(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
2018 年 7 月 19 日 (19.07.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/129724 A1

(51) 国际专利分类号:
H04W 8/20 (2009.01) *H04W 12/06* (2009.01)
H04W 88/18 (2009.01)

(21) 国际申请号: PCT/CN2017/071185

(22) 国际申请日: 2017 年 1 月 13 日 (13.01.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华 为 技 术 有 限 公 司 **(HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 高 林 毅 **(GAO, Linyi)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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。

WO 2018/129724 A1

(54) **Title:** SUBSCRIPTION PROFILE DOWNLOAD METHOD, DEVICE AND SERVER

(54) **发明名称:** 一种签约数据集的下载方法、设备及服务器

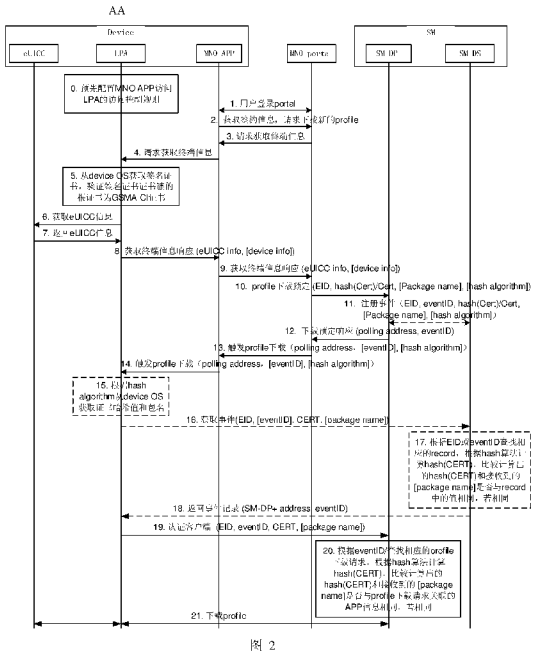

图 2

0	Pre-configuring access control rules for an MNO application to access an LPA
1	A user logging into a portal
2	Obtaining subscription information, requesting the download of a new profile
3, 4	Requesting to obtain terminal information
5	Obtaining a signature certificate from a device OS, verifying that a root certificate of a certificate chain of the signature certificate is a GSMA CI certificate
6	Obtaining eUICC information
7	Returning the eUICC information
8, 9	Obtaining a terminal information response (eUICC info, [device info])
10	Profile dowuload reservation (EID, hash(Cert)/Cert, [Package name], [hash algorithm])
11	Registered event (EID, eventID, hash(Cert)/Cert, [Package name], [hash algorithm])
12	Download reservation response (polling address, eventID)
13, 14	Triggering profile downlond (polling address, [eventID], [hash algorithm])
15	Obtaining a certificate hash value and a package name from the device OS according to a hash algorithm
16	Obtaining the event (EID, [eventID], CERT, [package name])
17	Retrieving a corresponding record according to EID or eventID, calculating a hash(CERT) according to the hash algorithm, determining whether the calculated hash(CERT) and the received [package name] have the same values as in the record. if yes
18	Returning an event record (SM-DP+address eventID)
19	Authenticating an client terminal (EID, [eventID], CERT, [package name])
20	Retrieving a corresponding profile download request according to the eventID/, calculating the hash(CERT) according to the hash algorithm, determining whether the calculated hash(CERT) and the received [package name] have the same information as in the application related to the profile download request, if yes
21	Downloading the profile
AA	Device

(57) **Abstract:** Provided in an embodiment of the present invention are a method, device and server for achieving the download of a subscription profile. In the method, when an application in a device triggers a subscription profile to be downloaded, a carrier server sends authentication information of the application which allows the download of a subscription profile to be initiated to a subscription management service device; when the device requests that authentication information be sent, the subscription management service device verifies the application in the device which initiates the download of the subscription profile by using the authentication infor-

[见续页]

(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, ST, 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))。

mation, and provides the download of the subscription profile for said device once the verification is successful. In another embodiment, the subscription management service device may send the authentication information to the device along with a previously downloaded subscription profile, and when downloading a different subscription profile, the device may verify the application by using the authentication information from the previously downloaded subscription profile.

(57) 摘要：本发明实施例提供了一种实现签约数据集下载的方法、设备及服务器，在所述方法中，设备中应用触发签约数据集下载时，运营商服务器会将允许发起签约数据集下载的应用的认证信息发送给签约管理服务设备，当设备请求通过发送认证信息时，所述签约管理服务设备会利用所述认证信息对所述设备中发起签约数据集下载的应用进行验证，在验证通过后，为所述设备提供签约数据集下载。在另一实施例中，签约管理服务设备可以将所述认证信息随前次下载的签约数据集发送至设备中，再次下载不同的签约数据集时，所述设备可以利用前次下载的签约数据集中的认证信息验证所述应用。

一种签约数据集的下载方法、设备及服务器

技术领域

本发明涉及通信领域，尤其涉及一种签约数据集的下载方法、设备及服务器。

背景技术

目前，终端用户向运营商购买 SIM（Subscriber Identification Module，客户识别模块）卡或 UICC（Universal Integrated Circuit Card，通用集成电路卡），将 SIM 卡或 UICC 插入设备（device）即可以根据卡中写入的数据集接入运营商的网络。eUICC 是指支持安全地远程管理签约数据集（profile）的 UICC 和/或支持本地管理 profile 的 UICC，签约数据集是 eUICC 上的文件结构、数据、应用程序等数据集合。

由于 eUICC 一般是由终端制造商集成在终端设备（即本文中所述设备）中，一般并不是由运营商采购制造，因此设备出厂后，eUICC 中可能并不包含可以接入运营商网络的数据。设备需要使用远程管理技术连接 SM-DP+（Subscription Manager Data Preparation+，签约管理-数据准备实体），接收 SM-DP+下发的 profile，并将 profile 下载到 eUICC 中，之后 eUICC 就可以利用该 profile 来接入运营商的网络。当 Profile 处于激活状态时，eUICC 的功能和传统的 UICC 相同，可用于接入相应的移动网络运营商的网络。设备中还包括 LPA（Local Profile Assistant，本地文件助手），用于对 eUICC 中的 profile 进行管理，例如下载其他新的 profile，激活已下载 profile，去激活 profile，删除 profile 等。

目前设备只能通过 LPA 对 eUICC 中的 profile 进行下载。

发明内容

本发明的实施例提供一种签约数据集的下载方法、设备及服务器，利用当前 eUICC 的系统架构和访问控制机制，使设备上的应用能够触发 LPA 下载签约数据集，并发送到 eUICC。

根据本发明一方面提供的一种签约数据集下载的方法，所述方法由签约管理服务器执行，其中，所述方法包括：首先，签约管理服务器接收运营商服务器发送的下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；然后，签约管理服务器根据所述下载预订请求向所述运营商服务器返回下载预订响应消息；接着，签约管理服务器接收设备发送的认证请求，所述认证请求包括所述设备中发起签约数据集下载的应用的信息，比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用；在验证通过后，签约管理服务器为所述设备下载所述签约数据集。

结合本发明第一方面第一实施例的描述，在第二实施例中，所述认证信

息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书或所述证书的哈希值。

结合本发明第一方面第二实施例的描述，在第三实施例中，所述的比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤包括：

比较所述运营商服务器允许发起签约数据集下载的应用的证书与所述设备中发起签约数据集下载的应用的证书是否一致，或比较所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值与所述设备中发起签约数据集下载的应用的证书的哈希值是否一致。

结合本发明第一方面第二实施例或第三实施例的描述，在第四实施例中，所述认证信息还包括所述运营商服务器允许发起签约数据集下载的应用的包名；所述设备中发起签约数据集下载的应用的信息还包括所述设备中发起签约数据集下载的应用的包名。

结合本发明第一方面第四实施例的描述，在第五实施例中，所述的比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤还包括：

比较所述运营商服务器允许发起签约数据集下载的应用的包名与所述设备中发起签约数据集下载的应用的包名是否一致。

结合本发明第一方面第一实施例至第五实施例中任一项的描述，在第六实施例中，所述签约管理服务器包括签约管理数据准备设备和签约管理发现服务设备，所述方法还包括：所述签约管理数据准备设备根据所述下载预订请求，向所述签约管理发现服务设备发送注册事件请求，所述注册事件请求包括所述认证信息；所述签约管理发现服务设备接收到所述设备发送的获取事件请求，所述获取事件请求包括所述设备中发起签约数据集下载的应用的信息；所述签约管理发现服务设备比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用；在验证通过后，则所述签约管理发现服务设备向所述设备返回事件记录。

结合本发明第一方面第一实施例至第六实施例中任一项的描述，在第七实施例中，所述下载预订请求还包括所述运营商服务器从所述设备获取的EID信息，所述EID信息为所述设备中eUICC的ID信息，所述认证请求还包括所述EID，所述下载预订响应消息包括签约管理服务器地址和查询ID，所述查询ID为下载预订请求匹配ID或事件ID。

根据本发明第二方面提供的一种提供签约数据集下载的方法，所述方法由运营商服务器执行，其中，所述方法包括：首先，运营商服务器向签约管理服务器发送下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；然后，运营商服务器接收所述签约管理服务根据所述下载预订请求所返回的下载预订响应消息；接着，运营商服务器根据所述下载预订响应消息，向所述设备发送触发下载消息。

结合本发明第二方面第一实施例的描述，在第二实施例中，在发送所述下载预订请求之前，所述方法还包括：基于所述下载请求向所述设备发送获

取终端信息请求；接收所述设备返回的终端信息响应消息。

根据本发明第三方面提供的一种进行签约数据集下载的方法，所述方法由设备执行，其中，所述设备中包括 eUICC， LPA 和应用，所述方法包括：所述应用触发所述 LPA 发起签约数据集下载；所述 LPA 向签约管理服务器发送认证请求，以使所述签约管理服务器利用所述运营商服务器所允许发起签约数据集下载的应用的认证信息，验证所述触发所述 LPA 发起签约数据集下载的应用，其中，所述认证请求包括所述设备中发起签约数据集下载的应用的信息；在所述签约管理服务器验证通过后，所述 LPA 下载所述签约数据集并发送至所述 eUICC。

结合本发明第三方面第一实施例的描述，在第二实施例中，所述应用触发所述 LPA 发起签约数据集下载的步骤包括：

接收所述运营商服务器发送的触发下载消息，并发送至所述 LPA，以触发所述 LPA 发起签约数据集下载。

结合本发明第三方面第一实施例或第二实施例的描述，在第三实施例中，在所述应用触发所述 LPA 发起签约数据集下载之前，所述方法还包括：所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；所述 LPA 或所述 eUICC 对所述应用进行验证；在验证通过后，所述应用生成所述终端信息响应消息，并发送至所述运营商服务器，以使所述运营商服务器向所述签约管理服务器发送下载预订请求。

结合本发明第三方面第一实施例至第三实施例中任一项的描述，在第四实施例中，所述 LPA 或所述 eUICC 对所述应用进行验证的步骤包括：所述 LPA 获取所述应用的证书并发送至所述 eUICC，所述 eUICC 根据预置的证书认证信息验证验证所述应用；或所述 LPA 获取所述应用的证书，并根据根据预置的证书认证信息验证所述应用。

结合本发明第三方面第一实施例至第四实施例中任一项的描述，在第五实施例中，所述应用触发所述 LPA 发起签约数据集下载之后，所述方法还包括：所述 LPA 向所述签约管理服务器发送获取事件请求，以使所述签约管理服务器验证所述发起签约数据集下载的应用并返回事件记录；所述 LPA 接收所述签约管理服务器返回的所述事件记录，所述事件记录用于，所述 LPA 根据所述事件记录向签约管理服务器发送认证请求。

根据本发明第四方面提供的一种在设备上进行签约数据集下载的方法，其中，所述设备具有 eUICC、LPA 和应用，所述方法包括：所述 eUICC 从签名管理服务器下载第一签约数据集，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；所述应用触发所述 LPA 发起签约数据集下载；所述 LPA 或所述 eUICC 利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；在验证通过后，所述 LPA 从所述签名管理服务器下载第二签约数据集，并发送至所述 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

结合本发明第四方面第一实施例的描述，在第二实施例中，所述 LPA 或所述 eUICC 利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用的步骤包括：所述 LPA 从所述 eUICC 中获取所述第一签约数据集的所述认证信息；所述 LPA 获取发起签约数据集下载的应用的信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

结合本发明第四方面第一实施例的描述，在第三实施例中，其中，所述 LPA 或所述 eUICC 利用所述第一签约数据集中所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用的步骤包括：所述 LPA 获取发起签约数据集下载的应用的信息并发送至所述 eUICC；所述 eUICC 从所述第一签约数据集的元数据信息获取所述认证信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的所述应用的信息，以验证所述发起签约数据集下载的应用。

结合本发明第四方面第二实施例或第三实施例的描述，在第四实施例中，所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；触发所述 LPA 发起签约数据集下载的所述应用的信息包括触发所述 LPA 发起签约数据集下载的所述应用的证书或所述证书的哈希值。

结合本发明第四方面第一实施例至第四实施例中任一项的描述，在第五实施例中，在所述应用触发所述 LPA 发起签约数据集下载之前，所述方法还包括：所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；所述 LPA 或所述 eUICC 对所述应用进行验证；在验证通过后，所述应用生成终端信息响应消息，并发送至所述运营商服务器。

结合本发明第四方面第五实施例的描述，在第六实施例中，所述 LPA 或所述 eUICC 对所述应用进行验证的步骤包括：所述 LPA 获取所述应用的证书并发送至所述 eUICC，所述 eUICC 根据预置的证书认证信息验证所述应用；或所述 LPA 获取所述应用的证书，并根据预置的证书认证信息验证所述应用。

结合本发明第四方面第五实施例或第六实施例的描述，在第七实施例中，所述 LPA 或所述 eUICC 对所述应用进行验证的步骤还包括：所述 LPA 基于所述获取终端信息请求，验证从所述 eUICC 获取的 EID 与所述获取终端信息请求中的 EID 是否相同，其中，所述 EID 为所述 eUICC 的 ID 信息。

结合本发明第五方面提供的一种在设备上进行签约数据集下载的方法，其中，所述设备具有第一 eUICC、第二 eUICC、LPA 和应用，所述方法包括：所述第一 eUICC 从签名管理服务器下载第一签约数据集，其中，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；所述应用触发所述 LPA 发起签约数据集下载；所述 LPA 或所述第一 eUICC 根据所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；在验证通过后，所述 LPA 从所述签名管理设备下载第二签约数据

集并发送至所述第二 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

结合本发明第五方面第一实施例的描述，在第二实施例中，在所述应用触发所述 LPA 发起签约数据集下载之前，所述方法还包括：所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；所述 LPA 或所述第一 eUICC 对所述应用进行验证；在验证通过后，所述应用从所述第二 eUICC 获取第二 eUICC 信息，并根据所述第二 eUICC 信息生成终端信息响应消息，并发送至所述运营商服务器。

结合本发明第五方面第二实施例的描述，在第三实施例中，所述方法还包括：所述 LPA 获取所述获取终端信息请求后，向所述设备的显示界面发送选择信息，以在所述显示界面显示供用户选择下载所述第二签约数据集的所述第二 eUICC。

根据本发明第六方面提供的一种提供签约数据集下载的签约管理服务器，其中，所述签约管理服务器包括：一个或多个处理器；存储器；所述存储器，用于存储计算机程序；所述处理器，用于运行所述计算机程序，执行下述流程：一个或多个处理器，所述处理器用于执行：接收运营商服务器发送的下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；根据所述下载预订请求向所述运营商服务器返回下载预订响应消息；接收设备发送的认证请求，所述认证请求包括所述设备中发起签约数据集下载的应用的信息，比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用；在验证通过后，为所述设备下载所述签约数据集。

结合本发明第六方面第二实施例的描述，在第三实施例中，所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书或所述证书的哈希值。

结合本发明第六方面第三实施例的描述，在第四实施例中，所述比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤包括：比较所述运营商服务器允许发起签约数据集下载的应用的证书与所述设备中发起签约数据集下载的应用的证书是否一致，或比较所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值与所述设备中发起签约数据集下载的应用的证书的哈希值是否一致。

结合本发明第六方面第三实施例或第四实施例的描述，在第五实施例中，所述认证信息还包括所述运营商服务器允许发起签约数据集下载的应用的包名；所述设备中发起签约数据集下载的应用的信息还包括所述设备中发起签约数据集下载的应用的包名。

结合本发明第六方面第五实施例的描述，在第六实施例中，所述的比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤还包括：比较所述运营商服务器允许发起签约数据集下载的应用的包名与所述设备中

发起签约数据集下载的应用的包名是否一致。

结合本发明第六方面第一实施例至第五实施例中任一项的描述，在第六实施例中，所述签约管理服务器包括签约管理数据准备设备和签约管理发现服务设备，其中，所述签约管理数据准备设备用于根据所述下载预订请求，向所述签约管理发现服务设备发送注册事件请求，所述注册事件请求包括所述认证信息；所述签约管理发现服务设备用于接收到所述设备发送的获取事件请求，并比较所述认证信息与所述获取事件请求中的所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用，在验证通过后，向所述设备返回事件记录。

根据本发明第七方面提供的一种提供签约数据集下载的运营商服务器，其中，所述运营商服务器包括：一个或多个处理器；存储器；所述存储器，用于存储计算机程序；所述处理器，用于运行所述计算机程序，执行下述流程：向签约管理服务器发送下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；接收所述签约管理服务根据所述下载预订请求所返回的下载预订响应消息；根据所述下载预订响应消息，向所述设备发送触发下载消息。

结合本发明第六方面第一实施例的描述，在第二实施例中，在发送所述下载预订请求之前，所述处理器还执行下述流程：基于所述下载请求向所述设备发送获取终端信息请求；接收所述设备返回的终端信息响应消息。

根据本发明第八方面提供的一种进行签约数据集下载的设备，其中，所述设备中包括：eUICC、LPA 和应用，其中，所述应用用于触发所述 LPA 发起签约数据集下载；所述 LPA 用于向签约管理服务器发送认证请求，以使所述签约管理服务器利用所述运营商服务器所允许发起签约数据集下载的应用的认证信息，验证所述触发所述 LPA 发起签约数据集下载的应用，其中，所述认证请求包括所述设备中发起签约数据集下载的应用的信息，并在所述签约管理服务器验证通过后，从所述签约管理服务器下载所述签约数据集并发送至所述 eUICC。

结合本发明第八方面第一实施例的描述，在第二实施例中，所述 LPA 用于接收所述运营商服务器发送的触发下载消息，并发送至所述 LPA，以触发所述 LPA 发起签约数据集下载。

结合本发明第八方面第一实施例或第二实施例的描述，在第三实施例中，所述应用还用于在触发所述 LPA 发起签约数据集下载之前，向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA，并在所述 LPA 或所述 eUICC 对所述应用进行验证通过后，生成所述终端信息响应消息，并发送至所述运营商服务器，以使所述运营商服务器向所述签约管理服务器发送下载预订请求；所述 LPA 用于对所述应用进行验证，或所述 eUICC 用于对所述应用进行验证。

结合本发明第八方面第三实施例的描述，在第四实施例中，所述 LPA 用于获取所述应用的证书并发送至所述 eUICC；所述 eUICC 用于根据预置的证

书认证信息验证所述应用。

结合本发明第八方面第三实施例的描述，在第五实施例中，所述 LPA 用于获取所述应用的证书，并根据预置的证书认证信息验证所述应用。

结合本发明第八方面第三实施例至第五实施例中任一项的描述，在第六实施例中，所述 LPA 用于在所述应用触发所述 LPA 发起签约数据集下载之后，向所述签约管理服务器发送获取事件请求，以使所述签约管理服务器验证所述发起签约数据集下载的应用并返回事件记录，并接收所述签约管理服务器返回的所述事件记录，其中，所述事件记录用于所述 LPA 根据所述事件记录向签约管理服务器发送认证请求。

根据本发明第九方面提供的一种在设备上进行签约数据集下载的设备，其中，所述设备具有 eUICC、LPA 和应用，其中，所述 eUICC 用于从签名管理服务器下载第一签约数据集，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；所述应用用于触发所述 LPA 发起签约数据集下载；所述 LPA 用于利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用，或所述 eUICC 用于利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；所述 LPA 还用于在验证通过后，从所述签名管理服务器下载第二签约数据集，并发送至所述 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

结合本发明第九方面第一实施例的描述，在第二实施例中，所述 LPA 用于从所述 eUICC 中获取所述第一签约数据集的所述认证信息，获取发起签约数据集下载的应用的信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

结合本发明第九方面第二实施例的描述，在第三实施例中，所述 LPA 用于获取发起签约数据集下载的应用的信息并发送至所述 eUICC；所述 eUICC 用于从所述第一签约数据集的元数据信息获取所述认证信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的所述应用的信息，以验证所述发起签约数据集下载的应用。

结合本发明第九方面第二实施例或第三实施例的描述，在第四实施例中，所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；触发所述 LPA 发起签约数据集下载的所述应用的信息包括触发所述 LPA 发起签约数据集下载的所述应用的证书或所述证书的哈希值。

结合本发明第九方面第一实施例或第四实施例的描述，在第五实施例中，所述应用用于向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；所述 LPA 用于对所述应用进行验证，或所述 eUICC 用于对所述应用进行验证；所述应用用于在验证通过后，生成终端信息响应消息，并发送至所述运营商服务器。

结合本发明第九方面第五实施例的描述，在第六实施例中，所述 LPA 用于获取所述应用的证书并发送至所述 eUICC；所述 eUICC 用于根据预置的证

书认证信息验证所述应用。

结合本发明第九方面第五实施例的描述，在第七实施例中，所述 LPA 用于获取所述应用的证书，并根据预置的证书认证信息验证所述应用。

结合本发明第九方面第六实施例或第七实施例的描述，在第八实施例中，所述 LPA 还用于基于所述获取终端信息请求，验证从所述 eUICC 获取的 EID 与所述获取终端信息请求中的 EID 是否相同，其中，所述 EID 为所述 eUICC 的 ID 信息。

根据本发明第十方面提供的一种进行签约数据集下载的设备，其中，所述设备具有第一 eUICC、第二 eUICC、LPA 和应用，所述第一 eUICC 用于从签名管理服务器下载第一签约数据集，其中，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；所述应用用于触发所述 LPA 发起签约数据集下载；所述 LPA 用于根据所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用，或所述第一 eUICC 用于根据所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；所述 LPA 还用于在验证通过后，从所述签名管理设备下载第二签约数据集并发送至所述第二 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

结合本发明第十方面第一实施例的描述，在第二实施例中，在所述应用触发所述 LPA 发起签约数据集下载之前，向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；所述 LPA 用于对所述应用进行验证，或所述第一 eUICC 对所述应用进行验证；所述应用还用于在验证通过后，从所述第二 eUICC 获取第二 eUICC 信息，并根据所述第二 eUICC 信息生成终端信息响应消息，并发送至所述运营商服务器。

结合本发明第十方面第一实施例或第二实施例的描述，在第三实施例中，所述 LPA 还用于获取所述获取终端信息请求后，向所述设备的显示界面发送选择信息，以在所述显示界面显示供用户选择下载所述第二签约数据集的所述第二 eUICC。

根据本发明第十一方面提供的一种在系统中实现签约数据集下载的方法，所述系统包括签约管理服务器、运营商服务器和设备，其中：所述设备中应用向运营商服务器发送下载请求；所述运营商服务器向签约管理服务器发送下载预订请求，其中，所述下载预订请求中具有所述运营商服务器所存储的设备中应用的访问控制信息；所述签约管理服务器处理所述下载预订请求，并向所述运营商服务器返回响应消息；所述运营商服务器基于所述响应消息，向所述设备发送触发下载消息；所述设备中 LPA 向所述签约管理服务器发送认证请求；所述签约管理服务器利用所述访问控制信息所述访问控制信息，验证发起下载请求的所述应用的的访问权限；在验证通过后，所述设备下载签约数据集。

根据本发明第十二方面提供的一种实现签约数据集下载的系统，所述系统包括签约管理服务器、运营商服务器和设备，其中，所述签约管理服务器

用于：接收运营商服务器发送的下载预订请求，其中，所述下载预订请求中包括发起下载请求的设备中应用的访问控制信息；处理所述下载预订请求，并向所述运营商服务器返回下载预订响应消息，以触发下载；当接收到所述设备发送的认证请求时，利用所述访问控制信息，验证发起下载请求的所述应用的访问权限；在验证通过后，为所述设备下载签约数据集；所述运营商服务器用于：接收设备发送的下载请求；向签约管理服务器发送下载预订请求，其中，所述下载预订请求中具有所述运营商服务器所存储的设备中应用的访问控制信息；接收所述签约管理服务基于处理所述下载预订请求所返回的响应消息；基于所述响应消息，向所述设备发送触发下载消息，以触发下载；所述设备包括应用、LPA 和 eUICC，所述设备用于：所述应用向运营商服务器发送下载请求，以使所述运营商服务器向签约管理服务器发送下载预订请求，其中，所述下载预订请求中具有所述运营商服务器所存储的设备中应用的访问控制信息；所述应用接收所述运营商服务器发送的触发下载消息，并触发所述 LPA 进行下载；所述 LPA 向签约管理服务器发送认证请求，以在所述签约管理服务器利用所述访问控制信息，验证发起下载请求的所述应用的访问权限；在验证通过后，所述 LPA 下载签约数据集，并发送至所述 eUICC。

综上所述，通过本实施例，本发明实施例提供了一种实现签约数据集下载的方法、设备及服务器，在所述方法中，设备中应用触发签约数据集下载时，运营商服务器会将允许发起签约数据集下载的应用的认证信息发送给签约管理服务设备，当设备请求通过发送认证信息时，所述签约管理服务设备会利用所述认证信息对所述设备中发起签约数据集下载的应用进行验证，在验证通过后，为所述设备提供签约数据集下载。在另一实施例中，签约管理服务设备可以将所述认证信息随前次下载的签约数据集发送至设备中，再次下载不同的签约数据集时，所述设备可以利用前次下载的签约数据集中的认证信息验证所述应用，从而利用当前 eUICC 的系统架构和访问控制机制，使设备上的应用能够触发 LPA 下载签约数据集，并发送到 eUICC。

附图说明

图 1 为本发明实施例提供的 eUICC 的远程管理系统的架构图；

图 2~图 8 为本发明一些实施例提供的签约数据集的下载方法的流程示意图；

图 9 为本发明实施例提供的设备的结构框图；

图 10 为本发明实施例提供的第一签约管理服务器的结构框图；

图 11 为本发明实施例提供的第二签约管理服务器的结构框图。

具体实施方式

现有的 SIM 卡或 UICC 卡一般是由 MNO（mobile network operator，移动

网络运营商）集中向卡商订购，所以在卡出厂前就已经将接入运营商网络所需的网络接入应用及数据下载到卡中，如：USIM（Universal Subscriber Identity Module，通用用户识别模块）、IMSI（International Mobile Subscriber Identity，国际移动用户识别码）、KI（Key Identity，个人身份鉴权键）等。这样，用户购买 SIM 卡或 UICC 卡后插入设备（device）即可接入运营商的网络。

不同于 UICC 卡，eUICC 一般是将 UICC 卡嵌入在设备中。对于 eUICC，并不一定是由运营商向卡商采购，也可能是由设备制造商采购后集成在设备。所以 eUICC 在出厂后可能并不包含有可以接入运营商网络的数据，需要远程下载这些数据，如：签约数据集（profile，即配置到 eUICC 中用来提供服务的数据和应用程序的集合），之后才能根据这些数据接入运营商网络。

为实现通过安装于设备中的应用（如由运营商提供的安装于手机上的应用，即 MNO APP，或第三方应用）下载 profile，本发明实施例提供如下两种技术方案。

一、或者 MNO portal 通过其他途径接收到触发下载信息（例如运营商服务设备接收到的用户通过客服电话或其他途径提供的）后，MNO portal 向 SM-DP+发送 profile 下载请求时，将 MNO APP 对 LPA API/eUICC/profile 的访问控制信息，即对 APP 的认证信息，携带在下载请求中发送给 SM-DP+，并且若 SM-DP+在 SM-DS 注册 profile 下载事件时，将 MNO APP 对 LPA API/eUICC/profile 的访问控制信息，携带在注册事件请求中发送给 SM-DS，当设备向 SM-DP+发送身份认证请求或向 SM-DS 发送获取事件请求（所述获取事件请求也可以是通过一个身份认证请求，如通过发送认证客户端（AuthenticateClient）消息，请求验证并从 SM-DS 获取事件记录）时，由 SM-DP+/SM-DS 验证 MNO APP 的访问权限，并在权限认证通过后，下载 profile。

二、设备对 MNO APP 的访问控制依赖于当前设备上已经下载的该运营商的 profile，即 MNO 将 MNO APP 对 LPA API/eUICC/Profile 的访问控制信息，设置到 profile metadata 中，随 profile 一起下载到 eUICC 中，当 MNO APP 调用 LPA API 下载新的 profile 时，由 LPA 或 eUICC 来验证利用已有的同一个运营商的 profile 中的 APP 的访问权限来进行访问控制。

首先，对本发明实施例涉及的系统、术语等作以下介绍：

一、如图 1 所示，是本发明实施例提供一种 eUICC 的远程管理系统的架构图。参考图 1，该系统包括 SM-DP+（Subscription Manager Data Preparation+，签约管理-数据准备）服务器、SM-DS（Subscription Manager-Discovery Server，签约管理-发现服务器）、运营商服务器（Operator），卡商（EUM），证书发布中心 CI（Certificate Issuer）和设备（Device）。

另外，对各个实体之间的接口作以介绍：ES6 是 eUICC 与运营商之间的接口，ES2+是是运营商和 SM-DP+之间的接口；ES8+是 eUICC 与 SM-DP+之间的接口； ES11 是设备的 LDS(local discovery service，本地发现服务)与 SM-DS 之间的接口；ES12 是 SM-DS 与 SM- DP+之间的接口；ES10a 是 LDS

与 eUICC 之间的接口；ES10c 是 LUI（local user interface，本地用户接口）与 eUICC；ESci 是 EUM 与 CI 之间的接口，或 CI 与 SM-DP+之间的接口；ESeum 是 EUM 与 eUICC 之间的接口；ESo 是用户（End User）与运营商交互的接口；ESeu 为 End User 与 LUI 之间的接口；ES9+为 SM-DP+与 LPD（local profile download，本地文件下载）之间的接口、ES10b 为 LPD 与 eUICC 之间的接口。

其中，SM-DP+的功能包括签约数据集（profile）的生成、签约数据集的保护（如：加密）、签约数据集的存储，签约数据集的绑定（如：将 profile 与 Event（事件）ID 绑定）、签约数据集的发送，远程签约数据集的管理，SM-DS 事件注册等。SM-DS 主要负责接受 SM-DP+发送的事件（Event）注册，并将事件发送给设备。事件包括签约数据集下载事件或签约数据集管理事件。设备根据签约数据集下载事件从 SM-DP+中下载签约数据集

根据运营商部署情况，在一些实施例中，签约管理服务器仅包括 SM-DP+，在一些实施例中，签约管理服务器包括至少一个 SM-DP+和至少一个 SM-DS，所述 SM-DP+和 SM-DS 可以是由运营商部署的，在一些实施例中，所述 SM-DP+为运营商部署的，所述 SM-DS 由一个统一的机构部署，例如运营商的一个组织。

进一步地，参考图 1，设备中有 LPA 和 eUICC，LPA 中包括 LDS，LPD 和 LUI。具体实现中，设备的 LDS 向 SM-DS 查询事件，LPD 负责下载签约数据集，即 LPD 通过 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议）安全链接从 SM-DP+下载 profile 到 LPD 中，然后通过本地 APDU 命令将下载下来的签约数据集再发送到 eUICC 中。这里的签约数据集是指文件结构、数据和应用程序等的集合，可以包括一个或多个网络接入应用及相应的网络接入信任状。需要说明的是，本发明实施例中，签约数据集是一个统称，包括安装到设备的 eUICC 上的签约数据集以及在 SM-DP+存储的 profile package。

另外，设备的 LUI 提供和用户的交互逻辑和界面，用户可以通过 LUI 来完成对 profile 的管理，如下载新的 profile，激活 profile，去激活 profile，删除 profile 等。

图 2~图 8 为本发明一些实施例提供的签约数据集的下载方法的流程示意，在各附图的信号流示意中，所传递的信息携带的参数，若采用“[]”括起的参数（例如图 2 中，步骤 8 终端信息响应的消息时传递的 “[device info]”），表示该参数为可选参数，具体请参见各实施例描述。

结合以上，根据本发明实施例提供的一种在签约管理服务器上提供签约数据集下载的方法，其中，所述方法包括步骤 101~步骤 104。

在步骤 101 中，签约管理服务器接收运营商服务器发送的下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

所述下载预订请求(profile order, 为 download order 和 confirm order 等 profile 预定请求的统称)可以是所述运营商服务器基于设备中应用发起的下

载请求发送的；也可以是基于从其他途径接收到的触发下载信息（例如运营商服务器接收到的用户通过客服电话或其他途径提供的）发送的；也可以是，在所述运营服务器向所述应用发送获取终端信息的请求之后，所述运营商服务器基于接收到的所述应用返回的终端信息响应的消息发送的。

所述下载预订请求中包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息。

在一些实施例中，所述认证信息可以包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值。所述认证信息可以是所述运营商服务器预先存储的，也可以是所述运营商服务器从其他认证的设备中获取。相比直接发送所述证书，所述证书的哈希值的数据量小，更方便发送。在一些实施例中，所述认证信息还可以包括所述运营商服务器允许发起签约数据集下载的应用的包名。

所述下载预订请求还可包括 eUICC 提供的 EID(eUICC 的 ID 信息)，用于在签约管理服务器中进行事件注册时，将 EID 与对应签约数据集绑定，还可以还可以将事件注册时的事件记录和 EID 相对应。

所述下载预订请求还可选择性地包括所述运营商服务器允许发起签约数据集下载的应用的包名。此外，所述下载预订请求还可选择性地包括用于计算签名证书哈希值的哈希函数(hash algorithm)，所述下载预订请求中的应用的签名证书或签名证书的哈希值、可选的应用的包名和哈希函数可以是预先配置于所述运营服务器上的，也可以是运营商服务器从与运营商服务器相关能够提供访问控制信息的服务器上获取的。

如果需要将下载事件注册到所述运营商服务器的 SM-DS，所述下载预订请求还可包括运营商服务器提供的 SM-DS 地址。在步骤 102 中，根据所述下载预订请求向所述运营商服务器返回下载预订响应消息；其中，所述下载预订响应消息包括签约管理服务器地址和查询 ID，所述查询 ID 为下载预订请求匹配 ID 或事件 ID。

在一些实施例中，所述签约管理服务器包括 SM-DP+（签约管理数据准备设备），所述 SM-DP+根据所述下载预订请求，生成相应的签约数据集（profile），并返回下载预订响应消息，所述下载预订响应消息包括 SM-DP+的地址和下载预订请求匹配 ID(matchingID)，随后，所述签约管理服务器向所述运营商服务器返回下载预订响应消息，所述下载预订响应消息中包括 SM-DP+的地址和下载预订请求匹配 ID。

在一些实施例中，所述签约管理服务器包括 SM-DP+（签约管理数据准备设备）和 SM-DS（签约管理发现服务设备）时，所述步骤 102 中，所述签约管理数据准备设备根据所述下载预订请求，向所述签约管理发现服务设备发送注册事件请求，以注册事件，所述注册事件请求包括所述认证信息。所述 SM-DP+根据所述下载预订请求，生成事件 ID(eventID)，并向 SM-DS 发送注册事件请求，所述注册事件请求包括所述认证信息（例如所述运营商服务器所允许发起签约数据集下载的应用的证书及证书的哈希值），所述注册事件请

求还可包括：事件 ID、如所述下载预订请求包括所述 EID、所述哈希函数及所述允许发起签约数据集下载的应用的包名，则所述注册事件请求还包括从所述下载预定请求中获取的所述 EID、所述哈希函数及所述允许发起签约数据集下载的应用的包名。在注册事件之后，所述签约管理服务器向所述运营商服务器返回下载预定响应消息，所述下载预定响应消息中包括所述签约管理服务器中 SM-DS 的地址和事件 ID 或下载预订请求匹配 ID。

在一些实施例中，所述签约管理服务器包括 SM-DP+和 SM-DS，所述签约管理服务器已注册事件，则在发送认证请求之前，所述设备会向所述 SM-DS 发送获取事件请求，所述 SM-DS 根据所述获取事件请求进行验证并在验证通过后返回事件记录。

具体地，所述方法还包括步骤 105、步骤 106 和步骤 107；

在所述步骤 105 中，所述签约管理发现服务设备接收所述设备发送的获取事件请求。

所述获取事件请求包括所述设备中发起签约数据集下载的应用的信息；其中，所述设备中发起签约数据集下载的应用的信息可以包括所述设备中发起签约数据集下载的应用的证书或所述证书的哈希值，所述设备中发起签约数据集下载的应用的信息还可以包括所述设备中发起签约数据集下载的应用的包名。

所述获取事件请求还可以包括从所述设备中获取的所述 EID；当所述下载预定响应消息包括所述事件 ID，则所述获取事件请求还可以包括所述事件 ID；当所述下载预定响应消息包括下载预订请求匹配 ID，则所述获取事件请求还可以包括所述下载预订请求匹配 ID 或与所述下载预订请求匹配 ID 相同或相对应的所述事件 ID。此外，所述获取事件请求还可包括所述设备中发起签约数据集下载的应用的包名。

在一些实施例中，所述获取事件请求也可以是通过一个身份认证请求，例如，通过发送认证客户端请求（AuthenticateClient），以请求验证并从 SM-DS 获取事件记录。

然后，所述签约管理发现服务设备从所述获取事件请求中获取所述设备中发起签约数据集下载的应用的信息，从所述获取事件请求中的所述 EID、所述事件 ID 或所述下载预订请求匹配 ID 查找相应的所述注册事件请求，从所述事件中获取所述认证信息。

接着，在所述步骤 106 中，所述签约管理发现服务设备验证所述应用，当所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书，所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书，所述签约管理发现服务设备比较所述运营商服务器允许发起签约数据集下载的应用的证书和所述设备中发起签约数据集下载的应用的证书；或当所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值，所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书的哈希值，所述签约管

理发现服务设备比较所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值和所述设备中发起签约数据集下载的应用的证书的哈希值；或当所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值，所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书，所述签约管理发现服务设备利用所述哈希函数计算所述设备中发起签约数据集下载的应用的证书的哈希值，比较所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值和所述设备中发起签约数据集下载的应用的证书的哈希值。

当所述认证信息还包括所述运营商服务器允许发起签约数据集下载的应用的包名，所述设备中发起签约数据集下载的应用的信息还包括所述设备中发起签约数据集下载的应用的包名，所述签约管理发现服务设备还可以通过比较所述运营商服务器允许发起签约数据集下载的应用的包名和所述设备中发起签约数据集下载的应用的包名，进一步验证所述应用。

在所述步骤 106 中，所述签约管理发现服务设备比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

接着，在所述步骤 107 中，在验证通过后，则所述签约管理发现服务设备向所述设备返回事件记录。

其中，所述事件记录包括 SM-DP+的地址和下载预订请求匹配 ID。其中，所述的下载预订请求匹配 ID 可以和所述事件 ID 可以相同。

接着，在步骤 103 中，所述签约管理服务器接收设备发送的认证请求，从所述认证请求中获取所述设备中发起签约数据集下载的应用的信息，比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

所述设备向所述签约管理服务器发送认证请求，以发起下载，所述认证请求(即认证客户端的请求)包括所述设备中发起签约数据集下载的应用的信息，其中，所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书或证书的哈希值，可参考前述实施例中所述步骤 105，为简明起见，不再追溯。

所述认证请求还包括下载预订响应消息中的下载预订请求匹配ID或所述事件记录中的下载预订请求匹配 ID（有注册下载事件时选择），从所述设备中获取的 EID，所述认证请求还可选择性地包括还可包括从设备中获取的应用的包名。

在一些实施例中，当所述签约管理服务器接收到所述设备发送的认证请求时，所述签约管理服务器从所述认证请求中获取所述设备中发起签约数据集下载的应用的信息；根据所述下载预订请求匹配 ID 查找对应的所述下载预订请求，获取所述下载预订请求中的所述认证信息；比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，包括比较证书或证书的哈希值，还可以包括比较应用的包名，来验证所述发起签约数据集下载的应用，其验证过程参考前述实施例中所述步骤 106 中的比较过程，为简明起见，不再追溯。

在步骤 104 中，在所述步骤 103 的验证通过后，所述签约管理服务器为所述设备下载所述签约数据集。在一些实施例中，由所述签约管理服务器中SM-DP+来准备所述签约数据集，在所述步骤 103 的验证通过后，允许所述设备下载。

根据本发明实施例提供的一种在运营商服务器上提供签约数据集下载的方法，其中，所述方法包括步骤 201~步骤 204。

在步骤 201 中，所述运营商服务器向签约管理服务器发送下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息。

所述下载预订请求和所述认证信息参考前述实施例中步骤 101、步骤 102、步骤 103、步骤 105 的描述，为简明起见，不再赘述。

在一些实施例中，在步骤 201 之前，所述方法还包括步骤 205 和步骤 206。

在步骤 205 中，所述运营商服务器基于所述下载请求向所述设备发送获取终端信息请求。

在步骤 206 中，所述运营商服务器接收所述设备返回的终端信息响应消息。

所述终端信息响应消息包括 eUICC 信息(eUICC info)，可选地还包括 EID、设备信息(device info)，所述运营商服务器会根据终端信息响应消息生成相应的下载预订请求。

所述 eUICC 信息可以包括 profile 包版本(Profile Package Version)，协议版本号(SVN: Specification Version Number)，固件版本(Firmware version)，可用的非易失性存储空间(Available amount of non-volatile memory)，UICC 能力(UICC capabilities)，支持的 Java 卡版本(Java card version)，支持的 GlobalPlatform 卡协议版本(GlobalPlatform version)，RSP 能力(RSP capabilities)等。

所述设备信息可以包括：终端类型分配码(Device type allocation code)，终端能力(The Device SHALL set all the capabilities it supports)，无线接入技术以及支持的版本(Radio access technologies, including release)，非接触式通信能力（Contactless），可选的 RSP 特性，国际移动设备身份码(IMEI)等。

所述运营商服务器根据 eUICC info 来判断应该向 SM-DP+预定的 profile 的类型（profile type），例如，根据 eUICC info 中协议版本号、eUICC 能力等，确定需要预订的 profile 的类型，如果所述终端信息响应消息有 device info，可利用 device info 进行判断向 SM-DP+预定的 profile 的类型，例如根据 device info 中的无线接入能力，确定需要预订的 profile 的类型，device info 能够帮助预订类型更准确的 profile。

在所述步骤 202 中，所述运营商服务器接收所述签约管理服务根据所述下载预订请求所返回的下载预订响应消息；

所述下载预订响应消息参考前述实施例中步骤 102、步骤 103、步骤 105 的描述，为简明起见，不再赘述。

在步骤 204 中，运营商服务器基于所述下载预订响应消息，向所述设备发送触发下载消息。

所述触发下载消息包括 SM-DP+的地址或 SM-DS 的地址，以及下载预订请求匹配 ID(matchingID)或事件 ID(eventID)。

在一些实施例中，所述签约管理服务器包括 SM-DP+，所述触发下载消息包括 SM-DP+的地址和下载预订请求匹配 ID。

在一些实施例中，所述签约管理服务器包括 SM-DP+和 SM-DS，所述触发下载消息包括 SM-DS 的地址和事件 ID。

所述下载预订请求匹配 ID 和事件 ID 参考前述实施例中步骤 102、步骤 103、步骤 105、步骤 106 的描述，为简明起见，不再赘述。

根据本发明实施例提供的一种在设备上进行签约数据集下载的方法，其中，所述设备中具有 eUICC， LPA 和应用，所述方法包括步骤 301~步骤 303。

其中，在所述步骤 301 中，所述应用触发所述 LPA 发起签约数据集下载。

在一些实施例中，在所述步骤 301 中，所述应用在接收所述运营商服务器发送的触发下载消息，并发送至所述 LPA，以此触发所述 LPA 发起签约数据集下载。

所述触发下载消息参考前述实施例中步骤 204 的描述，为简明起见，不再赘述。

在一些实施例中，所述应用可以不发送下载请求，由所述运营商服务器从其他渠道获取相关请求信息，在所述应用根据用户信息登录到所述运营商服务器后，所述运营商服务器主动发送获取终端信息请求，并基于获取的终端信息响应消息准备相应所述签约数据集。

在一些实施例中，所述设备会由所述应用向所述运营商服务器发送下载请求，并接收所述运营商服务器发送的获取终端信息请求，然后，由所述 LPA 或所述 eUICC 对应用的进行身份验证，例如验证所述应用的签名证书根证书的信息，例如应用的证书的证书链的根证书是否为 GSMA CI 证书，在验证通过之后，返回终端信息响应消息。结合以上，在所述步骤 301 之前，所述方法还包括步骤 304~步骤 306。

在步骤 304 中，所述应用向所述运营商服务器发送下载请求，并接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA。

在步骤 305 中，所述 LPA 或所述 eUICC 对所述应用进行验证。

在所述步骤 305 中，可以由所述 LPA 进行验证，具体地，所述 LPA 获取所述应用的证书并发送至所述 eUICC，所述 eUICC 根据预置的证书认证信息验证所述应用；或

也可以由所述 LPA 进行验证，具体地，所述 LPA 获取所述应用的证书，

并根据预置的证书认证信息验证所述应用。

其中，所述 LPA 可从 device OS（终端上的操作系统，例如 IOS 系统，安卓系统等）获取应用的证书，验证证书的根证书信息，例如 LPA 可以从终端的操作系统中获取该证书以验证该证书的根证书是否为 GMSA CI 证书，即验证应用的证书是否为 GSMA CI 为运营商签发的合法证书。

在所述步骤 306 中，在所述步骤 305 验证通过后，所述应用生成所述终端信息响应消息，并发送至所述运营商服务器，以使所述运营商服务器向所述签约管理服务器发送下载预订请求。

在所述步骤 305 验证通过后，所述 LPA 从所述 eUICC 获取 eUICC 信息，并发送至所述应用，可选地，所述 LPA 还从所述 eUICC 获取 EID，所述 EID 可在后续步骤中发送终端信息响应消息时携带。

所述终端信息响应消息参考前述实施例步骤 206 的描述，为简明起见，不再赘述。

在一些实施例中，若所述签约管理服务器包括 SM-DP+和 SM-DS，所述签约管理服务器会注册下载事件，则在所述步骤 302 之前，所述方法还可选地包括步骤 307 和步骤 308。

在所述步骤 307 中，在向签约管理服务器发送认证请求的步骤之前，所述 LPA 向所述签约管理服务器发送获取事件请求，以使所述签约管理服务器验证所述发起签约数据集下载的应用并返回事件记录；在所述步骤 308 中，所述 LPA 接收所述签约管理服务器根据所述获取事件请求发送的事件记录，所述事件记录用于，所述 LPA 根据所述事件记录向签约管理服务器发送认证请求。

所述获取事件请求参考前述实施例中步骤 105 的描述，所述事件记录参考前述实施例中步骤 106 的描述，为简明起见，不再赘述。

然后，在所述步骤 302 中，所述 LPA 向签约管理服务器发送认证请求，以使所述签约管理服务器利用所述运营商服务器所允许发起签约数据集下载的应用的认证信息，验证所述应用，其中，所述认证请求包括所述设备中发起签约数据集下载的应用的信息。

接着，在步骤 303 中，所述 LPA 向签约管理服务器发送认证请求，以在所述签约管理服务器执行如前述实施例步骤 103 的查找对应所述下载预订请求，利用对应获取所述下载预订请求中的所述访问控制信息认证信息，利用所述运营商服务器所允许发起签约数据集下载的应用的认证信息验证触发所述 LPA 发起签约数据集下载的应用发起所述认证请求的所述设备中应用的访问权限通过之后，所述 LPA 下载签约数据集，并发送至所述 eUICC。

所述认证请求、所述认证信息、所述设备中发起签约数据集下载的应用的信息的描述参考前述实施例中所述步骤 101~所述步骤 104、及所述步骤 105~所述步骤 107 的描述，为简明起见，不再赘述。

然后，在所述步骤 303 中，在所述签约管理服务器验证通过后，所述 LPA 下载所述签约数据集并发送至所述 eUICC。

根据本发明一实施例提供的一种在设备上进行签约数据集下载的方法，所述方法由设备执行，所述设备可以是终端，其中，所述设备具有 eUICC、LPA 和应用，在本实施例中，所述设备在已有一张从签约管理服务器下载的签约数据集情况下，再次从所述签约管理服务器下载新的签约数据集时，可以从前一已下载的签约数据集的元数据信息获取认证信息，并在设备一侧利用所述认证信息验证所述发起下载请求的应用。所述方法包括：步骤 401~步骤 404。

在所述步骤 401 中，所述 eUICC 从签名管理服务器下载第一签约数据集，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

在此，所述步骤 401 可以理解为，所述设备的 eUICC 已下载过一次签约数据集（即第一签约数据集），在下载过程中，运营商服务器将访问控制信息添加到了第一签约数据集的元数据信息，例如元数据（metadata）中。

其中，所述第一签约数据集信息还可包括用于计算应用签名证书的哈希值的哈希函数，还可包括 Allowed API(允许应用访问的接口)。

所述访问控制信息认证信息包括所述运营商服务器所允许发起签约数据集下载的应用所述设备中应用的签约证书或所述签约证书的哈希值，此外，所述认证信息还可包括所述运营商服务器所允许发起签约数据集下载的应用的包名。具体参考前述实施例中步骤 101、步骤 102、步骤 103、步骤 105 的描述，为简明起见，不再赘述。

在一些实施例中，在执行所述步骤 402 之前，所述方法还可以包括：步骤 405~步骤 407。

在所述步骤 405 中，所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA。所述获取终端信息请求包括 ICCID (第一签约数据集的 ID 信息)和 EID(所述 eUICC 的 ID 信息)。

在所述步骤 406 中，所述 LPA 或所述 eUICC 对所述应用进行验证。

在可选的步骤中，所述 LPA 基于所述获取终端信息请求，验证从所述 eUICC 获取的 EID 与所述获取终端信息请求中的 EID 是否相同，其中，所述 EID 为所述 eUICC 的 ID 信息。

具体地，所述 LPA 基于所述获取终端信息请求的 ICCID，从所述 eUICC 中获取所述 eUICC 所存储的第一签约数据集的元数据信息(如 metadata)。获取终端信息请求(Getprofileinfo)可以获取 profile 的很多信息，metadata 是其中的一个。

所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息，所述认证信息包括所述运营商服务器所允许发起签约数据集下载的应用的证书或所述证书的哈希值，所述第一签约数据集的元数据信息还可包括所述运营商服务器所允许发起签约数据集下载的应用的包名，其中，所述运营商服务器所允许发起签约数据集下载的应用的

证书或所述证书的哈希值或应用的包名可以是所述运营商服务器所预存储的或是由运营商服务器从其他认证的服务器中获取的。

所述 LPA 从所述第一签约数据集的元数据信息中获取所述认证信息，并从所述设备的操作系统中获取发起所述下载请求的应用的信息，比较所述认证信息和发送获取终端信息请求的所述应用的信息进行验证，来验证发起下载请求的应用。

或者，所述 LPA 向所述 eUICC 发送应用认证请求，所述应用认证请求包括所述发送终端信息请求的（即触发签约数据集下载的）应用的认证信息和所述 ICCID，所述应用认证请求还可包括接口信息，所述应用认证请求还可包括所述发送终端信息请求的（即触发签约数据集下载的）应用的的包名。所述 LPA 从所述设备的操作系统中获取发送获取终端信息请求的应用的信息，所述发送终端信息请求的（即触发签约数据集下载的）应用的认证信息可以是所述 LPA 从所述设备的操作系统中获取的。然后，所述 eUICC 根据到达 ICCID 获取所述第一签约数据集的元数据信息，并从所述第一签约数据集的元数据信息中获取所述认证信息，并比较所述认证信息和所述发起签约数据集下载的应用的信息，来验证发起下载请求的应用。

所述步骤 406 中所述 LPA 或所述 eUICC 对所述应用进行验证的过程参考前述实施例中所述步骤 106 的描述，为简明起见，不再赘述。

在所述步骤 406 验证通过后，在所述步骤 407 中，所述应用生成终端信息响应消息，并发送至所述运营商服务器。

接着，在所述步骤 402 中，所述应用触发所述 LPA 发起签约数据集下载；

在所述步骤 403 中，所述 LPA 或所述 eUICC 利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用。

所述步骤 403 的验证过程参考所述步骤 406，不再赘述。

所述 LPA 从所述 eUICC 中获取所述第一签约数据集的元数据信息，并从所述第一签约数据集的元数据信息获取所述认证信息；

所述 LPA 获取发起签约数据集下载的应用的信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

所述步骤 403 包括：所述 LPA 获取发起签约数据集下载的应用的信息并发送至所述 eUICC；

所述 eUICC 从所述第一签约数据集的元数据信息获取所述认证信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的所述应用的信息，以验证所述发起签约数据集下载的应用。

在一些实施例中，所述方法中，所述设备执行所述步骤 405~所述步骤 407 的验证过程之后再执行所述步骤 403~所述步骤 404 的验证过程。

在另一些实施例中，所述方法中，所述设备执行所述步骤 405~所述步骤 407 的验证过程后，不再执行步骤 403~所述步骤 404 的验证过程。

在有一些实施例中，所述方法，所述设备不执行所述步骤 405~所述步骤

的信息，以验证所述发起签约数据集下载通过后，签约管理服务器为所述设备下载所述签约数据集。

结合本发明第一方面第一实施例的描述，在第二实施例中，所述认证信s407的验证过程后，直接执行步骤403~所述步骤404的验证过程。

接着，在所述步骤403验证通过后，在所述步骤404中，所述LPA从所述签名管理服务器下载第二签约数据集，并发送至所述eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

根据本发明一实施例提供的一种在设备上进行签约数据集下载的方法，所述设备具有第一eUICC、第二eUICC、LPA和应用，所述方法包括步骤501~步骤506。

步骤501：所述第一eUICC从签名管理服务器下载第一签约数据集，其中，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；步骤502：所述应用触发所述LPA发起签约数据集下载；步骤503：所述LPA或所述第一eUICC利用所述第一签约数据集信息中所述访问控制信息验证发起所述下载请求的所述应用的访问权限；步骤504：在验证通过后，所述LPA从所述签名管理设备下载第二签约数据集并发送至所述第二eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

在一些实施例中，在所述步骤501和所述步骤502之间，所述方法还包括步骤505~步骤507，在所述步骤505中，所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述LPA；在所述步骤506中，所述LPA或所述第一eUICC对所述应用进行验证；在所述步骤507中，在验证通过后，所述应用从所述第二eUICC获取第二eUICC信息，并根据所述第二eUICC信息生成终端信息响应消息，并发送至所述运营商服务器。

在一些实施例中，在所述步骤505和所述步骤506之间，所述方法还包括步骤507，在所述步骤507中，所述LPA获取所述获取终端信息请求后，向所述设备的显示界面发送选择信息，以在所述显示界面显示供用户选择下载所述第二签约数据集的所述第二eUICC。

在以下实施例中，所述设备中应用可以为MNO APP， MNO portal（运营商服务节点）是运营商服务器的一部分，所述签约管理设备可以包括SM-DP+，或SM-DP+和SM-DS。

【实施例一】

以下参考图1所示内容。

0. 在LPA中预先配置MNO APP访问LPA的访问控制规则（Access Control Rule），在一些实施例中，访问控制规则是MNO APP签名证书的根证书，则LPA预先配置GSMA CI证书或GSMA CI公钥以及公钥ID，或通过ES10接口从eUICC中获取GSMA CI证书或GSMA CI公钥以及公钥ID。

1. 设备启动MNO App，通过MNO APP登录MNO Portal；

2. MNO APP发起下载新profile请求，向所述MNO portal请求下载profile；

3. MNO portal根据请求下载profile的消息，向所述MNO APP发送获取终端信

息请求；

4. MNO APP 调用 LPA API（LPA 接口），将所述获取终端信息的请求发送给 LPA；

5. LPA 可从 device OS（设备上的操作系统，例如 IOS 系统，安卓系统等）获取 MNO APP 的签名证书，验证签名证书证书链的根证书是否为 GSMA CI 证书，LPA 从操作系统中获取到的一般是 APP 的签名证书，APP 的签名证书里面有根证书的信息（例如根证书的公钥 ID 号，以及根证书的签名），LPA 利用预配的根证书即 GSMA CI 的信息（如 CI 证书，或 CI 公钥和公钥标识），来验证 APP 证书的根证书是否为 GSMA CI。

6. 在验证通过后，则 LPA 向 eUICC 发送获取 eUICC 信息的请求（(getEUICCInfo），可选地还可包括获取 EID（eUICC ID）的请求（GetEID）；

7. eUICC 将所述 eUICC 信息返回给 LPA，可选地还返回 EID；

8. LPA 根据所述 eUICC 信息，向所述 MNO APP 发送终端信息响应消息，所述终端信息响应消息包括 eUICC 信息，可选地还包括 EID，所述终端信息响应消息还可选择性包括设备信息（device info）；

9. MNO APP 将所述终端信息响应消息发送给 MNO portal；

10. MNO portal 根据所述终端信息响应消息，向 SM-DP+发送签约数据集下载订购请求（profile order），其中，MNO portal 会根据 eUICC info 来判断应该向 SM-DP+预定的 profile 的类型（profile type），例如，根据 eUICC info 中协议版本号 eUICC 能力等，确定需要预订的 profile 的类型，如果所述终端信息响应消息有 device info，可利用 device info 进行判断向 SM-DP+预定的 profile 的类型， 例如根据 device info 中的无线接入能力，确定需要预订的 profile 的类型，device info 能够帮助预订类型更准确的 profile。所述 profile order 中包含：EID、MNO APP 签名证书的哈希值（hash(Cert)）或签名证书（Cert），相比直接传递签名证书（Cert），传递 hash(Cert)数据量小，方便发送。所述 profile order 还可包括 MNO APP 包名(Package name)、MNO APP 签名证书的哈希函数(hash algorithm)；如果需要将下载事件注册到 SM-DS，MNO portal 还会提供 SM-DS 地址，其中，MNO APP 包名(Package name)、MNO APP 签名证书的哈希函数（hash algorithm）可用于后续对触发下载请求的 MNO APP 进行验证；

11. SM-DP+根据 profile order 生成事件 ID（eventID），并向 SM-DS 注册下载事件，发送参数包括：eventID, EID, hash(Cert)，可选地，发送参数还包括：MNO APP 包名（Package name）、MNO APP 签名证书的哈希函数（hash algorithm）等；

12. SM-DP+向 MNO portal 返回下载预订响应消息，消息中包括 polling address，polling address 为 SM-DP+地址或 SM-DS 地址，消息中还包括下载预订请求匹配 ID（matchingID）或事件 ID（EventID），其中，下载预订请求匹配 ID（matchingID）由 SM-DP+生成和存储；

13. MNO portal 向 MNO App 发送触发下载（如 trigger download）消息，该消息中包括 polling address，可选地还包括：matchingID（matchingID 用于在不使用 SM-DS 时发送）或 EventID，hash algorithm 等；

14. MNO App 调用 LPA API，将 trigger download 消息发送给 LPA；

15. 可选地，若 LPA 尚未对 MNO APP 进行验证，则 LPA 从 device OS 获取 MNO APP 的签名证书，验证签名证书证书链的根证书为 GSMA CI 证书。若 14 步中 LPA 接收到哈希函数（hash algorithm），则 LPA 根据 hash algorithm 从 device OS 获取证书的哈希值 hash(Cert)；

16. LPA 向 SM-DS 发送获取事件请求，获取事件请求中包括 EID, CERT（MNO APP 证书 Cert 或 hash(Cert), 可选地包括：事件 ID（evenID), MNO APP 包名（package name），以获取事件记录（event record）；

17. SM-DS 根据 EID 或 eventID 查找相应的事件记录（event record），从获取事件请求中获取 hash(Cert)，或者根据 MNO APP 证书，利用 hash 函数计算 hash(Cert)，比较 hash(Cert)和接收到的 MNO APP 包名（package name）是否与事件记录中相应的值相同，若相同则执行步骤 18；

18. SM-DS 向 LPA 返回事件记录，包括：SM-DP+ address 以及 matchingID；

19. LPA 向 SM-DP+发送认证客户端请求，包括 EID, matchingID, CERT（MNO APP 证书，或者 hash(Cert)）,可选的还可以包括 package name，以请求下载 profile；

20. 根据 matchingID 查找相应的签约数据集下载订购请求（profile order），若下载订购请求中发送的 CERT 信息为 MNO APP 证书，则 SM-DP+根据 hash 算法计算 hash(Cert)，SM-DP+比较计算出的的 hash(Cert)/从 LPA 接收到的 hash(Cert)和接收到的 package name 是否与 profile order 关联的 APP 信息相同，若相同；

21. LPA 从 SM-DP+下载 profile，并将 profile 发送给 eUICC，eUICC 完成安装。

通过本实施例，设备可以利用任何具有由 GSMA CI 颁发的证书签名的 MNO APP 发起 profile 下载请求，而不需要在 eUICC 中预置对特定 APP 的访问控制信息，由 SM-DP+或 SM-DS 对 MNO APP 的签名证书和包名的进行认证，确保相应的下载请求是来自受信的 MNO APP。

【实施例二】

在实施例的基础上，参考图 2 所示内容，若根据运营商未部署 SM-DS 的情况下，在步骤 10 后，不需执行步骤 11，在步骤 12 中，SM-DP+向 MNO portal 返回下载预订响应消息，响应消息中包含下载预订请求匹配 ID（Matching ID），随后设备无需向 SM-DS 发送获取事件请求，即省略步骤 16、步骤 17 和步骤 18。

【实施例三】

在本实施例中，参考图 3 所示内容，在实施例一的基础上，区别于实施例一，本实施例由 eUICC 根据 eUICC 中配置的 GSMA CI 信息验证 APP 签名证书证书链的根证书是否为 GSMA CI。

具体地，区别于实施例一步骤 0，在 eUICC 中预先配置 MNO APP 访问 LPA 的访问控制规则（Access Control Rule），在一些实施例中，在 eUICC 中预先配置 GSMA CI 证书或 CI 证书的公钥和公钥标识。

同时，区别于实施例一步骤 5，在本实施例中，在步骤 5.1 中，LPA 从 device OS 获取 MNO APP 的签名证书，在步骤 5.2 中，LPA 将所获取的所述签名证书发送至 eUICC，在步骤 5.3 中，eUICC 验证 LPA 发送的签名证书根证书的证书链是否为 GSMA

CI 证书。

相比于 LPA 的安全等级，eUICC 安全等级更高，因此，利用 eUICC 进行认证的安全性更高。

【实施例四】

在实施例三的基础上，参考图 4 所示内容，若根据运营商未部署 SM-DS 的情况下，省略步骤 11、步骤 16、步骤 17 和步骤 18，类似于实施例二，也可以实现利用当前 eUICC 的系统架构和访问控制机制，对设备上的 APP 调用该 LPA API 进行 profile 下载进行访问控制。

【实施例五】

本实施例用于双卡场景，参考图 5 所示内容，即当运营商在卡 1（eUICC1）中下载 profile 后，如果用户选择在卡 2（eUICC2）中下载同一个运营商的 profile，则可以利用卡 1 对 APP 进行认证，然后允许 APP 对卡 2 的访问，其中，涉及到 LPA 获取 APP 证书的方法和前述实施例相同：

1. MNO portal 在向 SM-DP+定制 profile（即第一签约数据集）时，将 MNO portal 所存储的 MNO App 的签名证书的哈希值，及可选地 MNO App 的包名（Package name）、哈希函数（Hash algorithm）和允许该 App 访问的 API（allowed API）发送给 SM-DP+，使 SM-DP+将以上信息添加到元数据（profile metadata）中；

2. SM-DP+将包含上述 profile metadata 信息的 profile 下载到 eUICC1 中；

3. 设备启动 MNO App，并通过 MNO APP 登录 MNO Portal；

4. MNO App 发起下载新 profile 请求，向所述 MNO portal 请求下载 profile

5. MNO portal 向 MNO App 发送获取终端信息请求，所述获取终端信息请求中包括 profile 的 ID 信息（ICCID），可选地还包括 eUICC1 的 ID 信息(EID1)；

6. MNO App 调用 LPA API，请求获取终端信息，消息中包括 ICCID, 可选地还包括 EID；

7. 如果第 6 步中 LPA 接收到的获取终端信息存在 EID1，则需要从 eUICC1 或 eUICC2 中获取 EID，以确认设备中两个 eUICC 中哪一个是 eUICC1；

8. LPA 判断步骤 7 中接收的 EID 和步骤 6 中接收的 EID 是否相同，或者如果步骤 6 中没有携带 EID，则 LPA 需要确定 eUICC1 或者 eUICC2 是否包含有 ICCID 对应的 profile，具体过程可以为 LPA 依次查询两个 eUICC 中已经安装的 profile（即第一签约数据集）的 ICCID，与第 6 步所接收的 ICCID 进行比对，在验证通过后，则执行步骤 9；

9. LPA 在设备显示界面上显示提示信息，以提示用户选择安装新 profile（对应第二签约数据集）的 eUICC，若用户选择 eUICC 2；

10. LPA 向 eUICC1 发送获取已安装的 profile 信息的请求（GetProfileInfo），所述获取第一签约数据集信息的请求携带 profile 的 ICCID；

11. eUICC1 将 ICCID 对应的已安装的 profile 的 profile metadata 返回给 LPA，包括 MNO App 的证书哈希值，和可选的 MNO App 的包名、哈希函数及允许该 App 访问的 API(allowed API)；

12. LPA 从 device OS 获取设备所存储的 MNO App 的证书，利用步骤 11 中

eUICC1 所返回的哈希函数计算设备所存储的 MNO App 的证书的哈希值，或者 LPA 根据 11 步中接收到的哈希函数，从设备中获取 MNO App 的证书的哈希值，并获取设备所存储的 MNO App 的包名；

13. LPA 判断步骤 12 中获得的哈希值以及 MNO App 的包名是否和步骤 11 中所获取的 profile metadata 中的哈希值和包名相同，以判断是否允许调用第 6 步中的 API，若验证都通过，执行步骤 14；

14. LPA 向 eUICC2 发送获取 eUICC 信息的请求（GetEUICCInfo），以获取 eUICC2 info，可选的还可以获取 eUICC2 的 ID 信息 EID2；

15. LPA 将获取的所述 eUICC2 信息(eUICC 2 info)，EID2，可选的增加设备信息（device info）合并，生成终端信息响应消息发送给 MNO APP；

16. MNO APP 将上述终端信息响应消息发送给 MNO Portal；

17. MNO portal 根据 eUICC2 info 和 device info，向 SM-DP+发送签约数据集下载预订请求（profile order），请求 SM-DP+生成新 profile（第二签约数据集）；

18. SM-DP+返回 SM-DP+地址以及下载预订请求匹配 ID（matchingID）；

19. MNO portal 向 MNO APP 发送下载触发请求，下载触发请求中携带 SM-DP+地址，matchingID，可选地还可以携带 EID2，EDI1，第一签约数据集的 ICCID，

20. MNO APP 将下载触发请求发送给 LPA

21. 如果在第 10 步和第 11 步之后 LPA 没有缓存获取的 profile metadata，则 LPA 再次从 eUICC1 获取所述 profile metadata；

22. 在步骤 21 之后，eUICC1 向 LPA 返回所述 profile metadata；

23. LPA 从 device OS 获取设备所存储的 MNO App 的证书，利用步骤 22 中 eUICC1 所返回的哈希函数计算设备所存储的 MNO App 的证书的哈希值，并获取设备所存储的 MNO App 的包名；

LPA判断步骤23中所计算的哈希值以及获取MNO App的包名是否和步骤22中所获取的profile metadata中的哈希值和包名相同，以判断是否允许调用第6步中的API，若验证都通过，执行步骤25；

在此，步骤23和步骤24可独立于步骤12和步骤13中对MNO APP的验证，步骤1和步骤2中allowed API为可选，如果步骤1和步骤2没有allowed API，则LPA默认APP有权限访问所有API，则可根据LPA实现规则，决定在步骤12和步骤13之后是否执行步骤23和步骤24，如果步骤1和步骤2有allowed API， 则在步骤12和步骤13之后，则在每次调用API时，都要进行验证，故一定会执行步骤23和步骤24；

24. 如果步骤 20 中 LPA 获取到 EID2，则 LPA 根据 EID2，选择 eUICC2，或者 LPA 根据第 9 步中的用户选择的 eUICC2，LPA 将新 profile（第二签约数据集）下载到 eUICC2，其中，所述第二签约数据集不同于第一签约数据集。

通过本实施例，借助于设备上的一个eUICC（eUICC1）中对MNO APP的访问控制信息，来判断MNO APP调用LPA API的权限，进而可以下载profile到一个不同的eUICC（eUICC2）中。

【实施例六】

参考图6所示内容，本实施例和实施例五的区别在于，本实施例用于双卡场景，

即当运营商在卡（eUICC）中下载profile后，通过一个卡1(eUICC1)中已经下载的profile中对该APP的访问控制信息进行访问控制。

具体地，区别于实施例五：

在步骤10中，LPA向eUICC1发送认证MNO App的请求，携带ICCID， MNO App的证书或者证书链，MNO APP的包名Package name, API 1，API 1就是APP调用的LPA API的一个标识，说明是调用哪个API。如果在metadata里面包括allowed API，则需要发送该信息，如果没有的话就不需要发送该信息；

11. eUICC1根据ICCID，获取所存储的对应的profile的metadata，根据哈希函数计算证书的哈希值（hash(Cert)）；

12. eUICC1判断计算出的hash(Cert)以及MNO APP的包名（package name）是否和profile metadata中的值相同，以判断是否允许访问LPA API；

13. eUICC1向LPA返回验证结果，如果验证通过，则继续步骤14.1、14.2、14.3，类似于实施例5中的步骤14。

本实施例相比于实施例五而言，进一步提高了安全性，是由需要下载profile的eUICC（即eUICC2）本身来对APP进行访问控制。

通过本实施例，在已有profile下载后时，不需要在要下载profile的eUICC中预置对特定APP的授权信息，可以通过一个eUICC中已经下载的profile中对该APP的访问控制信息进行访问控制。

【实施例七】

参考图7所示内容，在实施例五的基础上，可将第二签约数据集下载到同一个eUICC，即单卡中具有两个不同的签约数据集。

具体地，在实施例五基础上：

在步骤8中，LPA仅查询一个eUICC中是否已经安装的profile（即第一签约数据集）的ICCID即可；

省略实施例五中步骤9，即无需LPA在设备显示界面上显示提示信息；并且不同于实施例五；

在步骤14和步骤25中，由与步骤2、步骤7、步骤10、步骤11中相同的eUICC执行该步骤。

【实施例八】

参考图8所示内容，本实施例和实施例七的区别在于，由卡（eUICC）对APP进行访问权限认证，具体地，区别于实施例七，在本实施例中：

在步骤10中，LPA向eUICC发送认证MNO App的请求，携带ICCID， MNO App的证书或者证书链，MNO APP的包名（Package name）

11. eUICC根据ICCID，获取所存储的对应的profile的metadata，根据哈希函数计算证书的哈希值（hash(Cert)）；

12. eUICC判断计算出的hash(Cert)以及MNO APP的包名（package name）是否和profile metadata中的值相同，以判断是否允许访问；

13. eUICC向LPA返回验证结果，如果验证通过，则继续步骤14.1、14.2，类似于实施例七中的步骤14。

本实施例相比于实施例八而言，进一步提高了安全性，是由需要下载profile的eUICC（即eUICC）本身来对APP进行访问控制。通过本实施例，在已有profile下载后时，不需要在要下载profile的eUICC中预置对特定APP的授权信息，可以通过一个eUICC中已经下载的profile中对该APP的访问控制信息进行访问控制。

另外，本发明实施例提供一种设备，该设备用于执行以上签约数据集的安装方法中的设备所执行的步骤。本发明实施例提供的设备可以包括相应步骤所对应的模块。

本发明实施例可以根据上述方法示例对设备进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

在采用集成的单元的情况下，图9示出了上述实施例中所涉及的设备的一种可能的结构示意图。如图9所示，设备包括处理器701、存储器702、集成电路卡eUICC703以及系统总线704、通信接口705。其中，所述设备用于前述实施例示出方法的步骤101~步骤106、或步骤401~步骤407、或步骤501~步骤506，此外，所述设备的应用的计算机程序存储于存储器702中，所述处理器会执行相应计算机代码执行应用的功能。所述LPA也属于设备中的一种应用，设备通过通信接口705与其他设备进行交互，如：运营商服务器、签约管理服务器。

在本发明具体实施方式中，存储器702可以包括易失性存储器，例如NVRAM（Nonvolatile Random Access Memory，非挥发性动态随机存取内存）、PRAM（Phase Change RAM，相变化随机存取内存）、MRAM（Magnetic Random Access Memory，磁阻式随机存取内存）等；存储器702还可以包括非易失性存储器，例如至少一个磁盘存储器件、EEPROM（Electrically Erasable Programmable Read-Only Memory，电子可擦除可编程只读存储器）、闪存器件，例如反或闪存（NOR flash memory)或是反及闪存(NAND flash memory)。非易失存储器储存处理器所执行的操作系统及应用程序。处理器701从非易失存储器加载运行程序与数据到内存并将数据内容储存于大量储存装置中。

处理器701是设备的控制中心。处理器701利用各种接口和线路连接整个设备的各个部分，通过运行或执行存储在存储器172内的软件程序和/或应用模块，以及调用存储在存储器702内的数据，执行设备的各种功能和处理数据，从而对设备进行整体监控。

处理器701可以仅包括CPU，也可以是CPU、GPU（Graphic Processing Unit，图像处理器）、DSP以及通信单元中的控制芯片（例如基带芯片）的组合。在本发明实施方式中，CPU可以是单运算核心，也可以包括多运算核心。

系统总线704可以是ISA（Industry Standard Architecture，工业标准体系结构）总线、PCI（Peripheral Component Interconnect，外部设备互连）总线或EISA（Extended Industry Standard Architecture，扩展工业标准体系结构）总线等。该系统总线704可以分为地址总线、数据总线、控制总线等。本发明实施例中为了清楚说明，在图9中

将各种总线都示意为系统总线704。

图10示出了上述实施例中所涉及的运营商服务器的一种可能的结构示意图。如图10所示，所述运营商服务器包括处理器801、存储器802以及系统总线803、通信接口804。其中，处理器801用于前述实施例中步骤201~步骤204。运营商服务服务器通过通信接口804与其他设备进行交互，如：设备、签约管理服务器。

图11示出了上述实施例中所涉及的签约管理服务器的一种可能的结构示意图。如图11所示，签约管理服务器包括处理器901、存储器902以及系统总线903、通信接口904。其中，处理器901用于执行前述实施例所示方法步骤的301~306。签约管理服务器通过通信接口904与其他设备进行交互，如：运营商服务服务器、设备。

所述签约管理服务器也可以是一个云部署，由多个签约管理服务设备组成，例如至少一个签约管理数据准备设备，或包括至少一个签约管理数据准备设备和至少一个签约管理发现服务设备，每个签约管理服务设备可以具有自己的处理器、存储器以及系统总线、通信接口，签约管理服务设备之间可以通过网络通信。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将移动设备的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。上述描述的系统，移动设备和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本发明所提供的几个实施例中，应该理解到，所揭露的系统，移动设备和方法，可以通过其它的方式实现。例如，以上所描述的移动设备实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，移动设备或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施例所

述方法的全部或部分步骤。而前述的存储介质包括：U盘（Universal Serial Bus flash disk，通用串行总线闪存盘）、移动硬盘、ROM、 RAM、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1. 一种签约数据集下载的方法，所述方法由签约管理服务器执行，其中，所述方法包括：

接收运营商服务器发送的下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

根据所述下载预订请求向所述运营商服务器返回下载预订响应消息；

接收设备发送的认证请求，所述认证请求包括所述设备中发起签约数据集下载的应用的信息，比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用；

在验证通过后，为所述设备下载所述签约数据集。

2. 根据权利要求 1 所述的方法，其中，所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书或所述证书的哈希值。

3. 根据权利要求 2 所述的方法，其中，所述的比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤包括：

比较所述运营商服务器允许发起签约数据集下载的应用的证书与所述设备中发起签约数据集下载的应用的证书是否一致，或比较所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值与所述设备中发起签约数据集下载的应用的证书的哈希值是否一致。

4. 根据权利要求 2 或 3 所述的方法，其中，所述认证信息还包括所述运营商服务器允许发起签约数据集下载的应用的包名；所述设备中发起签约数据集下载的应用的信息还包括所述设备中发起签约数据集下载的应用的包名。

5. 根据权利要求 4 所述的方法，其中，所述的比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤还包括：

比较所述运营商服务器允许发起签约数据集下载的应用的包名与所述设备中发起签约数据集下载的应用的包名是否一致。

6. 根据权利要求 1 至 5 中任一项所述的方法，其中，所述签约管理服务器包括签约管理数据准备设备和签约管理发现服务设备，所述方法还包括：

所述签约管理数据准备设备根据所述下载预订请求，向所述签约管理发现服务设备发送注册事件请求，所述注册事件请求包括所述认证信息；

所述签约管理发现服务设备接收到所述设备发送的获取事件请求，所述获取事件请求包括所述设备中发起签约数据集下载的应用的信息；

所述签约管理发现服务设备比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用；

在验证通过后，则所述签约管理发现服务设备向所述设备返回事件记录。

7. 根据权利要求 1 至 6 中任一项所述的方法，其中，所述下载预订请求还包括所述运营商服务器从所述设备获取的 EID 信息，所述 EID 信息为所述设备中 eUICC 的 ID 信息，所述认证请求还包括所述 EID，所述下载预订响应消息包

括签约管理服务器地址和查询 ID，所述查询 ID 为下载预订请求匹配 ID 或事件 ID。

8. 一种提供签约数据集下载的方法，所述方法由运营商服务器执行，其中，所述方法包括：

向签约管理服务器发送下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

接收所述签约管理服务根据所述下载预订请求所返回的下载预订响应消息；

根据所述下载预订响应消息，向所述设备发送触发下载消息。

9. 根据权利要求 8 所述的方法，其中，在发送所述下载预订请求之前，所述方法还包括：

基于所述下载请求向所述设备发送获取终端信息请求；

接收所述设备返回的终端信息响应消息。

10. 一种进行签约数据集下载的方法，所述方法由设备执行，其中，所述设备中包括 eUICC， LPA 和应用，所述方法包括：

所述应用触发所述 LPA 发起签约数据集下载；

所述 LPA 向签约管理服务器发送认证请求，以使所述签约管理服务器利用所述运营商服务器所允许发起签约数据集下载的应用的认证信息，验证所述触发所述 LPA 发起签约数据集下载的应用，其中，所述认证请求包括所述设备中发起签约数据集下载的应用的信息；

在所述签约管理服务器验证通过后，所述 LPA 下载所述签约数据集并发送至所述 eUICC。

11. 根据权利要求 10 所述的方法，其中，所述应用触发所述 LPA 发起签约数据集下载的步骤包括：

接收所述运营商服务器发送的触发下载消息，并发送至所述 LPA，以触发所述 LPA 发起签约数据集下载。

12. 根据权利要求 10 或 11 所述的方法，其中，在所述应用触发所述 LPA 发起签约数据集下载之前，所述方法还包括：

所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；

所述 LPA 或所述 eUICC 对所述应用进行验证；

在验证通过后，所述应用生成所述终端信息响应消息，并发送至所述运营商服务器，以使所述运营商服务器向所述签约管理服务器发送下载预订请求。

13. 根据权利要求 12 所述的方法，其中，所述 LPA 或所述 eUICC 对所述应用进行验证的步骤包括：

所述 LPA 获取所述应用的证书并发送至所述 eUICC，所述 eUICC 根据预置的证书认证信息验证验证所述应用；或

所述 LPA 获取所述应用的证书，并根据根据预置的证书认证信息验证所述应用。

14. 根据权利要求 10 至 13 中任一项所述的方法，其中，所述应用触发所述 LPA

发起签约数据集下载之后，所述方法还包括：

所述 LPA 向所述签约管理服务器发送获取事件请求，以使所述签约管理服务器验证所述发起签约数据集下载的应用并返回事件记录；

所述 LPA 接收所述签约管理服务器返回的所述事件记录，所述事件记录用于，所述 LPA 根据所述事件记录向签约管理服务器发送认证请求。

15. 一种在设备上进行签约数据集下载的方法，其中，所述设备具有 eUICC、LPA 和应用，所述方法包括：

所述 eUICC 从签名管理服务器下载第一签约数据集，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

所述应用触发所述 LPA 发起签约数据集下载；

所述 LPA 或所述 eUICC 利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；

在验证通过后，所述 LPA 从所述签名管理服务器下载第二签约数据集，并发送至所述 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

16. 根据权利要求 15 所述的方法，其中，所述 LPA 或所述 eUICC 利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用的步骤包括：

所述 LPA 从所述 eUICC 中获取所述第一签约数据集的所述认证信息；

所述 LPA 获取发起签约数据集下载的应用的信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

17. 根据权利要求 15 所述的方法，其中，所述 LPA 或所述 eUICC 利用所述第一签约数据集中所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用的步骤包括：

所述 LPA 获取发起签约数据集下载的应用的信息并发送至所述 eUICC；

所述 eUICC 从所述第一签约数据集的元数据信息获取所述认证信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的所述应用的信息，以验证所述发起签约数据集下载的应用。

18. 根据权利要求 16 或 17 所述的方法，其中，所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；触发所述 LPA 发起签约数据集下载的所述应用的信息包括触发所述 LPA 发起签约数据集下载的所述应用的证书或所述证书的哈希值。

19. 根据权利要求 15 至 18 中任一项所述的方法，其中，在所述应用触发所述 LPA 发起签约数据集下载之前，所述方法还包括：

所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；

所述 LPA 或所述 eUICC 对所述应用进行验证；

在验证通过后，所述应用生成终端信息响应消息，并发送至所述运营商服务器。

20. 根据权利要求 19 所述的方法，其中，所述 LPA 或所述 eUICC 对所述应用进行验证的步骤包括：

所述 LPA 获取所述应用的证书并发送至所述 eUICC，所述 eUICC 根据预置的证书认证信息验证所述应用；或

所述 LPA 获取所述应用的证书，并根据预置的证书认证信息验证所述应用。

21. 根据权利要求 19 或 20 所述的方法，其中，所述 LPA 或所述 eUICC 对所述应用进行验证的步骤还包括：

所述 LPA 基于所述获取终端信息请求，验证从所述 eUICC 获取的 EID 与所述获取终端信息请求中的 EID 是否相同，其中，所述 EID 为所述 eUICC 的 ID 信息。

22. 一种在设备上进行签约数据集下载的方法，其中，所述设备具有第一 eUICC、第二 eUICC、LPA 和应用，所述方法包括：

所述第一 eUICC 从签名管理服务器下载第一签约数据集，其中，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

所述应用触发所述 LPA 发起签约数据集下载；

所述 LPA 或所述第一 eUICC 根据所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；

在验证通过后，所述 LPA 从所述签名管理设备下载第二签约数据集并发送至所述第二 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

23. 根据权利要求 22 所述的方法，其中，在所述应用触发所述 LPA 发起签约数据集下载之前，所述方法还包括：

所述应用向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；

所述 LPA 或所述第一 eUICC 对所述应用进行验证；

在验证通过后，所述应用从所述第二 eUICC 获取第二 eUICC 信息，并根据所述第二 eUICC 信息生成终端信息响应消息，并发送至所述运营商服务器。

24. 根据权利要求 23 所述的方法，其中，所述方法还包括：

所述 LPA 获取所述获取终端信息请求后，向所述设备的显示界面发送选择信息，以在所述显示界面显示供用户选择下载所述第二签约数据集的所述第二 eUICC。

25. 一种提供签约数据集下载的签约管理服务器，其中，所述签约管理服务器包括：

一个或多个处理器；

存储器；所述存储器，用于存储计算机程序；

所述处理器，用于运行所述计算机程序，执行下述流程：

一个或多个处理器，所述处理器用于执行：

接收运营商服务器发送的下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

根据所述下载预订请求向所述运营商服务器返回下载预订响应消息；

接收设备发送的认证请求，所述认证请求包括所述设备中发起签约数据集下载的应用的信息，比较所述认证信息与所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用；

在验证通过后，为所述设备下载所述签约数据集。

26. 根据权利要求 25 所述的签约管理服务器，其中，所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；所述设备中发起签约数据集下载的应用的信息包括所述设备中发起签约数据集下载的应用的证书或所述证书的哈希值。

27. 根据权利要求 26 所述的签约管理服务器，其中，所述比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤包括：

比较所述运营商服务器允许发起签约数据集下载的应用的证书与所述设备中发起签约数据集下载的应用的证书是否一致，或比较所述运营商服务器允许发起签约数据集下载的应用的证书的哈希值与所述设备中发起签约数据集下载的应用的证书的哈希值是否一致。

28. 根据权利要求 26 或 27 所述的签约管理服务器，其中，所述认证信息还包括所述运营商服务器允许发起签约数据集下载的应用的包名；所述设备中发起签约数据集下载的应用的信息还包括所述设备中发起签约数据集下载的应用的包名。

29. 根据权利要求 28 所述的签约管理服务器，其中，所述的比较所述认证信息与所述设备中发起签约数据集下载的应用的信息步骤还包括：

比较所述运营商服务器允许发起签约数据集下载的应用的包名与所述设备中发起签约数据集下载的应用的包名是否一致。

30. 根据权利要求 25 至 29 中任一项所述的签约管理服务器，其中，所述签约管理服务器包括签约管理数据准备设备和签约管理发现服务设备，其中，

所述签约管理数据准备设备用于根据所述下载预订请求，向所述签约管理发现服务设备发送注册事件请求，所述注册事件请求包括所述认证信息；

所述签约管理发现服务设备用于接收到所述设备发送的获取事件请求，并比较所述认证信息与所述获取事件请求中的所述设备中发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用，在验证通过后，向所述设备返回事件记录。

31. 一种提供签约数据集下载的运营商服务器，其中，所述运营商服务器包括：

一个或多个处理器；

存储器；所述存储器，用于存储计算机程序；

所述处理器，用于运行所述计算机程序，执行下述流程：

向签约管理服务器发送下载预订请求，其中，所述下载预订请求包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

接收所述签约管理服务根据所述下载预订请求所返回的下载预订响应消息；

根据所述下载预订响应消息，向所述设备发送触发下载消息。

32. 根据权利要求 31 所述的运营商服务器，其中，在发送所述下载预订请求之前，所述处理器还执行下述流程：

基于所述下载请求向所述设备发送获取终端信息请求；

接收所述设备返回的终端信息响应消息。

33. 一种进行签约数据集下载的设备，其中，所述设备中包括：eUICC、LPA 和应用，其中，

所述应用用于触发所述 LPA 发起签约数据集下载；

所述 LPA 用于向签约管理服务器发送认证请求，以使所述签约管理服务器利用所述运营商服务器所允许发起签约数据集下载的应用的认证信息，验证所述触发所述 LPA 发起签约数据集下载的应用，其中，所述认证请求包括所述设备中发起签约数据集下载的应用的信息，并在所述签约管理服务器验证通过后，从所述签约管理服务器下载所述签约数据集并发送至所述 eUICC。

34. 根据权利要求 33 所述的设备，其中，所述 LPA 用于接收所述运营商服务器发送的触发下载消息，并发送至所述 LPA，以触发所述 LPA 发起签约数据集下载。

35. 根据权利要求 23 或 34 所述的设备，其中：

所述应用还用于在触发所述 LPA 发起签约数据集下载之前，向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA，并在所述 LPA 或所述 eUICC 对所述应用进行验证通过后，生成所述终端信息响应消息，并发送至所述运营商服务器，以使所述运营商服务器向所述签约管理服务器发送下载预订请求；

所述 LPA 用于对所述应用进行验证，或所述 eUICC 用于对所述应用进行验证。

36. 根据权利要求 35 所述的设备，其中：

所述 LPA 用于获取所述应用的证书并发送至所述 eUICC；

所述 eUICC 用于根据预置的证书认证信息验证所述应用。

37. 根据权利要求 35 所述的设备，其中：

所述 LPA 用于获取所述应用的证书，并根据预置的证书认证信息验证所述应用。

38. 根据权利要求 33 至 37 中任一项所述的设备，其中：

所述 LPA 用于在所述应用触发所述 LPA 发起签约数据集下载之后，向所述签约管理服务器发送获取事件请求，以使所述签约管理服务器验证所述发起签约数据集下载的应用并返回事件记录，并接收所述签约管理服务器返回的所述事件记录，其中，所述事件记录用于所述 LPA 根据所述事件记录向签约管理服务器发送认证请求。

39. 一种在设备上进行签约数据集下载的设备，其中，所述设备具有 eUICC、LPA 和应用，其中，

所述 eUICC 用于从签名管理服务器下载第一签约数据集，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的

认证信息；

所述应用用于触发所述 LPA 发起签约数据集下载；

所述 LPA 用于利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用，或所述 eUICC 用于利用所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；

所述 LPA 还用于在验证通过后，从所述签名管理服务器下载第二签约数据集，并发送至所述 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

40. 根据权利要求 39 所述的设备，其中，

所述 LPA 用于从所述 eUICC 中获取所述第一签约数据集的所述认证信息，获取发起签约数据集下载的应用的信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的应用的信息，以验证所述发起签约数据集下载的应用。

41. 根据权利要求 39 所述的设备，其中，

所述 LPA 用于获取发起签约数据集下载的应用的信息并发送至所述 eUICC；

所述 eUICC 用于从所述第一签约数据集的元数据信息获取所述认证信息，并比较所述认证信息与触发所述 LPA 发起签约数据集下载的所述应用的信息，以验证所述发起签约数据集下载的应用。

42. 根据权利要求 40 或 41 所述的设备，其中，所述认证信息包括所述运营商服务器允许发起签约数据集下载的应用的证书或所述证书的哈希值；触发所述 LPA 发起签约数据集下载的所述应用的信息包括触发所述 LPA 发起签约数据集下载的所述应用的证书或所述证书的哈希值。

43. 根据权利要求 39 至 42 中任一项所述的设备，其中，

所述应用用于向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；

所述 LPA 用于对所述应用进行验证，或所述 eUICC 用于对所述应用进行验证；

所述应用用于在验证通过后，生成终端信息响应消息，并发送至所述运营商服务器。

44. 根据权利要求 43 所述的设备，其中，其中：

所述 LPA 用于获取所述应用的证书并发送至所述 eUICC；

所述 eUICC 用于根据预置的证书认证信息验证所述应用。

45. 根据权利要求 43 所述的设备，其中，其中：

所述 LPA 用于获取所述应用的证书，并根据预置的证书认证信息验证所述应用。

46. 根据权利要求 44 或 45 所述的设备，其中，

所述 LPA 还用于基于所述获取终端信息请求，验证从所述 eUICC 获取的 EID 与所述获取终端信息请求中的 EID 是否相同，其中，所述 EID 为所述 eUICC 的 ID 信息。

47. 一种进行签约数据集下载的设备，其中，所述设备具有第一 eUICC、第二

eUICC、LPA 和应用，

所述第一 eUICC 用于从签名管理服务器下载第一签约数据集，其中，所述第一签约数据集的元数据信息包括所述运营商服务器所允许发起签约数据集下载的应用的认证信息；

所述应用用于触发所述 LPA 发起签约数据集下载；

所述 LPA 用于根据所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用，或所述第一 eUICC 用于根据所述认证信息验证触发所述 LPA 发起签约数据集下载的所述应用；

所述 LPA 还用于在验证通过后，从所述签名管理设备下载第二签约数据集并发送至所述第二 eUICC，其中，所述第二签约数据集与所述第一签约数据集不同。

48. 根据权利要求 47 中任一项所述的设备，其中，

所述应用用于，在所述应用触发所述 LPA 发起签约数据集下载之前，向所述运营商服务器发送下载请求，接收所述运营商服务器发送的获取终端信息请求并发送至所述 LPA；

所述 LPA 用于对所述应用进行验证，或所述第一 eUICC 对所述应用进行验证；

所述应用还用于在验证通过后，从所述第二 eUICC 获取第二 eUICC 信息，并根据所述第二 eUICC 信息生成终端信息响应消息，并发送至所述运营商服务器。

49. 根据权利要求 47 或 48 中任一项所述的设备，其中，

所述 LPA 还用于获取所述获取终端信息请求后，向所述设备的显示界面发送选择信息，以在所述显示界面显示供用户选择下载所述第二签约数据集的所述第二 eUICC。

50. 一种在系统中实现签约数据集下载的方法，所述系统包括签约管理服务器、运营商服务器和设备，其中：

所述设备中应用向运营商服务器发送下载请求；

所述运营商服务器向签约管理服务器发送下载预订请求，其中，所述下载预订请求中具有所述运营商服务器所存储的设备中应用的访问控制信息；

所述签约管理服务器处理所述下载预订请求，并向所述运营商服务器返回响应消息；

所述运营商服务器基于所述响应消息，向所述设备发送触发下载消息；

所述设备中 LPA 向所述签约管理服务器发送认证请求；

所述签约管理服务器利用所述访问控制信息所述访问控制信息，验证发起下载请求的所述应用的的访问权限；

在验证通过后，所述设备下载签约数据集。

51. 一种实现签约数据集下载的系统，所述系统包括签约管理服务器、运营商服务器和设备，其中，

所述签约管理服务器用于：

接收运营商服务器发送的下载预订请求，其中，所述下载预订请求中包括发起下载请求的设备中应用的访问控制信息；

处理所述下载预订请求，并向所述运营商服务器返回下载预订响应消息，以触发下载；

当接收到所述设备发送的认证请求时，利用所述访问控制信息，验证发起下载请求的所述应用的访问权限；

在验证通过后，为所述设备下载签约数据集；

所述运营商服务器用于：

接收设备发送的下载请求；

向签约管理服务器发送下载预订请求，其中，所述下载预订请求中具有所述运营商服务器所存储的设备中应用的访问控制信息；

接收所述签约管理服务基于处理所述下载预订请求所返回的响应消息；

基于所述响应消息，向所述设备发送触发下载消息，以触发下载；

所述设备包括应用、LPA 和 eUICC，所述设备用于：

所述应用向运营商服务器发送下载请求，以使所述运营商服务器向签约管理服务器发送下载预订请求，其中，所述下载预订请求中具有所述运营商服务器所存储的设备中应用的访问控制信息；

所述应用接收所述运营商服务器发送的触发下载消息，并触发所述 LPA 进行下载；

所述 LPA 向签约管理服务器发送认证请求，以在所述签约管理服务器利用所述访问控制信息，验证发起下载请求的所述应用的访问权限；

在验证通过后，所述 LPA 下载签约数据集，并发送至所述 eUICC。

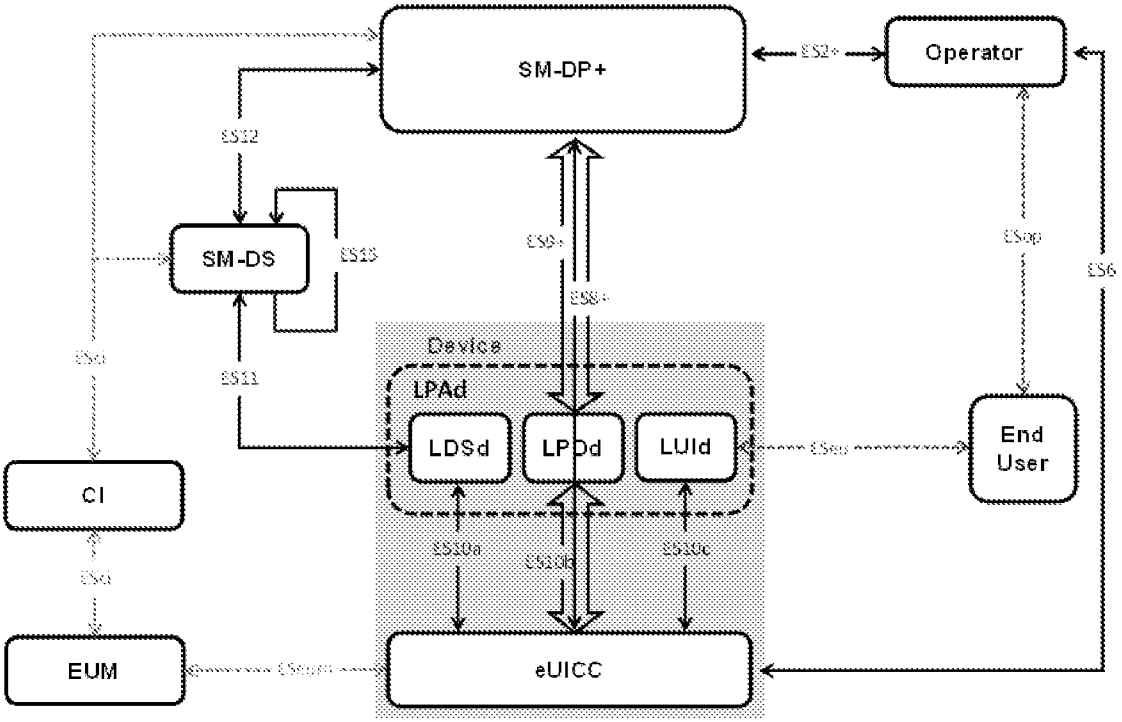
SM-DP+
Operator
SM-DS
Device
LPAd
LDSd
LPDd
LUId
End User
CI
EUM
eUICC

图 1

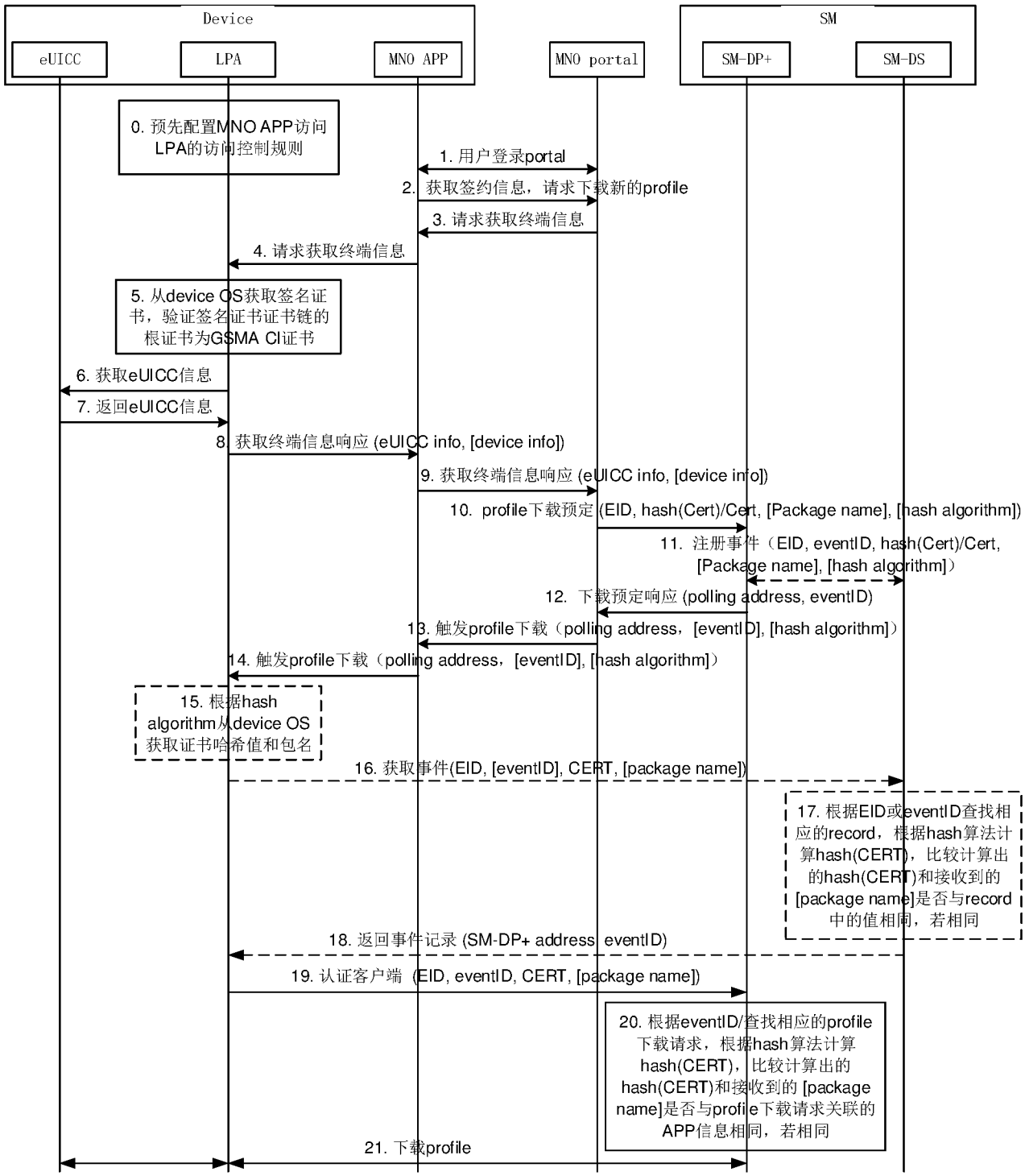
Device
eUICC
LPA
MNO APP
MNO portal
SM
SM-DP+
SM-DS
0. 预先配置MNO APP访问LPA的访问控制规则
1. 用户登录portal
2. 获取签约信息，请求下载新的profile
3. 请求获取终端信息
4. 请求获取终端信息
5. 从device OS获取签名证书，验证签名证书证书链的根证书为GSMA CI证书
6. 获取eUICC信息
7. 返回eUICC信息
8. 获取终端信息响应 (eUICC info, [device info])
9. 获取终端信息响应 (eUICC info, [device info])
10. profile下载预定 (EID, hash(Cert)/Cert, [Package name], [hash algorithm])
11. 注册事件（EID, eventID, hash(Cert)/Cert, [Package name], [hash algorithm]）
12. 下载预定响应 (polling address, eventID)
13. 触发profile下载（polling address，[eventID], [hash algorithm]）
14. 触发profile下载（polling address，[eventID], [hash algorithm]）
15. 根据hash algorithm从device OS获取证书哈希值和包名
16. 获取事件(EID, [eventID], CERT, [package name])
17. 根据EID或eventID查找相应的record，根据hash算法计算hash(CERT)，比较计算出的hash(CERT)和接收到的[package name]是否与record中的值相同，若相同
18. 返回事件记录 (SM-DP+ address, eventID)
19. 认证客户端 (EID, eventID, CERT, [package name])
20. 根据eventID查找相应的profile下载请求，根据hash算法计算hash(CERT)，比较计算出的hash(CERT)和接收到的 [package name]是否与profile下载请求关联的APP信息相同，若相同
21. 下载profile

图 2

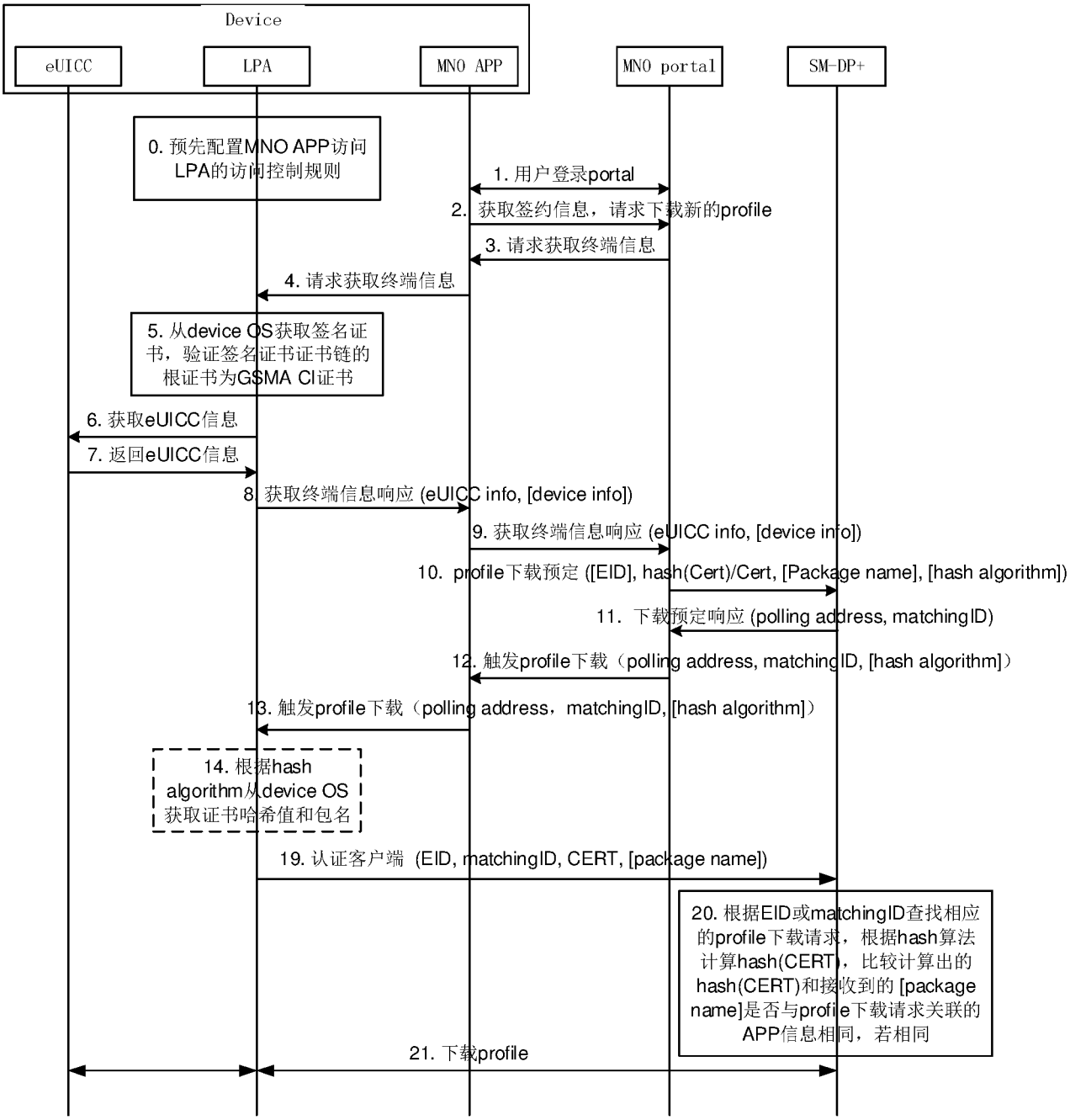
Device
eUICC
LPA
MNO APP
MNO portal
SM-DP+
0. 预先配置MNO APP访问LPA的访问控制规则
1. 用户登录portal
2. 获取签约信息，请求下载新的profile
3. 请求获取终端信息
4. 请求获取终端信息
5. 从device OS获取签名证书，验证签名证书证书链的根证书为GSMA CI证书
6. 获取eUICC信息
7. 返回eUICC信息
8. 获取终端信息响应 (eUICC info, [device info])
9. 获取终端信息响应 (eUICC info, [device info])
10. profile下载预定 ([EID], hash(Cert)/Cert, [Package name], [hash algorithm])
11. 下载预定响应 (polling address, matchingID)
12. 触发profile下载（polling address, matchingID, [hash algorithm]）
13. 触发profile下载（polling address，matchingID, [hash algorithm]）
14. 根据hash algorithm从device OS获取证书哈希值和包名
19. 认证客户端 (EID, matchingID, CERT, [package name])
20. 根据EID或matchingID查找相应的profile下载请求，根据hash算法计算hash(CERT)，比较计算出的hash(CERT)和接收到的 [package name]是否与profile下载请求关联的APP信息相同，若相同
21. 下载profile

图 3

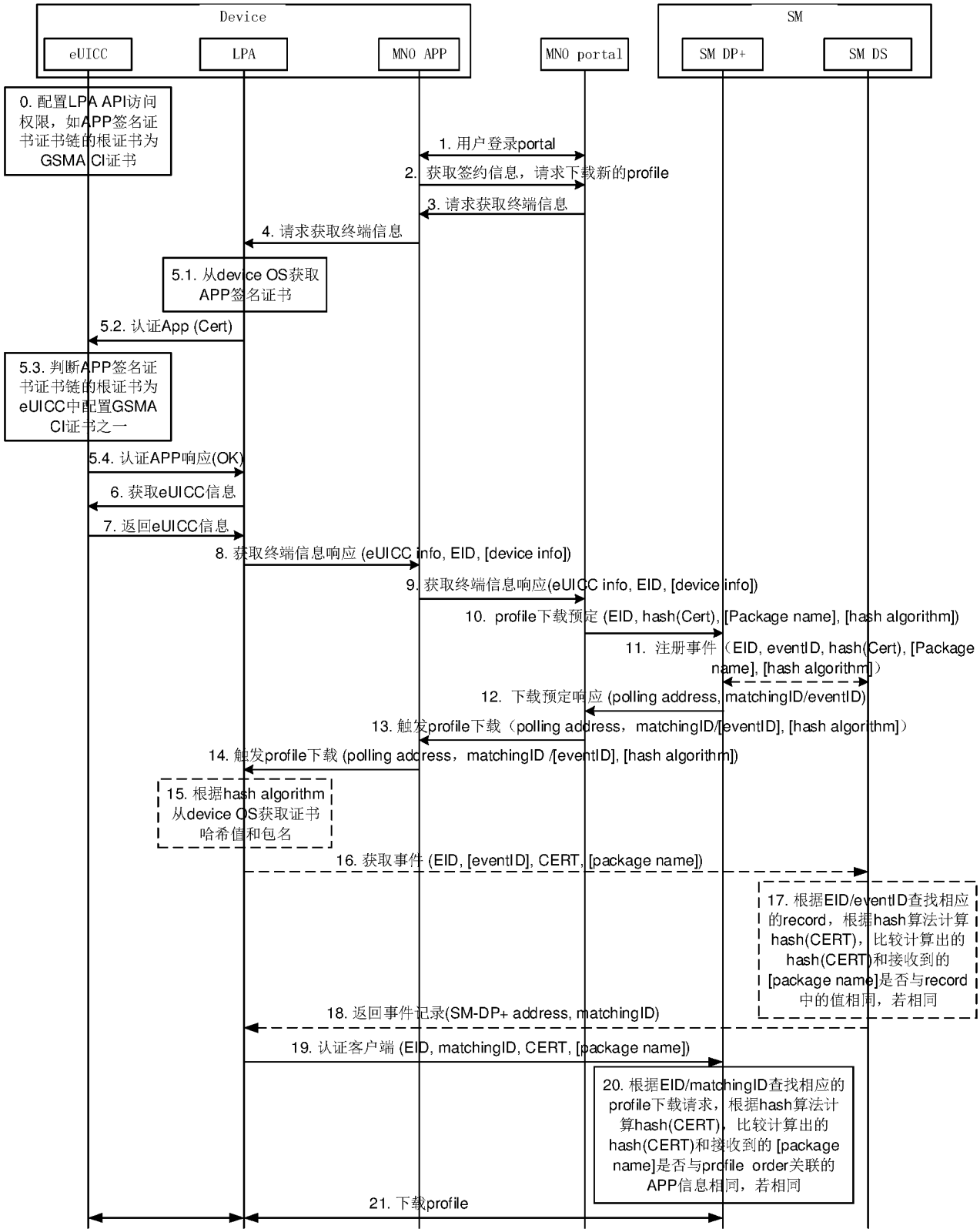
Device
eUICC
LPA
MNO APP
MNO portal
SM
SM DP+
SM DS
0. 配置LPA API访问权限，如APP签名证书证书链的根证书为GSMA CI证书
1. 用户登录portal
2. 获取签约信息，请求下载新的profile
3. 请求获取终端信息
4. 请求获取终端信息
5.1. 从device OS获取APP签名证书
5.2. 认证App (Cert)
5.3. 判断APP签名证书证书链的根证书为eUICC中配置GSMA CI证书之一
5.4. 认证APP响应(OK)
6. 获取eUICC信息
7. 返回eUICC信息
8. 获取终端信息响应 (eUICC info, EID, [device info])
9. 获取终端信息响应(eUICC info, EID, [device info])
10. profile下载预定 (EID, hash(Cert), [Package name], [hash algorithm])
11. 注册事件（EID, eventID, hash(Cert), [Package name], [hash algorithm]）
12. 下载预定响应 (polling address, matchingID/eventID)
13. 触发profile下载（polling address，matchingID/[eventID], [hash algorithm]）
14. 触发profile下载 (polling address，matchingID /[eventID], [hash algorithm])
15. 根据hash algorithm从device OS获取证书哈希值和包名
16. 获取事件 (EID, [eventID], CERT, [package name])
17. 根据EID/eventID查找相应的record，根据hash算法计算hash(CERT)，比较计算出的hash(CERT)和接收到的[package name]是否与record中的值相同，若相同
18. 返回事件记录(SM-DP+ address, matchingID)
19. 认证客户端 (EID, matchingID, CERT, [package name])
20. 根据EID/matchingID查找相应的profile下载请求，根据hash算法计算hash(CERT)，比较计算出的hash(CERT)和接收到的 [package name]是否与profile order关联的APP信息相同，若相同
21. 下载profile

图 4

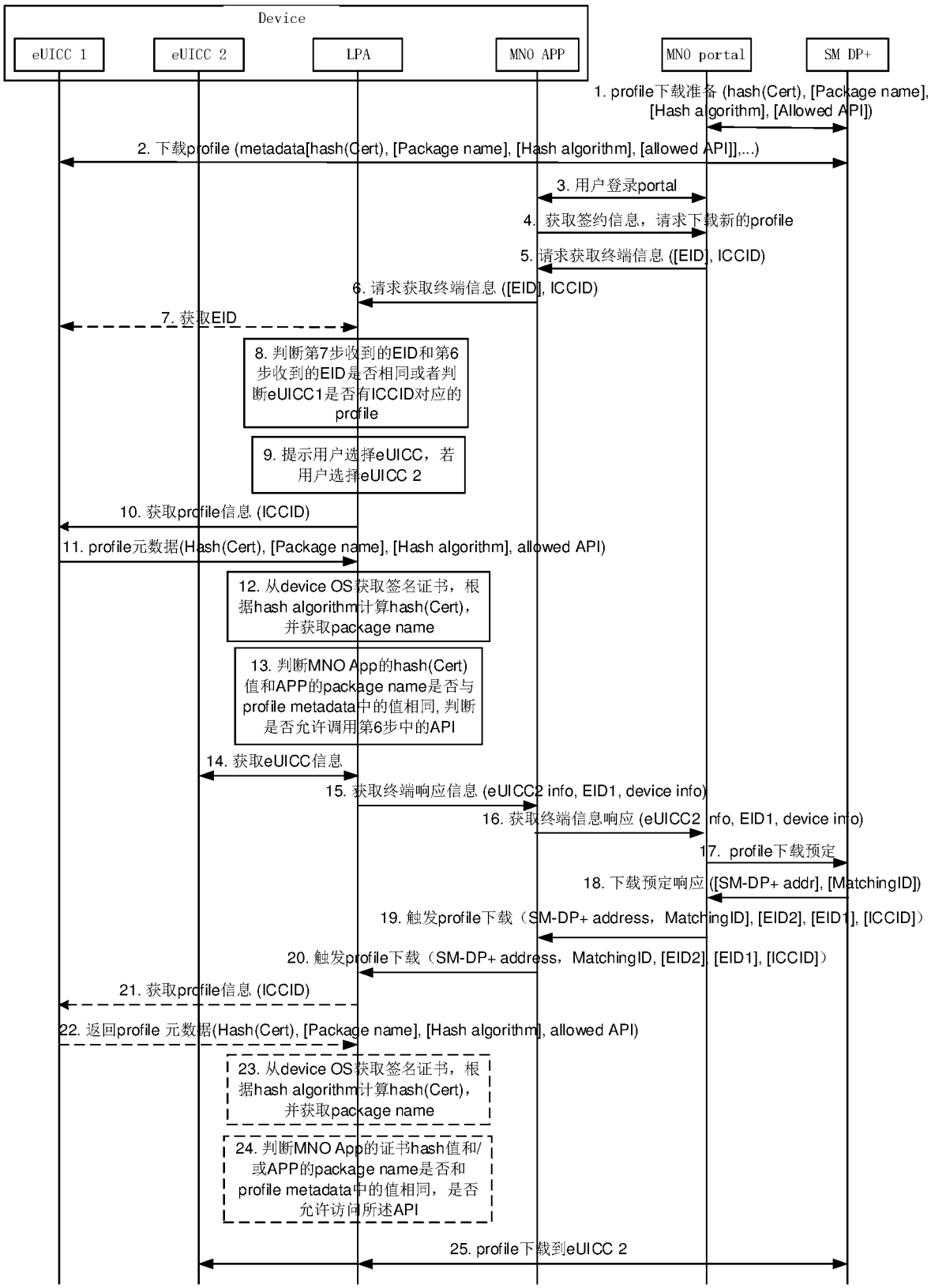
Device
eUICC 1
eUICC 2
LPA
MNO APP
MNO portal
SM DP+
1. profile下载准备 (hash(Cert), [Package name], [Hash algorithm], [Allowed API])
2. 下载profile (metadata[hash(Cert), [Package name], [Hash algorithm], [allowed API]],...)
3. 用户登录portal
4. 获取签约信息，请求下载新的profile
5. 请求获取终端信息 ([EID], ICCID)
6. 请求获取终端信息 ([EID], ICCID)
7. 获取EID
8. 判断第7步收到的EID和第6步收到的EID是否相同或者判断eUICC1是否有ICCID对应的profile
9. 提示用户选择eUICC，若用户选择eUICC 2
10. 获取profile信息 (ICCID)
11. profile元数据(Hash(Cert), [Package name], [Hash algorithm], allowed API)
12. 从device OS获取签名证书，根据hash algorithm计算hash(Cert)，并获取package name
13. 判断MNO App的hash(Cert)值和APP的package name是否与profile metadata中的值相同, 判断是否允许调用第6步中的API
14. 获取eUICC信息
15. 获取终端响应信息 (eUICC2 info, EID1, device info)
16. 获取终端信息响应 (eUICC2 info, EID1, device info)
17. profile下载预定
18. 下载预定响应 ([SM-DP+ addr], [MatchingID])
19. 触发profile下载（SM-DP+ address，MatchingID], [EID2], [EID1], [ICCID]）
20. 触发profile下载（SM-DP+ address，MatchingID, [EID2], [EID1], [ICCID]）
21. 获取profile信息 (ICCID)
22. 返回profile 元数据(Hash(Cert), [Package name], [Hash algorithm], allowed API)
23. 从device OS获取签名证书，根据hash algorithm计算hash(Cert)，并获取package name
24. 判断MNO App的证书hash值和/或APP的package name是否和profile metadata中的值相同，是否允许访问所述API
25. profile下载到eUICC 2

图 5

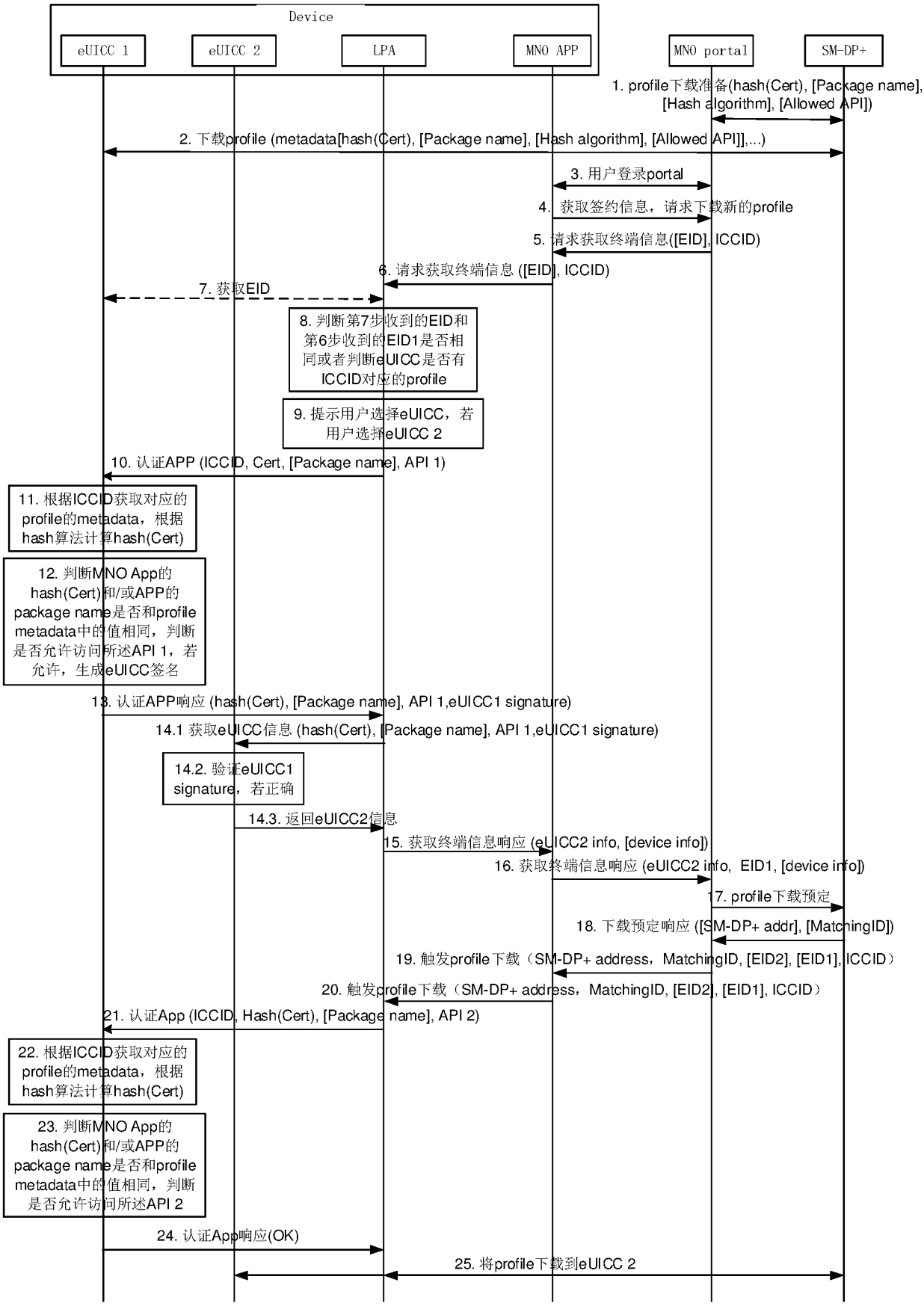
Device
eUICC 1
eUICC 2
LPA
MNO APP
MNO portal
SM-DP+
1. profile下载准备(hash(Cert), [Package name], [Hash algorithm], [Allowed API])
2. 下载profile (metadata[hash(Cert), [Package name], [Hash algorithm], [Allowed API]],...)
3. 用户登录portal
4. 获取签约信息，请求下载新的profile
5. 请求获取终端信息([EID], ICCID)
6. 请求获取终端信息 ([EID], ICCID)
7. 获取EID
8. 判断第7步收到的EID和第6步收到的EID1是否相同或者判断eUICC是否有ICCID对应的profile
9. 提示用户选择eUICC，若用户选择eUICC 2
10. 认证APP (ICCID, Cert, [Package name], API 1)
11. 根据ICCID获取对应的profile的metadata，根据hash算法计算hash(Cert)
12. 判断MNO App的hash(Cert)和/或APP的package name是否和profile metadata中的值相同，判断是否允许访问所述API 1，若允许，生成eUICC签名
13. 认证APP响应 (hash(Cert), [Package name], API 1,eUICC1 signature)
14.1 获取eUICC信息 (hash(Cert), [Package name], API 1,eUICC1 signature)
14.2. 验证eUICC1 signature，若正确
14.3. 返回eUICC2信息
15. 获取终端信息响应 (eUICC2 info, [device info])
16. 获取终端信息响应 (eUICC2 info, EID1, [device info])
17. profile下载预定
18. 下载预定响应 ([SM-DP+ addr], [MatchingID])
19. 触发profile下载（SM-DP+ address，MatchingID, [EID2], [EID1], ICCID）
20. 触发profile下载（SM-DP+ address，MatchingID, [EID2], [EID1], ICCID）
21. 认证App (ICCID, Hash(Cert), [Package name], API 2)
22. 根据ICCID获取对应的profile的metadata，根据hash算法计算hash(Cert)
23. 判断MNO App的hash(Cert)和/或APP的package name是否和profile metadata中的值相同，判断是否允许访问所述API 2
24. 认证App响应(OK)
25. 将profile下载到eUICC 2

图 6

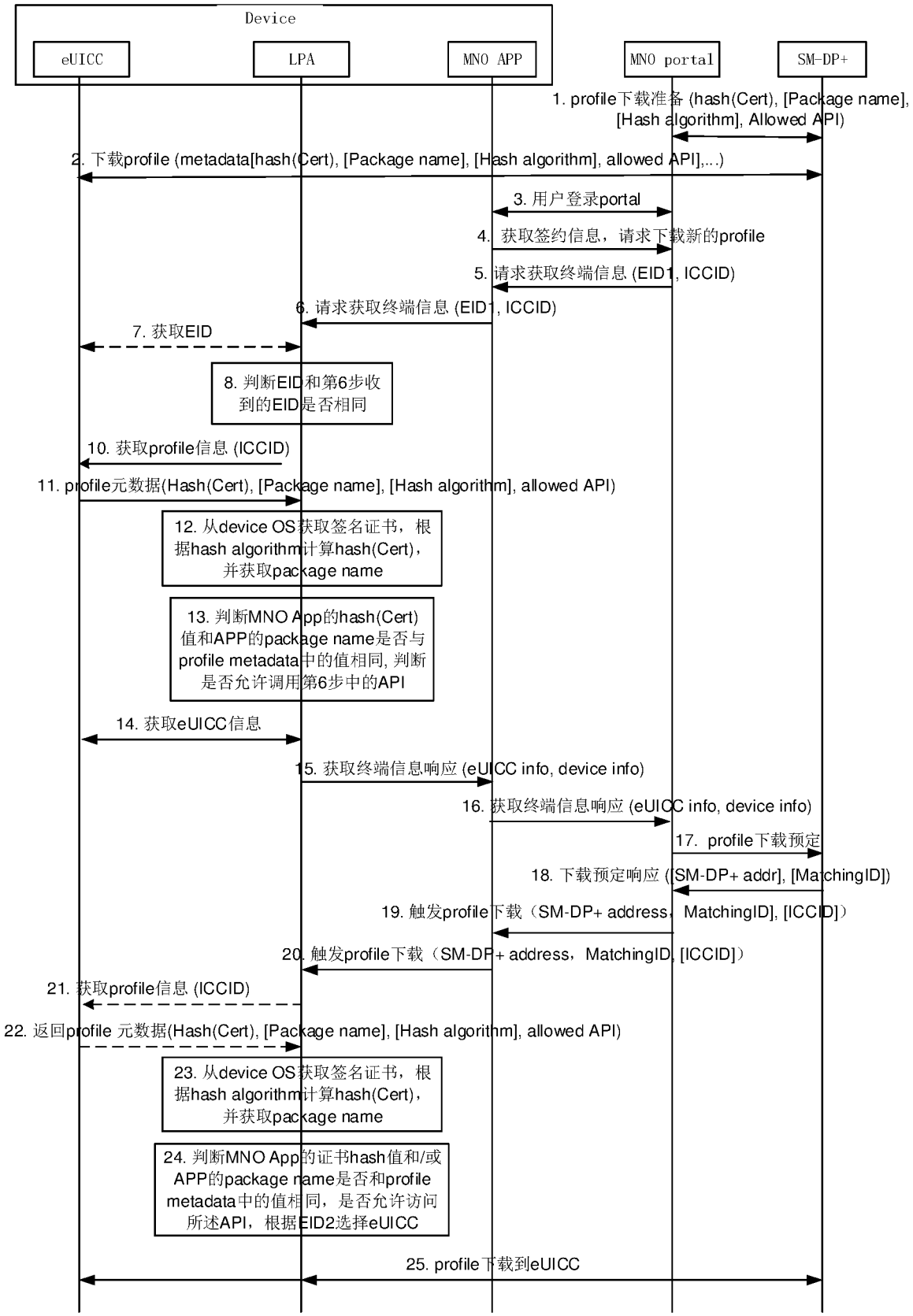
Device
eUICC
LPA
MNO APP
MNO portal
SM-DP+
1. profile下载准备 (hash(Cert), [Package name], [Hash algorithm], Allowed API)
2. 下载profile (metadata[hash(Cert), [Package name], [Hash algorithm], allowed API],...)
3. 用户登录portal
4. 获取签约信息，请求下载新的profile
5. 请求获取终端信息 (EID1, ICCID)
6. 请求获取终端信息 (EID1, ICCID)
7. 获取EID
8. 判断EID和第6步收到的EID是否相同
10. 获取profile信息 (ICCID)
11. profile元数据(Hash(Cert), [Package name], [Hash algorithm], allowed API)
12. 从device OS获取签名证书，根据hash algorithm计算hash(Cert)，并获取package name
13. 判断MNO App的hash(Cert)值和APP的package name是否与profile metadata中的值相同, 判断是否允许调用第6步中的API
14. 获取eUICC信息
15. 获取终端信息响应 (eUICC info, device info)
16. 获取终端信息响应 (eUICC info, device info)
17. profile下载预定
18. 下载预定响应 ([SM-DP+ addr], [MatchingID])
19. 触发profile下载（SM-DP+ address，MatchingID], [ICCID]）
20. 触发profile下载（SM-DP+ address，MatchingID, [ICCID]）
21. 获取profile信息 (ICCID)
22. 返回profile 元数据(Hash(Cert), [Package name], [Hash algorithm], allowed API)
23. 从device OS获取签名证书，根据hash algorithm计算hash(Cert)，并获取package name
24. 判断MNO App的证书hash值和/或APP的package name是否和profile metadata中的值相同，是否允许访问所述API，根据EID2选择eUICC
25. profile下载到eUICC

图 7

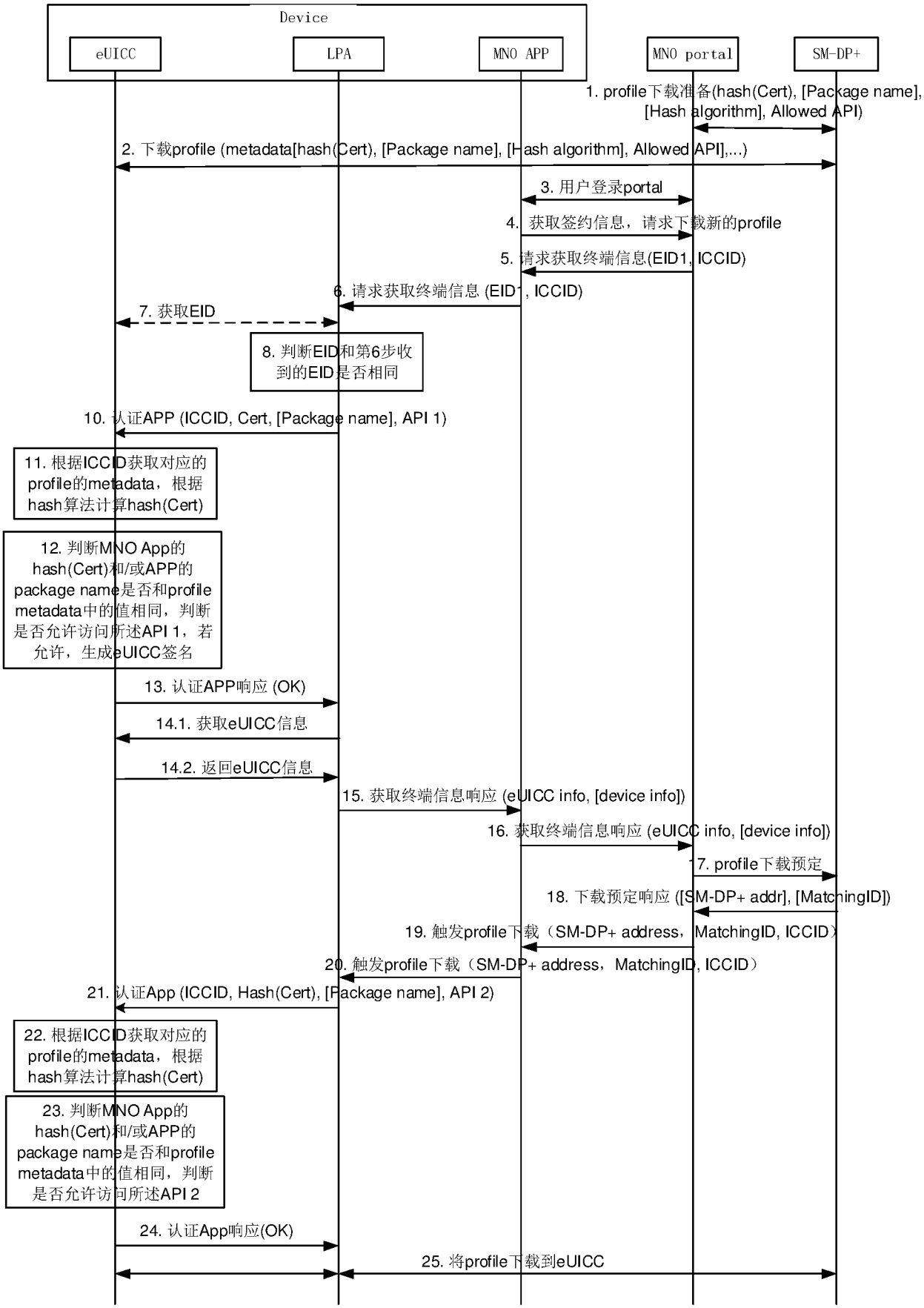
Device
eUICC
LPA
MNO APP
MNO portal
SM-DP+
1. profile下载准备(hash(Cert), [Package name], [Hash algorithm], Allowed API)
2. 下载profile (metadata[hash(Cert), [Package name], [Hash algorithm], Allowed API],...)
3. 用户登录portal
4. 获取签约信息，请求下载新的profile
5. 请求获取终端信息(EID1, ICCID)
6. 请求获取终端信息 (EID1, ICCID)
7. 获取EID
8. 判断EID和第6步收到的EID是否相同
10. 认证APP (ICCID, Cert, [Package name], API 1)
11. 根据ICCID获取对应的profile的metadata，根据hash算法计算hash(Cert)
12. 判断MNO App的hash(Cert)和/或APP的package name是否和profile metadata中的值相同，判断是否允许访问所述API 1，若允许，生成eUICC签名
13. 认证APP响应 (OK)
14.1. 获取eUICC信息
14.2. 返回eUICC信息
15. 获取终端信息响应 (eUICC info, [device info])
16. 获取终端信息响应 (eUICC info, [device info])
17. profile下载预定
18. 下载预定响应 ([SM-DP+ addr], [MatchingID])
19. 触发profile下载（SM-DP+ address，MatchingID, ICCID）
20. 触发profile下载（SM-DP+ address，MatchingID, ICCID）
21. 认证App (ICCID, Hash(Cert), [Package name], API 2)
22. 根据ICCID获取对应的profile的metadata，根据hash算法计算hash(Cert)
23. 判断MNO App的hash(Cert)和/或APP的package name是否和profile metadata中的值相同，判断是否允许访问所述API 2
24. 认证App响应(OK)
25. 将profile下载到eUICC

图 8

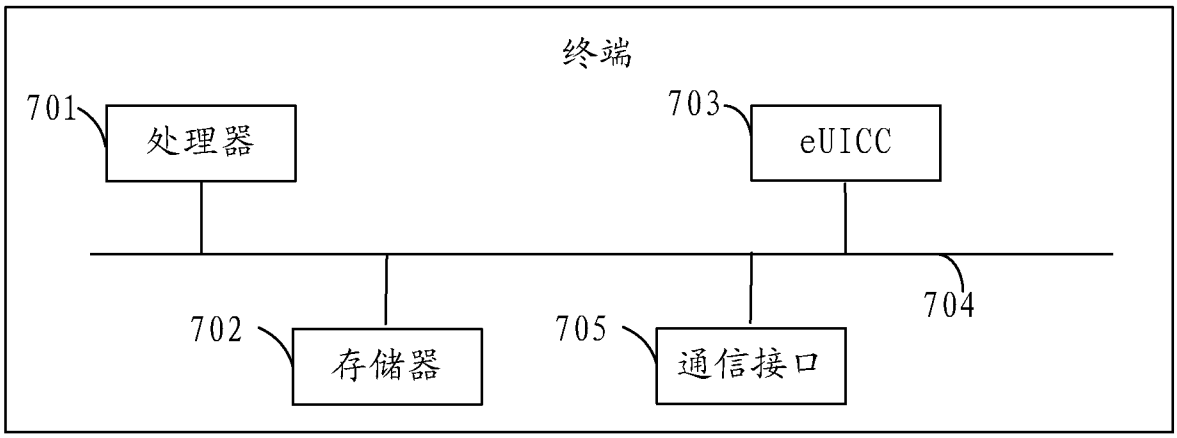
终端
701
处理器
703
eUICC
704
702
存储器
705
通信接口

图 9

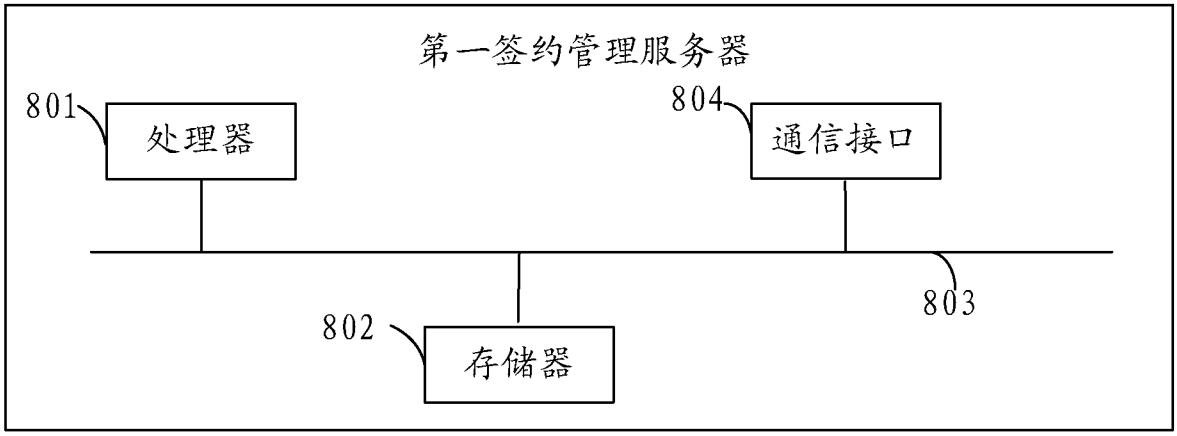
第一签约管理服务器
801
处理器
804
通信接口
803
802
存储器

图 10

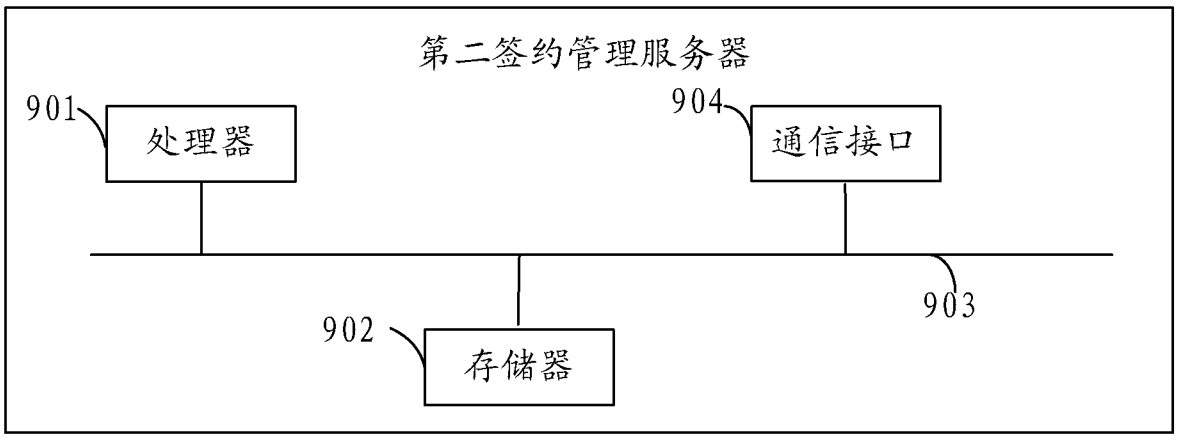
第二签约管理服务器
901
处理器
904
通信接口
903
902
存储器

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/071185

A. CLASSIFICATION OF SUBJECT MATTER

H04W 8/20 (2009.01) i; H04W 88/18 (2009.01) i; H04W 12/06 (2009.01) 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)

H04L; H04W

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)

CNABS, CNTXT, CNKI, VEN, USTXT, EPTXT, WOTXT: 签约数据库, 文件, 简档, eUICC, 嵌入式通用集成电路卡, LPA, 本地文件助手, 认证, 验证, 应用, APP, 运营商, MNO, 下载, profile, local profile assistant, authentication, application, operator, download

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2016003200 A1 (SAMSUNG ELECTRONICS CO., LTD.), 07 January 2016 (07.01.2016), entire document	1-51
A	CN 104703170 A (HUAWEI DEVICE CO., LTD.), 10 June 2015 (10.06.2015), entire document	1-51
A	CN 103974250 A (HUAWEI DEVICE CO., LTD.), 06 August 2014 (06.08.2014), entire document	1-51
A	CN 104703199 A (HUAWEI DEVICE CO., LTD.), 10 June 2015 (10.06.2015), entire document	1-51
A	US 2015180847 A1 (NIX, J.A.), 25 June 2015 (25.06.2015), entire document	1-51

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 September 2017	20 September 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer SU, Qin Telephone No. (86-10) 62089136

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/071185

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2016003200 A1	07 January 2016	KR 20160003992 A	12 January 2016
		US 2016006728 A1	07 January 2016
		EP 2963955 A1	06 January 2016
		CN 106664545 A	10 May 2017
		IN 201647044702 A	05 May 2017
CN 104703170 A	10 June 2015	EP 3065431 A4	26 October 2016
		US 2016283216 A1	29 September 2016
		WO 2015081882 A1	11 June 2015
		EP 3065431 A1	07 September 2016
		CN 104703170 B	12 April 2017
CN 103974250 A	06 August 2014	None	
CN 104703199 A	10 June 2015	US 2016286380 A1	29 September 2016
		KR 20160089522 A	27 July 2016
		JP 2016541200 A	28 December 2016
		JP 6139800 B2	31 May 2017
		KR 101665492 B1	12 October 2016
		WO 2015081884 A1	11 June 2015
		EP 3073777 A1	28 September 2016
US 2015180847 A1	25 June 2015	US 9351162 B2	24 May 2016

国际检索报告

国际申请号
PCT/CN2017/071185

A. 主题的分类

H04W 8/20(2009.01)i; H04W 88/18(2009.01)i; H04W 12/06(2009.01)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)

H04L; H04W

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））

CNABS, CNTXT, CNKI, VEN, USTXT, EPTXT, WOTXT：签约数据库，文件，简档，eUICC，嵌入式通用集成电路卡，LPA，本地文件助手，认证，验证，应用，APP，运营商，MNO，下载，profile，local profile assistant，authentication，application，operator，download

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
A	WO 2016003200 A1 (三星电子株式会社) 2016年 1月 7日 (2016-01-07) 全文	1-51
A	CN 104703170 A (华为终端有限公司) 2015年 6月 10日 (2015-06-10) 全文	1-51
A	CN 103974250 A (华为终端有限公司) 2014年 8月 6日 (2014-08-06) 全文	1-51
A	CN 104703199 A (华为终端有限公司) 2015年 6月 10日 (2015-06-10) 全文	1-51
A	US 2015180847 A1 (NIX JOHN A) 2015年 6月 25日 (2015-06-25) 全文	1-51

☐ 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	国际检索报告邮寄日期
2017年 9月 2日	2017年 9月 20日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 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 苏琴 电话号码 (86-10)62089136

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/071185

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
WO	2016003200	A1	2016年 1月 7日	KR	20160003992	A	2016年 1月 12日
				US	2016006728	A1	2016年 1月 7日
				EP	2963955	A1	2016年 1月 6日
				CN	106664545	A	2017年 5月 10日
				IN	201647044702	A	2017年 5月 5日
CN	104703170	A	2015年 6月 10日	EP	3065431	A4	2016年 10月 26日
				US	2016283216	A1	2016年 9月 29日
				WO	2015081882	A1	2015年 6月 11日
				EP	3065431	A1	2016年 9月 7日
				CN	104703170	B	2017年 4月 12日
CN	103974250	A	2014年 8月 6日	无			
CN	104703199	A	2015年 6月 10日	US	2016286380	A1	2016年 9月 29日
				KR	20160089522	A	2016年 7月 27日
				JP	2016541200	A	2016年 12月 28日
				JP	6139800	B2	2017年 5月 31日
				KR	101665492	B1	2016年 10月 12日
				WO	2015081884	A1	2015年 6月 11日
				EP	3073777	A1	2016年 9月 28日
US	2015180847	A1	2015年 6月 25日	US	9351162	B2	2016年 5月 24日