

# (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局

(43) 国际公布日  
2014 年 1 月 23 日 (23.01.2014)



(10) 国际公布号  
WO 2014/012468 A1

- (51) 国际专利分类号:  
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2013/079364
- (22) 国际申请日: 2013 年 7 月 15 日 (15.07.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201210247048.3 2012 年 7 月 17 日 (17.07.2012) CN
- (71) 申请人: 中国移动通信集团公司 (CHINA MOBILE COMMUNICATIONS CORPORATION) [CN/CN]; 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。
- (72) 发明人: 乐祖晖 (YUE, Zuhui); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。 罗红 (LUO, Hong); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。
- (74) 代理人: 北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区西直门北大街 32 号院枫蓝国际中心 2 号楼 10 层, Beijing 100082 (CN)。

- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

## 本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: DATA CONFIGURATION METHOD, APPARATUS AND SYSTEM FOR UNIVERSAL INTEGRATED CIRCUIT CARD, COMPUTER PROGRAM AND STORAGE MEDIUM

(54) 发明名称: 通用集成电路卡的数据配置方法、装置、系统、计算机程序及存储介质

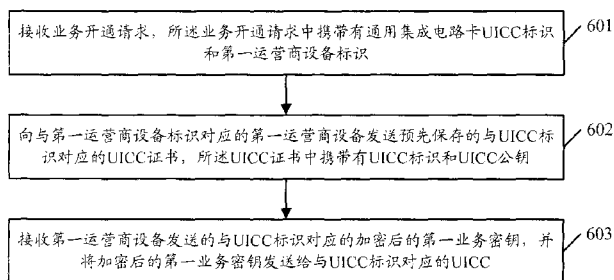


图 6 / Fig. 6

- 601 RECEIVING A SERVICE OPEN REQUEST, A UNIVERSAL INTEGRATED CIRCUIT CARD (UICC) IDENTIFICATION AND A FIRST OPERATOR DEVICE IDENTIFICATION BEING CARRIED IN THE SERVICE OPEN REQUEST
- 602 SENDING A PRE-STORED UICC CERTIFICATE CORRESPONDING TO THE UICC IDENTIFICATION TO FIRST OPERATOR DEVICE CORRESPONDING TO THE FIRST OPERATOR DEVICE IDENTIFICATION, THE UICC IDENTIFICATION AND A UICC PUBLIC KEY BEING CARRIED IN THE UICC CERTIFICATE
- 603 RECEIVING AN ENCRYPTED FIRST SERVICE ENCRYPTION KEY CORRESPONDING TO THE UICC IDENTIFICATION SENT FROM THE FIRST OPERATOR DEVICE, AND SENDING THE ENCRYPTED FIRST SERVICE ENCRYPTION KEY TO A UICC CORRESPONDING TO THE UICC IDENTIFICATION

(57) Abstract: Disclosed are a data configuration method, apparatus and system for a universal integrated circuit card, a computer program and a storage medium. The method comprises: receiving a service open request, a UICC identification and a first operator device identification being carried in the service open request; sending a pre-stored UICC certificate corresponding to the UICC identification to a first operator device corresponding to the first operator device identification, the UICC identification and a UICC public key being carried in the UICC certificate; and receiving an encrypted first service encryption key corresponding to the UICC identification sent from the first operator device, and sending the encrypted first service encryption key to a UICC corresponding to the UICC identification. Compared with the prior art, the data configuration method, apparatus and system for a universal integrated circuit card, the computer program and the storage medium proposed in the present invention can dynamically configure operator data in a universal integrated circuit card in an M2M terminal, thus expanding the usage range of M2M terminals.

(57) 摘要:

[见续页]



---

本发明公开了一种通用集成电路卡的数据配置方法、装置、系统、计算机程序及存储介质，该方法包括：接收业务开通请求，所述业务开通请求中携带有 UICC 标识和第一运营商设备标识；向与第一运营商设备标识对应的第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥；接收第一运营商设备发送的与 UICC 标识对应的加密后的第一业务密钥，并将加密后的第一业务密钥发送给与 UICC 标识对应的 UICC。和现有技术相比，本发明提出的通用集成电路卡的数据配置方法、装置、系统、计算机程序及存储介质，能够对 M2M 终端中的通用集成电路卡中的运营商数据进行动态配置，扩大了 M2M 终端的使用范围。

## 通用集成电路卡的数据配置方法、装置、系统、计算机程序及存储介质

本申请要求在 2012 年 7 月 17 日提交中国专利局、申请号为 201210247048.3、发明名称为“通用集成电路卡的数据配置方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

### 技术领域

本发明涉及数据通信技术，特别涉及一种通用集成电路卡的数据配置方法、装置、系统、计算机程序及存储介质。

### 背景技术

随着物联网业务的迅速发展，M2M（机器对机器）终端的应用遍及电力、交通、工业控制、医疗以及公共事业管理等多个行业。M2M 通常是指机器设备通过移动通信网络与其他设备或系统的通信。为了能够接入到移动通信网络，M2M 终端上需要安装运营商提供的智能卡，由于 M2M 终端的应用环境与普通手机终端有较大的不同，因此需要在 M2M 终端中使用 M2M 专用智能卡。

M2M 专用智能卡一般指在现有智能卡的基础上，通过对现有智能卡的软硬件以及相关支撑平台进行升级后的智能卡，以满足 M2M 行业的需求。M2M 专用智能卡承载着运营商提供的码号资源，即 M2M 终端接入移动通信网络的身份标识，同时 M2M 专用智能卡还可以承载和处理运营商提供的各种增值服务。

根据应用场景和技术实现的不同，目前的 M2M 专用智能卡分为如下两种：MP 卡和 MS 卡。

MP 卡是 M2M Plug-In 卡的简称，即可插拔式 SIM 卡，采用能够适应特殊环境要求的特殊芯片和特殊的卡基材料，物理性能较高，可以满足更长使用寿命和更恶劣环境的要求。

MS 卡是 M2M SMD（Surface Mount Device，表面组装设备）卡的简称，即焊接式 SIM 卡，它完全具备传统 SIM 卡的全部功能，同时采用 SMD 贴片

封装工艺使得 SIM 卡芯片可以直接焊接在 M2M 终端模组上，以实现紧密牢固的物理连接和可靠的接口通信。

在实现本发明的过程中，发明人发现现有技术中至少存在如下问题：

现有的 MP 卡和 MS 卡中的运营商数据是通过运营商进行预先配置的，并且 MP 卡和 MS 卡在使用之后无法更换运营商数据，导致 M2M 终端只能和预定的运营商进行通信，限制了 M2M 终端的使用范围。

## 发明内容

有鉴于此，本发明的主要目的在于提供三种通用集成电路卡的数据配置方法，能够实现对 M2M 终端中的通用集成电路卡的运营商数据进行动态配置，扩大了 M2M 终端的使用范围。

本发明的另一目的在于提供四种通用集成电路卡的数据配置装置，能够实现对 M2M 终端中的通用集成电路的运营商数据进行动态配置，扩大了 M2M 终端的使用范围。

本发明的又一目的在于提供一种通用集成电路卡的数据配置系统，能够实现对 M2M 终端中的通用集成电路卡的运营商数据进行动态配置，扩大了 M2M 终端的使用范围。

本发明的又一目的在于提供一种计算机程序，能够实现对 M2M 终端中的通用集成电路卡的运营商数据进行动态配置，扩大了 M2M 终端的使用范围。

本发明的又一目的在于提供一种存储介质，够实现对 M2M 终端中的通用集成电路卡的运营商数据进行动态配置，扩大了 M2M 终端的使用范围。

为达到上述目的，本发明的技术方案是这样实现的：

一种通用集成电路卡的数据配置方法，所述方法包括：

接收业务开通请求，所述业务开通请求中携带有通用集成电路卡 UICC 标识和第一运营商设备标识；

向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和 UICC 公钥；

接收所述第一运营商设备发送的与所述 UICC 标识对应的加密后的第一业务密钥，并将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC。

一种计算机程序，用于执行上述通用集成电路卡的数据配置方法。

一种存储介质，用于存储上述计算机程序。

一种通用集成电路卡管理平台，包括：第一接收单元和第一发送单元；

所述第一接收单元，用于接收业务开通请求，所述业务开通请求中携带有通用集成电路卡 UICC 标识和第一运营商设备标识，将所述业务开通请求发送给所述第一发送单元；

所述第一发送单元，用于向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和 UICC 公钥；

所述第一接收单元，还用于接收所述第一运营商设备发送的与所述 UICC 标识对应的加密后的第一业务密钥，将所述加密后的第一业务密钥发送给所述第一发送单元；

所述第一发送单元，还用于将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC。

一种第一运营商设备，包括：第二接收单元、业务密钥生成单元、第二发送单元和第一业务交互单元；

所述第二接收单元，用于接收通用集成电路卡 UICC 管理平台发送的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥，将所述 UICC 证书发送给所述业务密钥生成单元；

所述业务密钥生成单元，用于当对所述 UICC 证书验证通过时，根据预设方法生成与所述 UICC 标识对应的第一业务密钥，使用所述 UICC 公钥对所述第一业务密钥进行加密，将所述第一业务密钥发送给第一业务交互单元，将加密后的第一业务密钥发送给所述第二发送单元；

所述第二发送单元，用于将加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC；

所述第二接收单元，还用于获取所述 UICC 在获取到所述第一业务密钥

之后发送的业务开通执行响应，所述业务开通执行响应中携带有所述 UICC 预先保存的所述 UICC 标识；

所述第一业务交互单元，用于使用所述第一业务密钥和所述 UICC 进行业务交互。

一种通用集成电路卡，包括：第三接收单元、解密单元、第三发送单元和第二业务交互单元；

所述第三接收单元，用于接收通用集成电路卡 UICC 管理平台发送的加密后的第一业务密钥，将所述加密后的第一业务密钥发送给所述解密单元；

所述解密单元，用于使用预先保存的与 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密，获取第一业务密钥，将所述第一业务密钥发送给第二业务交互单元，并向所述第三发送单元发送一个第一发送指令；

所述第三发送单元，用于在接收到所述第一发送指令之后，向第一运营商设备发送业务开通执行响应，所述业务开通执行响应中携带有预先保存的 UICC 标识；

所述第二业务交互单元，用于使用所述第一业务密钥和所述第一运营商设备进行业务交互。

一种用户终端，包括：第三存储单元和通用集成电路卡 UICC；

所述第三存储单元，用于存储所述 UICC；

所述 UICC，用于接收 UICC 管理平台发送的加密后的第一业务密钥；使用预先保存的与 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密，获取第一业务密钥；向第一运营商设备发送业务开通执行响应，所述业务开通执行响应中携带有预先保存的 UICC 标识；使用所述第一业务密钥和所述第一运营商设备进行业务交互。

一种通用集成电路卡的数据配置系统，包括：通用集成电路卡 UICC 管理平台、第一运营商设备和 UICC；

所述 UICC 管理平台，用于接收业务开通请求，所述业务开通请求中携带有 UICC 标识和第一运营商设备标识，向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和与所述 UICC 标识对应的 UICC 公钥；

接收所述第一运营商设备发送的与所述 UICC 标识对应的加密后的第一业务密钥,并将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC;

所述第一运营商设备,用于接收所述 UICC 管理平台发送的 UICC 证书,所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥;当对所述 UICC 证书验证通过时,根据预设方法生成与所述 UICC 标识对应的第一业务密钥,使用所述 UICC 公钥对所述第一业务密钥进行加密,并通过所述 UICC 管理平台将加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC;获取所述 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应,所述业务开通执行响应中携带有所述 UICC 预先保存的所述 UICC 标识;使用所述第一业务密钥和所述 UICC 进行业务交互;

所述 UICC,用于接收所述 UICC 管理平台发送的所述加密后的第一业务密钥;使用预先保存的与所述 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密,获取所述第一业务密钥;向所述第一运营商设备发送业务开通执行响应,所述业务开通执行响应中携带有预先保存的所述 UICC 标识;使用所述第一业务密钥和所述第一运营商设备进行业务交互。

可见,采用本发明的技术方案,UICC 管理平台根据业务开通请求中携带的 UICC 标识和第一运营商设备标识,获取第一运营商设备生成的与 UICC 标识对应的加密后的第一业务密钥,UICC 在获取到所述加密后的第一业务密钥之后使用预先保存的 UICC 私钥对加密后的第一业务密钥进行解密,使用解密后得到的第一业务密钥与第一运营商设备进行业务交互。由于用户发送的业务开通请求中携带有第一运营商设备标识,UICC 管理平台根据所述第一运营商设备标识为通用集成电路卡开通与第一运营商设备标识对应的第一运营商设备之间的业务交互,因此运营商能够灵活地对通用集成电路卡中的运营商数据进行动态配置,无需 M2M 终端在生产过程中需要根据运营商进行定制开发,因此本发明提出的通用集成电路卡的数据配置方法、装置及系统,解决了现有技术中 M2M 终端只能和预定的运营商进行通信的技术问题,扩大了 M2M 终端的使用范围;另外,本发明所述方法实现起来简单方便,便于普及。

## 附图说明

图 1 为本发明开通通用集成电路卡的第一实现流程图。

图 2 为本发明通用集成电路卡证书的生成方法的实现流程图。

图 3 为本发明开通通用集成电路卡的第一实施例的实现流程图。

图 4 为本发明传输子密钥的生成方法示意图。

图 5 为本发明开通通用集成电路卡的第二实施例的实现流程图。

图 6 为本发明开通通用集成电路卡的第二实现流程图。

图 7 为本发明开通通用集成电路卡的第三实现流程图。

图 8 为本发明开通通用集成电路卡的第四实现流程图。

图 9 为本发明终止通用集成电路卡的第一实现流程图。

图 10 为本发明终止通用集成电路卡的第一实施例的实现流程图。

图 11 为本发明终止通用集成电路卡的第二实施例的实现流程图。

图 12 为本发明终止通用集成电路卡的第二实现流程图。

图 13 为本发明终止通用集成电路卡的第三实现流程图。

图 14 为本发明终止通用集成电路卡的第四实现流程图。

图 15 为本发明通用集成电路卡切换运营商的第一实现流程图。

图 16 为本发明通用集成电路卡切换运营商的第一实施例的实现流程图。

图 17 为本发明通用集成电路卡切换运营商的第二实施例的实现流程图。

图 18 为本发明通用集成电路卡切换运营商的第二实现流程图。

图 19 为本发明通用集成电路卡切换运营商的第三实现流程图。

图 20 为本发明通用集成电路卡切换运营商的第四实现流程图。

图 21 为本发明通用集成电路卡管理平台的结构示意图。

图 22 为本发明第一运营商设备的结构示意图。

图 23 为本发明通用集成电路卡的结构示意图。

图 24 为本发明用户终端的结构示意图。

图 25 为本发明通用集成电路卡的数据配置系统结构示意图。

## 具体实施方式

针对现有技术中存在的问题，本发明中提出一种改进后的通用集成电路

卡的数据配置方案，能够实现对 M2M 终端中的通用集成电路卡进行动态数据配置，扩大了 M2M 终端的使用范围。

为使本发明的技术方案更加清楚、明白，以下参照附图并举实施例，对本发明所述方案作进一步地详细说明。

图 1 为本发明开通通用集成电路卡的第一实现流程图。如图 1 所示，包括如下所述的步骤：

步骤 101：通用集成电路卡 UICC 管理平台接收业务开通请求消息，所述业务开通请求消息中携带有 UICC 标识和第一运营商设备标识。

通用集成电路卡（Universal Integrated Circuit Card, UICC）是一种可移动的智能卡，它用于存储用户信息、鉴权密钥、电话簿和短消息等信息。

在本发明的具体实施例中，所述 UICC 标识可以是 UICC ID，也可以是 UICC 的其他标识信息。在本步骤中，UICC 管理平台可以采用如下两种方式接收业务开通请求：

第一种方式，用户申请归属的第一运营商设备 MNO1 接收用户提交业务申请请求，所述业务申请请求中携带有 UICC 标识；第一运营商设备向 UICC 管理平台发送业务开通请求，所述业务开通请求中携带有 UICC 标识和第一运营商设备预先保存的第一运营商设备标识。

例如，用户在购买 UICC 时，即可获得与所述 UICC 对应的 UICC 标识，当用户向第一运营商设备申请开通 UICC 时，向第一运营商设备提交业务申请请求，所述业务申请请求中携带有所述 UICC 标识。

第二种方式，UICC 管理平台直接接收用户提交的业务开通请求，所述业务开通请求消息中携带有 UICC 标识和第一运营商设备标识。

步骤 102：UICC 管理平台向与第一运营商设备标识对应的第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

较佳地，在本发明的具体实施例中，在 UICC 管理平台向第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书之前，UICC 管理平台查询与 UICC 标识对应的 UICC 是否被激活，若未被激活，则向第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书；若已被激活，则向第一运

营商设备发送错误提示信息。具体地，所述 UICC 被激活是指所述 UICC 已经开通了与运营商设备之间的业务交互；所述 UICC 未被激活是指所述 UICC 没有开通与运营商设备之间的业务交互，或者所述 UICC 已经终止与运营商设备之间的业务交互。

在本步骤之前，UICC 管理平台需要预先保存与 UICC 标识对应的 UICC 证书。图 2 为本发明通用集成电路卡证书的生成方法的实现流程图。如图 2 所示，包括如下所述的步骤：

步骤 201：UICC 在接收到 UICC 厂商设备发送的密钥请求之后，随机生成 UICC 公私钥对，将 UICC 公钥发送给 UICC 厂商设备，保存 UICC 私钥。

步骤 202：UICC 管理平台接收 UICC 厂商设备发送的 UICC 卡片信息，所述 UICC 卡片信息中携带有 UICC 标识和 UICC 公钥。

在本发明的具体实施例中，UICC 管理平台统一管理 UICC 标识，具体地，UICC 管理平台可以随机生成两个以上 UICC 标识，将所述两个以上 UICC 标识分配给 UICC 厂商设备，UICC 厂商设备在接收到 UICC 管理平台发送的两个以上 UICC 标识之后，根据所述两个以上 UICC 标识中的每个 UICC 标识生成 UICC。

步骤 203：UICC 管理平台将 UICC 卡片信息发送给认证中心。

在本步骤中，UICC 管理平台在接收到 UICC 厂商发送的 UICC 卡片信息之后，将 UICC 卡片信息发送给认证中心。

步骤 204：当认证中心对 UICC 卡片信息认证通过时，向 UICC 管理平台返回 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

在本步骤中，认证中心在接收到 UICC 管理平台发送的 UICC 卡片信息之后，按照现有技术中的认证方法对所述 UICC 卡片信息进行认证，当认证中心对 UICC 卡片信息认证通过时，向 UICC 管理平台返回 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

步骤 205：UICC 管理平台保存与 UICC 标识对应的 UICC 证书。

在本步骤中，UICC 管理平台在接收到认证中心返回的 UICC 证书之后，保存与 UICC 标识对应的 UICC 证书。

步骤 103：当第一运营商设备对 UICC 证书验证通过时，根据预设方法生

成与 UICC 标识对应的第一业务密钥，使用 UICC 公钥对第一业务密钥进行加密，并通过 UICC 管理平台将加密后的第一业务密钥发送给与 UICC 标识对应的 UICC。

在本步骤中，第一运营商设备在接收到 UICC 管理平台发送的与 UICC 标识对应的 UICC 证书之后，对接收到的 UICC 证书进行验证，当第一运营商设备对 UICC 证书验证通过时，根据现有技术中的密钥生成方法生成与 UICC 标识对应的第一业务密钥，使用 UICC 公钥对第一业务密钥进行加密，第一运营商设备将加密后的第一业务密钥发送给 UICC 管理平台，UICC 管理平台将接收到的加密后的第一业务密钥转发给与 UICC 标识对应的 UICC。

步骤 104：UICC 使用预先保存的与 UICC 公钥对应的 UICC 私钥对加密后的第一业务密钥进行解密，获取第一业务密钥。

在本步骤中，UICC 在接收到 UICC 管理平台发送的加密后的第一业务密钥之后，使用预先保存的 UICC 私钥对加密后的第一业务密钥进行解密，获取第一业务密钥。

步骤 105：第一运营商设备获取 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应，所述业务开通执行响应中携带有 UICC 预先保存的 UICC 标识。

在本步骤之前，UICC 在获取到第一业务密钥之后，向 UICC 管理平台返回业务开通执行响应，所述业务开通执行响应中携带有 UICC 预先保存的 UICC 标识，UICC 管理平台在接收到 UICC 发送的业务开通执行响应之后，将与 UICC 标识对应的 UICC 标记为已被激活，并将业务开通执行响应发送给第一运营商设备。

步骤 106：第一运营商设备和 UICC 使用第一业务密钥进行业务交互。

通过上述对步骤 101~106 的描述可知，由于用户发送的业务开通请求中携带有第一运营商设备标识，UICC 管理平台根据该第一运营商设备标识为通用集成电路卡开通与第一运营商设备标识对应的第一运营商设备之间的业务交互，因此运营商能够灵活地对通用集成电路卡中的运营商数据进行动态配置，无需 M2M 终端在生产过程中需要根据运营商进行定制开发。下面结合出两个具体的实施例对通用集成电路卡的开通流程进行详细描述：

图 3 为本发明开通通用集成电路卡的第一实施例的实现流程图。如图 3 所示，包括如下所述的步骤：

步骤 301：第一运营商设备 MNO1 接收用户提交的业务申请请求，所述业务申请请求中携带有 UICC ID。

步骤 302：MNO1 向 UICC 管理平台发送业务开通请求，所述业务开通请求中携带有 UICC ID 和第一运营商设备标识。

步骤 303：UICC 管理平台查询与 UICC ID 对应的 UICC 是否被激活，若未被激活，执行步骤 304，否则，执行步骤 305。

步骤 304：UICC 管理平台向 MNO1 发送预先保存的与 UICC ID 对应的 UICC 证书，执行步骤 306。

步骤 305：UICC 管理平台向 MNO1 发送错误提示信息，结束通用集成电路卡的开通流程。

步骤 306：当 MNO1 对 UICC 证书验证通过时，根据预设方法生成与 UICC ID 对应的第一业务密钥 AUICCKey1，使用 UICC 公钥 PubUICCKey 对 AUICCKey1 进行加密，获得加密后的第一业务密钥 [AUICCKey1]PubUICCKey。

步骤 307：MNO1 将加密后的第一业务密钥 [AUICCKey1]PubUICCKey 发送给 UICC 管理平台。

步骤 308：UICC 管理平台将加密后的第一业务密钥 [AUICCKey1]PubUICCKey 转发给与 UICC ID 对应的 UICC。

在本步骤中，UICC 管理平台可以使用有线网络或无线网络将加密后的第一业务密钥 [AUICCKey1]PubUICCKey 发送给与 UICC 标识对应的 UICC。

较佳地，在本发明的具体实施例中，UICC 管理平台与 UICC 之间的数据交互可以通过传输子密钥 TUICCKey 进行加密和鉴权。例如，UICC 管理平台在将加密后的第一业务密钥 [AUICCKey1]PubUICCKey 转发给与 UICC 标识对应的 UICC 时，UICC 管理平台可以使用传输子密钥 TUICCKey 对 [AUICCKey1]PubUICCKey 进行加密，UICC 在接收到 UICC 管理平台使用 TUICCKey 加密后的 [AUICCKey1]PubUICCKey 后，使用 TUICCKey 对加密后的 [AUICCKey1]PubUICCKey 进行解密，获得 [AUICCKey1]PubUICCKey。

图 4 为本发明传输子密钥的生成方法示意图。如图 4 所示, UICC 管理平台和 UICC 厂商设备分别与加密机 1 和加密机 2 相连接, 在加密机 1 和加密机 2 中分别预先保存传输根密钥 TRootkey, UICC 管理平台和 UICC 厂商设备均可以根据 UICC ID 获取传输子密钥 TUICCkey。具体地, UICC 管理平台将 UICC ID 发送给加密机 1, 加密机 1 使用预先保存的传输根密钥 TRootkey 对 UICC ID 进行加密, 获得与 UICC ID 对应的传输子密钥 TUICCkey, 并将 TUICCkey 返回给 UICC 管理平台。同样地, UICC 厂商设备将 UICC ID 发送给加密机 2, 加密机 2 使用预先保存的传输根密钥 TRootkey 对 UICC ID 进行加密, 获得与 UICC ID 对应的传输子密钥 TUICCkey, 并将 TUICCkey 返回给 UICC 厂商设备。

步骤 309: UICC 使用预先保存的与 UICC 公钥 PubUICCkey 对应的 UICC 私钥 PriUICCkey 对加密后的第一业务密钥[AUICCkey1]PubUICCkey 进行解密, 得到第一业务密钥 AUICCkey1。

在本步骤中, UICC 可以按照现有技术中的解密方法对加密后的第一业务密钥[AUICCkey1]PubUICCkey 进行解密, 获得第一业务密钥 AUICCkey1。

步骤 310: UICC 在获取到 AUICCkey1 之后向 UICC 管理平台返回业务开通执行响应, 所述业务开通执行响应中携带有 UICC 预先保存的 UICC ID。

步骤 311: UICC 管理平台将与 UICC ID 对应的 UICC 标记为已被激活。

步骤 312: UICC 管理平台将业务开通执行响应发送给 MNO1。

步骤 313: MNO1 和 UICC 使用第一业务密钥 AUICCkey1 进行业务交互。

图 5 为本发明开通通用集成电路卡的第二实施例的实现流程图。如图 5 所示, 包括如下所述的步骤:

步骤 501: UICC 管理平台接收用户提交的业务开通请求, 所述业务开通请求中携带有 UICC ID 和第一运营商设备标识。

步骤 502: UICC 管理平台查询与 UICC ID 对应的 UICC 是否被激活, 若未被激活, 执行步骤 503, 否则, 执行步骤 504。

步骤 503: UICC 管理平台向与第一运营商设备标识对应的 MNO1 发送预先保存的与 UICC ID 对应的 UICC 证书, 所述 UICC 证书中携带有 UICC ID 和 UICC 公钥, 执行步骤 505。

步骤 504: UICC 管理平台向用户发送错误提示信息, 结束通用集成电路卡的开通流程。

步骤 505: 当 MNO1 对 UICC 证书验证通过时, 根据预设方法生成与 UICC ID 对应的第一业务密钥 AUICCkey1, 使用 UICC 公钥 PubUICCkey 对 AUICCkey1 进行加密, 获得加密后的第一业务密钥 [AUICCkey1]PubUICCkey。

步骤 506: MNO1 将加密后的第一业务密钥 [AUICCkey1]PubUICCkey 发送给 UICC 管理平台。

步骤 507: UICC 管理平台将加密后的第一业务密钥 [AUICCkey1]PubUICCkey 转发给与 UICC ID 对应的 UICC。

步骤 508: UICC 使用预先保存的与 UICC 公钥 PubUICCkey 对应的 UICC 私钥 PriUICCkey 对加密后的第一业务密钥 [AUICCkey1]PubUICCkey 进行解密, 得到第一业务密钥 AUICCkey1。

步骤 509: UICC 在获取到 AUICCkey1 之后向 UICC 管理平台返回业务开通执行响应, 所述业务开通执行响应中携带有 UICC 预先保存的 UICC ID。

步骤 510: UICC 管理平台将与 UICC ID 对应的 UICC 标记为已被激活。

步骤 511: UICC 管理平台将业务开通执行响应发送给 MNO1。

步骤 512: MNO1 和 UICC 使用第一业务密钥 AUICCkey1 进行业务交互。

通过上述对两个开通通用集成电路卡的实施例的描述可知, UICC 管理平台根据业务开通请求中携带的 UICC 标识和第一运营商设备标识, 获取第一运营商设备生成的与 UICC 标识对应的加密后的第一业务密钥, UICC 在获取到所述加密后的第一业务密钥之后使用预先保存的 UICC 私钥对加密后的第一业务密钥进行解密, 使用解密后得到的第一业务密钥与第一运营商设备进行业务交互。由于用户发送的业务开通请求中携带有第一运营商设备标识, UICC 管理平台根据所述第一运营商设备标识为通用集成电路卡开通与第一运营商设备标识对应的第一运营商设备之间的业务交互, 因此运营商能够灵活地对通用集成电路卡中的运营商数据进行动态配置, 无需 M2M 终端在生产过程中需要根据运营商进行定制开发, 因此本发明提出的通用集成电路卡的数据配置方法、设备及系统, 解决了现有技术中 M2M 终端只能和预定的

运营商进行通信的技术问题，扩大了 M2M 终端的使用范围。

图 6 为本发明开通通用集成电路卡的第二实现流程图。如图 6 所示，包括如下所述的步骤：

步骤 601：接收业务开通请求，所述业务开通请求中携带有通用集成电路卡 UICC 标识和第一运营商设备标识。

在本步骤中，UICC 管理平台接收业务开通请求消息，所述业务开通请求消息中携带有 UICC 标识和第一运营商设备标识。

进一步的，UICC 管理平台可以采用如下两种方式接收业务开通请求：

第一种方式，用户申请归属的第一运营商设备 MNO1 接收用户提交业务申请请求，所述业务申请请求中携带有 UICC 标识；第一运营商设备向 UICC 管理平台发送业务开通请求，所述业务开通请求中携带有 UICC 标识和第一运营商设备预先保存的第一运营商设备标识。

例如，用户在购买 UICC 时，即可获得与所述 UICC 对应的 UICC 标识，当用户向第一运营商设备申请开通 UICC 时，向第一运营商设备提交业务申请请求，所述业务申请请求中携带有所述 UICC 标识。

第二种方式，UICC 管理平台直接接收用户提交的业务开通请求，所述业务开通请求消息中携带有 UICC 标识和第一运营商设备标识。

步骤 602：向与第一运营商设备标识对应的第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

在本步骤中，UICC 管理平台向与第一运营商设备标识对应的第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

较佳地，在本发明的具体实施例中，在 UICC 管理平台向第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书之前，UICC 管理平台可以查询与 UICC 标识对应的 UICC 是否被激活，若未被激活，则向第一运营商设备发送预先保存的与 UICC 标识对应的 UICC 证书；若已被激活，则向第一运营商设备发送错误提示信息。

步骤 603：接收第一运营商设备发送的与 UICC 标识对应的加密后的第一

业务密钥，并将加密后的第一业务密钥发送给与 UICC 标识对应的 UICC。

在本步骤中，UICC 管理平台接收第一运营商设备发送的与 UICC 标识对应的加密后的第一业务密钥，并将加密后的第一业务密钥发送给与 UICC 标识对应的 UICC。

图 7 为本发明开通通用集成电路卡的第三实现流程图。如图 7 所示，包括如下所述的步骤：

步骤 701：接收 UICC 管理平台发送的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

在本步骤中，第一运营商设备接收 UICC 管理平台发送的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

较佳的，在本发明的具体实施例中，第一运营商设备可以接收用户提交业务申请请求，所述业务申请请求中携带有 UICC 标识；第一运营商设备向 UICC 管理平台发送业务开通请求，所述业务开通请求中携带有 UICC 标识和第一运营商设备预先保存的第一运营商设备标识。

步骤 702：当对 UICC 证书验证通过时，根据预设方法生成与 UICC 标识对应的第一业务密钥，使用 UICC 公钥对第一业务密钥进行加密，并通过 UICC 管理平台将加密后的第一业务密钥发送给与 UICC 标识对应的 UICC。

在本步骤中，第一运营商设备在接收到 UICC 管理平台发送的与 UICC 标识对应的 UICC 证书之后，对接收到的 UICC 证书进行验证，当第一运营商设备对 UICC 证书验证通过时，根据现有技术中的密钥生成方法生成与 UICC 标识对应的第一业务密钥，使用 UICC 公钥对第一业务密钥进行加密，第一运营商设备将加密后的第一业务密钥发送给 UICC 管理平台，UICC 管理平台将接收到的加密后的第一业务密钥转发给与 UICC 标识对应的 UICC。

步骤 703：获取 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应，所述业务开通执行响应中携带有 UICC 预先保存的 UICC 标识。

在本步骤中，第一运营商设备获取 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应，所述业务开通执行响应中携带有 UICC 预先保存的 UICC 标识。

步骤 704：使用第一业务密钥和 UICC 进行业务交互。

在本步骤中，第一运营商设备使用第一业务密钥和 UICC 进行业务交互。

图 8 为本发明开通通用集成电路卡的第四实现流程图。如图 8 所示，包括如下所述的步骤：

步骤 801：接收 UICC 管理平台发送的加密后的第一业务密钥。

在本步骤中，UICC 接收 UICC 管理平台发送的加密后的第一业务密钥。

步骤 802：使用预先保存的与 UICC 公钥对应的 UICC 私钥对加密后的第一业务密钥进行解密，获取第一业务密钥。

在本步骤中，UICC 在接收到 UICC 管理平台发送的加密后的第一业务密钥之后，使用预先保存的 UICC 私钥对加密后的第一业务密钥进行解密，获取第一业务密钥。

步骤 803：向第一运营商设备发送的业务开通执行响应，所述业务开通执行响应中携带有预先保存的 UICC 标识。

在本步骤中，UICC 在获取到第一业务密钥之后，向 UICC 管理平台返回业务开通执行响应，所述业务开通执行响应中携带有 UICC 预先保存的 UICC 标识，UICC 管理平台在接收到 UICC 发送的业务开通执行响应之后，将与 UICC 标识对应的 UICC 标记为已被激活，并将业务开通执行响应发送给第一运营商设备。

步骤 804：使用第一业务密钥和第一运营商设备进行业务交互。

在本步骤中，UICC 使用第一业务密钥和第一运营商设备进行业务交互。

进一步的，在本发明的具体实施例中，在第一运营商设备和 UICC 使用所述第一业务密钥进行业务交互之后，还可以包括终止通用集成电路卡的实现流程，图 9 为本发明终止通用集成电路卡的第一实现流程图。如图 9 所示，包括如下所述的步骤：

步骤 901：UICC 管理平台接收第一运营商设备发送的业务终止请求，所述业务终止请求中携带有 UICC 标识和第一运营商设备根据第一业务密钥生成的第一报文鉴别码。

较佳地，UICC 管理平台在接收到第一运营商设备发送的业务终止请求之后，查询与 UICC 标识对应的 UICC 是否被激活，若已被激活，则将业务终止请求发送给与 UICC 标识对应的 UICC，否则，向第一运营商设备发送

错误提示信息。

此外, UICC 管理平台还可以在接收到第一运营商设备发送的业务终止请求之前, 接收用户提交的业务取消请求, 所述业务取消请求中携带有 UICC 标识, UICC 管理平台查询与 UICC 标识对应的 UICC 是否被激活, 若已被激活, 则向第一运营商设备转发业务取消请求, 否则, 向用户发送错误提示信息。

步骤 902: UICC 管理平台将业务终止请求发送给与 UICC 标识对应的 UICC。

在本步骤中, 当与 UICC 标识对应的 UICC 已被激活时, UICC 管理平台将业务终止请求发送给与 UICC 标识对应的 UICC。

步骤 903: 当 UICC 对第一报文鉴别码校验通过时, 终止与第一运营商设备进行业务交互。

在本步骤中, UICC 可以按照现有技术中的报文鉴别码的校验方法对接收到的第一报文鉴别码进行校验, 当 UICC 对第一报文鉴别码校验通过时, 终止与第一运营商设备进行业务交互。

步骤 904: 第一运营商设备获取 UICC 在终止与第一运营商设备进行业务交互之后发送的业务终止执行响应, 所述业务终止执行响应中携带有 UICC 标识。

较佳地, 在本步骤中, 当 UICC 终止与第一运营商设备进行业务交互之后, 向 UICC 管理平台发送业务终止执行响应, 所述业务终止执行响应中携带有 UICC 标识。UICC 管理平台在接收到 UICC 发送的业务终止执行响应之后, 将与 UICC 标识对应的 UICC 标记为未被激活, 并将业务终止执行响应发送给第一运营商设备。

通过上述对步骤 901~904 的描述可知, 能够实现终止通用集成电路卡与第一运营商设备之间的业务交互。下面结合出两个具体的实施例对通用集成电路卡的终止流程进行详细描述:

图 10 为本发明终止通用集成电路卡的第一实施例的实现流程图。如图 10 所示, 包括如下所述的步骤:

步骤 1001: MNO1 接收用户提交的业务取消请求, 所述业务取消请求中

携带有 UICC ID。

步骤 1002: MNO1 根据第一业务密钥生成与 UICC ID 对应的第一报文鉴别码, 向 UICC 管理平台发送业务终止请求, 所述业务终止请求中携带有 UICC ID 和第一报文鉴别码。

在本步骤中, MNO1 可以按照现有技术中的报文鉴别码的生成方法, 根据第一业务密钥生成的与 UICC ID 对应的第一报文鉴别码。

步骤 1003: UICC 管理平台查询与 UICC ID 对应的 UICC 是否被激活, 若未被激活, 执行步骤 1004, 否则, 执行步骤 1005。

步骤 1004: UICC 管理平台向 MNO1 返回错误提示信息, 结束终止通用集成电路卡的流程。

步骤 1005: UICC 管理平台将业务终止请求发送给与 UICC ID 对应的 UICC。

步骤 1006: 当 UICC 对第一报文鉴别码校验通过时, 终止与 MNO1 进行业务交互。

步骤 1007: UICC 在终止与 MNO1 进行业务交互之后向 UICC 管理平台发送业务终止执行响应, 所述业务终止执行响应中携带有 UICC ID。

步骤 1008: UICC 管理平台将与 UICC ID 对应的 UICC 标记为未被激活。

步骤 1009: UICC 管理平台将业务终止执行响应发送给 MNO1。

图 11 为本发明终止通用集成电路卡的第二实施例的实现流程图。如图 11 所示, 包括如下所述的步骤:

步骤 1101: UICC 管理平台接收用户提交的业务取消请求, 所述业务取消请求中携带有 UICC ID。

步骤 1102: UICC 管理平台查询与 UICC ID 对应的 UICC 是否被激活, 若未被激活, 执行步骤 1103, 否则, 执行步骤 1104。

步骤 1103: UICC 管理平台向用户返回错误提示信息, 结束终止通用集成电路卡的流程。

步骤 1104: UICC 管理平台将业务取消请求转发给 MNO1。

步骤 1105: MNO1 根据第一业务密钥生成的与 UICC ID 对应的第一报文鉴别码, 向 UICC 管理平台发送业务终止请求, 所述业务终止请求中携带有

UICC ID 和第一报文鉴别码。

步骤 1106: UICC 管理平台将业务终止请求发送给与 UICC ID 对应的 UICC。

步骤 1107: 当 UICC 对第一报文鉴别码校验通过时, 终止与 MNO1 进行业务交互。

步骤 1108: UICC 在终止与 MNO1 进行业务交互之后向 UICC 管理平台发送业务终止执行响应, 所述业务终止执行响应中携带有 UICC ID。

步骤 1109: UICC 管理平台将与 UICC ID 对应的 UICC 标记为未被激活。

步骤 1110: UICC 管理平台将业务终止执行响应发送给 MNO1。

通过上述对两个终止通用集成电路卡的实施例的描述可知, UICC 管理平台根据业务终止请求中携带的 UICC 标识和第一运营商设备标识, 终止通用集成电路卡与第一运营商设备标识对应的第一运营商设备之间的业务交互。

图 12 为本发明终止通用集成电路卡的第二实现流程图。如图 12 所示, 包括如下所述的步骤:

步骤 1201: 接收第一运营商设备发送的业务终止请求, 所述业务终止请求中携带有 UICC 标识和第一运营商设备根据第一业务密钥生成的第一报文鉴别码。

在本步骤中, UICC 管理平台接收第一运营商设备发送的业务终止请求, 所述业务终止请求中携带有 UICC 标识和第一运营商设备根据第一业务密钥生成的第一报文鉴别码。

较佳地, UICC 管理平台在接收到第一运营商设备发送的业务终止请求之后, 查询与 UICC 标识对应的 UICC 是否被激活, 若已被激活, 则将业务终止请求发送给与所述 UICC 标识对应的 UICC, 否则, 向第一运营商设备发送错误提示信息。

此外, UICC 管理平台还可以在接收到第一运营商设备发送的业务终止请求之前, 接收用户提交的业务取消请求, 所述业务取消请求中携带有 UICC 标识, UICC 管理平台查询与 UICC 标识对应的 UICC 是否被激活, 若已被激活, 则向第一运营商设备转发业务取消请求, 否则, 向用户发送错误提示信息。

步骤 1202：将业务终止请求发送给与 UICC 标识对应的 UICC。

在本步骤中，UICC 管理平台将业务终止请求发送给与 UICC 标识对应的 UICC。

进一步的，UICC 管理平台接收 UICC 在终止与第一运营商设备进行业务交互之后发送的业务终止执行响应，所述业务终止执行响应中携带有 UICC 标识，UICC 管理平台在接收到 UICC 发送的业务终止执行响应之后，将与 UICC 标识对应的 UICC 标记为未被激活，并将业务终止执行响应发送给第一运营商设备。

图 13 为本发明终止通用集成电路卡的第三实现流程图。如图 13 所示，包括如下所述的步骤：

步骤 1301：向 UICC 管理平台发送业务终止请求，所述业务终止请求中携带有 UICC 标识和根据第一业务密钥生成的第一报文鉴别码。

在本步骤中，第一运营商设备向 UICC 管理平台发送业务终止请求，所述业务终止请求中携带有 UICC 标识和第一运营商设备根据第一业务密钥生成的第一报文鉴别码。

步骤 1302：获取 UICC 发送的业务终止执行响应，所述业务终止执行响应中携带有 UICC 标识。

在本步骤中，第一运营商设备获取 UICC 在终止与第一运营商设备进行业务交互之后发送的业务终止执行响应，所述业务终止执行响应中携带有 UICC 标识。

图 14 为本发明终止通用集成电路卡的第四实现流程图。如图 14 所示，包括如下所述的步骤：

步骤 1401：接收 UICC 管理平台发送的业务终止请求，所述业务终止请求中携带有 UICC 标识和第一运营商设备根据第一业务密钥生成的第一报文鉴别码。

在本步骤中，UICC 接收 UICC 管理平台发送的业务终止请求，所述业务终止请求中携带有 UICC 标识和第一运营商设备根据第一业务密钥生成的第一报文鉴别码。

步骤 1402：当对第一报文鉴别码校验通过时，终止与第一运营商设备进

行业务交互。

在本步骤中, UICC 可以按照现有技术中的报文鉴别码的校验方法对接收到的第一报文鉴别码进行校验, 当 UICC 对第一报文鉴别码校验通过时, 终止与第一运营商设备进行业务交互。

步骤 1403: 向第一运营商设备发送业务终止执行响应, 所述业务终止执行响应中携带有 UICC 标识。

在本步骤中, 当 UICC 终止与第一运营商设备进行业务交互之后, 向 UICC 管理平台发送业务终止执行响应, 所述业务终止执行响应中携带有 UICC 标识。UICC 管理平台在接收到 UICC 发送的业务终止执行响应之后, 将与 UICC 标识对应的 UICC 标记为未被激活, 并将业务终止执行响应发送给第一运营商设备。

进一步的, 在本发明的具体实施例中, 在第一运营商设备和 UICC 使用所述第一业务密钥进行业务交互之后, 还可以包括通用集成电路卡切换运营商的实现流程, 图 15 为本发明通用集成电路卡切换运营商的第一实现流程图。如图 15 所示, 包括如下所述的步骤:

步骤 1501: UICC 管理平台接收运营商切换请求, 所述运营商切换请求中携带有 UICC 标识和第二运营商设备标识。

在本步骤中, UICC 管理平台可以采用如下两种方式接收运营商切换请求:

第一种方式, 用户申请切换至的第二运营商设备 MNO2 接收用户提交的运营商切换申请, 所述运营商切换申请中携带有 UICC 标识; 第二运营商设备向 UICC 管理平台发送业务切换请求, 所述业务切换请求中携带有 UICC 标识和第二运营商设备预先保存的第二运营商设备标识。

第二种方式, UICC 管理平台直接接收用户提交的运营商切换请求, 所述运营商切换请求中携带有 UICC 标识和第二运营商设备标识。

步骤 1502: 当第一运营商设备允许与 UICC 标识对应的 UICC 切换运营商设备时, UICC 管理平台向与第二运营商设备标识对应的第二运营商设备发送 UICC 证书, 所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

在本步骤中, UICC 管理平台根据 UICC 标识, 查询与 UICC 标识对应的

UICC 当前归属的运营商设备标识, UICC 管理平台向与 UICC 标识对应的 UICC 当前归属的第一运营商设备转发运营商切换申请, 第一运营商设备向 UICC 管理平台返回运营商切换响应, UICC 管理平台在接收到第一运营商设备发送的允许与 UICC 标识对应的 UICC 切换运营商的运营商切换响应之后, 向与第二运营商设备标识对应的第二运营商设备发送 UICC 证书, 所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

步骤 1503: 当第二运营商设备对 UICC 证书验证通过时, 根据预设方法生成与 UICC 标识对应的第二业务密钥, 使用 UICC 公钥对第二业务密钥进行加密, 将与 UICC 标识对应的加密后的第二业务密钥发送给 UICC 管理平台。

在本步骤中, 第二运营商设备在接收到 UICC 管理平台发送的与 UICC 标识对应的 UICC 证书之后, 对接收到的 UICC 证书进行验证, 当第二运营商设备对 UICC 证书验证通过时, 根据现有技术中的密钥生成方法生成与 UICC 标识对应的第二业务密钥, 使用 UICC 公钥对第二业务密钥进行加密, 第二运营商设备将与 UICC 标识对应的加密后的第二业务密钥发送给 UICC 管理平台。

步骤 1504: UICC 管理平台将与 UICC 标识对应的加密后的第二业务密钥发送给第一运营商设备, 接收第一运营商设备根据加密后的第二业务密钥生成的与 UICC 标识对应的第二报文鉴别码。

在本步骤中, UICC 管理平台在接收到第二运营商设备发送的与 UICC 标识对应的加密后的第二业务密钥之后, 将所述加密后的第二业务密钥发送给第一运营商设备, 第一运营商设备根据所述加密后的第二业务密钥生成与 UICC 标识对应的第二报文鉴别码, 将第二报文鉴别码发送给 UICC 管理平台。

步骤 1505: UICC 管理平台将加密后的第二业务密钥和第二报文鉴别码发送给与 UICC 标识对应的 UICC。

步骤 1506: 当 UICC 对第二报文鉴别码校验通过时, 使用 UICC 私钥对加密后的第二业务密钥进行解密, 获取第二业务密钥。

步骤 1507: 第二运营商设备获取 UICC 在获取到第二业务密钥之后发送的运营商切换执行响应, 所述运营商切换执行响应中携带有 UICC 标识。

步骤 1508: 第二运营商设备与 UICC 使用第二业务密钥进行业务交互。

通过上述对步骤 1501~1508 的描述可知, 能够实现通用集成电路卡从第一运营商设备切换到第二运营商设备。下面结合出两个具体的实施例对通用集成电路卡切换运营商的流程进行详细描述:

图 16 为本发明通用集成电路卡切换运营商的第一实施例的实现流程图。如图 16 所示, 包括如下所述的步骤:

步骤 1601: 第二运营商设备 MNO2 接收用户提交的运营商切换申请, 所述运营商切换申请中携带有 UICC ID。

步骤 1602: MNO2 向 UICC 管理平台转发运营商切换请求, 所述运营商切换申请中携带有 UICC ID 和第二运营商标识。

步骤 1603: UICC 管理平台查询与 UICC ID 对应的 UICC 当前归属的运营商设备标识。

步骤 1604: UICC 管理平台向与 UICC ID 对应的 UICC 当前归属的运营商设备 MNO1 转发运营商切换申请。

步骤 1605: MNO1 向 UICC 管理平台返回运营商切换响应。

在本步骤中, 所述运营商切换响应中可以携带 MNO1 允许与 UICC 标识对应的 UICC 切换运营商设备的信息, 也可以携带 MNO1 不允许与 UICC 标识对应的 UICC 切换运营商设备的信息。

步骤 1606: 当 MNO1 允许与 UICC ID 对应的 UICC 切换运营商设备时, UICC 管理平台向 MNO2 发送预先保存的与 UICC ID 对应的 UICC 证书, 所述 UICC 证书中携带有 UICC ID 和 UICC 公钥 PubUICCkey。

步骤 1607: 当 MNO2 对 UICC 证书验证通过时, 根据预设方法生成与 UICC ID 对应的第二业务密钥 AUICCkey2, 并使用 PubUICCkey 对 AUICCkey2 进行加密。

步骤 1608: MNO2 向 UICC 管理平台发送与 UICC ID 对应的加密后的第二业务密钥[AUICCkey2]PubUICCkey。

步骤 1609: UICC 管理平台将[AUICCkey2]PubUICCkey 发送给 MNO1。

步骤 1610: MNO1 根据[AUICCkey2]PubUICCkey 生成第二报文鉴别码。

步骤 1611: MNO1 将第二报文鉴别码发送给 UICC 管理平台。

步骤 1612: UICC 管理平台向与 UICC ID 对应的 UICC 发送 [AUICCkey2]PubUICCkey 和第二报文鉴别码。

步骤 1613: 当 UICC 对第二报文鉴别码校验通过时, 使用 UICC 私钥 PriUICCkey 对 [AUICCkey2]PubUICCkey 进行解密, 获得第二业务密钥 AUICCkey2。

步骤 1614: UICC 在获取到 AUICCkey2 之后向 UICC 管理平台返回运营商切换执行响应, 所述运营商切换执行响应中携带有 UICC ID。

步骤 1615: UICC 管理平台将该 UICC 当前归属的运营商设备修改为 MNO2。

步骤 1616: UICC 管理平台向 MNO1 返回运营商切换执行响应;

步骤 1617: UICC 管理平台向 MNO2 返回运营商切换执行响应。

步骤 1618: MNO2 与 UICC 使用第二业务密钥 AUICCkey2 进行业务交互。

图 17 为本发明通用集成电路卡切换运营商的第二实施例的实现流程图。如图 17 所示, 包括如下所述的步骤:

步骤 1701: UICC 管理平台接收用户提交的运营商切换请求, 所述运营商切换请求中携带有 UICC ID 和第二运营商设备标识。

步骤 1702: UICC 管理平台查询与 UICC ID 对应的 UICC 当前归属的运营商设备标识。

步骤 1703: UICC 管理平台向与 UICC ID 对应的 UICC 当前归属的运营商设备 MNO1 转发所述运营商切换申请。

步骤 1704: MNO1 向 UICC 管理平台返回运营商切换响应。

步骤 1705: 当 MNO1 允许与 UICC 标识对应的 UICC 切换运营商设备时, UICC 管理平台向 MNO2 发送预先保存的与 UICC ID 对应的 UICC 证书, 所述 UICC 证书中携带有 UICC ID 和 UICC 公钥 PubUICCkey。

步骤 1706: 当 MNO2 对 UICC 证书验证通过时, 根据预设方法生成与 UICC ID 对应的第二业务密钥 AUICCkey2, 并使用 PubUICCkey 对 AUICCkey2 进行加密。

步骤 1707: MNO2 向 UICC 管理平台发送与 UICC ID 对应的加密后的第二业务密钥 [AUICCkey2]PubUICCkey。

步骤 1708: UICC 管理平台将[AUICCkey2]PubUICCkey 发送给 MNO1。

步骤 1709: MNO1 根据[AUICCkey2]PubUICCkey 生成第二报文鉴别码。

步骤 1710: MNO1 将第二报文鉴别码发送给 UICC 管理平台。

步骤 1711: UICC 管理平台向与 UICC ID 对应的 UICC 发送 [AUICCkey2]PubUICCkey 和第二报文鉴别码。

步骤 1712: 当 UICC 对第二报文鉴别码校验通过时, 使用 UICC 私钥 PriUICCkey 对[AUICCkey2]PubUICCkey 进行解密, 获得第二业务密钥 AUICCkey2。

步骤 1713: UICC 在获取到 AUICCkey2 之后向 UICC 管理平台返回运营商切换执行响应, 所述运营商切换执行响应中携带有 UICC ID。

步骤 1714: UICC 管理平台将该 UICC 当前归属的运营商设备修改为 MNO2。

步骤 1715: UICC 管理平台向 MNO1 返回运营商切换执行响应;

步骤 1716: UICC 管理平台向 MNO2 返回运营商切换执行响应。

步骤 1717: MNO2 与 UICC 使用第二业务密钥 AUICCkey2 进行业务交互。

图 18 为本发明通用集成电路卡切换运营商的第二实现流程图。如图 18 所示, 包括如下所述的步骤:

步骤 1801: 接收运营商切换请求, 所述运营商切换请求中携带有 UICC 标识和第二运营商设备标识。

在本步骤中, UICC 管理平台接收运营商切换请求, 所述运营商切换请求中携带有 UICC 标识和第二运营商设备标识。

进一步的, UICC 管理平台可以采用如下两种方式接收运营商切换请求:

第一种方式, 用户申请切换至的第二运营商设备 MNO2 接收用户提交的运营商切换申请, 所述运营商切换申请中携带有 UICC 标识; 第二运营商设备向 UICC 管理平台发送业务切换请求, 所述业务切换请求中携带有 UICC 标识和第二运营商设备预先保存的第二运营商设备标识。

第二种方式, UICC 管理平台直接接收用户提交的运营商切换请求, 所述运营商切换请求中携带有 UICC 标识和第二运营商设备标识。

步骤 1802: 当第一运营商设备允许与 UICC 标识对应的 UICC 切换运营

商设备时,向与第二运营商设备标识对应的第二运营商设备发送 UICC 证书,所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

在本步骤中,当第一运营商设备允许与 UICC 标识对应的 UICC 切换运营商设备时,UICC 管理平台向与第二运营商设备标识对应的第二运营商设备发送 UICC 证书,所述 UICC 证书中携带有 UICC 标识和 UICC 公钥。

步骤 1803:接收第二运营商设备发送的与 UICC 标识对应的加密后的第二业务密钥,并将与所述 UICC 标识对应的加密后的第二业务密钥发送给所述第一运营商设备。

在本步骤中,UICC 管理平台接收第二运营商设备发送的与 UICC 标识对应的加密后的第二业务密钥,并将加密后的第二业务密钥发送给第一运营商设备。第一运营商设备根据加密后的第二业务密钥生成与 UICC 标识对应的第二报文鉴别码,将第二报文鉴别码发送给 UICC 管理平台。

步骤 1804:接收第一运营商设备根据加密后的第二业务密钥生成的与 UICC 标识对应的第二报文鉴别码。

在本步骤中,UICC 管理平台接收第一运营商设备根据加密后的第二业务密钥生成的与 UICC 标识对应的第二报文鉴别码。

步骤 1805:将加密后的第二业务密钥和第二报文鉴别码发送给与 UICC 标识对应的 UICC。

在本步骤中,UICC 管理平台将加密后的第二业务密钥和第二报文鉴别码发送给与 UICC 标识对应的 UICC。

图 19 为本发明通用集成电路卡切换运营商的第三实现流程图。如图 19 所示,包括如下所述的步骤:

步骤 1901:接收 UICC 管理平台发送的与 UICC 标识对应的加密后的第二业务密钥。

在本步骤中,第一运营商设备接收 UICC 管理平台发送的与 UICC 标识对应的加密后的第二业务密钥。

步骤 1902:向 UICC 管理平台发送根据加密后的第二业务密钥生成的与 UICC 标识对应的第二报文鉴别码。

在本步骤中,第一运营商设备向 UICC 管理平台发送根据加密后的第二

业务密钥生成的与 UICC 标识对应的第二报文鉴别码。

图 20 为本发明通用集成电路卡切换运营商的第四实现流程图。如图 20 所示，包括如下所述的步骤：

步骤 2001：接收 UICC 管理平台发送的加密后的第二业务密钥和第二报文鉴别码。

在本步骤中，UICC 接收 UICC 管理平台发送的加密后的第二业务密钥和第二报文鉴别码。

步骤 2002：当对第二报文鉴别码校验通过时，使用 UICC 私钥对加密后的第二业务密钥进行解密，获取第二业务密钥。

在本步骤中，当 UICC 当对第二报文鉴别码校验通过时，使用 UICC 私钥对加密后的第二业务密钥进行解密，获取第二业务密钥。

步骤 2003：向第二运营商设备发送运营商切换执行响应，所述运营商切换执行响应中携带有 UICC 标识。

在本步骤中，UICC 在获取到第二业务密钥之后，向第二运营商设备发送运营商切换执行响应，所述运营商切换执行响应中携带有 UICC 标识。

步骤 2004：使用第二业务密钥和第二运营商设备进行业务交互。

在本步骤中，UICC 使用第二业务密钥和第二运营商设备进行业务交互。

本发明提出的通用集成电路卡的数据配置方法，UICC 管理平台根据业务开通请求中携带的 UICC 标识和第一运营商设备标识，获取第一运营商设备生成的与 UICC 标识对应的加密后的第一业务密钥，UICC 在获取到所述加密后的第一业务密钥之后使用预先保存的 UICC 私钥对加密后的第一业务密钥进行解密，使用解密后得到的第一业务密钥与第一运营商设备进行业务交互。由于用户发送的业务开通请求中携带有第一运营商设备标识，UICC 管理平台根据所述第一运营商设备标识为通用集成电路卡开通与第一运营商设备标识对应的第一运营商设备之间的业务交互，因此运营商能够灵活地对通用集成电路卡中的运营商数据进行动态配置，无需 M2M 终端在生产过程中需要根据运营商进行定制开发，因此本发明提出的通用集成电路卡的数据配置方法，解决了现有技术中 M2M 终端只能和预定的运营商进行通信的技术问题，扩大了 M2M 终端的使用范围；另外，本发明所述方法实现起来简单方便，便

于普及。

图 21 为本发明通用集成电路卡管理平台的结构示意图。如图 21 所示，包括：第一接收单元 2101 和第一发送单元 2102；

所述第一接收单元 2101，用于接收业务开通请求，所述业务开通请求中携带有通用集成电路卡 UICC 标识和第一运营商设备标识，将所述业务开通请求发送给所述第一发送单元 2102；

所述第一发送单元 2102，用于向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和 UICC 公钥；

所述第一接收单元 2101，还用于接收所述第一运营商设备发送的与所述 UICC 标识对应的加密后的第一业务密钥，将所述加密后的第一业务密钥发送给所述第一发送单元 2102。

所述第一发送单元 2102，还用于将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC。

进一步的，所述第一接收单元 2101，具体用于接收所述第一运营商设备发送的所述业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备预先保存的所述第一运营商设备标识；

或者，接收用户发送的业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备标识。

进一步的，所述通用集成电路卡管理平台还包括：查询单元 2103；

所述查询单元 2103，用于查询与所述 UICC 标识对应的 UICC 是否被激活，若未被激活，则向所述第一运营商设备发送所述 UICC 证书，否则，向所述第一运营商设备发送错误提示信息。

进一步的，所述通用集成电路卡管理平台还包括：标记单元 2104；

所述第一接收单元 2101，还用于接收所述 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应，所述业务开通响应中携带有所述 UICC 标识，将所述业务开通执行响应发送给所述标记单元 2104 和所述第一发送单元 2102；

所述标记单元 2104，用于将与所述 UICC 标识对应的 UICC 标记为已被

激活；

所述第一发送单元 2102，还用于将所述业务开通执行响应发送给所述第一运营商设备。

进一步的，所述通用集成电路卡管理平台还包括：第一存储单元 2105；

所述第一接收单元 2101，还用于接收 UICC 厂商设备发送的 UICC 卡片信息，所述 UICC 卡片信息中携带有所述 UICC 标识和所述 UICC 公钥，将所述 UICC 卡片信息发送给所述第一发送单元 2102；

所述第一发送单元 2102，还用于将所述 UICC 卡片信息发送给认证中心；

所述第一接收单元 2101，还用于当所述认证中心对所述 UICC 卡片信息认证通过时，接收所述认证中心返回的所述 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥，将所述 UICC 证书发送给所述第一存储单元 2105；

所述第一存储单元 2105，用于保存与所述 UICC 标识对应的所述 UICC 证书。

进一步的，所述第一接收单元 2101，还用于接收所述第一运营商设备发送的业务终止请求，所述业务终止请求中携带有所述 UICC 标识和与所述第一运营商设备根据所述第一业务密钥生成的第一报文鉴别码，将所述业务终止请求发送给所述第一发送单元 2102；

所述第一发送单元 2102，还用于将所述业务终止请求发送给与所述 UICC 标识对应的 UICC。

进一步的，所述查询单元 2103，还用于查询与所述 UICC 标识对应的 UICC 是否被激活，若已被激活，则将所述业务终止请求发送给与所述 UICC 标识对应的 UICC，否则，向所述第一运营商设备发送错误提示信息。

进一步的，所述第一接收单元 2101，还用于接收用户提交的业务取消请求，所述业务取消请求中携带有所述 UICC 标识，将所述业务取消请求发送给所述查询单元 2103；

所述查询单元 2103，还用于查询与所述 UICC 标识对应的 UICC 是否被激活，若已被激活，则向所述第一运营商设备转发所述业务取消请求，否则，向所述用户发送错误提示信息。

进一步的,所述第一接收单元 2101,还用于接收所述 UICC 在终止与所述第一运营商设备进行业务交互之后发送的所述业务终止执行响应,所述业务终止执行响应中携带有所述 UICC 标识,将所述业务终止执行响应发送给所述标记单元 2104 和所述第一发送单元 2102;

所述标记单元 2104,还用于将与所述 UICC 标识对应的 UICC 标记为未被激活;

所述第一发送单元 2102,还用于将所述业务终止执行响应发送给所述第一运营商设备。

进一步的,所述第一接收单元 2101,还用于接收运营商切换请求,所述运营商切换请求中携带有所述 UICC 标识和第二运营商设备标识,将所述运营商切换请求发送给所述第一发送单元 2102;

所述第一发送单元 2102,还用于当所述第一运营商设备允许与所述 UICC 标识对应的 UICC 切换运营商设备时,向与所述第二运营商设备标识对应的第二运营商设备发送所述 UICC 证书,所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥;

所述第一接收单元 2101,还用于接收所述第二运营商设备发送的与所述 UICC 标识对应的加密后的第二业务密钥,将所述加密后的第二业务密钥发送给所述第一发送单元 2102;

所述第一发送单元 2102,还用于将所述加密后的第二业务密钥发送给所述第一运营商设备;

所述第一接收单元 2101,还用于接收所述第一运营商设备根据所述加密后的第二业务密钥生成的与所述 UICC 标识对应的第二报文鉴别码,将所述第二报文鉴别码发送给所述第一发送单元 2102;

所述第一发送单元 2102,还用于将所述加密后的第二业务密钥和所述第二报文鉴别码发送给与所述 UICC 标识对应的 UICC。

进一步的,所述第一接收单元 2101,具体用于接收所述第二运营商设备发送的所述运营商切换请求,所述运营商切换请求中携带有所述 UICC 标识和所述第二运营商设备标识;

或者,接收用户提交的所述运营商切换请求,所述运营商切换请求中携

带有所述 UICC 标识和所述第二运营商设备标识。

图 22 为本发明第一运营商设备的结构示意图。如图 22 所示，包括：第二接收单元 2201、业务密钥生成单元 2202、第二发送单元 2203 和第一业务交互单元 2204；

所述第二接收单元 2201，用于接收通用集成电路卡 UICC 管理平台发送的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥，将所述 UICC 证书发送给所述业务密钥生成单元 2202；

所述业务密钥生成单元 2202，用于当第一运营商设备对所述 UICC 证书验证通过时，根据预设方法生成与所述 UICC 标识对应的第一业务密钥，使用所述 UICC 公钥对所述第一业务密钥进行加密，将所述第一业务密钥发送给第一业务交互单元 2204，将加密后的第一业务密钥发送给所述第二发送单元 2203；

所述第二发送单元 2203，用于将加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC；

所述第二接收单元 2201，还用于获取所述 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应，所述业务开通执行响应中携带有所述 UICC 预先保存的所述 UICC 标识；

所述第一业务交互单元 2204，用于使用所述第一业务密钥和所述 UICC 进行业务交互。

进一步的，所述第二接收单元 2201，还用于接收用户提交的业务申请请求，所述业务申请请求中携带有所述 UICC 标识，将所述业务申请请求发送给所述第二发送单元 2203；

所述第二发送单元 2203，还用于向所述 UICC 管理平台发送所述业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备预先保存的所述第一运营商设备标识。

进一步的，所述第二发送单元 2203，还用于向所述 UICC 管理平台发送业务终止请求，所述业务终止请求中携带有所述 UICC 标识和所述第一运营商设备根据所述第一业务密钥生成的第一报文鉴别码；

所述第二接收单元 2201，还用于获取所述 UICC 在终止与所述第一运营

商设备进行业务交互之后发送的业务终止执行响应，所述业务终止执行响应中携带有所述 UICC 标识。

进一步的，所述第二接收单元 2201，还用于接收所述 UICC 管理平台发送的与所述 UICC 标识对应的加密后的第二业务密钥；

所述第二发送单元 2203，还用于向所述 UICC 管理平台发送根据所述加密后的第二业务密钥生成的与所述 UICC 标识对应的第二报文鉴别码。

图 23 为本发明通用集成电路卡的结构示意图。如图 23 所示，包括：第三接收单元 2301、解密单元 2302、第三发送单元 2303 和第二业务交互单元 2304；

所述第三接收单元 2301，用于接收通用集成电路卡 UICC 管理平台发送的加密后的第一业务密钥，将所述加密后的第一业务密钥发送给所述解密单元 2302；

所述解密单元 2302，用于使用预先保存的与 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密，获取第一业务密钥，将所述第一业务密钥发送给第二业务交互单元 2304，并向所述第三发送单元 2303 发送一个第一发送指令；

所述第三发送单元 2303，用于在接收到所述第一发送指令之后，向第一运营商设备发送业务开通执行响应，所述业务开通执行响应中携带有预先保存的 UICC 标识；

所述第二业务交互单元 2304，用于使用所述第一业务密钥和所述第一运营商设备进行业务交互。

进一步的，所述通用集成电路卡还包括：公私钥对生成单元 2305 和第二存储单元 2306；

所述第三接收单元 2301，还用于接收 UICC 厂商设备发送的密钥请求，将所述密钥请求发送给所述公私钥对生成单元 2305；

所述公私钥对生成单元 2305，用于随机生成 UICC 公私钥对，将所述 UICC 公钥发送给第三发送单元 2303，将所述 UICC 私钥发送给所述第二存储单元 2306；

所述第三发送单元 2303，还用于将所述 UICC 公钥发送给所述 UICC 厂

商设备；

所述第二存储单元 2306，用于保存所述 UICC 私钥。

进一步的，通用集成电路卡还包括：业务终止单元 2307；

所述第三接收单元 2301，还用于接收所述 UICC 管理平台发送的业务终止请求，所述业务终止请求中携带有所述 UICC 标识和所述第一运营商设备根据所述第一业务密钥生成的第一报文鉴别码，将所述业务终止请求发送给所述业务终止单元 2307 和所述第三发送单元 2303；

所述业务终止单元 2307，用于当对所述第一报文鉴别码校验通过时，终止与所述第一运营商设备进行业务交互，向所述第三发送单元 2303 发送一个第二发送指令；

所述第三发送单元 2303，还用于在接收到所述第二发送指令之后，向第一运营商设备发送业务终止执行响应，所述业务终止执行响应中携带有所述 UICC 标识。

进一步的，所述第三接收单元 2301，还用于接收所述 UICC 管理平台发送的与所述 UICC 标识对应的加密后的第二业务密钥和第二报文鉴别码，将所述加密后的第二业务密钥发送给所述解密单元 2302；

所述解密单元 2302，还用于当对所述第二报文鉴别码校验通过时，使用所述 UICC 私钥对所述加密后的第二业务密钥进行解密，获取所述第二业务密钥，将所述第二业务密钥发送给所述第二业务交互单元 2304，并向所述第三发送单元 2303 发送一个第三发送指令；

所述第三发送单元 2303，还用于在接收到所述第三发送指令之后，向所述第二运营商设备发送运营商切换执行响应，所述运营商切换执行响应中携带有所述 UICC 标识；

所述第二业务交互单元 2304，用于使用所述第二业务密钥和所述第二运营商设备进行业务交互。

图 24 为本发明用户终端的结构示意图。如图 24 所示，包括：第三存储单元 2401 和通用集成电路卡 UICC2402；

所述第三存储单元 2401，用于存储所述 UICC2402；

所述 UICC2402，用于接收 UICC 管理平台发送的加密后的第一业务密钥；

使用预先保存的与 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密, 获取第一业务密钥; 向第一运营商设备发送业务开通执行响应, 所述业务开通执行响应中携带有预先保存的 UICC 标识; 使用所述第一业务密钥和所述第一运营商设备进行业务交互。

本发明提出的通用集成电路卡的数据配置装置, UICC 管理平台根据业务开通请求中携带的 UICC 标识和第一运营商设备标识, 获取第一运营商设备生成的与 UICC 标识对应的加密后的第一业务密钥, UICC 在获取到所述加密后的第一业务密钥之后使用预先保存的 UICC 私钥对加密后的第一业务密钥进行解密, 使用解密后得到的第一业务密钥与第一运营商设备进行业务交互。由于用户发送的业务开通请求中携带有第一运营商设备标识, UICC 管理平台根据所述第一运营商设备标识为通用集成电路卡开通与第一运营商设备标识对应的第一运营商设备之间的业务交互, 因此运营商能够灵活地对通用集成电路卡中的运营商数据进行动态配置, 无需 M2M 终端在生产过程中需要根据运营商进行定制开发, 因此本发明提出的通用集成电路卡的数据配置装置, 解决了现有技术中 M2M 终端只能和预定的运营商进行通信的技术问题, 扩大了 M2M 终端的使用范围; 另外, 本发明所述方法实现起来简单方便, 便于普及。

图 25 为本发明通用集成电路卡的数据配置系统结构示意图。如图 25 所示, 包括: 通用集成电路卡 UICC 管理平台 2501、第一运营商设备 2502 和 UICC2503;

所述 UICC 管理平台 2501, 用于接收业务开通请求, 所述业务开通请求中携带有 UICC 标识和第一运营商设备标识, 向与所述第一运营商设备标识对应的第一运营商设备 2502 发送预先保存的与所述 UICC 标识对应的 UICC 证书, 所述 UICC 证书中携带有所述 UICC 标识和与所述 UICC 标识对应的 UICC 公钥; 接收所述第一运营商设备 2502 发送的与所述 UICC 标识对应的加密后的第一业务密钥, 并将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC2503;

所述第一运营商设备 2502, 用于接收 UICC 管理平台 2501 发送的 UICC 证书, 所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥; 当对所述

UICC 证书验证通过时,根据预设方法生成与所述 UICC 标识对应的第一业务密钥,使用所述 UICC 公钥对所述第一业务密钥进行加密,并通过所述 UICC 管理平台 2501 将加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC2503;获取所述 UICC2503 在获取到所述第一业务密钥之后发送的业务开通执行响应,所述业务开通执行响应中携带有所述 UICC 预先保存的所述 UICC 标识;使用所述第一业务密钥和所述 UICC2503 进行业务交互;

所述 UICC2503,用于接收 UICC 管理平台 2501 发送的所述加密后的第一业务密钥;使用预先保存的与所述 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密,获取所述第一业务密钥;向所述第一运营商设备 2502 发送业务开通执行响应,所述业务开通执行响应中携带有预先保存的 UICC 标识;使用所述第一业务密钥和所述第一运营商设备 2502 进行业务交互。

本发明提出的通用集成电路卡的数据配置系统,UICC 管理平台根据业务开通请求中携带的 UICC 标识和第一运营商设备标识,获取第一运营商设备生成的与所述 UICC 标识对应的加密后的第一业务密钥,UICC 在获取到所述加密后的第一业务密钥之后使用预先保存的 UICC 私钥对加密后的第一业务密钥进行解密,使用解密后得到的第一业务密钥与第一运营商设备进行业务交互。由于用户发送的业务开通请求中携带有第一运营商设备标识,UICC 管理平台根据所述第一运营商设备标识为通用集成电路卡开通与第一运营商设备标识对应的第一运营商设备之间的业务交互,因此运营商能够灵活地对通用集成电路卡中的运营商数据进行动态配置,无需 M2M 终端在生产过程中需要根据运营商进行定制开发,因此本发明提出的通用集成电路卡的数据配置系统,解决了现有技术中 M2M 终端只能和预定的运营商进行通信的技术问题,扩大了 M2M 终端的使用范围;另外,本发明所述方法实现起来简单方便,便于普及。

图 12 和 13 所示装置实施例的具体工作流程请参照图 1 所示方法实施例中的相应说明,不再赘述。

以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在

本发明保护的范围之内。

## 权 利 要 求 书

1、一种通用集成电路卡的数据配置方法，其特征在于，包括：

接收业务开通请求，所述业务开通请求中携带有通用集成电路卡 UICC 标识和第一运营商设备标识；

向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和 UICC 公钥；

接收所述第一运营商设备发送的与所述 UICC 标识对应的加密后的第一业务密钥，并将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC。

2、根据权利要求 1 所述的方法，其特征在于，所述接收业务开通请求，包括：

接收所述第一运营商设备发送的所述业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备预先保存的所述第一运营商设备标识；

或者，接收用户发送的所述业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备标识。

3、根据权利要求 1 所述的方法，其特征在于，在所述向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书之前，还包括：

查询与所述 UICC 标识对应的 UICC 是否被激活，若未被激活，则向所述第一运营商设备发送所述 UICC 证书，否则，向所述第一运营商设备发送错误提示信息。

4、根据权利要求 1 所述的方法，其特征在于，在所述将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC 之后，还包括：

接收所述 UICC 在获取到第一业务密钥之后发送的业务开通执行响应，所述业务开通执行响应中携带有所述 UICC 标识；

将与所述 UICC 标识对应的 UICC 标记为已被激活；

将所述业务开通执行响应发送给所述第一运营商设备。

5、根据权利要求 1 所述的方法，其特征在于，在所述接收业务开通请求之前，还包括：

接收 UICC 厂商设备发送的 UICC 卡片信息，所述 UICC 卡片信息中携带有所述 UICC 标识和 UICC 公钥；

将所述 UICC 卡片信息发送给认证中心；

当所述认证中心对所述 UICC 卡片信息认证通过时，接收所述认证中心返回的所述 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥；

保存与所述 UICC 标识对应的所述 UICC 证书。

6、根据权利要求 1 所述的方法，其特征在于，在所述将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC 之后，还包括：

接收所述第一运营商设备发送的业务终止请求，所述业务终止请求中携带有所述 UICC 标识和所述第一运营商设备根据所述第一业务密钥生成的第一报文鉴别码；

将所述业务终止请求发送给与所述 UICC 标识对应的 UICC。

7、根据权利要求 6 所述的方法，其特征在于，在所述将所述业务终止请求发送给与所述 UICC 标识对应的 UICC 之前，还包括：

查询与所述 UICC 标识对应的 UICC 是否被激活，若已被激活，则将所述业务终止请求发送给与所述 UICC 标识对应的 UICC，否则，向所述第一运营商设备发送错误提示信息。

8、根据权利要求 6 所述的方法，其特征在于，在所述接收所述第一运营商设备发送的业务终止请求之前，还包括：

接收用户提交的业务取消请求，所述业务取消请求中携带有所述 UICC 标识；

查询与所述 UICC 标识对应的 UICC 是否被激活，若已被激活，则向所述第一运营商设备转发所述业务取消请求，否则，向所述用户发送错误提示信息。

9、根据权利要求 6 所述的方法，其特征在于，在所述将所述业务终止请

求发送给与所述 UICC 标识对应的 UICC 之后，还包括：

接收所述 UICC 在终止与所述第一运营商设备进行业务交互之后发送的所述业务终止执行响应，所述业务终止执行响应中携带有所述 UICC 标识；

将与所述 UICC 标识对应的 UICC 标记为未被激活；

将所述业务终止执行响应发送给所述第一运营商设备。

10、根据权利要求 1 所述的方法，其特征在于，在所述将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC 之后，还包括：

接收运营商切换请求，所述运营商切换请求中携带有所述 UICC 标识和第二运营商设备标识；

当所述第一运营商设备允许与所述 UICC 标识对应的 UICC 切换运营商设备时，向与所述第二运营商设备标识对应的第二运营商设备发送所述 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥；

接收所述第二运营商设备发送的与所述 UICC 标识对应的加密后的第二业务密钥，并将与所述 UICC 标识对应的加密后的第二业务密钥发送给所述第一运营商设备；

接收所述第一运营商设备根据所述加密后的第二业务密钥生成的与所述 UICC 标识对应的第二报文鉴别码；

将所述加密后的第二业务密钥和所述第二报文鉴别码发送给与所述 UICC 标识对应的 UICC。

11、根据权利要求 10 所述的方法，其特征在于，所述接收运营商切换请求，包括：

接收所述第二运营商设备发送的所述运营商切换请求，所述运营商切换请求中携带有所述 UICC 标识和所述第二运营商设备标识；

或者，接收用户提交的所述运营商切换请求，所述运营商切换请求中携带有所述 UICC 标识和所述第二运营商设备标识。

12、一种通用集成电路卡管理平台，其特征在于，包括：第一接收单元和第一发送单元；

所述第一接收单元，用于接收业务开通请求，所述业务开通请求中携带有通用集成电路卡 UICC 标识和第一运营商设备标识，将所述业务开通请求

发送给所述第一发送单元；

所述第一发送单元，用于向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和 UICC 公钥；

所述第一接收单元，还用于接收所述第一运营商设备发送的与所述 UICC 标识对应的加密后的第一业务密钥，将所述加密后的第一业务密钥发送给所述第一发送单元；

所述第一发送单元，还用于将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC。

13、根据权利要求 12 所述的通用集成电路卡管理平台，其特征在于，所述第一接收单元，具体用于接收所述第一运营商设备发送的所述业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备预先保存的所述第一运营商设备标识；

或者，接收用户发送的所述业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备标识。

14、根据权利要求 12 所述的通用集成电路卡管理平台，其特征在于，还包括：查询单元；

所述查询单元，用于查询与所述 UICC 标识对应的 UICC 是否被激活，若未被激活，则向所述第一运营商设备发送所述 UICC 证书，否则，向所述第一运营商设备发送错误提示信息。

15、根据权利要求 12 所述的通用集成电路卡管理平台，其特征在于，还包括：标记单元；

所述第一接收单元，还用于接收所述 UICC 在获取到第一业务密钥之后发送的业务开通执行响应，所述业务开通响应中携带有所述 UICC 标识，将所述业务开通执行响应发送给所述标记单元和所述第一发送单元；

所述标记单元，用于将与所述 UICC 标识对应的 UICC 标记为已被激活；

所述第一发送单元，还用于将所述业务开通执行响应发送给所述第一运营商设备。

16、根据权利要求 12 所述的通用集成电路卡管理平台，其特征在于，还

包括：第一存储单元；

所述第一接收单元，还用于接收 UICC 厂商设备发送的 UICC 卡片信息，所述 UICC 卡片信息中携带有所述 UICC 标识和所述 UICC 公钥，将所述 UICC 卡片信息发送给所述第一发送单元；

所述第一发送单元，还用于将所述 UICC 卡片信息发送给认证中心；

所述第一接收单元，还用于当所述认证中心对所述 UICC 卡片信息认证通过时，接收所述认证中心返回的所述 UICC 证书，所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥，将所述 UICC 证书发送给所述第一存储单元；

所述第一存储单元，用于保存与所述 UICC 标识对应的所述 UICC 证书。

17、根据权利要求 12 所述的通用集成电路卡管理平台，其特征在于，所述第一接收单元，还用于接收所述第一运营商设备发送的业务终止请求，所述业务终止请求中携带有所述 UICC 标识和与所述第一运营商设备根据所述第一业务密钥生成的第一报文鉴别码，将所述业务终止请求发送给所述第一发送单元；

所述第一发送单元，还用于将所述业务终止请求发送给与所述 UICC 标识对应的 UICC。

18、根据权利要求 17 所述的通用集成电路卡管理平台，其特征在于，所述查询单元，还用于查询与所述 UICC 标识对应的 UICC 是否被激活，若已被激活，则将所述业务终止请求发送给与所述 UICC 标识对应的 UICC，否则，向所述第一运营商设备发送错误提示信息。

19、根据权利要求 17 所述的通用集成电路卡管理平台，其特征在于，所述第一接收单元，还用于接收用户提交的业务取消请求，所述业务取消请求中携带有所述 UICC 标识，将所述业务取消请求发送给所述查询单元；

所述查询单元，还用于查询与所述 UICC 标识对应的 UICC 是否被激活，若已被激活，则向所述第一运营商设备转发所述业务取消请求，否则，向所述用户发送错误提示信息。

20、根据权利要求 17 所述的通用集成电路卡管理平台，其特征在于，所述第一接收单元，还用于接收所述 UICC 在终止与所述第一运营商设备进行

业务交互之后发送的业务终止执行响应, 所述业务终止执行响应中携带有所述 UICC 标识, 将所述业务终止执行响应发送给所述标记单元和所述第一发送单元;

所述标记单元, 还用于将与所述 UICC 标识对应的 UICC 标记为未被激活;

所述第一发送单元, 还用于将所述业务终止执行响应发送给所述第一运营商设备。

21、根据权利要求 12 所述的通用集成电路卡管理平台, 其特征在于, 所述第一接收单元, 还用于接收运营商切换请求, 所述运营商切换请求中携带有所述 UICC 标识和第二运营商设备标识, 将所述运营商切换请求发送给所述第一发送单元;

所述第一发送单元, 还用于当所述第一运营商设备允许与所述 UICC 标识对应的 UICC 切换运营商设备时, 向与所述第二运营商设备标识对应的第二运营商设备发送所述 UICC 证书, 所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥;

所述第一接收单元, 还用于接收所述第二运营商设备发送的与所述 UICC 标识对应的加密后的第二业务密钥, 将所述加密后的第二业务密钥发送给所述第一发送单元;

所述第一发送单元, 还用于将所述加密后的第二业务密钥发送给所述第一运营商设备;

所述第一接收单元, 还用于接收所述第一运营商设备根据所述加密后的第二业务密钥生成的与所述 UICC 标识对应的第二报文鉴别码, 将所述第二报文鉴别码发送给所述第一发送单元;

所述第一发送单元, 还用于将所述加密后的第二业务密钥和所述第二报文鉴别码发送给与所述 UICC 标识对应的 UICC。

22、根据权利要求 21 所述的通用集成电路卡管理平台, 其特征在于, 所述第一接收单元, 具体用于接收所述第二运营商设备发送的所述运营商切换请求, 所述运营商切换请求中携带有所述 UICC 标识和所述第二运营商设备标识;

或者, 接收用户提交的所述运营商切换请求, 所述运营商切换请求中携

带有所述 UICC 标识和所述第二运营商设备标识。

23、一种第一运营商设备，其特征在于，包括：第二接收单元、业务密钥生成单元、第二发送单元和第一业务交互单元；

所述第二接收单元，用于接收通用集成电路卡 UICC 管理平台发送的 UICC 证书，所述 UICC 证书中携带有 UICC 标识和 UICC 公钥，将所述 UICC 证书发送给所述业务密钥生成单元；

所述业务密钥生成单元，用于当对所述 UICC 证书验证通过时，根据预设方法生成与所述 UICC 标识对应的第一业务密钥，使用所述 UICC 公钥对所述第一业务密钥进行加密，将所述第一业务密钥发送给第一业务交互单元，将加密后的第一业务密钥发送给所述第二发送单元；

所述第二发送单元，用于将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC；

所述第二接收单元，还用于获取所述 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应，所述业务开通执行响应中携带有所述 UICC 预先保存的所述 UICC 标识；

所述第一业务交互单元，用于使用所述第一业务密钥和所述 UICC 进行业务交互。

24、根据权利要求 23 所述的第一运营商设备，其特征在于，所述第二接收单元，还用于接收用户提交的业务申请请求，所述业务申请请求中携带有所述 UICC 标识，将所述业务申请请求发送给所述第二发送单元；

所述第二发送单元，还用于向所述 UICC 管理平台发送所述业务开通请求，所述业务开通请求中携带有所述 UICC 标识和所述第一运营商设备预先保存的所述第一运营商设备标识。

25、根据权利要求 23 所述的第一运营商设备，其特征在于，所述第二发送单元，还用于向所述 UICC 管理平台发送业务终止请求，所述业务终止请求中携带有所述 UICC 标识和根据所述第一业务密钥生成的第一报文鉴别码；

所述第二接收单元，还用于获取所述 UICC 发送的业务终止执行响应，所述业务终止执行响应中携带有所述 UICC 标识。

26、根据权利要求 23 所述的第一运营商设备，其特征在于，所述第二接

收单元，还用于接收所述 UICC 管理平台发送的与所述 UICC 标识对应的加密后的第二业务密钥；

所述第二发送单元，还用于向所述 UICC 管理平台发送根据所述加密后的第二业务密钥生成的与所述 UICC 标识对应的第二报文鉴别码。

27、一种通用集成电路卡，其特征在于，包括：第三接收单元、解密单元、第三发送单元和第二业务交互单元；

所述第三接收单元，用于接收通用集成电路卡 UICC 管理平台发送的加密后的第一业务密钥，将所述加密后的第一业务密钥发送给所述解密单元；

所述解密单元，用于使用预先保存的与 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密，获取第一业务密钥，将所述第一业务密钥发送给所述第二业务交互单元，并向所述第三发送单元发送一个第一发送指令；

所述第三发送单元，用于在接收到所述第一发送指令之后，向第一运营商设备发送业务开通执行响应，所述业务开通执行响应中携带有预先保存的 UICC 标识；

所述第二业务交互单元，用于使用所述第一业务密钥和所述第一运营商设备进行业务交互。

28、根据权利要求 27 所述的通用集成电路卡，其特征在于，还包括：公私钥对生成单元和第二存储单元；

所述第三接收单元，还用于接收 UICC 厂商设备发送的密钥请求，将所述密钥请求发送给所述公私钥对生成单元；

所述公私钥对生成单元，随机生成 UICC 公私钥对，将所述 UICC 公钥发送给第三发送单元，将所述 UICC 私钥发送给所述第二存储单元；

所述第三发送单元，还用于将所述 UICC 公钥发送给所述 UICC 厂商设备；

所述第二存储单元，用于保存所述 UICC 私钥。

29、根据权利要求 27 所述的通用集成电路卡，其特征在于，还包括：业务终止单元；

所述第三接收单元，还用于接收所述 UICC 管理平台发送的业务终止请求，所述业务终止请求中携带有所述 UICC 标识和所述第一运营商设备根据

所述第一业务密钥生成的第一报文鉴别码，将所述业务终止请求发送给所述业务终止单元和所述第三发送单元；

所述业务终止单元，用于当对所述第一报文鉴别码校验通过时，终止与所述第一运营商设备进行业务交互，向所述第三发送单元发送一个第二发送指令；

所述第三发送单元，还用于在接收到所述第二发送指令之后，向所述第一运营商设备发送业务终止执行响应，所述业务终止执行响应中携带有所述 UICC 标识。

30、根据权利要求 27 所述的通用集成电路卡，其特征在于，所述第三接收单元，还用于接收所述 UICC 管理平台发送的加密后的第二业务密钥和第二报文鉴别码，将所述加密后的第二业务密钥发送给所述解密单元；

所述解密单元，还用于当对所述第二报文鉴别码校验通过时，使用所述 UICC 私钥对所述加密后的第二业务密钥进行解密，获取所述第二业务密钥，将所述第二业务密钥发送给所述第二业务交互单元，并向所述第三发送单元发送一个第三发送指令；

所述第三发送单元，还用于在接收到所述第三发送指令之后，向所述第二运营商设备发送运营商切换执行响应，所述运营商切换执行响应中携带有所述 UICC 标识；

所述第二业务交互单元，用于使用所述第二业务密钥和所述第二运营商设备进行业务交互。

31、一种用户终端，其特征在于，包括：第三存储单元和通用集成电路卡 UICC；

所述第三存储单元，用于存储所述 UICC；

所述 UICC，用于接收 UICC 管理平台发送的加密后的第一业务密钥；使用预先保存的与 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密，获取第一业务密钥；向第一运营商设备发送业务开通执行响应，所述业务开通执行响应中携带有预先保存的 UICC 标识；使用所述第一业务密钥和所述第一运营商设备进行业务交互。

32、一种通用集成电路卡的数据配置系统，其特征在于，包括：通用集

成电路卡 UICC 管理平台、第一运营商设备和 UICC;

所述 UICC 管理平台, 用于接收业务开通请求, 所述业务开通请求中携带有 UICC 标识和第一运营商设备标识, 向与所述第一运营商设备标识对应的第一运营商设备发送预先保存的与所述 UICC 标识对应的 UICC 证书, 所述 UICC 证书中携带有所述 UICC 标识和与所述 UICC 标识对应的 UICC 公钥; 接收所述第一运营商设备发送的与所述 UICC 标识对应的加密后的第一业务密钥, 并将所述加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC;

所述第一运营商设备, 用于接收所述 UICC 管理平台发送的 UICC 证书, 所述 UICC 证书中携带有所述 UICC 标识和所述 UICC 公钥; 当对所述 UICC 证书验证通过时, 根据预设方法生成与所述 UICC 标识对应的第一业务密钥, 使用所述 UICC 公钥对所述第一业务密钥进行加密, 并通过所述 UICC 管理平台将加密后的第一业务密钥发送给与所述 UICC 标识对应的 UICC; 获取所述 UICC 在获取到所述第一业务密钥之后发送的业务开通执行响应, 所述业务开通执行响应中携带有所述 UICC 预先保存的所述 UICC 标识; 使用所述第一业务密钥和所述 UICC 进行业务交互;

所述 UICC, 用于接收所述 UICC 管理平台发送的所述加密后的第一业务密钥; 使用预先保存的与所述 UICC 公钥对应的 UICC 私钥对所述加密后的第一业务密钥进行解密, 获取所述第一业务密钥; 向所述第一运营商设备发送业务开通执行响应, 所述业务开通执行响应中携带有预先保存的所述 UICC 标识; 使用所述第一业务密钥和所述第一运营商设备进行业务交互。

33、一种计算机程序, 其特征在于, 用于执行如权利要求 1-11 所述的通用集成电路卡的数据配置方法。

34、一种存储介质, 其特征在于, 用于存储如权利要求 33 所述的计算机程序。

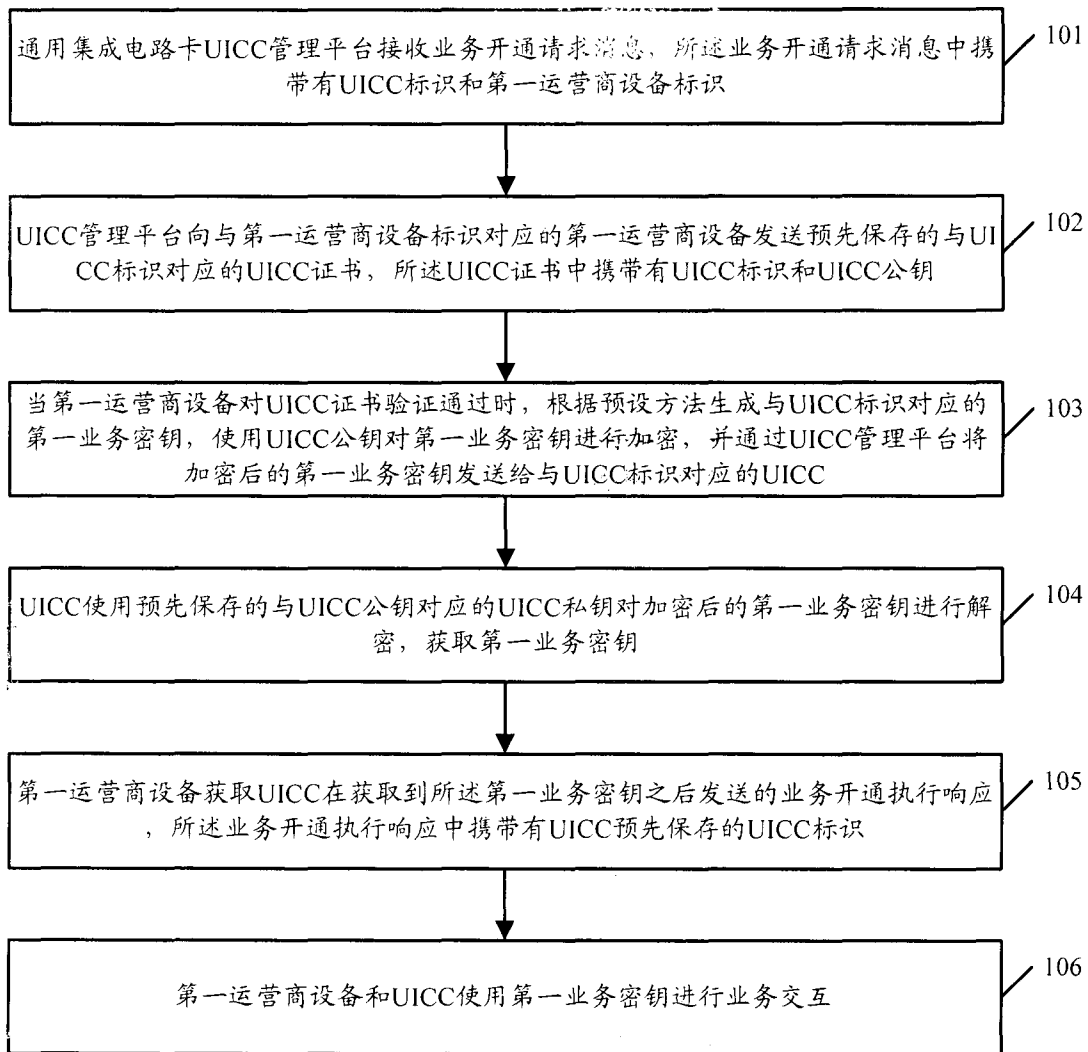


图 1

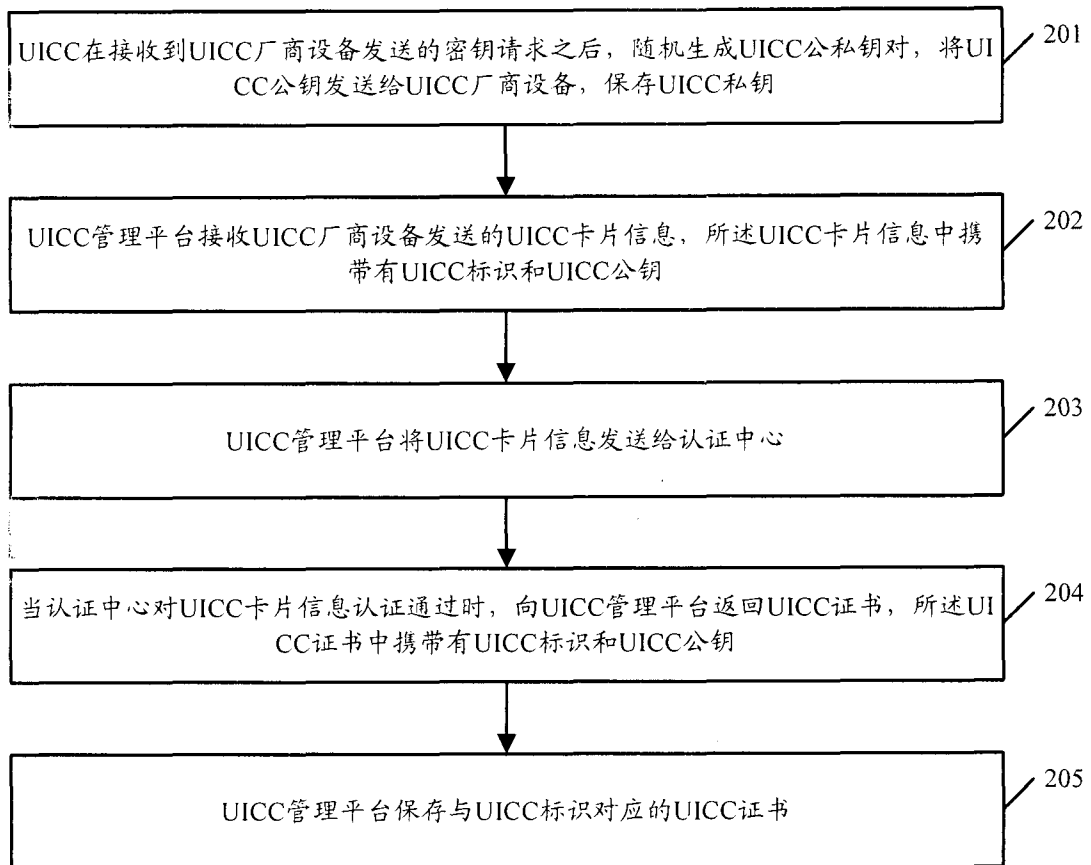


图 2

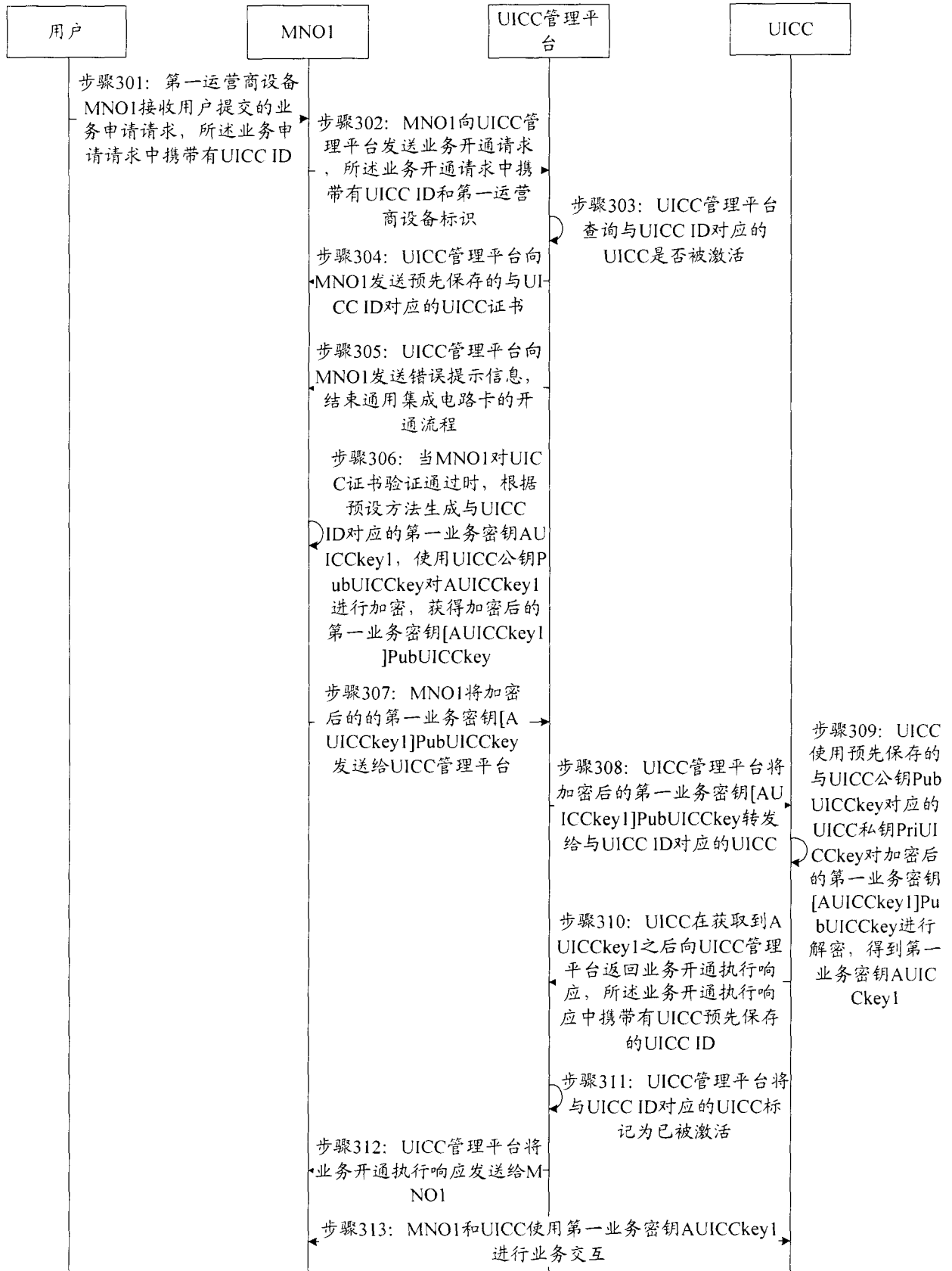


图 3

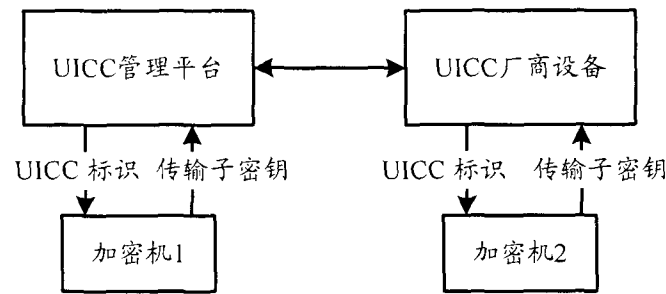


图 4

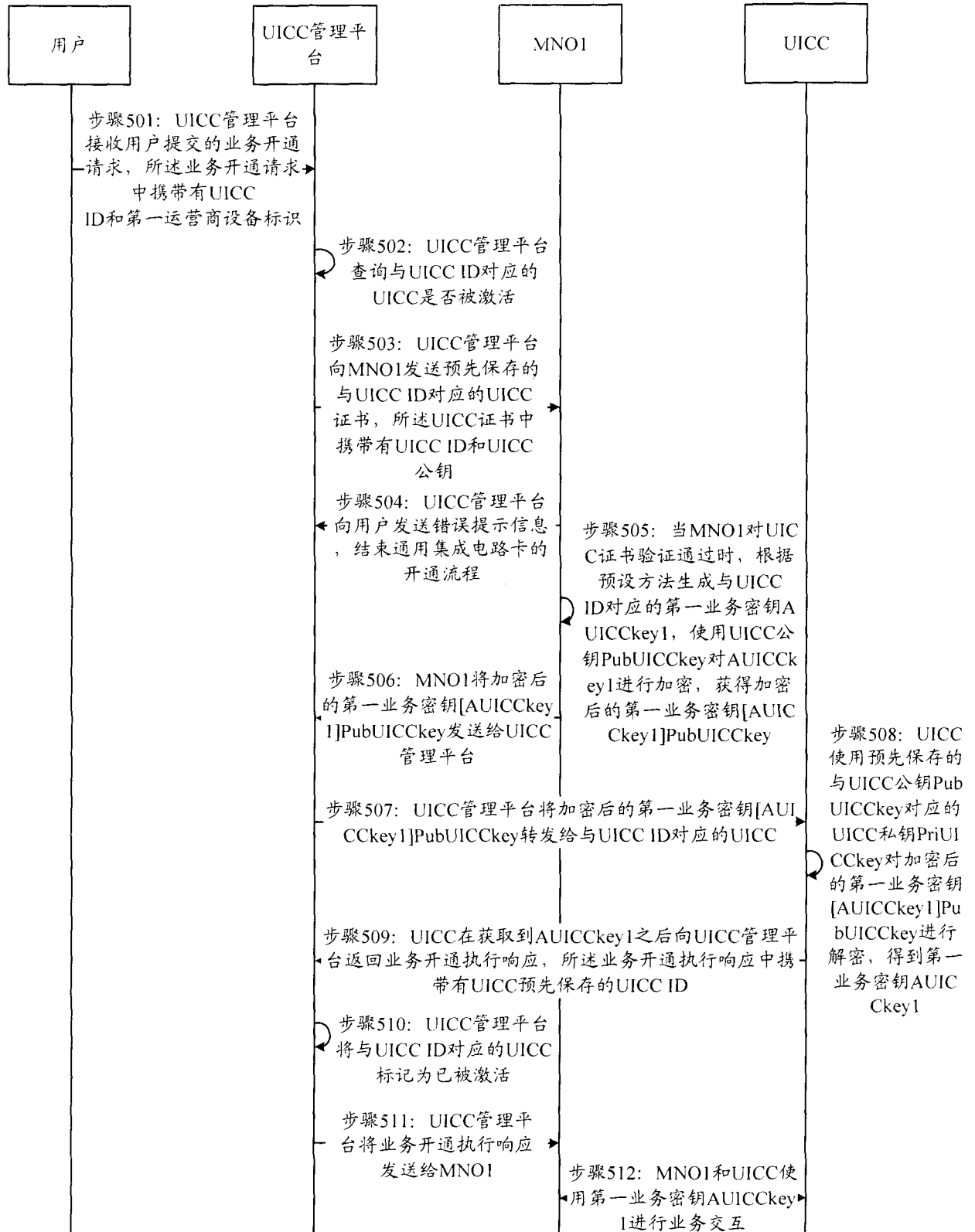


图 5

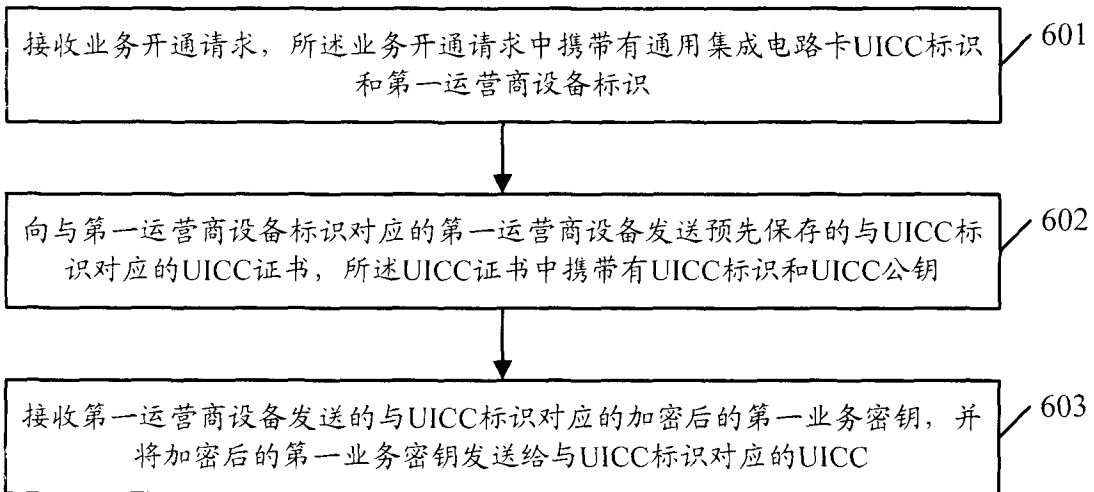


图 6

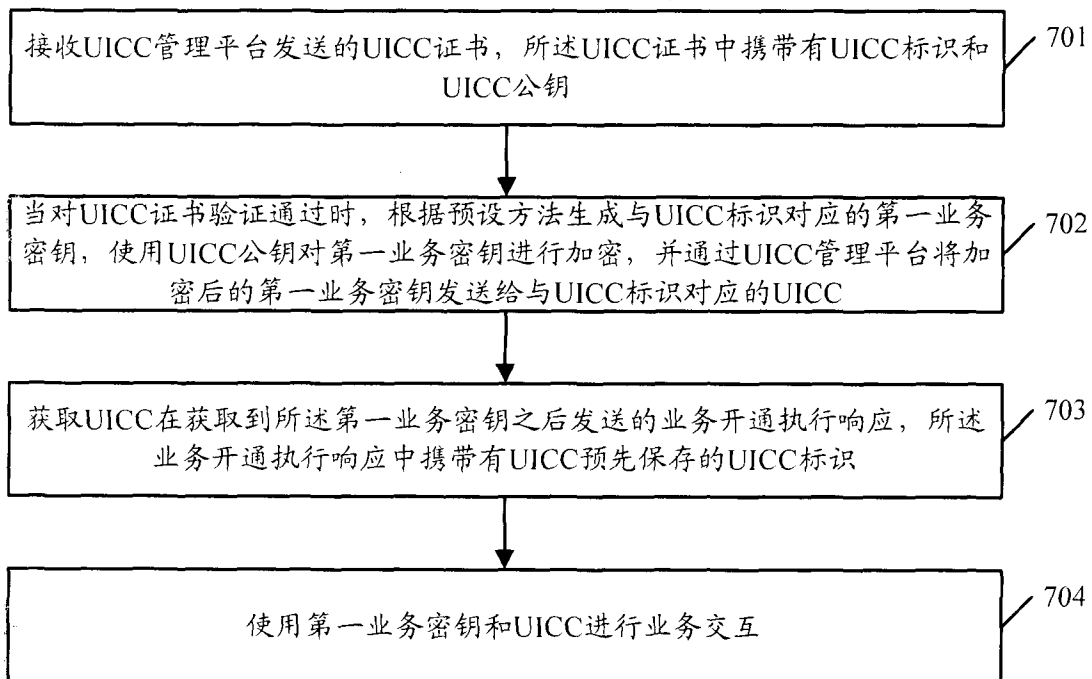


图 7

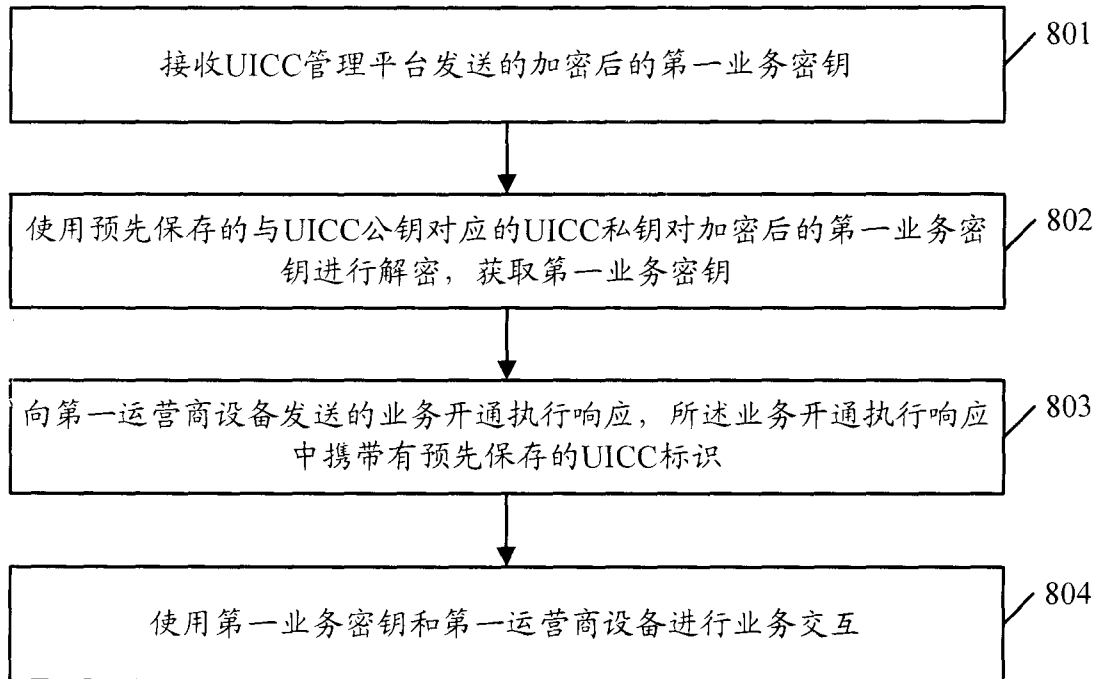


图 8

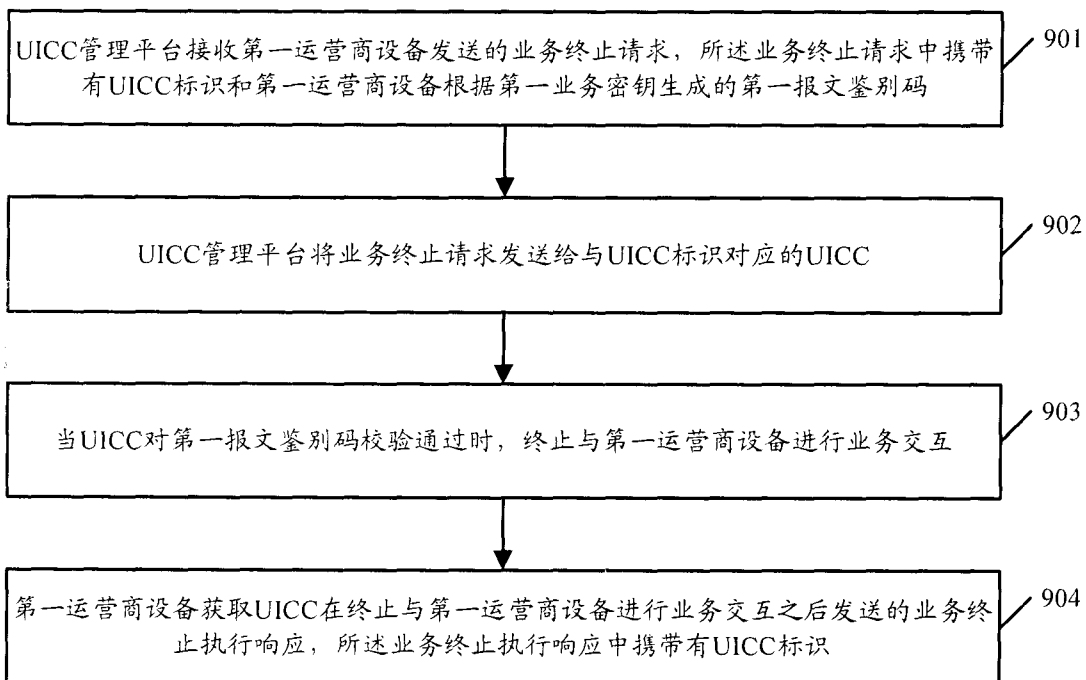


图 9

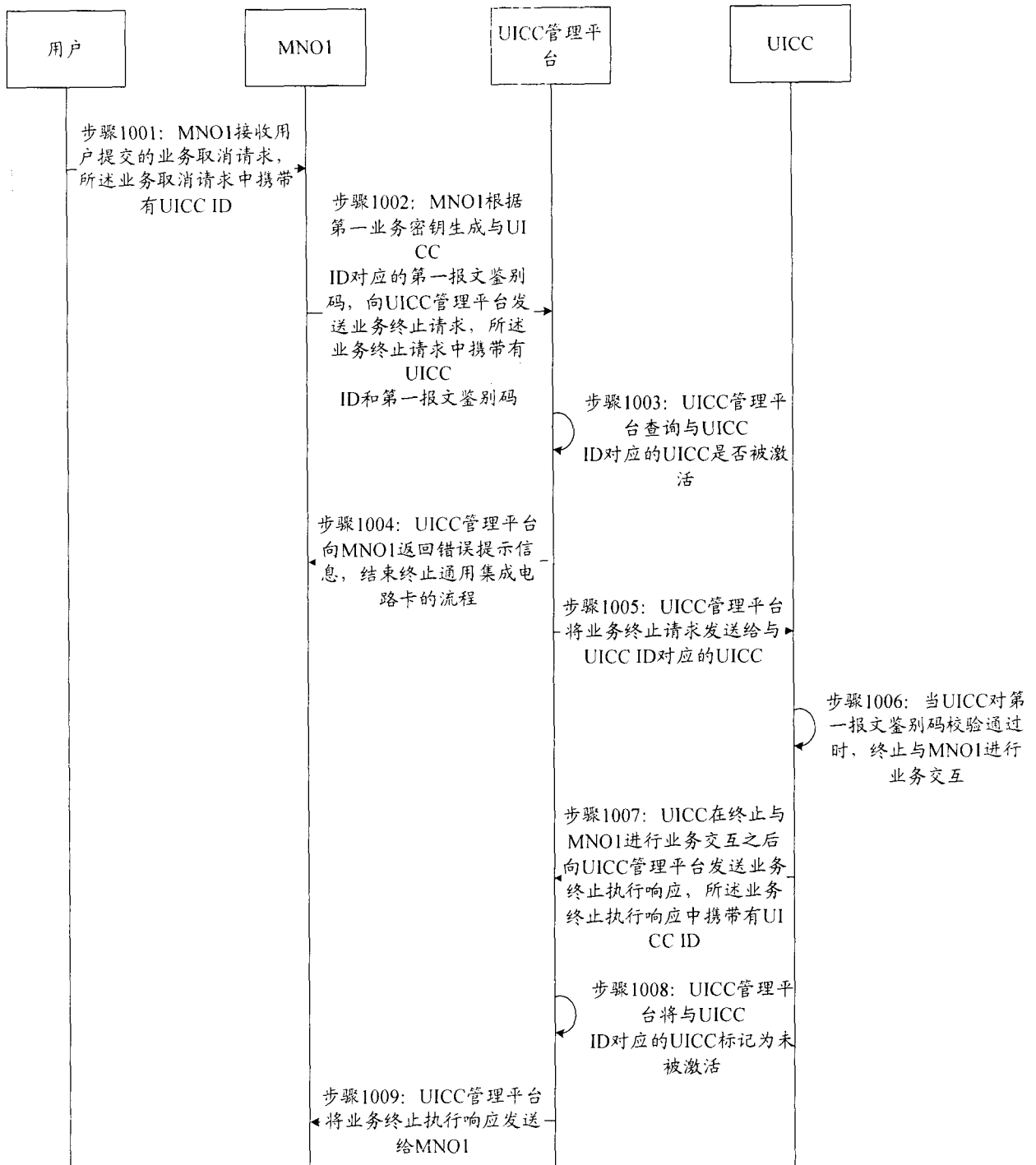


图 10

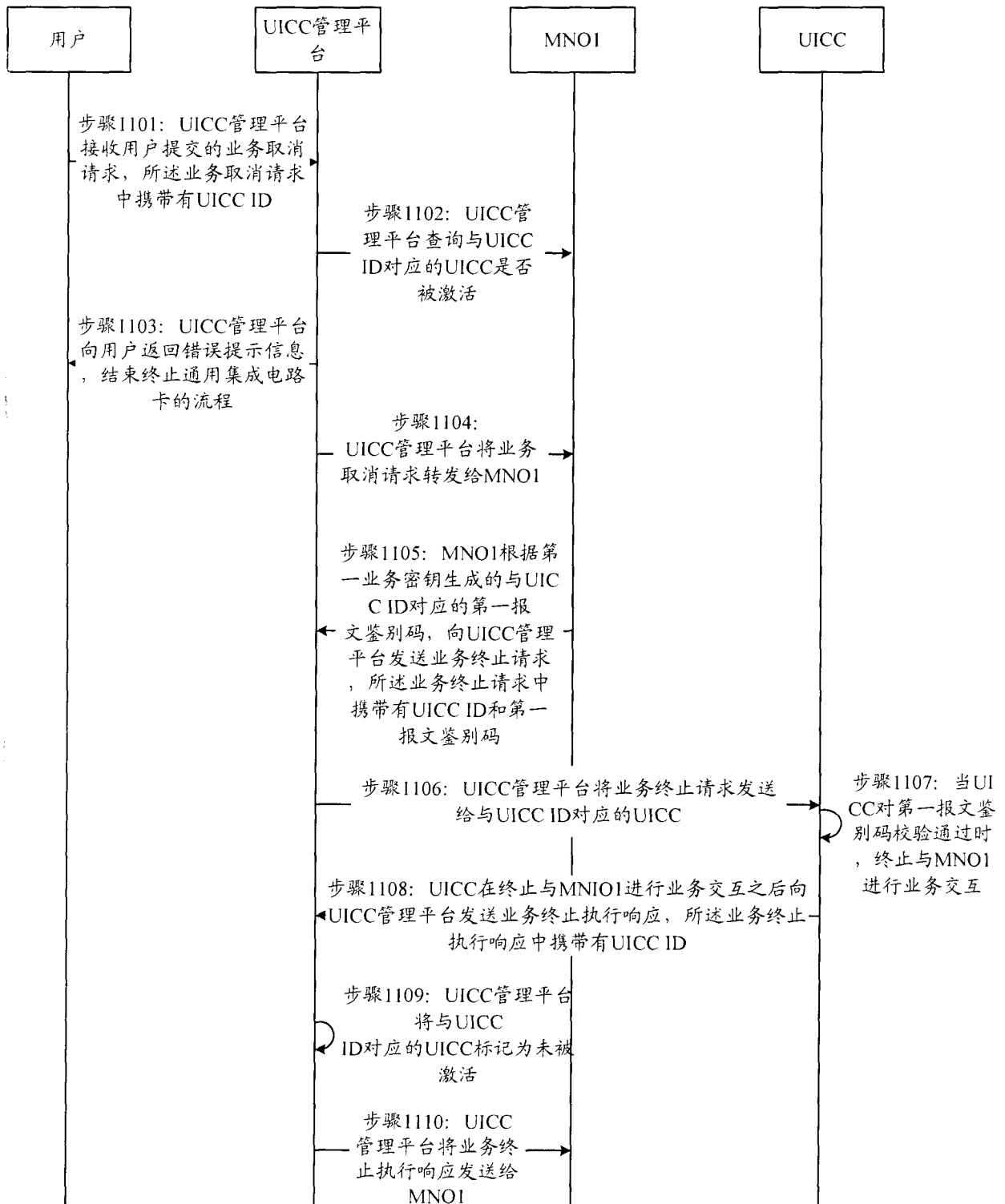


图 11

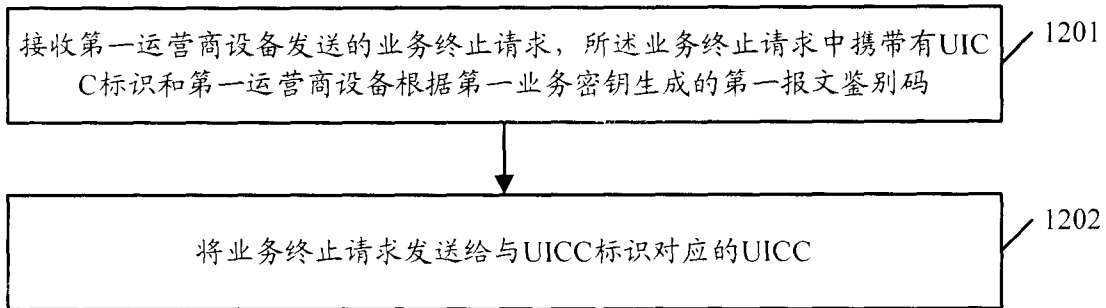


图 12

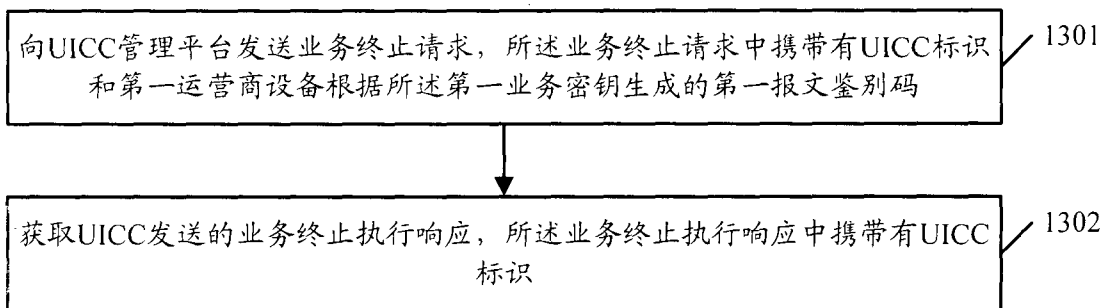


图 13

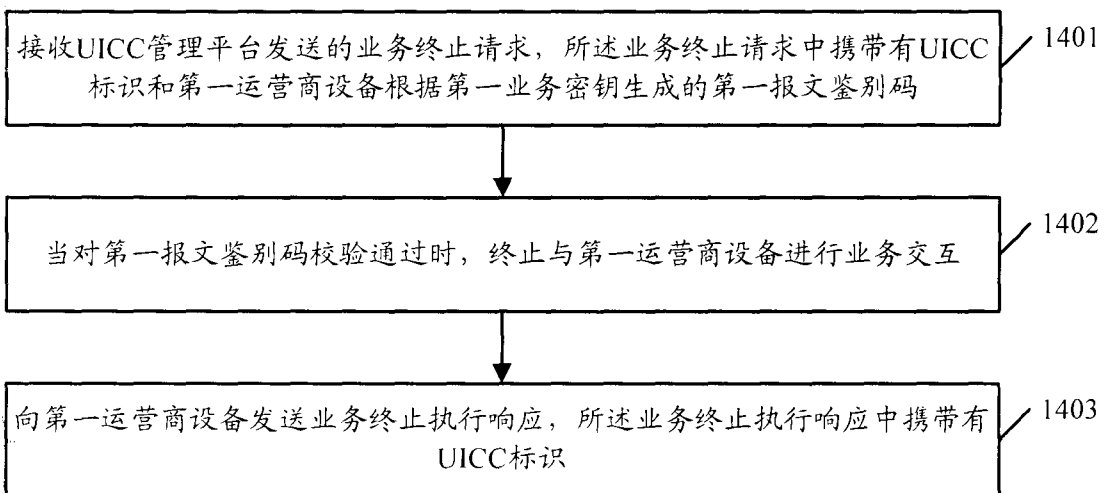


图 14

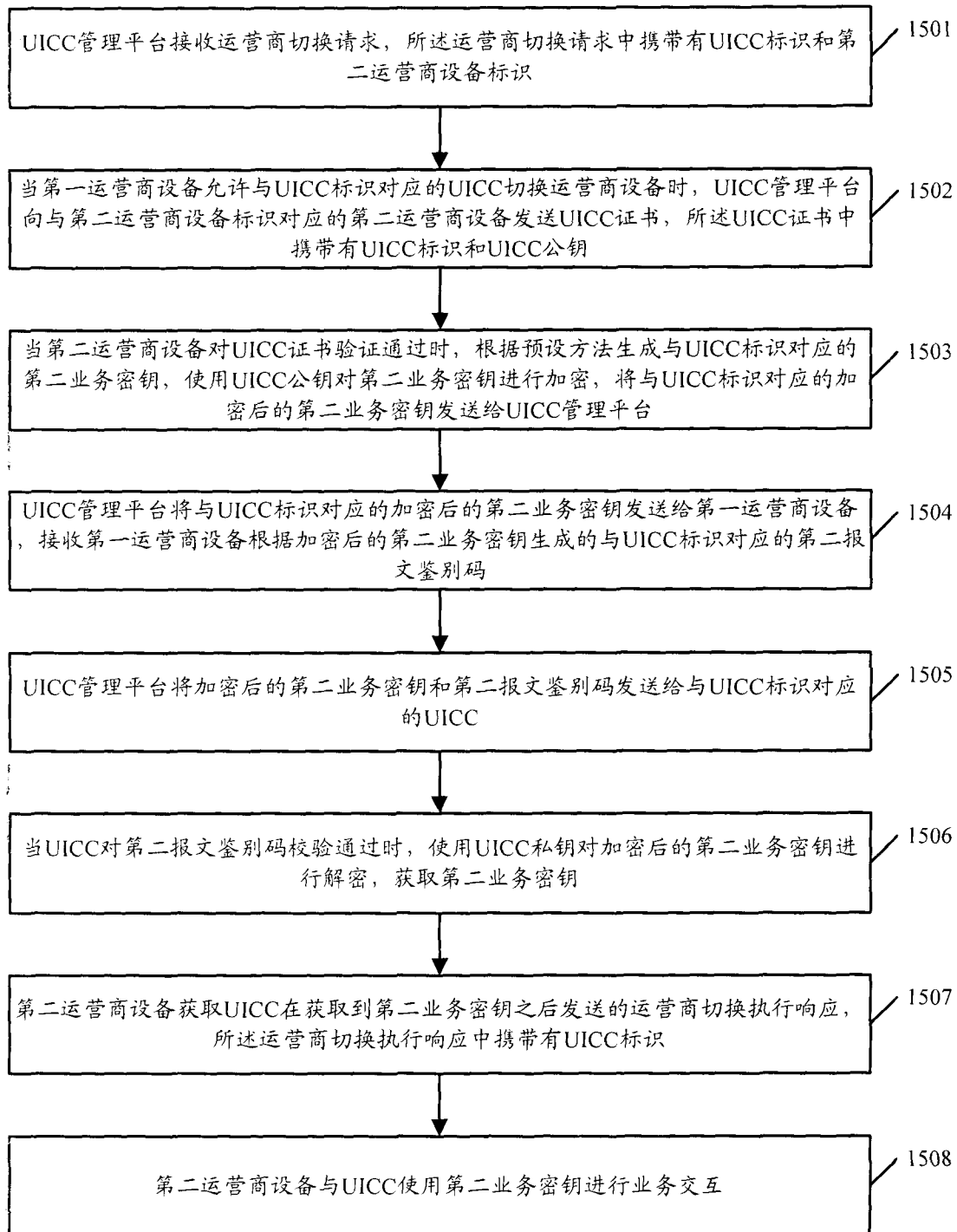


图 15

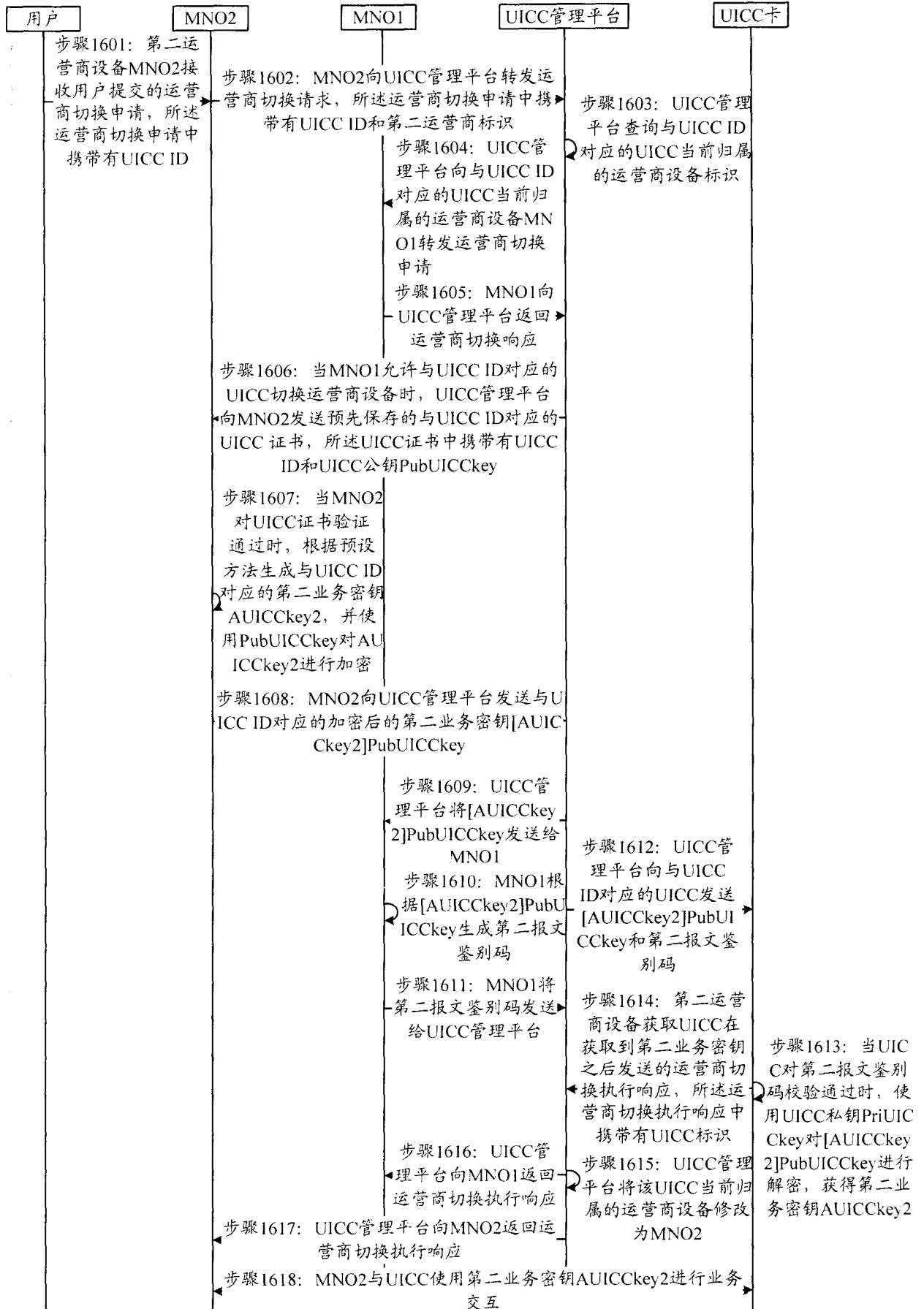


图 16

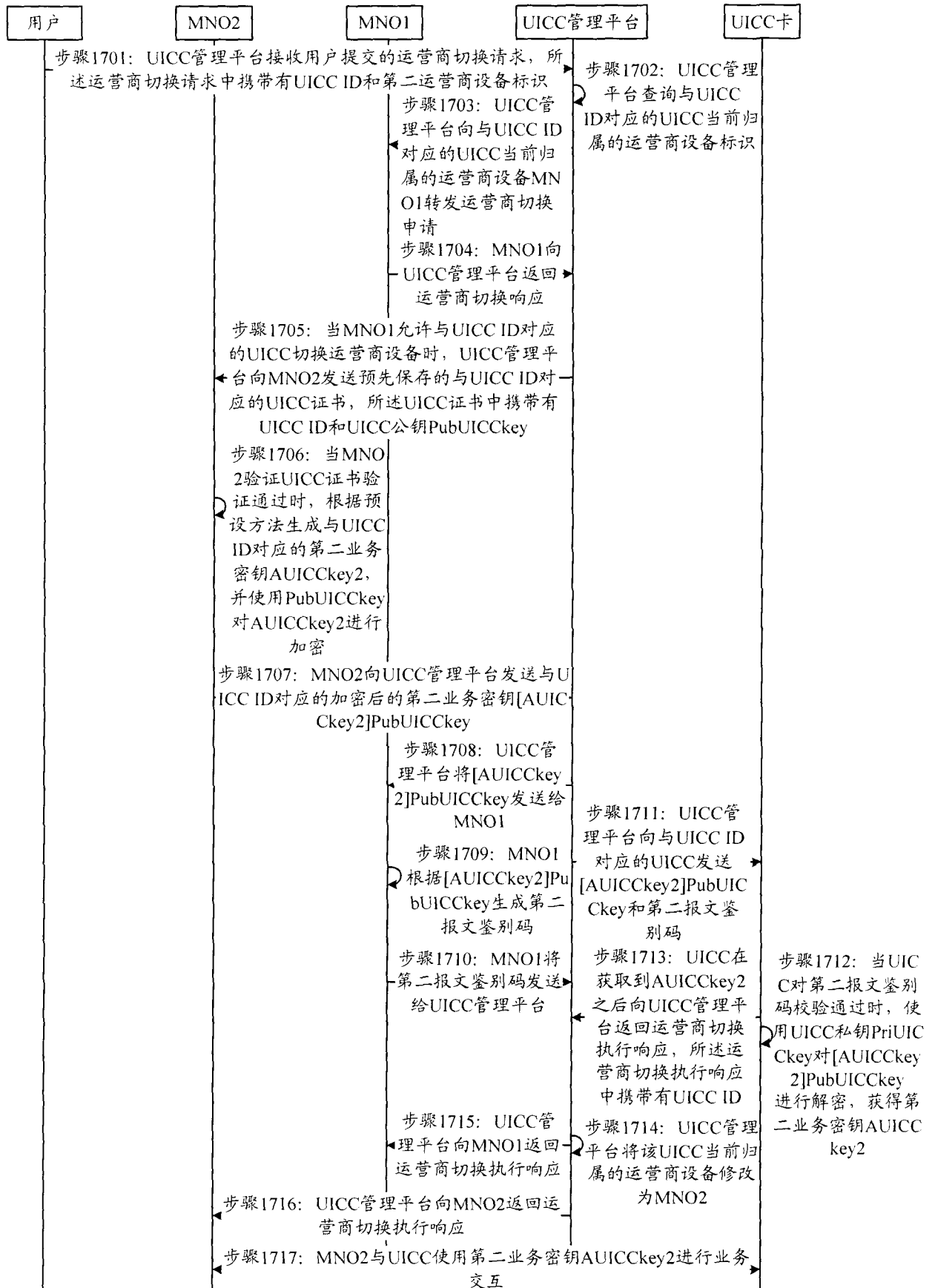


图 17

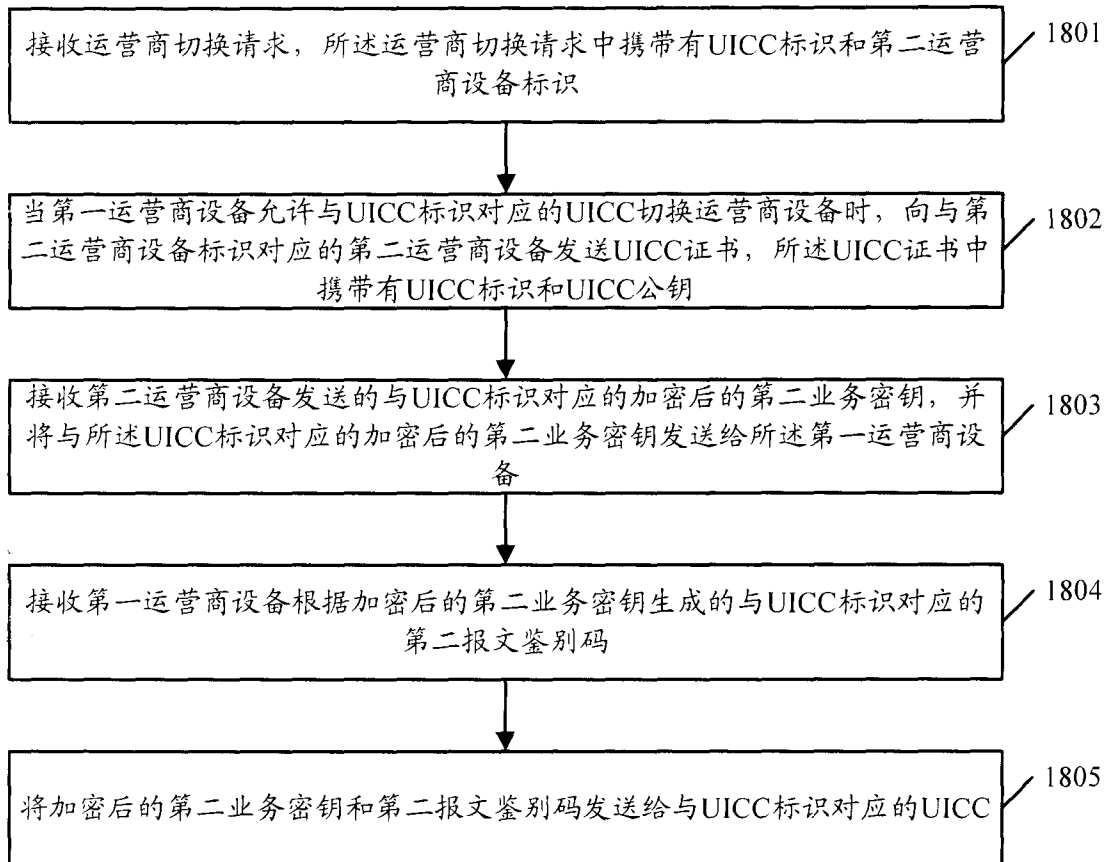


图 18

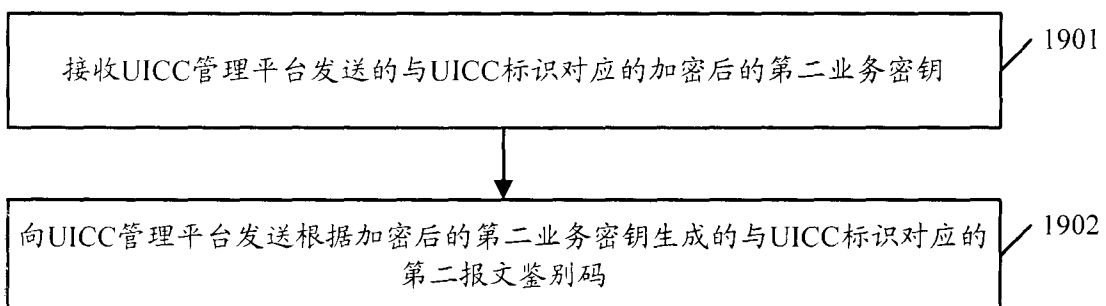


图 19

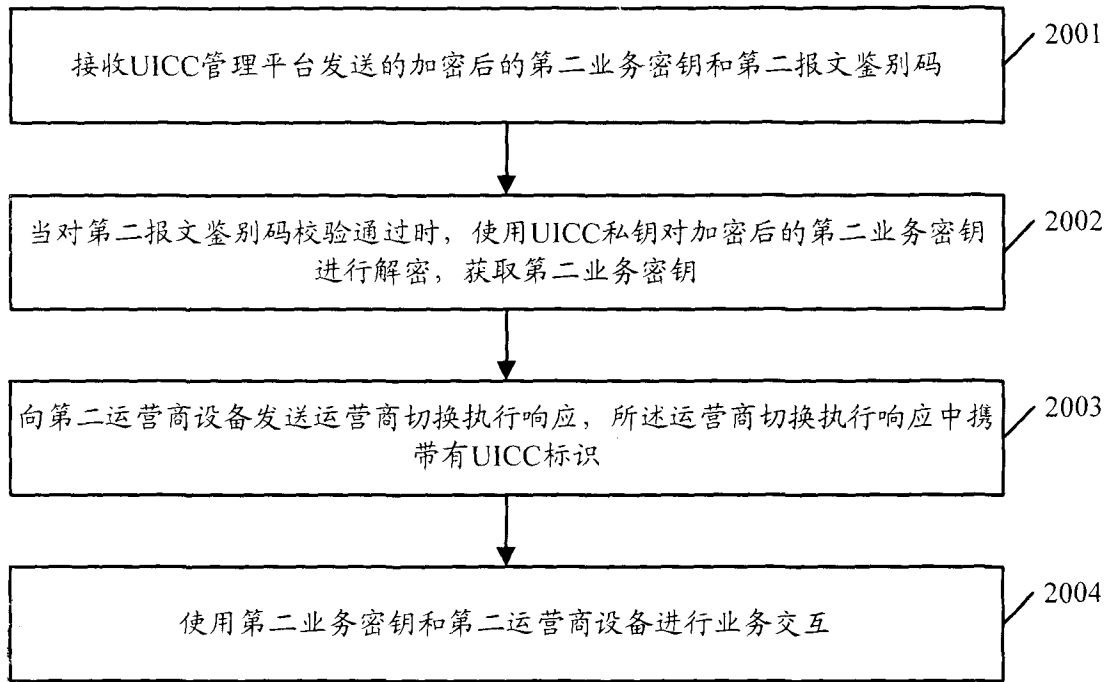


图 20

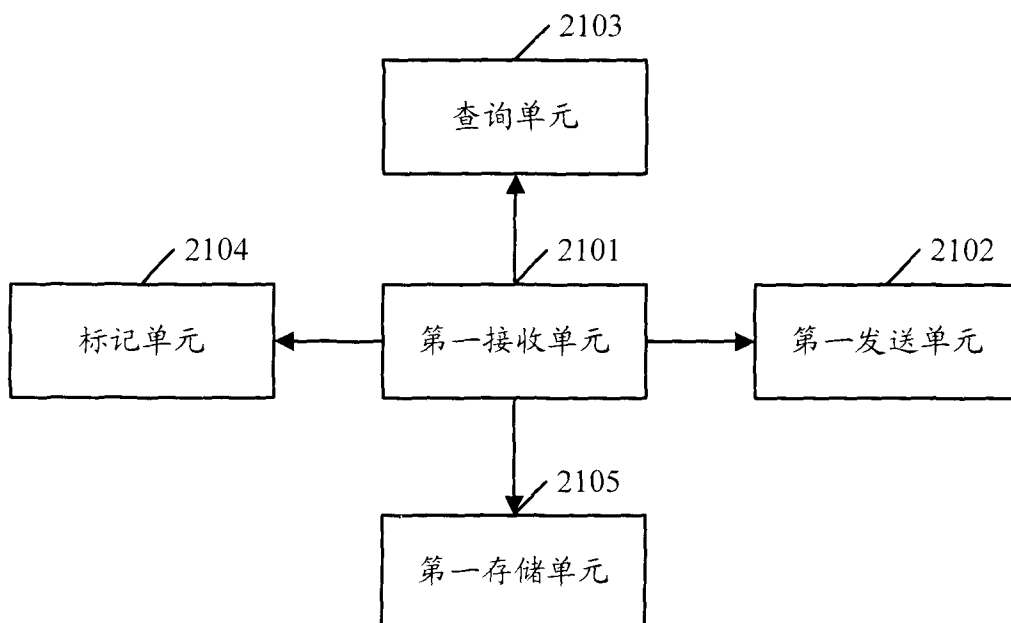


图 21

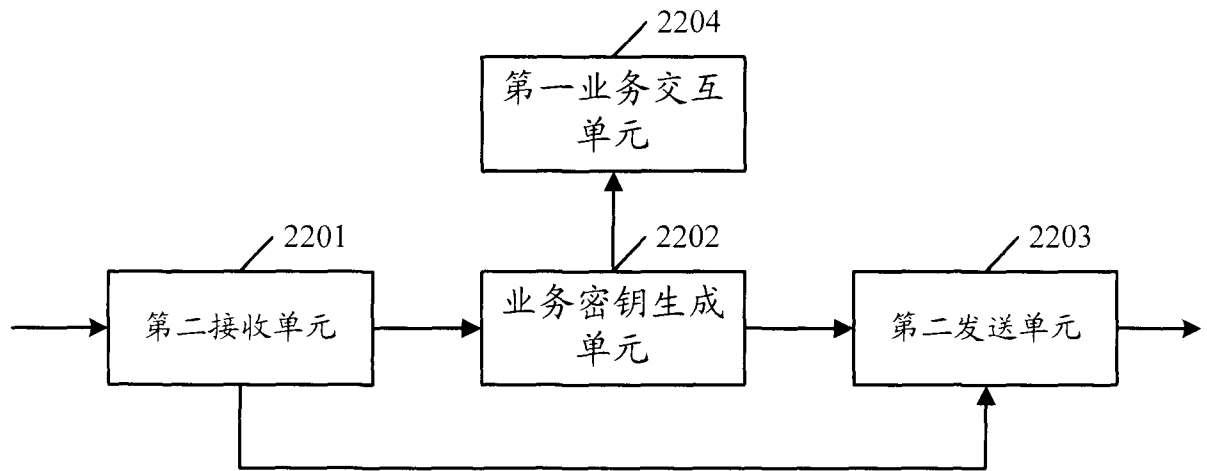


图 22

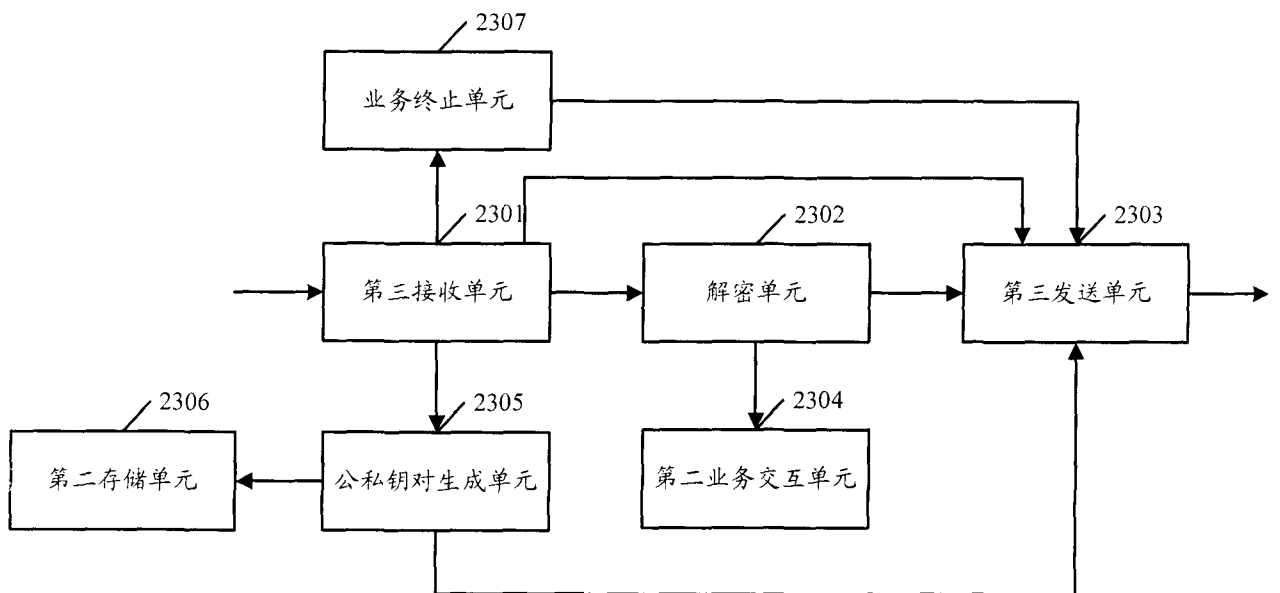


图 23

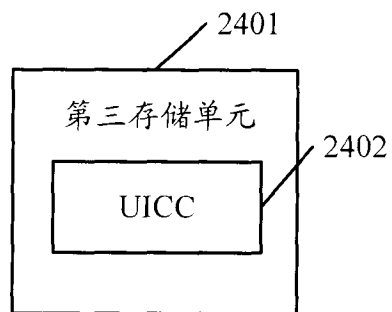


图 24

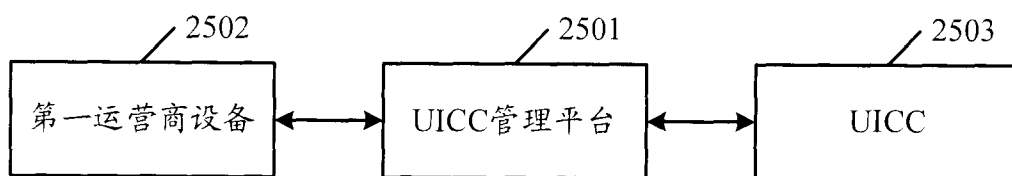


图 25

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/CN2013/079364

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNKI, CNPAT, IEEE: UICC, integrated w circuit w card, security, terminal, authentication, key, certificate, M2M;

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                       | Relevant to claim No.           |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| X         | CN 101005359 A (HUAWEI TECHNOLOGIES CO., LTD.) 25 July 2007 (25.07.2007) description, pages 1, 2, 15 and 16, and figure 5                | 1-5, 12-16, 23-24, 27-28, 31-34 |
| X         | CN 101765105 A (BEIJING WATCH DATA SYSTEM CO., LTD. et al.) 30 June 2010 (30.06.2010) description, paragraphs [0005]-[0069] and figure 2 | 1-5, 12-16, 23-24, 27-28, 31-34 |
| A         | CN 102209317 A (ZTE CORPORATION) 05 October 2011 (05.10.2011) the whole document                                                         | 1-34                            |
| A         | US 2009209232 A1 (INTERDIGITAL TECHNOLOGY CORPORATION) 20 August 2009 (20.08.2009) the whole document                                    | 1-34                            |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

|                                                                                                                                                                         |                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * Special categories of cited documents:                                                                                                                                | “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention                                              |
| “A” document defining the general state of the art which is not considered to be of particular relevance                                                                | “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone                                                                     |
| “E” earlier application or patent but published on or after the international filing date                                                                               | “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | “&” document member of the same patent family                                                                                                                                                                                                    |
| “O” document referring to an oral disclosure, use, exhibition or other means                                                                                            |                                                                                                                                                                                                                                                  |
| “P” document published prior to the international filing date but later than the priority date claimed                                                                  |                                                                                                                                                                                                                                                  |

|                                                                                                                                                                                                               |                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Date of the actual completion of the international search<br>27 September 2013 (27.09.2013)                                                                                                                   | Date of mailing of the international search report<br>24 October 2013 (24.10.2013) |
| Name and mailing address of the ISA<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No. (86-10) 62019451 | Authorized officer<br><br>WANG, Jing<br><br>Telephone No. (86-10) 62413627         |

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/CN2013/079364

| Patent Documents referred<br>in the Report | Publication Date | Patent Family    | Publication Date |
|--------------------------------------------|------------------|------------------|------------------|
| CN 101005359 A                             | 25.07.2007       | None             |                  |
| CN 101765105 A                             | 30.06.2010       | None             |                  |
| CN 102209317 A                             | 05.10.2011       | None             |                  |
| US 2009209232 A1                           | 20.08.2009       | WO 2009046400 A1 | 09.04.2009       |
|                                            |                  | TW 200917781 A   | 16.04.2009       |
|                                            |                  | EP 2210436 A1    | 28.07.2010       |
|                                            |                  | KR 20100083840 A | 22.07.2010       |
|                                            |                  | CN 101822082 A   | 01.09.2010       |
|                                            |                  | JP 2011501908 A  | 13.01.2011       |
|                                            |                  | TW 201014314 A   | 01.04.2010       |
|                                            |                  | KR 100084938 B1  | 18.11.2011       |
|                                            |                  | CN 102857912 A   | 02.01.2013       |

# 国际检索报告

国际申请号

**PCT/CN2013/079364**

## A. 主题的分类

H04L 9/32 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

## B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L;

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI,EPODOC,CNKI,CNPAT,IEEE: 证书, 运营商, 开通, 密钥, 公钥, 智能卡, 集成电路卡, 机器对机器;  
UICC, INTEGRATED W CIRCUIT W CARD, SECURITY, TERMINAL, AUTHENTICATION, KEY, CERTIFICATE,  
M2M;

## C. 相关文件

| 类 型* | 引用文件, 必要时, 指明相关段落                                                                | 相关的权利要求                     |
|------|----------------------------------------------------------------------------------|-----------------------------|
| X    | CN101005359A(华为技术有限公司)25.7 月 2007 (25.07.2007) 说明书第 1-2, 15-16 页, 附图 5           | 1-5,12-16,23-24,27-28,31-34 |
| X    | CN101765105A(北京握奇数据系统有限公司等)30.6 月 2010 (30.06.2010) 说明书第 0005-0069 段, 附图 2       | 1-5,12-16,23-24,27-28,31-34 |
| A    | CN102209317A(中兴通讯股份有限公司)05.10 月 2011 (05.10.2011) 全文                             | 1-34                        |
| A    | US2009209232A1 (INTERDIGITAL TECHNOLOGY CORPORATION) 20.8 月 2009 (20.08.2009) 全文 | 1-34                        |

☐ 其余文件在 C 栏的续页中列出。

☒ 见同族专利附件。

\* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期  
27.9 月 2013 (27.09.2013)

国际检索报告邮寄日期  
**24.10 月 2013 (24.10.2013)**

ISA/CN 的名称和邮寄地址:  
中华人民共和国国家知识产权局  
中国北京市海淀区蓟门桥西土城路 6 号 100088  
传真号: (86-10)62019451

受权官员  
  
王晶  
电话号码: (86-10) **62413627**

# 国际检索报告

关于同族专利的信息

国际申请号

**PCT/CN2013/079364**

| 检索报告中引用的<br>专利文件 | 公布日期       | 同族专利             | 公布日期       |
|------------------|------------|------------------|------------|
| CN101005359A     | 25.07.2007 | 无                |            |
| CN101765105A     | 30.06.2010 | 无                |            |
| CN102209317A     | 05.10.2011 | 无                |            |
| US 2009209232 A1 | 20.08.2009 | WO 2009046400 A1 | 09.04.2009 |
|                  |            | TW 200917781 A   | 16.04.2009 |
|                  |            | EP 2210436 A1    | 28.07.2010 |
|                  |            | KR 20100083840 A | 22.07.2010 |
|                  |            | CN 101822082 A   | 01.09.2010 |
|                  |            | JP 2011501908 A  | 13.01.2011 |
|                  |            | TW 201014314 A   | 01.04.2010 |
|                  |            | KR 100084938 B1  | 18.11.2011 |
|                  |            | CN 102857912 A   | 02.01.2013 |