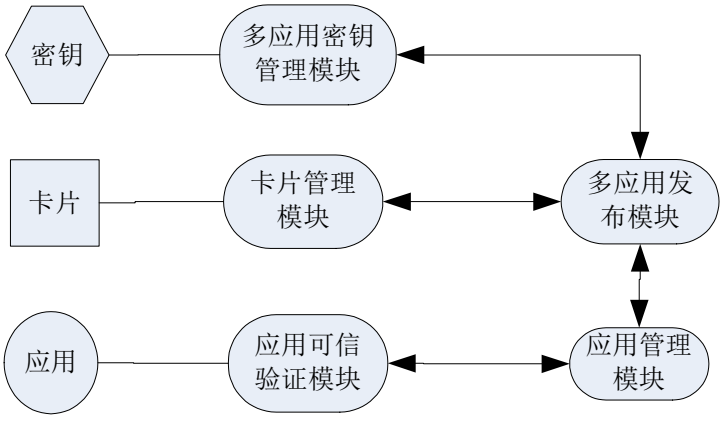

图 7 各模块相互关系

5.4.2 卡片管理模块

卡片管理模块应对卡片生命周期进行管理，并可提供其他与卡片相关的服务。

5.4.3 应用可信验证模块

应用可信验证模块应对应用的有效性、安全性及完整性等内容进行验证。

5.4.4 应用管理模块

应用管理模块是对应用的生命周期进行管理，可包括注册应用、应用进行可信化验证、应用存储管理及发布可信应用。同时生成持卡人可加载的应用列表和对卡片内已装载的应用进行管理。

5.4.5 多应用发布模块

多应用发布模块包括应用列表发布、应用下载、应用预个人化、应用个人化四大功能。根据不同的发卡模式及不同的行业特点有效组合完成行业应用的加载服务。

——应用列表发布应向持卡人提供有效的应用列表。

——应用下载是指将应用下载至卡片中。如果应用已经掩膜至卡片中，则不需要下载应用。在必要时还包括了辅助安全域的创建、删除、锁定解锁工作。

——应用预个人化是指创建应用所需的文件以及目录。

——应用个人化是指将用户的个人信息以及密钥写入应用中的过程。

其中，应用下载定义了下述两种模式：

——动态下载模式

在卡片发行后，完成应用下载、预个人化、及应用数据个人化的工作模式；

——应用预置模式

在卡片发行前，预先在卡内完成了应用下载、预个人化和个人化的工作模式。

5.4.6 多应用密钥管理模块

多应用密钥管理模块是对系统所需密钥进行全生命周期管理，包括密钥产生、密钥存储、分发、作废等过程。

多应用密钥管理涉及行业应用接入所需密钥、完成金融IC卡行业应用加载所需的密钥。多应用密钥管理在行业应用授权下可管理行业应用业务密钥。

6 行业多应用管理

6.1 多应用平台管理概述

金融IC卡多应用平台负责行业应用的管理，具体内容应包括：应用提交、应用审核注册、应用发布、应用下载、应用个人化、应用更新、应用下架及应用全局注册表的维护。

金融IC卡多应用平台维护一张全局应用注册表，该注册表登记了所有已注册应用的基本信息，当应用发布、更新、下架时，均应更新注册表中该应用的状态。应用注册表信息包括但不限于：应用AID、应用类型、应用版本、应用功能说明、应用占有空间、应用权限、应用提供机构代码、应用提供方机构代码、应用的安全等级、应用发布范围、应用有效期、应用生命周期状态等。

金融IC卡动态加载应用如图8所示，由应用提供方提供应用给到金融IC卡多应用平台，平台完成应用可信验证、应用注册、应用发布等工作。卡片发行方提交应用下载申请，由金融IC卡行业多应用平台

处理此应用下载申请，同时加载行业应用数据至平台，待平台准备完此次申请所需内容后，将应用下载所需文件及数据下发至应用发行方，由卡片发行方完成应用及数据写入卡片工作。

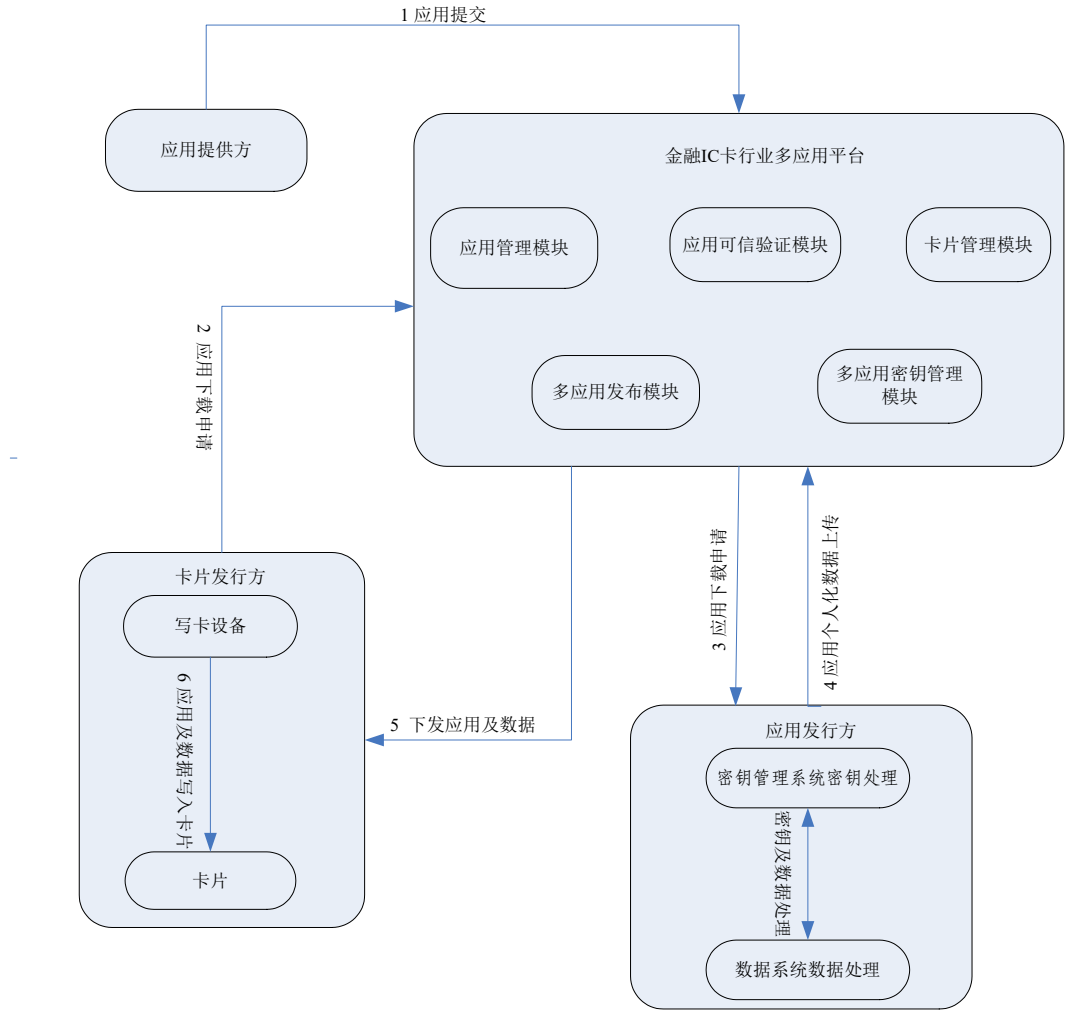

图8　金融IC卡动态加载应用示意图

6.2　应用提交

应用提供方将行业应用文件包提交到金融IC卡多应用平台。

6.3　应用审核注册

应用提供方通过金融IC卡多应用平台向应用管理方提交注册申请，提交注册应用的信息可包括：应用名、应用类型、应用版本、AID标识号 、所属行业、安全信息、应用开发商、开发日期、使用范围、支持的一卡多应用标准等。

金融IC卡多应用平台收到应用提供方提交的应用后进行审核处理，审核处理应包括：应用的有效性、安全性及完整性、对金融IC卡提供方提供的应用经第三方专业检测机构的检测报告等内容。

6.4　应用发布

金融IC卡多应用平台将审核通过的各类应用展示给应用发行方，或向持卡人提供有效的应用列表，以供应用发行方或持卡人选择下载。

6.5 应用下载

应用下载将应用文件安全可靠地下载到金融IC卡并安装应用，安装应用是生成应用实例的过程。应用下载流程见图9。

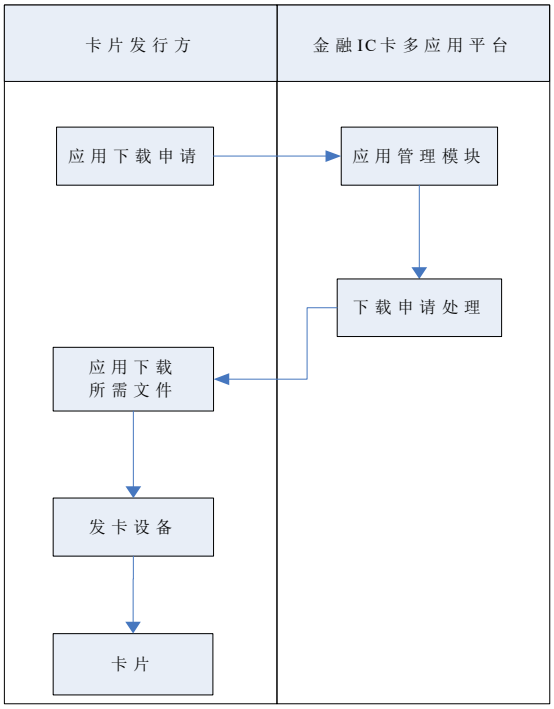

图 9 应用下载流程图

应用下载过程中应执行的操作：

步骤一：应用发行方发起应用下载申请；

步骤二：金融IC卡多应用平台处理下载申请；

步骤三：应用发行方下载应用到卡片并将应用实例化。

应用下载前卡片应执行的操作，具体如下：

——检查金融 IC 卡片状态；

——排查卡片应用列表；

——查看卡片应用相关安全域；

——审查安全域状态。

应用下载前金融IC卡多应用平台应执行的操作，具体如下：

——审核应用申请的有效性；

——确定下发应用的时效性；

——确保下发应用文件的准确性；

——保证下发应用数据的完整性。

6.6 应用个人化

应用个人化是金融 IC 卡上的行业应用实例加载个人数据的过程，金融 IC 卡多应用平台转发应用发行方从应用提供方获取的个人化数据至应用使用方，并将个人化数据加载到上金融 IC 卡上。应用个人化流程见图 10。

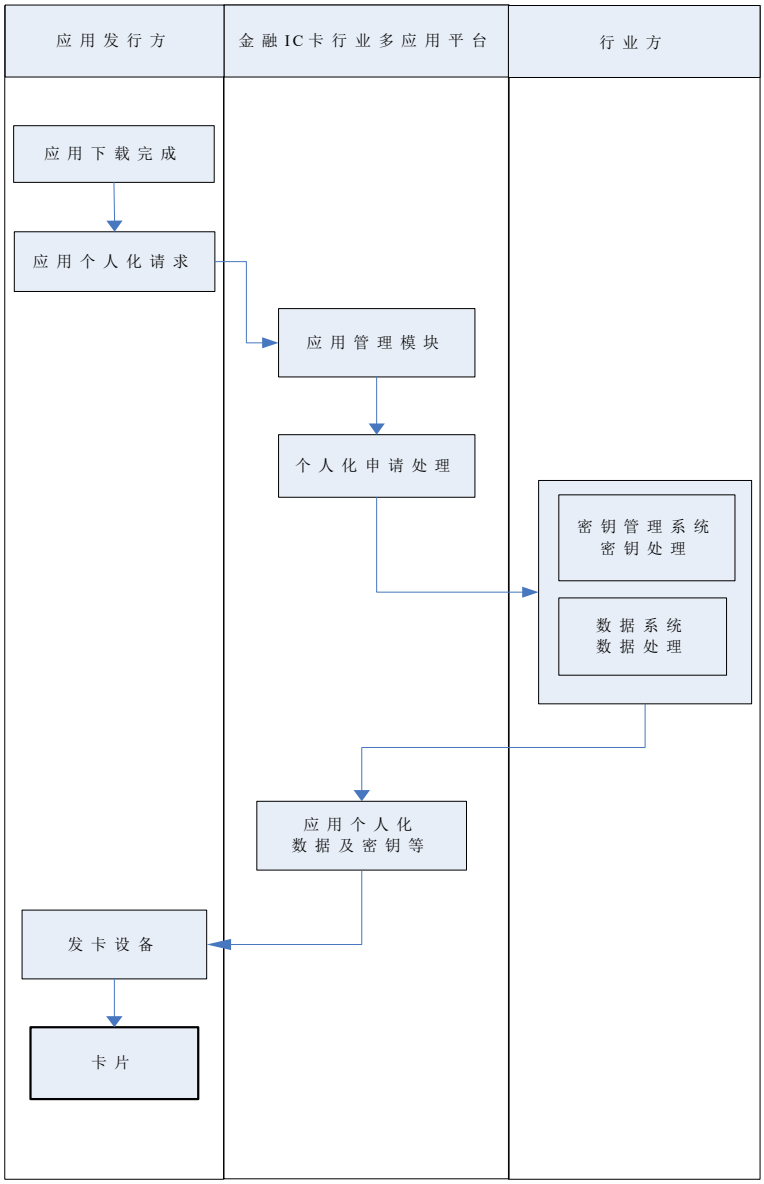

图 10　应用个人化流程图

应用个人化过程中应执行的操作，在应用个人化前应判断应用是否下载，若下载完成执行下方内容，若应用未下载完成则需先安装应用：

——应用发行方发送个人化请求；

——金融 IC 卡行业多应用平台处理个人化请求；

——行业应用方处理个人化请求；

——金融 IC 卡多应用平台传送个人化数据；

——应用发行方进行卡片应用个人化。

6.7 应用更新

当应用提供方更新应用版本时，新版本沿用老版本 AID，并向金融 IC 卡多应用平台通告发布。金融 IC 卡多应用平台收到通告后进行备案，并更新全局应用注册表中该应用的版本、升级方式等。

6.8 应用下架

应用提供方、金融 IC 卡多应用平台可以对已经上线的应用进行下架。下架操作完成后，金融 IC 卡多应用平台更新全局应用注册表中该应用的状态，该应用不能再被用户查询和下载。

7 行业多应用安全技术要求

7.1 总体安全要求

应严格落实国家网络安全和信息技术安全有关政策，涉及的系统平台、受理终端、银行卡等应使用经国家密码管理机构认可的商用密码产品，采用的芯片应通过国家认证认可管理部门认可机构的安全评估。

7.2 芯片的安全要求

为抵抗金融多应用IC卡的芯片集成电路威胁，保护智能卡硬件平台，本部分定义了芯片集成电路的安全要求。具体要求包括如下内容：

——应支持国家密码管理机构认可的密码算法；
——采用的芯片应通过国家认证认可管理部门认可机构的安全评估；
——应支持基于国家密码管理机构认可的密码算法的行业多应用；
——应保证将芯片模块从卡片上移除会导致可见的损坏，如果无可见损坏的情况下，应保证将芯片模块装回或替换，整个芯片无法工作；
——应保证触及 IC 卡表面或将芯片表面的覆盖层剥离，如环氧树脂或聚酰胺等，会破坏芯片，使芯片无法使用；
——应保证芯片具有抵抗物理测定储存器单元逻辑内容的保护能力；
——应保证存储器单元逻辑或芯片内部布线已暴露时，芯片具有抵抗根据存储器单元逻辑恢复有用代码或信息的能力；
——应保证芯片具有抵抗通过旁道分析导致存储器敏感信息暴露的保护能力，如分析运行芯片功耗图，电磁场辐射或者主要处理功能的时序等；
——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；
——应保证以电压对比和电子束探测等攻击方式难以暴露存储器信息；
——应保证芯片应用不受操作环境变化干扰的影响，如果探测到内部变化或时钟频率、电压、复位脉冲宽度以及温度等规范外的赋值，使其无效；
——应保证芯片应用的执行不受探测攻击的影响；
——应保证芯片存储器单元和保护系统不易被修改，如果修改需要由具有全面芯片设计知识人员使用高端专门工具才能实现；
——应保证芯片能够抵抗具有全面的芯片设计知识的人员使用高端专门工具通过 FIB 系统或激光切割机对芯片修改的能力；
——应保证芯片受到光学错误攻击、电磁场和放射线的干扰时，芯片不受影响可正确的执行和使用；
——应保证智能 IC 卡的设计具有一定的难度性，攻击者必须通过大量的努力和使用高端专业工具才能对 IC 卡建立模块进行反向工程提取；

——应保证安全芯片的存储器在分配或释放资源时，确保该资源中任何以前的信息内容不再可用。

7.3 多应用卡片平台安全要求

7.3.1 平台安全恢复

平台提供安全恢复的防护功能，安全恢复防护机制不能影响应用的执行。

7.3.2 平台注册表服务

平台提供注册表服务。平台注册表是一个以层次结构保存并提供检索的数据库，维护芯片卡上的所有资源信息、芯片卡管理信息和其他重要数据，注册表内容可以由平台程序自动更新，也可以通过授权的应用执行更新操作。

7.3.3 平台安全通讯机制

平台能够为应用提供所需的安全通讯机制。

平台提供的安全通讯机制服务包括：

——真实性：通讯的双方包括卡内或是卡外实体必须通过身份认证；

——不可抵赖性：发送方应对数据的传送产生原发证据，接收方能对数据的原发证据进行验证；

——完整性：平台提供数据完整性校验以防止通讯数据被修改、删除、插入；

——机密性：平台提供数据机密性防护，防止机密数据被泄露。

在应用无需安全保证机制时，金融IC卡多应用平台能够提供非安全通讯机制，为通讯双方建立通道，但不保证该通道的传输数据的完整性、机密性。

7.3.4 平台存储管理

平台存储管理保护芯片卡存储器内敏感数据的完整性和机密性。

7.3.5 卡片状态管理

多应用芯片卡状态管理功能必须保证不能非法利用芯片卡生命周期中的状态和数据，即使芯片卡在不同状态中用到的数据被非授权用户非法获取后，也不能影响芯片卡安全性。

7.3.6 平台攻击检测

平台提供攻击检测防护功能：

——芯片具有环境检测功能，如电压检测、温度检测等以抵御故障注入攻击。

——平台具有资源检测功能，防止资源被攻击者故意耗尽。当平台检测到应用不断申请超出配额的资源时，可以自动锁定该应用。

7.3.7 平台安全审计

平台应对影响安全的关键事件进行记录，并保证记录不被非法修改和删除。

7.3.8 平台应用调度

平台提供应用调度功能，在芯片卡平台处于平台安全状态的情形下允许外部设备对卡内应用进行选择并执行。芯片卡平台的应用调度功能通过应用AID来选择、区分应用。在成功选择应用后，芯片卡平台将接受的后续命令发送给当前选择的应用处理。

7.3.9 平台识别与认证

平台提供识别与认证防护机制。

认证过程是通过被认证者提供身份证明或是安全属性如应用标识、生命周期状态、卡外实体的授权码等，认证者则通过此身份执行认证过程，决定被认证者身份，同时决定是否对被认证者进行授权，如允许被认证者访问认证者资源。

7.3.10 平台应用编程接口

平台通过提供平台应用编程接口执行芯片卡资源的访问控制。

7.3.11 增加应用的安全要求

应用的增加是一种具有安全属性的用户数据的输入。应用从多应用芯片卡安全控制范围之外导入芯片卡内部时，应执行访问控制。应用增加的安全属性包括应用下载者的身份凭证、应用的标识。不同的芯片卡管理模式下，应用下载者的身份验证过程是不同的。

7.3.12 删除应用的安全要求

多应用芯片卡内的应用可以被安全的删除。拥有权限的主体才可执行应用删除操作，拥有权限的主体包括卡片发行机构以及通过卡片发行机构进行授权或是委托的被授权机构和代理机构。

应用的删除可以是物理删除或是逻辑删除，如在非易失性存储区中的应用可以被完全删除，而在永久性存储区中的应用只能被逻辑删除。任何对被删除应用的存储空间的访问都是非法的。应用在删除后，其残留的数据将被覆盖或是禁止访问。

7.3.13 应用之间的通讯环境

应用受到代码空间、运行环境双重环境隔离，在不同环境下应用间不能直接进行通讯，应用间的通讯应通过平台的通讯服务来实现。

金融IC卡多应用平台提供共享接口对象的服务以及基于共享接口机制的功能服务如事件通知功能，来完成应用间的通讯。

8 卡片个人化模式

8.1 预个人化要求

预个人化阶段的工作是由应用/卡发行方为行业应用的个人化所做的准备工作。

预个人化的工作内容主要包括：

——确定行业应用所处的安全域，必要时为其创建辅助安全域。

——应用/卡片发行方与行业应用提供方宜协商一个授权密钥，由应用/卡片发行方负责写入卡中。后期行业应用个人化过程中被行业应用提供方专属密钥替换，以保障行业应用的数据及密钥的安全性。

——将行业应用加载到上述的安全域中。如果行业应用有自己专属辅助安全域，则此工作的安全保障由行业应用根据自己的规范完成。否则，由所在安全域的管理者负责保障行业应用的加载安全。

——根据行业需求或行业规范创建应用相关的文件和数据结构，为行业应用个人化做好准备工作。

预个人化的上述四项工作根据需要可有选择的执行。

预个人化的工作方式包括下述两种加载方式：

——集中加载方式：由应用/卡片发行方一次性完成片内的所有应用，包括金融应用和行业应用的

预个人化。集中预个人化的方式主要用于应用发行方和应用提供方的需求明确，合作方式固定的场景。

——动态加载方式：行业应用预个人化工作在多应用平台上完成。在该实施模式下，应用发行方可以对已经发行的卡片，增加新的行业应用并完成个人化。

应用发行方通过其发行渠道（包括但不限于柜面、自助终端、智能手机客户端等）与金融IC卡多应用平台以及行业应用提供方的后台系统连接，以获取相应的授权信息和数据。动态加载时，根据需要分为下述两种模式：

——先进行预个人化，再进行应用个人化。该模式下卡片在递交到持卡人手上时，卡内未包含该行业应用逻辑，因此需要先加载行业应用，完成预个人化，再进行应用个人化。

——不进行预个人化，只进行应用数据个人化。卡片在递交给持卡人之前，已经预先安装了该行业应用，持卡人如果要开通此类行业应用，只需要进行应用数据的个人化，无需加载应用包。其个人化流程与上述模式的流程类似，但不进行行业应用加载，直接对行业应用进行个人化。

8.2 个人化

个人化是为金融IC卡上的行业应用的应用实例加载个人数据的过程。对金融IC卡加载行业应用进行个人化的前提条件为金融应用IC卡已经完成了该行业应用的下载并已经按照应用提供方的要求进行了必要的预个人化处理。

在行业应用个人化的过程中，应用提供方负责提供个人化数据和密钥，应用发行方向应用提供方请求个人化数据和密钥并负责将个人化数据写入金融IC卡，按照本标准的安全要求完成与金融IC卡的安全交互。

行业数据的获取方式包含下述方式：

——行业数据可以是批量方式提交到金融 IC 卡多应用平台；

——平台通过接口实时获取行业数据；

——客户在应用发行方渠道终端完成行业数据的填写并上送。

行业密钥的获取方式包含下述方式：

——行业根据自己的规范，由自己的密钥管理系统导出到加密机中，加密机部署在金融 IC 卡多应用平台，完成发卡工作；

——行业应用提供者委托应用发行方管理密钥，完成发卡工作。

行业应用个人化开通方式包含下述方式：

——利用行业密钥管理产生的专属密钥替换预个人化完成的授权密钥；

——在行业专属密钥保护下完成个人化工作。

金融 IC 卡加载行业应用的个人化处理流程见图 11。

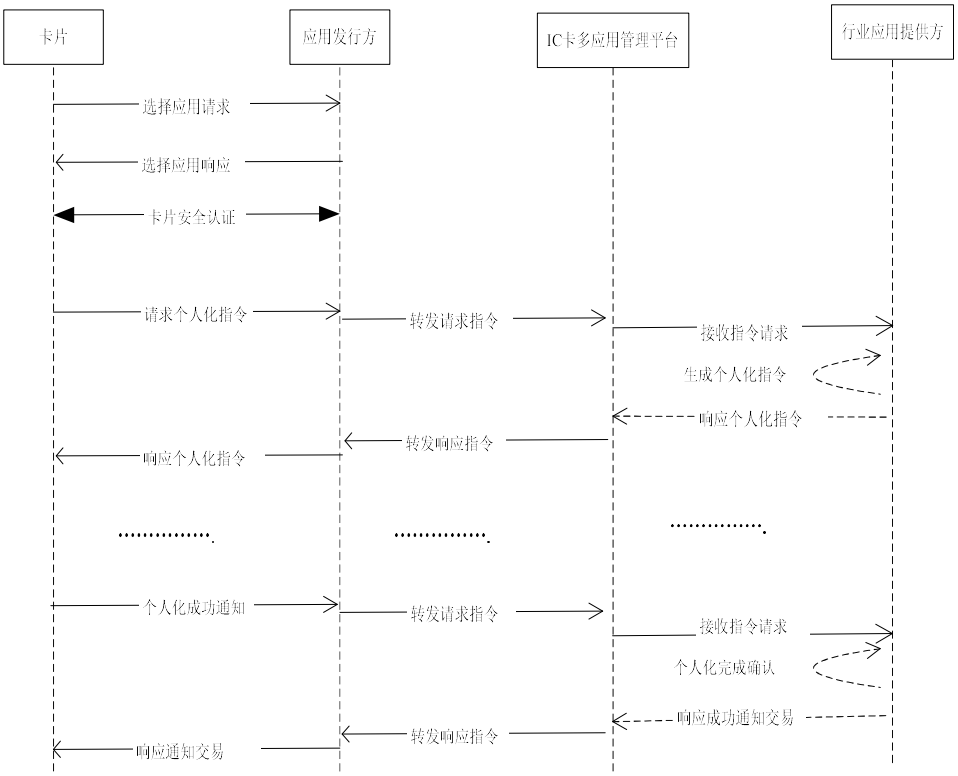

图 11 个人化处理流程

关于个人化还有以下几个方面值得注意：

——应用选择：应用选择的前提条件为需要完成个人化的金融 IC 卡中已经完成了相应应用的加载。应用被安装后，需要完成个人化数据的加载，包括应用使用的密钥和特有的应用数据。金融 IC 卡发行方在具有多应用加载功能的发行渠道（包括但不限于银行柜面或者自助终端）进行应用个人化。当卡片插入具有读写功能的终端时，终端将显示用户可选择需要进行个人化的应用。

——卡片安全认证：卡片安全认证是金融 IC 卡与个人化设备的双向认证过程。该过程中金融 IC 卡和个人化设备建立安全的通讯机制，保证个人化过程中交互过程的安全性和完整性。

——行业应用个人化过程：行业应用个人化的前提是金融 IC 卡的发行方必须按照本规范的安全要求与金融 IC 卡建立安全通讯机制。应用发行方向应用提供方申请获取个人化数据，并将获得的个人化数据加载到金融 IC 卡上。从应用提供方获取相关应用的个人化数据包括：应用数据、密钥、指令等。应用发行方负责组织个人化数据或者指令，并传输给卡片。

——个人化完成通知交易：个人化过程结束，当个人化最后一条指令完成后，在终端金融 IC 卡读写设备收到最后一条个人化指令后，并成功完成写卡，需要发送写卡成功通知应用提供方以供应用提供方更新其应用的管理状态。

参 考 文 献

[1] JR/T 0025.3 中国金融集成电路（IC）卡规范 第3部分：与应用无关的IC卡与终端接口规范
[2] JR/T 0025.6 中国金融集成电路（IC）卡规范 第6部分：借记贷记应用终端规范
[3] JR/T 0025.7 中国金融集成电路（IC）卡规范 第7部分：借记贷记应用安全规范
[4] JR/T 0025.8 中国金融集成电路（IC）卡规范 第8部分：与应用无关的非接触式规范
[5] JR/T 0025.11 中国金融集成电路（IC）卡规范 第11部分：非接触式IC卡通讯规范
[6] JR/T 0025.17 中国金融集成电路（IC）卡规范 第17部分：借记贷记应用安全增强规范
[7] GlobalPlatform Card Specification v2.2.1