(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101742481 B
(45)授权公告日 2013.03.20

(21)申请号 200810177016.4

(22)申请日 2008.11.10

(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法律部

(72)发明人 余万涛 马景旺 贾倩

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 龙洪 霍育栋

(51)Int.Cl.
H04L 9/08(2006.01)
H04W 8/24(2009.01)
H04W 12/04(2009.01)
G06K 19/067(2006.01)
G06Q 20/34(2012.01)

审查员 张文明

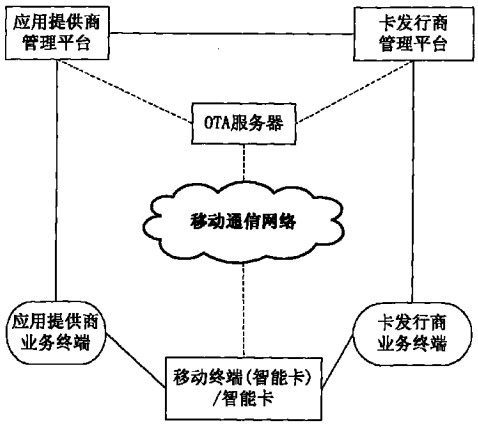
权利要求书 2 页 说明书 6 页 附图 2 页

(54)发明名称

智能卡的从安全域初始密钥分发方法和系统、移动终端

(57)摘要

本发明提供了一种智能卡的从安全域初始密钥分发方法和系统，该系统包括具有电子支付应用功能的智能卡、卡发行商管理平台及业务终端；所述智能卡通过所述业务终端与所述卡发行商管理平台进行通信；所述卡发行商管理平台，用于通过所述业务终端将从安全域初始密钥分发给所述智能卡。本发明解决在发卡后，针对对称密钥的情况，在创建从安全域时，将卡发行商管理平台生成的从安全域初始密钥安全的导入到从安全域，从而实现从安全域初始密钥的安全分发。



CN 101742481 B

1. 智能卡的从安全域初始密钥分发方法，其特征在于，该方法基于移动终端电子支付系统实现，该系统包括具有电子支付应用功能的智能卡、卡发行商管理平台及业务终端，所述智能卡为一独立设备或安装在移动终端上；所述智能卡通过所述业务终端与所述卡发行商管理平台进行通信，所述卡发行商管理平台通过所述业务终端将从安全域初始密钥分发给所述智能卡；该方法包括：

(a) 用户通过智能卡程序或业务终端客户端程序触发应用下载请求，并向所述卡发行商管理平台提交应用下载请求，所述应用下载请求中包括智能卡标识信息、应用标识及应用提供商身份信息；

(b) 所述卡发行商管理平台收到应用下载请求信息后，所述卡发行商管理平台和所述智能卡主安全域之间建立安全信道；

(c) 所述卡发行商管理平台创建从安全域及生成从安全域初始密钥，通过建立的安全信道经由所述业务终端将安全域初始密钥导入到所述智能卡从安全域。

2. 如权利要求 1 所述的方法，其特征在于，

步骤 (b) 之后，步骤 (c) 之前，还包括：所述卡发行商管理平台根据所述智能卡标识信息，应用标识及应用提供商身份信息，或者根据智能卡状态信息，判断是否创建从安全域。

3. 如权利要求 1 所述的方法，其特征在于，

步骤 (b) 建立安全信道的过程包括：(b1) 所述卡发行商管理平台与智能卡主安全域经由所述业务终端进行互认证，所述互认证过程经由所述业务终端在所述卡发行商管理平台和所述智能卡主安全域之间完成；(b2) 所述卡发行商管理平台与所述智能卡主安全域之间建立临时会话密钥，从而建立安全信道。

4. 如权利要求 1 至 3 中任一项所述的方法，其特征在于，

所述业务终端为卡发行商业务终端，所述卡发行商管理平台与所述智能卡间的交互信息通过卡发行商业务终端转发；或者，所述业务终端为应用提供商业务终端，从所述卡发行商管理平台到所述智能卡的消息依次通过应用提供商管理平台和应用提供商业务终端转发，从所述智能卡到所述卡发行商管理平台的消息依次通过应用提供商业务终端和应用提供商管理平台转发。

5. 智能卡的从安全域初始密钥分发系统，其特征在于，该系统包括具有电子支付应用功能的智能卡、卡发行商管理平台及业务终端；

所述智能卡通过所述业务终端与所述卡发行商管理平台进行通信；还用于提供向所述卡发行商管理平台提交应用下载请求的支持，与卡发行商管理平台进行互认证及建立临时会话密钥，还用于解密获得的从安全域初始密钥，以及对从安全域进行初始化；

所述卡发行商管理平台，用于通过所述业务终端将从安全域初始密钥分发给所述智能卡；还用于与所述智能卡主安全域进行互认证及建立临时会话密钥，还用于根据应用下载请求或智能卡状态信息判断是否建立从安全域，以及建立从安全域，生成并向智能卡分发从安全域初始密钥。

6. 如权利要求 5 所述的系统，其特征在于，

所述业务终端为卡发行商业务终端，用于对所述卡发行商管理平台与所述智能卡间的交互信息进行转发；或者；

所述业务终端为应用提供商业务终端，所述系统还包括应用提供商管理平台；

所述应用提供商业务终端，用于接收所述应用提供商管理平台发送的消息并转发给所述智能卡；还用于接收所述智能卡发送的消息并转发给所述应用提供商管理平台；

所述应用提供商管理平台，用于接收所述卡发行商管理平台发送的消息并转发给所述应用提供商业务终端；还用于接收所述应用提供商业务终端发送的消息并转发给所述卡发行商管理平台。

7. 如权利要求 5 或 6 所述的系统，其特征在于，

所述智能卡为一独立设备或安装在移动终端上。

8. 一种采用如权利要求 1 所述智能卡的从安全域初始密钥分发方法的移动终端，所述移动终端包括具有电子支付应用功能的智能卡，其特征在于，所述智能卡从安全域的初始密钥由卡发行商管理平台通过卡发行商业务终端分发，或者通过应用提供商管理平台和应用提供商业务终端分发。

智能卡的从安全域初始密钥分发方法和系统、移动终端

技术领域

[0001] 本发明涉及移动终端电子支付技术，尤其涉及智能卡的从安全域初始密钥分发方法和系统、移动终端。

背景技术

[0002] IC 卡特别是非接触式 IC 卡经过十多年的发展，已经被广泛应用于公交、门禁、小额电子支付等领域。与此同时，手机经历 20 多年的迅速发展，在居民中基本得到普及，给人们的工作及生活带来很大的便利。手机的功能越来越强大，并存在集成更多功能的趋势。将手机和非接触式 IC 卡技术结合，手机应用于电子支付领域，会进一步扩大手机的使用范围，给人们的生活带来便捷，存在着广阔的应用前景。

[0003] 近场通信技术 (Near Field Communication，NFC) 是工作于 13.56MHz 的一种近距离无线通信技术，由射频识别 RFID(Radio Frequency Identification) 技术及互连技术融合演变而来。手机等移动通信终端集成 NFC 技术后，可以模拟非接触式 IC 卡，用于电子支付的有关应用。移动通信终端上实现该方案需要在终端上增加 NFC 模拟前端芯片和 NFC 天线，并使用支持电子支付的智能卡。

[0004] 为实现基于 NFC 技术的移动电子支付，需要建立移动终端电子支付系统，通过该系统实现对基于 NFC 的移动终端电子支付的管理，包括 :智能卡的发行，电子支付应用的下载、安装和个人化，采用相关技术和管理策略实现电子支付应用的安全等。

[0005] 基于 NFC 技术的移动终端电子支付系统的业务框架通常采用全球平台 GP(Global Platform) 规范的多应用框架，在该框架下，支持 Global Platform 规范的智能卡指的是符合全球平台卡规范 (Global Platform Card Specification)V2.1.1/V2.2 的 IC 芯片或智能卡，从物理形式上可以为 SIM/USIM 卡即客户识别模块 (Subscriber Identity Model)/通用移动通信系统客户识别模块 (UMTSSubscriber Identity Module UMTS)、可插拔的智能存储卡或者集成在移动终端上的 IC 芯片。

[0006] 如果基于近场通信 (NFC) 技术的移动终端电子支付系统支持 GP2.1.1 规范，安全信道协议需要支持 SCP02(基于对称密钥)，如果基于近场通信技术的移动终端电子支付系统支持 GP2.2 规范，安全信道协议需要支持 SCP02(基于对称密钥) 和 SCP10(基于非对称密钥)，卡发行商、应用提供商可以根据安全策略需求进行选择。

[0007] 一般情况下，基于 NFC 的移动终端近距离电子支付系统主要由卡发行商管理平台、一个或多个应用提供商管理平台和支持具有电子支付应用功能智能卡的移动终端组成。

[0008] 在支持 Global Platform 规范的智能卡上可以安装多个应用，为了实现电子支付应用的安全，智能卡被分隔为若干个独立的安全域，以保证多个应用相互之间的隔离以及独立性，各个应用提供商管理各自的安全域以及应用、应用数据等。

[0009] 安全域是卡外实体包括卡发行商和应用提供商在卡上的代表，它们包含用于支持安全信道协议运作以及智能卡内容管理的密钥。安全域包括主安全域和从安全域等。主安

全域是卡发行商在智能卡上的强制的卡上代表，一个智能卡只包含一个主安全域。从安全域是卡发行商或应用提供商在智能卡上的附加的可选卡上代表。

[0010] 安全域的密钥生成与分发由管理该安全域的卡发行商或应用提供商负责，这保证了来自不同应用提供者的应用和数据可以共存于同一个卡上。安全域的密钥包括主安全域密钥、从安全域初始密钥和从安全域密钥。主安全域密钥和从安全域初始密钥由卡发行商管理平台生成，从安全域密钥由管理从安全域的卡发行商管理平台或应用提供商管理平台生成。

[0011] 在将电子支付应用下载并安装到智能卡之前，需要在智能卡上为该应用先创建从安全域，智能卡从安全域的创建是由卡发行商管理平台完成的。在智能卡发行后，创建智能卡从安全域时，从安全域初始密钥必须由卡发行商管理平台通过安全途径导入到智能卡上的从安全域。

[0012] 从安全域初始密钥的分发过程与系统网络架构的具体实现方式有关。为了实现智能卡的安全性管理和支付应用的下载、安装等，智能卡需要和卡发行商管理平台以及应用提供商管理平台建立通信。智能卡可以通过业务终端和管理平台建立通信。业务终端是可以对智能卡进行读写的设备，如与计算机相连的 POS 机等。在使用业务终端时，针对对称密钥的情况，如何将卡发行商管理平台生成的从安全域初始密钥安全的导入到智能卡上的从安全域，是移动终端电子支付需要解决的一个问题。

发明内容

[0013] 本发明要解决的技术问题是提供一种智能卡的从安全域初始密钥分发方法和系统、移动终端，以将卡发行商管理平台生成的从安全域初始密钥安全的导入到从安全域，从而实现从安全域初始密钥的安全分发。

[0014] 为了解决上述技术问题，智能卡的从安全域初始密钥分发方法，该方法基于移动终端电子支付系统实现，该系统包括具有电子支付应用功能的智能卡、卡发行商管理平台及业务终端，所述智能卡为一独立设备或安装在移动终端上；所述智能卡通过所述业务终端与所述卡发行商管理平台进行通信，所述卡发行商管理平台通过所述业务终端将从安全域初始密钥分发给所述智能卡。

[0015] 进一步地，该方法包括：(a) 用户向所述卡发行商管理平台提交应用下载请求；(b) 所述卡发行商管理平台收到应用下载请求信息后，所述卡发行商管理平台和所述智能卡主安全域之间建立安全信道；(c) 所述卡发行商管理平台创建从安全域及生成从安全域初始密钥，通过建立的安全信道经由所述业务终端将安全域初始密钥导入到所述智能卡从安全域。

[0016] 进一步地，步骤 (a) 中用户通过所述智能卡程序或所述业务终端客户端程序触发应用下载请求，所述应用下载请求中包括智能卡标识信息、应用标识及应用提供商身份信息，步骤 (b) 之后，步骤 (c) 之前，还包括：所述卡发行商管理平台根据所述智能卡标识信息，应用标识及应用提供商身份信息，或者根据智能卡状态信息，判断是否创建从安全域。

[0017] 进一步地，步骤 (b) 建立安全信道的过程包括：(b1) 所述卡发行商管理平台与智能卡主安全域经由所述业务终端进行互认证，所述互认证过程经由所述业务终端在所述卡发行商管理平台和所述智能卡主安全域之间完成；(b2) 所述卡发行商管理平台与所述智

能卡主安全域之间建立临时会话密钥，从而建立安全信道。

[0018] 进一步地，所述业务终端为卡发行商业务终端，所述卡发行商管理平台与所述智能卡间的交互信息通过卡发行商业务终端转发；或者，所述业务终端为应用提供商业务终端，从所述卡发行商管理平台到所述智能卡的消息依次通过应用提供商管理平台和应用提供商业务终端转发，从所述智能卡到所述卡发行商管理平台的消息依次通过应用提供商业务终端和应用提供商管理平台转发。

[0019] 为了解决上述技术问题，本发明还提供了一种智能卡的从安全域初始密钥分发系统，该系统包括具有电子支付应用功能的智能卡、卡发行商管理平台及业务终端；所述智能卡通过所述业务终端与所述卡发行商管理平台进行通信；所述卡发行商管理平台，用于通过所述业务终端将从安全域初始密钥分发给所述智能卡。

[0020] 进一步地，所述智能卡，还用于提供向所述卡发行商管理平台提交应用下载请求的支持，与卡发行商管理平台进行互认证及建立临时会话密钥，还用于解密获得的从安全域初始密钥，以及对从安全域进行初始化；所述卡发行商管理平台，还用于与所述智能卡主安全域进行互认证及建立临时会话密钥，还用于根据应用下载请求或智能卡状态信息判断是否建立从安全域，以及建立从安全域，生成并向智能卡分发从安全域初始密钥。

[0021] 进一步地，所述业务终端为卡发行商业务终端，用于对所述卡发行商管理平台与所述智能卡间的交互信息进行转发；或者；

[0022] 所述业务终端为应用提供商业务终端，所述系统还包括应用提供商管理平台；所述应用提供商业务终端，用于接收所述应用提供商管理平台发送的消息并转发给所述智能卡；还用于接收所述智能卡发送的消息并转发给所述应用提供商管理平台；所述应用提供商管理平台，用于接收所述卡发行商管理平台发送的消息并转发给所述应用提供商业务终端；还用于接收所述应用提供商业务终端发送的消息并转发给所述卡发行商管理平台。

[0023] 进一步地，所述智能卡为一独立设备或安装在移动终端上。

[0024] 本发明还提供了一种移动终端，所述移动终端包括具有电子支付应用功能的智能卡，所述智能卡从安全域的初始密钥由卡发行商管理平台通过卡发行商业务终端分发，或者通过应用提供商管理平台和应用提供商业务终端分发。

[0025] 本发明可以解决在发卡后，针对对称密钥的情况，在创建从安全域时，将卡发行商管理平台生成的从安全域初始密钥安全的导入到从安全域，从而实现从安全域初始密钥的安全分发。

附图说明

[0026] 图 1 是本发明中基于近场通信技术的移动终端电子支付系统架构示意图；

[0027] 图 2 是本发明中实施例一中通过卡发行商业务终端进行从安全域初始密钥分发的流程示意图；

[0028] 图 3 是本发明中实施例二中通过应用提供商业务终端进行从安全域初始密钥分发的流程示意图。

具体实施方式

[0029] 如图 1 所示，本发明中移动终端电子支付系统包括：应用提供商管理平台、卡发行

商管理平台、应用提供商管理平台、业务终端（包括卡发行商业务终端和应用提供商业务终端）、移动终端和具有电子支付应用功能的智能卡，本系统中的智能卡可以安装在一移动终端上。在其它实施例中，此系统也可以不包括移动终端，此时该智能卡是一独立设备。

[0030] 所述智能卡支持Global Platform Card Specification V2.1.1/V2.2规范；具有电子支付应用功能的智能卡可以直接通过卡发行商业务终端和应用提供商业务终端分别与卡发行商管理平台或应用提供商管理平台连接，当具有电子支付应用功能的智能卡安装在移动终端上时，移动终端可以通过卡发行商业务终端或应用提供商业务终端分别与卡发行商管理平台和应用提供商管理平台连接。

[0031] 所述智能卡可以安装在移动终端上，所述智能卡和所述移动终端可以支持 OTA 功能，移动终端可以通过移动通信网络与 OTA 服务器相连，OTA 服务器分别与卡发行商管理平台和应用提供商管理平台连接。

[0032] 卡发行商管理平台，负责智能卡的发行和管理，对智能卡的资源和生命周期、密钥、证书进行管理，负责从安全域的创建，并与其他安全域交互应用数据，其中包括创建从安全域，与所述智能卡进行互认证及建立临时会话密钥，以及生成从安全域初始密钥和新的从安全域密钥。就具体实现而言，卡发行商管理平台可以包括卡片管理系统、应用管理系统、密钥管理系统、证书管理系统、应用提供商管理系统等，其中证书管理系统在支持非对称密钥的情况下使用，证书管理系统和卡片发行商认证机构 (CA) 系统连接；

[0033] 应用提供商管理平台，负责电子支付应用的提供和管理功能，提供各种业务应用，并对智能卡上与其对应的从安全域进行安全管理，对所述从安全域的应用密钥、证书、数据等进行控制，提供应用的安全下载、安装等功能。其中包括与所述智能卡进行互认证及建立临时会话密钥，以及生成新的从安全域密钥。就具体实现而言，应用提供商管理平台可以包括应用管理系统、密钥管理系统、证书管理系统，其中证书管理系统在支持非对称密钥的情况下使用，证书管理系统和应用提供商认证机构 (CA) 系统连接。

[0034] 卡发行商管理平台和应用提供商管理平台可以通过各自的业务终端提供电子支付有关服务：参与处理电子支付用户信息管理，参与从安全域的创建和密钥分发、电子支付应用的下载、以及电子支付应用的个人化等。应用提供商管理平台和卡发行商管理平台之间可以通过安全连接（如专线连接）进行通信。

[0035] 所述智能卡，可以安装在所述移动终端上，用于通过移动终端及业务终端与所述卡发行商管理平台进行通信，也可以直接通过业务终端与所述卡发行商管理平台进行通信；还用于提供向所述卡发行商管理平台提交应用下载请求的支持，与卡发行商管理平台进行互认证及建立临时会话密钥，还用于解密获得的从安全域初始密钥，以及对从安全域进行初始化；

[0036] 卡发行商业务终端，由卡发行商管理平台管理；用于对所述卡发行商管理平台与所述智能卡间的交互信息进行转发。

[0037] 应用提供商业务终端，由应用提供商管理平台管理；用于接收所述应用提供商管理平台发送的消息并转发给所述智能卡；还用于接收所述智能卡发送的消息并转发给所述应用提供商管理平台。

[0038] 本发明基于图 1 所示的移动终端电子支付系统架构为例进行描述，但不限于图 1 所示移动终端电子支付系统架构。

[0039] 如图 2 所示，实施例一中，卡发行商管理平台通过卡发行商业务终端向智能卡分发安全域初始密钥，具体包括以下步骤：

[0040] 步骤 201，用户通过卡发行商业务终端客户端程序或智能卡程序触发应用下载申请，并向卡发行商管理平台提交应用下载申请，应用下载申请可以包含智能卡用户识别信息、应用标识及应用提供商身份等信息；

[0041] 步骤 202，卡发行商管理平台经由卡发行商业务终端向智能卡发送 SELECT 命令报文，选择主安全域；

[0042] 步骤 203，智能卡经由卡发行商业务终端向卡发行商管理平台提交 SELECT 命令响应；

[0043] 步骤 204，卡发行商管理平台与智能卡主安全域经由卡发行商业务终端建立 SCP02 安全信道；

[0044] 所述卡发行商管理平台启动所述卡发行商管理平台和所述智能卡主安全域的互认证，完成互认证后，卡发行商管理平台与智能卡主安全域之间建立起临时会话密钥，从而建立安全信道。该临时会话密钥可以遵循 GlobalPlatform Card Specification V2.1.1/V2.2 规范建立，也可以通过其它方法建立；

[0045] 所述互认证过程经由卡发行商业务终端在所述卡发行商管理平台和所述智能卡主安全域之间完成。

[0046] 步骤 205，卡发行商管理平台判断是否需要创建从安全域，如果不需要创建从安全域，则终止从安全域创建过程；如果需要创建从安全域，则继续执行后续步骤；

[0047] 所述卡发行商管理平台根据所述智能卡 ICCID 信息、应用标识及应用提供商身份等信息，或者通过智能卡状态信息等方式，判断是否创建从安全域。

[0048] 智能卡状态信息由卡发行商管理平台从智能卡主安全域获取。

[0049] 步骤 206，卡发行商管理平台经由卡发行商业务终端向智能卡发送 INSTALL 命令；

[0050] 步骤 207，智能卡经由卡发行商业务终端向卡发行商管理平台提交 INSTALL 命令响应；

[0051] 步骤 208，卡发行商管理平台生成初始密钥，通过 PUTKEY 命令，经由卡发行商业务终端向智能卡主安全域发送从安全域初始密钥；

[0052] 步骤 209，智能卡主安全域接收到从安全域初始密钥后，用接收到的从安全域初始密钥初始化从安全域；

[0053] 步骤 210，智能卡主安全域经由卡发行商业务终端向卡发行商管理平台发送 PUTKEY 命令响应，结束从安全域初始密钥分发过程。

[0054] 实施例一中卡发行商管理平台与智能卡间的交互信息通过卡发行商业务终端转发；在实施例二中，从卡发行商管理平台到智能卡的消息依次通过应用提供商管理平台和应用提供商业务终端转发，从智能卡到卡发行商管理平台的消息依次通过应用提供商业务终端和应用提供商管理平台转发。如图 3 所示，实施例二中，分发从安全域初始密钥的方法具体包括以下步骤：

[0055] 步骤 301，用户通过应用提供商业务终端客户端程序或智能卡程序触发应用下载申请，并经由应用提供商管理平台向卡发行商管理平台提交应用下载申请，应用下载申请可以包含智能卡用户识别信息、应用标识及应用提供商身份等信息；

[0056] 步骤 302，卡发行商管理平台经由应用提供商管理平台和应用提供商业务终端向智能卡发送 SELECT 命令报文，选择主安全域；

[0057] 步骤 303，智能卡经由应用提供商业务终端和应用提供商管理平台向卡发行商管理平台提交 SELECT 命令响应；

[0058] 步骤 304，卡发行商管理平台与智能卡主安全域经由应用提供商管理平台和应用提供商业务终端建立 SCP02 安全信道；

[0059] 所述卡发行商管理平台启动所述卡发行商管理平台和所述智能卡主安全域的互认证，完成互认证后，卡发行商管理平台与智能卡主安全域之间建立起临时会话密钥，从而建立安全信道。该临时会话密钥可以遵循 GlobalPlatform Card Specification V2.1.1/V2.2 规范建立，也可以通过其它方法建立；

[0060] 所述互认证过程经由应用提供商管理平台和应用提供商业务终端在所述卡发行商管理平台和所述智能卡主安全域之间完成。

[0061] 步骤 305，卡发行商管理平台判断是否需要创建从安全域，如果不需要创建从安全域，则终止从安全域创建过程；如果需要创建从安全域，则继续执行后续步骤；

[0062] 所述卡发行商管理平台根据所述智能卡 ICCID 信息、应用标识及应用提供商身份等信息，或者通过智能卡状态信息等方式，判断是否创建从安全域。

[0063] 智能卡状态信息由卡发行商管理平台从智能卡主安全域获取。

[0064] 步骤 306，卡发行商管理平台经由应用提供商管理平台和应用提供商业务终端向智能卡发送 INSTALL 命令；

[0065] 步骤 307，智能卡经由应用提供商业务终端和应用提供商管理平台向卡发行商管理平台提交 INSTALL 命令响应；

[0066] 步骤 308，卡发行商管理平台通过 PUTKEY 命令，经由应用提供商管理平台和应用提供商业务终端向智能卡主安全域发送从安全域初始密钥；

[0067] 步骤 309，智能卡主安全域接收到从安全域初始密钥后，用接收到的从安全域初始密钥初始化从安全域；

[0068] 步骤 310，智能卡主安全域经由应用提供商业务终端和应用提供商管理平台向卡发行商管理平台发送 PUTKEY 命令响应，结束从安全域初始密钥分发过程。

[0069] 本发明智能卡从安全域初始密钥分发方法和系统，可以解决在发卡后，针对对称密钥的情况，在创建从安全域时，将卡发行商管理平台生成的从安全域初始密钥安全的导入到从安全域，从而实现从安全域初始密钥的安全分发。

[0070] 本发明还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明做出各种相应的改变和变形，这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

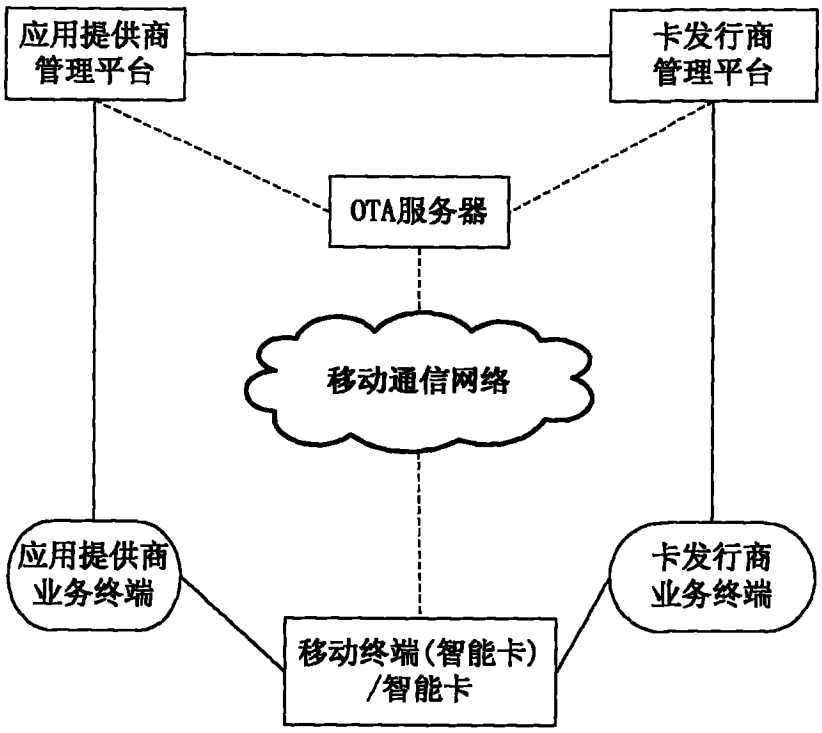

应用提供商
管理平台
卡发行商
管理平台
OTA服务器
移动通信网络
应用提供商
业务终端
卡发行商
业务终端
移动终端(智能卡)
/智能卡

图 1

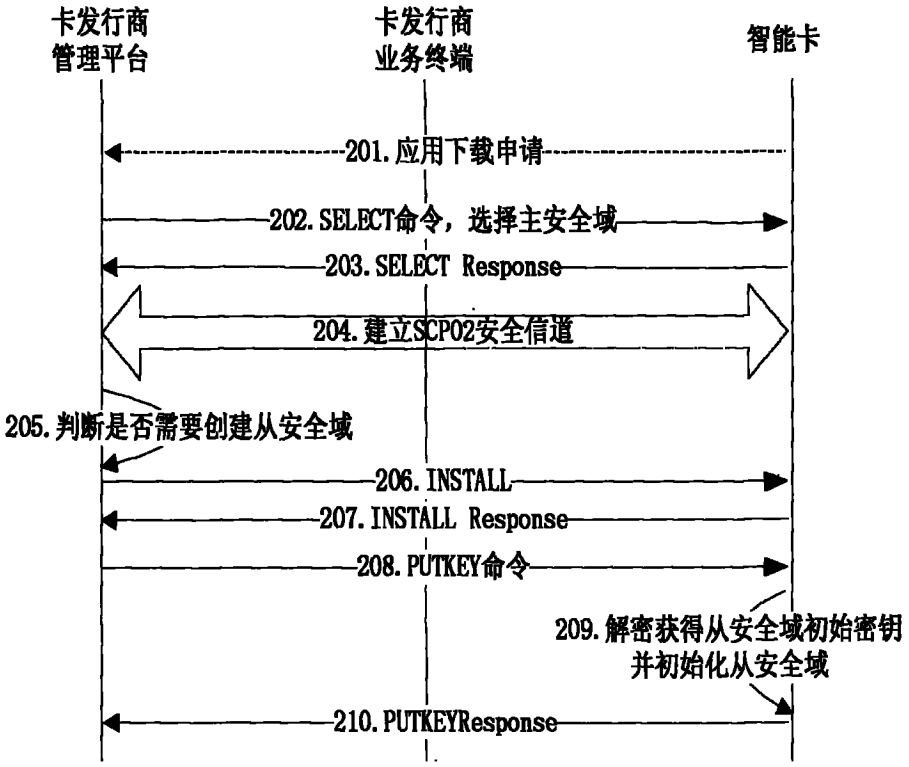

卡发行商
管理平台
卡发行商
业务终端
智能卡
201. 应用下载申请
202. SELECT命令，选择主安全域
203. SELECT Response
204. 建立SCP02安全信道
205. 判断是否需要创建从安全域
206. INSTALL
207. INSTALL Response
208. PUTKEY命令
209. 解密获得从安全域初始密钥
并初始化从安全域
210. PUTKEYResponse

图 2

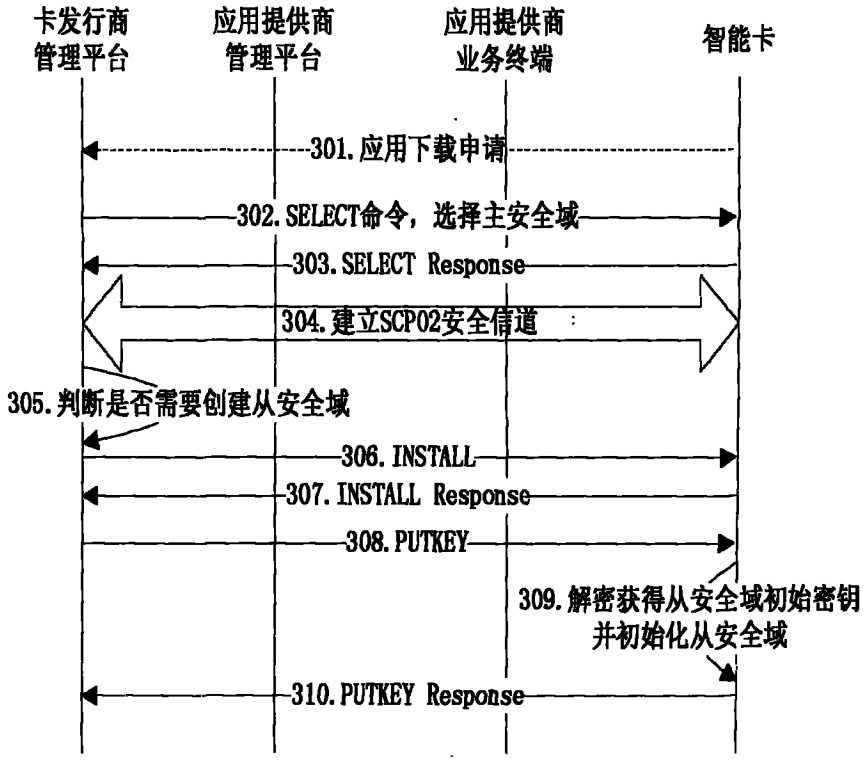

卡发行商
管理平台
应用提供商
管理平台
应用提供商
业务终端
智能卡
301. 应用下载申请
302. SELECT命令，选择主安全域
303. SELECT Response
304. 建立SCP02安全信道
305. 判断是否需要创建从安全域
306. INSTALL
307. INSTALL Response
308. PUTKEY
309. 解密获得从安全域初始密钥
并初始化从安全域
310. PUTKEY Response

图 3