(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112913263 A
(43)申请公布日 2021.06.04

(21)申请号 201980068989.0

(22)申请日 2019.10.21

(30)优先权数据
10-2018-0125437 2018.10.19 KR
10-2018-0132539 2018.10.31 KR

(85)PCT国际申请进入国家阶段日
2021.04.19

(86)PCT国际申请的申请数据
PCT/KR2019/013822 2019.10.21

(87)PCT国际申请的公布数据
WO2020/080909 EN 2020.04.23

(71)申请人 三星电子株式会社
地址 韩国京畿道

(72)发明人 李德基 朴钟汉 李慧远 李祥洙

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 刘虹

(51)Int.Cl.
H04W 4/60(2018.01)
H04W 8/20(2009.01)
H04W 12/069(2021.01)

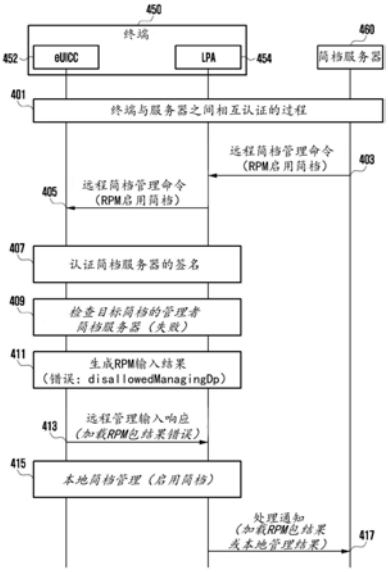
权利要求书2页 说明书35页 附图24页

(54)发明名称

用于处理远程简档管理异常的方法和装置

(57)摘要

本公开涉及一种用于将IoT技术与支持高于超4G系统的数据传输速率的数据传输速率的5G通信系统组合的通信技术及其系统。本公开适用于基于5G通信技术和IoT相关技术的智能服务(例如,智能家居、智能建筑、智能城市、智能汽车或联网汽车、医疗保健、数字教育、零售业务、安保和安全相关服务)。一种终端的方法包括:从简档服务器接收与第一功能相关的请求;识别是否能够执行所述第一功能;如果无法执行所述第一功能,则识别是否有可能切换为第二功能;以及如果有可能切换为所述第二功能,则基于所述第二功能处理所述请求。终端包括收发器和至少一个处理器。至少一个处理器从简档服务器接收远程管理命令,确定是否能够处理远程管理命令,执行接收到的远程管理命令,如果需要,则根据执行远程管理命令的结果将远程管理命令切换为本地管理命令,并且控制收发器以便将执行远程管理命令或本地管理命令的结果发送到简档服务器。



CN 112913263 A

1.一种终端的方法,所述方法包括:

从简档服务器接收与第一功能相关的请求;

识别是否能够执行所述第一功能;

如果无法执行所述第一功能,则识别是否有可能切换为第二功能;以及

如果有可能切换为所述第二功能,则基于所述第二功能处理所述请求。

2.根据权利要求1所述的方法,其中,通过包括至少一个远程管理命令和简档服务器的数字签名的终端响应消息或者通过包括简档标识符的命令代码执行请求消息来发送与第一功能相关的请求。

3.根据权利要求1所述的方法,其中,所述识别是否能够执行所述第一功能还包括:基于所述终端的嵌入式通用集成电路卡(eUICC)的版本信息或eUICC的功能列表来识别是否能够执行所述第一功能。

4.根据权利要求1所述的方法,其中,所述识别是否有可能切换为第二功能还包括:基于所述终端的目标简档的简档服务器列表、所述终端的eUICC的版本信息或所述eUICC的功能列表来识别是否有可能切换为所述第二功能。

5.根据权利要求1所述的方法,其中,所述识别是否有可能切换为第二功能包括附加地认证所述简档服务器。

6.根据权利要求5所述的方法,其中,基于简档服务器是否包括在终端的简档服务器列表中,或者特定数据是否包括在与第一功能相关的请求中来执行附加认证。

7.根据权利要求1所述的方法,还包括:

将基于所述第二功能的处理结果切换为所述第一功能的处理结果;以及

将切换的处理结果发送到简档服务器。

8.一种终端,包括:

收发器;以及

控制器,被配置为从简档服务器接收与第一功能相关的请求,识别是否能够执行所述第一功能,如果无法执行所述第一功能,则识别是否有可能切换为第二功能,并且如果有可能切换为所述第二功能,则基于所述第二功能处理所述请求。

9.根据权利要求8所述的终端,其中,通过包括至少一个远程管理命令和简档服务器的数字签名的终端响应消息或者通过包括简档标识符的命令代码执行请求消息来发送与第一功能相关的请求。

10.根据权利要求8所述的终端,其中,所述控制器被配置为基于所述终端的嵌入式通用集成电路卡(eUICC)的版本信息或eUICC的功能列表来识别是否能够执行所述第一功能。

11.根据权利要求11所述的终端,其中,所述控制器被配置为基于所述终端的目标简档的简档服务器列表、所述终端的嵌入式通用集成电路卡(eUICC)的版本信息或eUICC的功能列表来识别是否有可能切换为所述第二功能。

12.根据权利要求8所述的终端,其中,所述控制器被配置为附加地认证所述简档服务器。

13.根据权利要求12所述的终端,其中,所述控制器被配置为基于简档服务器是否包括在终端的简档服务器列表中或者特定数据是否包括在与第一功能相关的请求中来认证简档服务器。

14.根据权利要求8所述的终端,其中,所述控制器被配置为将基于所述第二功能的处理结果切换为所述第一功能的处理结果,并且将切换的处理结果发送到所述简档服务器。

用于处理远程简档管理异常的方法和装置

技术领域

[0001] 本公开涉及能够远程管理简档的方法和装置。

[0002] 另外，本公开涉及一种无线通信系统，更具体地，涉及一种用于在无线通信系统中将用于通信服务的SIM简档下载和安装到终端，然后建立通信连接的方法和装置。

[0003] 另外，本公开涉及用于高效地管理关于一个或更多个终端的SIM简档的方法和装置。

背景技术

[0004] 为了满足在4G通信系统商业化之后增长的无线数据业务需求，已经做出了开发改进的5G通信系统或准5G通信系统的努力。因此，5G通信系统或准5G通信系统被称为超4G网络通信系统或后LTE系统。为了实现高数据传输速率，正在考虑在mmWave频带(例如，60GHz频带)中实现5G通信系统。在5G通信系统中，正在讨论诸如波束成形、大规模MIMO、全维MIMO(FD-MIMO)、阵列天线、模拟波束成形和大规模天线技术之类的技术作为减轻超高频带中的传播路径损耗并增加传播传输距离的手段。此外，已经开发了诸如演进小型小区、高级小型小区、云无线电接入网络(云RAN)、超密集网络、设备到设备通信(D2D)、无线回程、移动网络、协作通信、协调多点(CoMP)和干扰消除的技术，以改进5G通信系统中的系统网络。此外，5G系统已经开发了诸如混合FSK和QAM调制(FQAM)和滑动窗口叠加编码(SWSC)的高级编码调制(ACM)方案，以及诸如滤波器组多载波(FBMC)、非正交多址(NOMA)和稀疏码多址(SCMA)的高级接入技术。

[0005] 同时，互联网已经从人类生成和消费信息的面向人类的连接网络演进为物联网(IoT)网络，其中，诸如对象的分布式组件交换和处理信息。已经出现了万物联网(IoE)技术，其中，涉及与云服务器等的连接的大数据处理技术与IoT技术相结合。为了实现IoT，正在对诸如感测技术、有线/无线通信和网络基础设施、服务接口技术和安全技术的技术因素进行研究，因此需要诸如传感器网络、机器到机器(M2M)、机器类型通信(MTC)等的技术用于对象之间的连接。在IoT环境中，可以提供智能互联网技术(IT)服务，其收集和分析从连接的对象生成的数据并在人们的生活中创造新的价值。通过传统信息技术(IT)和各种行业的融合，IoT可以应用于诸如智能家居、智能建筑、智能城市、智能汽车、联网汽车、智能电网、医疗保健、智能家用电器或高科技医疗服务的领域。

[0006] 因此，进行将5G通信应用于IoT网络的各种尝试。例如，诸如传感器网络、M2M通信和MTC的5G通信技术通过波束成形、MIMO和阵列天线方案来实现。云RAN作为大数据处理技术的应用可以是5G技术和IoT技术的融合的示例。

[0007] 如上所述，移动通信系统的发展已经使得可以提供各种服务，因此需要一种用于有效地提供这种服务的方案。

[0008] 上述信息仅作为背景技术信息呈现，以帮助理解本公开。关于上述内容中的任何一个是否能够作为关于本公开的现有技术适用，没有做出任何确定，也没有做出断言。

发明内容

[0009] 技术问题

[0010] 实施例提供了一种能够在移动通信系统中有效地提供服务的装置和方法。

[0011] 特别地，本公开的一方面在于提供一种方法和装置，其中，如果无法处理来自简档服务器的远程管理命令，则异常地处理远程管理命令。

[0012] 另外，本公开的另一方面在于提供一种装置和方法，其中，在通信系统中不可能操纵其中安装有eUICC的终端的屏幕的情况下(例如，如果需要远程管理终端)，可以远程管理用于在终端中安装简档、启用安装的简档、禁用安装的SIM简档等的操作。

[0013] 技术方案

[0014] 根据本公开的一方面，一种终端的方法包括：从简档服务器接收与第一功能相关的请求；识别是否能够执行所述第一功能；如果无法执行所述第一功能，则识别是否有可能切换为第二功能；以及如果有可能切换为所述第二功能，则基于所述第二功能处理所述请求。

[0015] 根据本公开的一方面，一种终端包括：收发器；以及控制器，其被配置为从简档服务器接收与第一功能相关的请求，识别是否能够执行第一功能，如果无法执行第一功能，则识别是否有可能切换为第二功能，并且如果有可能切换为第二功能，则基于第二功能处理请求。

[0016] 根据实施例，可以提供一种方法，包括：从简档服务器接收远程简档管理命令；识别所述远程简档管理命令是否能够被处理；附加地识别所述简档服务器是否是管理者简档服务器；处理所述远程简档管理命令并附加地识别其结果；基于识别的结果，将远程简档管理命令切换为本地简档管理命令，并对其进行处理；以及将处理远程简档管理命令和/或本地简档管理命令的结果作为回复发送到简档服务器。

[0017] 另外，根据一些实施例，可以提供一种终端：收发器；以及控制器，其被配置为从简档服务器接收远程简档管理命令，识别是否能够处理远程简档管理命令，附加地识别简档服务器是否是管理者简档服务器，处理远程简档管理命令并附加地识别其结果，基于识别的结果将远程简档管理命令切换为本地简档管理命令并对其进行处理，并将处理远程简档管理命令或本地简档管理命令的结果作为回复发送到简档服务器。

[0018] 本公开中追求的技术主题可以不限于上述技术主题，并且本公开领域的技术人员可以通过以下描述清楚地理解未提及的其他技术主题。

[0019] 根据各种实施例，通信系统中的终端可以基于eUICC是否能够处理远程管理命令并且基于管理安装的简档的SM-DP+信息等来检查已经发送远程管理命令的简档服务器的权限，并且如果由于简档中没有管理者简档服务器信息而无法检查关于简档服务器的远程管理命令的权限，或者如果eUICC无法处理远程管理命令，则可以将远程管理命令切换为本地管理命令并执行该本地管理命令。

[0020] 另外，根据实施例，即使无法控制其中安装有eUICC的终端，也可以远程管理终端中的简档。

[0021] 在进行下面的详细描述之前，阐述贯穿本专利文件使用的特定词语和短语的定义可能是有利的：术语“包括”和“包含”及其派生词意指包括但不限于；术语“或”是包含性的，意指和/或；短语“与...相关联”和“与其相关联”及其派生词可以意指包括、被包括在...

内、与...互连、包含、被包含在...内、连接到或与...连接、耦合到或与...耦合、可与...通信、与...协作、交错、并置、接近于、绑定到或与...绑定、具有、具有...的性质等;并且术语“控制器”意指控制至少一个操作的任何设备、系统或其部分,这样的设备可以以硬件、固件或软件或其中至少两个的某种组合来实现。应当注意,与任何特定控制器相关联的功能可以是集中式的或分布式的,无论是本地的还是远程的。

[0022] 此外,下面描述的各种功能可以由一个或更多个计算机程序实现或支持,每个计算机程序由计算机可读程序代码形成并体现在计算机可读介质中。术语“应用”和“程序”是指适于在合适的计算机可读程序代码中实现的一个或更多个计算机程序、软件组件、指令集、过程、函数、对象、类、实例、相关数据或其部分。短语“计算机可读程序代码”包括任何类型的计算机代码,包括源代码、目标代码和可执行代码。短语“计算机可读介质”包括能够由计算机接入的任何类型的介质,诸如只读存储器(ROM)、随机存取存储器(RAM)、硬盘驱动器、压缩盘(CD)、数字视频盘(DVD)或任何其他类型的存储器。“非暂态”计算机可读介质不包括传输暂态电信号或其他信号的有线、无线、光学或其他通信链路。非暂时性计算机可读介质包括能够永久存储数据的介质和可以存储数据并稍后重写的介质,诸如可重写光盘或可擦除存储器设备。

[0023] 贯穿本专利文件提供了对特定单词和短语的定义,本领域普通技术人员应当理解,在许多情况下(如果不是大多数情况),这样的定义适用于这样定义的单词和短语的先前以及将来的使用。

[0024] 本发明的有益效果

[0025] 根据各种实施例,通信系统中的终端可以基于eUICC是否能够处理远程管理命令并且基于管理安装的简档的SM-DP+信息等来检查已经发送远程管理命令的简档服务器的权限,并且,如果由于简档中没有管理者简档服务器信息而无法检查关于简档服务器的远程管理命令的权限,或者如果eUICC无法处理远程管理命令,则可以将远程管理命令切换为本地管理命令并执行该本地管理命令。

[0026] 另外,根据实施例,即使无法控制其中安装有eUICC的终端,也可以远程管理终端中的简档。

附图说明

[0027] 为了更完整地理解本公开及其优点,现在结合附图参考以下描述,其中相同的附图标记表示相同的部分:

[0028] 图1示出用于由根据实施例的终端通过使用其中加载了嵌入式简档的UICC来连接到移动通信网络的方法的示图;

[0029] 图2示出根据实施例的终端从简档服务器接收远程管理命令并对其进行处理的正常过程的示例的示图;

[0030] 图3示出正常过程的示例的示图,其中,根据实施例的终端已经从简档服务器接收到远程管理命令,但是由于简档服务器未被描述为目标简档的管理者简档服务器(管理SM-DM+)而在远程管理中失败;

[0031] 图4A示出终端操作过程的示例的示图,其中,根据实施例的终端已经从简档服务器接收到远程管理命令,但是由于简档服务器未被描述为目标简档的管理者简档服务器而

将远程管理命令切换为本地管理命令；

[0032] 图4B示出终端操作过程的示例的示图，其中，根据实施例的终端已经从简档服务器接收到远程管理命令，但是由于简档服务器未被描述为目标简档的管理者简档服务器而执行将远程管理命令切换为本地管理命令的连续操作；

[0033] 图5示出终端操作过程的示例的示图，其中，根据实施例的终端已经从简档服务器接收到远程管理命令，但是由于eUICC不支持远程简档管理而将远程管理命令切换为本地管理命令；

[0034] 图6A示出根据实施例的终端通过特定应用程序成功地处理命令代码的终端操作过程的示例的示图；

[0035] 图6B示出根据实施例的终端未能通过特定应用程序处理命令代码的终端操作过程的示例的示图；

[0036] 图6C示出终端操作过程的示例的示图，其中，当根据实施例的终端通过特定应用程序处理命令代码时，LPA将命令代码切换为激活代码并处理该激活代码；

[0037] 图7示出终端操作过程的示例的示图，其中，根据实施例的终端已经从简档服务器接收到远程管理命令，但是未能认证简档服务器的签名并因此拒绝远程管理；

[0038] 图8示出正常操作过程的示例的示图，其中，根据实施例的终端已经从简档服务器接收到远程管理命令，但是由于eUICC不支持远程简档管理而无法进行远程管理；

[0039] 图9示出根据实施例的终端用本地管理命令替换远程管理命令的过程的示例的示图；

[0040] 图10示出根据实施方案的终端用等同的第二版本功能替换无法由第二版本eUICC处理的第一版本eSIM功能的过程的示例的示图；

[0041] 图11A示出根据本公开的用于下载简档的方法的示图，并且图11B示出根据本公开的用于下载简档的方法的示图；

[0042] 图12A示出根据实施例的用于安装和启用简档的方法的示图，并且图12B示出根据实施例的用于安装和启用简档的方法的示图；

[0043] 图13A示出根据实施例的用于安装和启用简档的另一方法的示图，并且图13B示出根据实施例的用于安装和启用简档的另一方法的示图；

[0044] 图14AA示出根据实施例的用于安装和启用简档的另一方法的示图，图14AB示出根据实施例的用于安装和启用简档的另一方法的示图，并且图14B示出根据实施例的用于安装和启用简档的另一方法的示图；

[0045] 图15示出根据实施例的可以与图12、图13和图14一起实现的更具体的操作的示图；

[0046] 图16示出根据实施例的终端的配置的示图；

[0047] 图17示出根据实施例的简档服务器的配置的示图；以及

[0048] 图18示出根据实施例的服务服务器的配置的示图。

具体实施方式

[0049] 下面讨论的示图1至图18以及用于在本专利文件中描述本公开的原理的各种实施例仅是说明性的，并且不应以任何方式解释为限制本公开的范围。本领域技术人员将理解，

本公开的原理可以在任何适当布置的系统或设备中实现。

[0050] 在下文中,将参考附图详细描述本公开的实施例。

[0051] 在描述实施例时,可以省略对本领域技术人员已知的并且与本公开不直接相关的技术的描述。这种不必然要的描述的省略旨在防止模糊本公开的主要构思,并且更清楚地传达主要构思。

[0052] 出于相同的原因,在附图中,一些元件可以被夸大、省略或示意性地示出。此外,每个元件的大小不完全反映实际大小。在附图中,相同或对应的元件设置有相同的附图标记。

[0053] 通过参考下面结合附图详细描述的实施例,本公开的优点和特征以及实现它们的方式将是清楚的。然而,本公开不限于下面描述的实施例,而是可以以各种不同的形式实现。单独提供实施例是为了使本公开完整并且向本公开所属领域的技术人员通知本公开的全部范围。本公开仅由权利要求的范围限定。在整个说明书中,相同或相似的附图标记表示相同或相似的元件。

[0054] 这里,将理解,流程图图示的每个框以及流程图图示中的框的组合可以由计算机程序指令实现。这些计算机程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以生成机器,使得经由计算机或其他可编程数据处理装置的处理器执行的指令创建用于实现一个或更多个流程图框中指定的功能的装置。这些计算机程序指令还可以存储在计算机可用或计算机可读存储器中,该计算机可用或计算机可读存储器可以指示计算机或其他可编程数据处理装置以特定方式起作用,使得存储在计算机可用或计算机可读存储器中的指令生成包括实现一个或更多个流程图框中指定的功能的指令装置的制品。计算机程序指令还可以被加载到计算机或其他可编程数据处理装置上,以促使在计算机或其他可编程装置上执行一系列操作步骤,以生成计算机实现的过程,使得在计算机或其他可编程装置上执行的指令提供用于实现在一个或更多个流程图框中指定的功能的步骤。

[0055] 流程图图示的每个框可以表示代码的模块、片段或部分,其包括用于实现指定的逻辑功能的一个或更多个可执行指令。还应当注意,在一些替代实施方式中,框中提到的功能可以不按顺序发生。例如,连续示出的两个框实际上可以基本上同时执行,或者这些框有时可以以相反的顺序执行,这取决于所涉及的功能。

[0056] 如本文所使用的,“单元”是指执行预定功能的软件元件或硬件元件,诸如现场可编程门阵列(FPGA)或专用集成电路(ASIC)。然而,“单元”并不总是具有限于软件或硬件的含义。“单元”可以被构造为存储在可寻址存储介质中或执行一个或更多个处理器。因此,“单元”包括例如软件元素、面向对象的软件元素、类元素或任务元素、进程、函数、属性、过程、子例程、程序代码段、驱动程序、固件、微代码、电路、数据、数据库、数据结构、表、阵列和参数。由“单元”提供的元件和功能可以组合成较少数量的元件“单元”,或者分成较大数量的元件“单元”。此外,元件和“单元”可以被实现以再现设备或安全多媒体卡内的一个或更多个CPU。

[0057] 提供本文使用的特定术语是为了便于理解本公开,并且在不脱离本公开的精神和范围的情况下,可以将这些特定术语改变为其他形式。

[0058] 通用集成电路卡(UICC)是在被插入移动通信终端等的同时使用的智能卡,并且也被称为UICC卡。UICC可以包括用于接入移动通信运营商的网络的接入控制模块。接入控制

模块的示例包括通用订户身份模块(USIM)、订户身份模块(SIM)和IP多媒体服务身份模块(ISIM)。包括USIM的UICC也被称为USIM卡。同样地,包括SIM模块的UICC也被称为SIM卡。

[0059] 在本公开中,术语“SIM卡”、“UICC卡”、“USIM卡”和“包括ISIM的UICC”在下文中可以以相同的含义使用。此外,可以对USIM卡、ISIM卡或普通UICC卡进行与SIM卡相同的技术应用。

[0060] SIM卡存储移动通信订户的个人信息,在接入移动通信网络时认证订户,并生成业务安全密钥,从而实现安全的移动通信使用。

[0061] 在本公开的提议时间点,SIM卡通常应特定移动通信运营商的请求被制造为用于对应运营商的专用卡,并且用于接入对应运营商的网络的认证信息(例如,USIM应用、国际移动订户身份(IMSI)、K值或OPc值)在卡被装运之前被加载到卡中。因此,所制造的SIM卡被交付给对应的移动通信运营商,然后提供给订户,并且还可以通过使用诸如空中下载(OTA)之类的技术来管理(例如,安装、修改或删除)UICC内的应用。订户可以将UICC卡插入他/她自己的移动通信终端,从而使用对应移动通信运营商的网络和应用服务。当更换终端时,可以将UICC卡从现有终端移动/插入到新终端中,使得存储在UICC卡中的相同认证信息、移动通信电话号码、个人电话号码簿等可以在新终端中。

[0062] 然而,当移动通信终端用户想要从另一移动通信运营商接收服务时,SIM卡给他/她带来不便。也就是说,为了从移动通信运营商接收服务,移动通信终端用户需要不方便地物理获取SIM卡。例如,当他/她正在另一国家旅行时,需要获取本地SIM以接收本地移动通信服务,这是不方便的。漫游服务可以在一定程度上消除这种不便,但是存在服务相对昂贵的问题,并且如果相关通信运营商之间没有联系,则服务不可用。

[0063] 如果SIM模块被远程下载并安装在UICC卡中,则可以在一定程度上消除这种不便。也就是说,可以在用户期望的时间点将要使用的移动通信服务的SIM模块下载到UICC卡。可以在UICC卡中下载和安装多个SIM模块,并且可以仅选择和使用一个SIM模块。这样的UICC卡可以嵌入在终端中或者可以不嵌入在其中。在被嵌入终端中的同时使用的UICC被称为嵌入式UICC(eUICC)。eUICC通常可以指UICC卡,其在被嵌入终端中的同时被使用,并且其被配置为使得可以远程下载和选择SIM模块。

[0064] 在本公开中,被配置为使得可以远程下载和选择SIM模块的任何类型的UICC卡整体上都将被称为eUICC。也就是说,被配置为使得可以远程下载和选择SIM模块的UICC卡在下文中将被称为eUICC,而不管其是否嵌入终端中。此外,下载的SIM模块信息通常将被称为eUICC简档,或者更简单地称为简档。

[0065] 在下文中,将更详细地描述本公开中使用的术语。

[0066] 如本文所使用的,“UICC”是在被插入移动通信终端中的同时使用的智能卡,并且可以指被配置为存储移动通信订户的个人信息(诸如网络接入认证信息、电话号码簿和SMS)的芯片,使得当接入移动通信网络(例如,GSM、WDCMA或LTE)时,订户被认证,并且生成流量安全密钥,从而实现安全的移动通信使用。根据订户接入的移动通信网络的类型,UICC可以具有加载在其中的通信应用(例如,SIM、USIM或ISIM)。UICC还可以提供用于在其中加载各种应用(例如,电子钱包、票务和电子护照)的更上层安全功能。

[0067] 如本文所使用的,“eUICC”是指嵌入终端中的芯片型安全模块,其无法插入终端/从终端拆卸(非“可附接/可拆卸类型”)。可以通过使用OTA技术来下载简档并将其安装在

eUICC中。换句话讲，eUICC可以是被配置为使得可将简档下载并安装在其中的UICC。

[0068] 在本公开中，用于通过使用OTA技术下载简档并将其安装在eUICC中的方法也适用于可以插入终端和从终端拆卸的可附接/可拆卸UICC。也就是说，实施例也适用于被配置为使得可以通过使用OTA技术将简档下载和安装在其中的UICC。尽管将参考被配置为使得可以将简档下载和安装在其中的eUICC来描述本公开，但是本公开的内容不限于嵌入在终端(eUICC)中的芯片型安全模块，并且还可适用于被配置为使得可以将简档下载和安装在其中的可附接/可拆卸UICC。

[0069] 在本公开中，术语“UICC”可以与“SIM”互换使用，并且术语“eUICC”可以与“eSIM”互换使用。

[0070] 如本文所使用的，“简档”可以指存储在UICC中并且以软件类型打包的应用、文件系统、认证密钥等。

[0071] 如本文所使用的，“USIM简档”可以在与简档相同的意义上使用，或者可以指包括在简档内部的USIM应用中并且以软件类型打包的信息。

[0072] 如本文所使用的，终端的启用简档的操作可以指将简档的状态改变为“启用”，从而将终端配置为能够通过已经提供简档的通信运营商接收通信服务的操作。处于启用状态的简档可以被描述为“启用简档”。

[0073] 如本文所使用的，终端的禁用简档的操作可以指将简档的状态改变为“禁用”并且由此将终端配置为无法通过已经提供简档的通信运营商接收通信服务的操作。处于禁用状态的简档可以被描述为“禁用简档”。

[0074] 如本文所使用的，终端的删除简档的操作可以指将对应简档的状态改变为“被删除”并且从而将终端配置为不再能够启用或禁用简档的操作。处于被删除状态的简档可以被描述为“被删除简档”。

[0075] 如本文所使用的，终端的启用、禁用或删除简档的操作可以具有以下含义：代替立即将每个简档的状态改变为“启用”、“禁用”或“删除”，终端可以首先关于每个简档进行“要启用”、“要禁用”或“要删除”的标记，并且在执行特定操作(例如，执行“刷新”或“重置”命令)之后，终端或终端的UICC可以将每个简档改变为“启用”、“禁用”或“删除”。对关于特定简档的已调度状态(例如，“要启用”、“要禁用”或“要删除”)进行标记的操作不必然限于关于一个简档标记一个已调度状态，并且还可以用相同或不同的已调度状态标记一个或更多个简档，用一个或更多个已调度状态标记一个简档，或者用相同或不同的一个或更多个已调度状态标记一个或更多个简档。

[0076] 此外，当终端用一个或更多个调度状态标记特定简档时，可将两个标记合并为一个。例如，如果特定简档标记有“要禁用”和“要删除”，则简档可以整体标记有“要禁用和删除”。

[0077] 另外，终端用已调度状态标记一个或更多个简档的操作可以连续或同时执行。另外，终端用已调度状态标记一个或更多个简档，然后改变简档的实际状态的操作可以依次或同时执行。

[0078] 在本公开中，简档供应服务器可以包括生成简档、加密所生成的简档、生成远程简档管理指令或加密所生成的远程简档管理指令的功能。简档供应服务器可以表示为以下中的至少一个：订阅管理者数据准备(SM-DP)、订阅管理者数据准备增强(SM-DP+)、管理者简

档服务器、管理订阅管理者数据准备增强(管理SM-DP+)、简档域的脱卡实体、简档加密服务器、简档生成服务器、简档供应者(PP)、简档提供商和简档供应凭证持有者(PPC持有者)。

[0079] 在本公开中,简档管理服务器可以表示为订阅管理者安全路由(SM-SR)、订阅管理者安全路由增强(SM-SR+)、eUICC简档管理者的脱卡实体、简档管理凭证持有者(PMC持有者)或eUICC管理者(EM)中的至少一个。

[0080] 如本文所使用的,简档供应服务器还可以并入简档管理服务器的功能。因此,下面描述的各种实施例中的简档供应服务器的操作也可以由简档管理服务器执行。同样,关于简档管理服务器或SM-SR描述的操作也可以由简档供应服务器执行。另外,如本文所使用的简档供应服务器或简档管理服务器可以表示为简档服务器。简档服务器可以是简档供应服务器或简档管理服务器中的一个,或者可以是包括简档供应服务器和简档管理服务器两者的设备。另外,简档供应服务器和简档管理服务器可以分别被称为第一简档服务器和第二简档服务器。

[0081] 如本文所使用的,开放/中介服务器可以表示为订阅管理者发现服务(SM-DS)、发现服务(DS)、根SM-DS或替代SM-DS中的至少一个。开放/中介服务器可以从一个或更多个简档供应服务器或开放/中介服务器接收注册事件请求或事件注册请求。此外,可以组合使用一个或更多个开放/中介服务器,并且在这种情况下的第一开放/中介服务器不仅可以从简档供应服务器接收事件注册请求,而且可以从第二开放/中介服务器接收事件注册请求。简档服务器还可以包括一个或更多个开放/中介服务器。

[0082] 如本文所使用的,简档供应服务器和开放/中介服务器可以共同被称为远程SIM供应(RSP)服务器。RSP服务器可以表示为订阅管理者XX(SM-XX)。

[0083] 本文中使用的术语“终端”可以被称为移动站(MS)、用户设备(UE)、用户终端(UT)、无线终端、接入终端(AT)、终端、订户单元、订户站(SS)、无线设备、无线通信设备、无线发送/接收单元(WTRU)、移动节点、移动设备或其他术语。

[0084] 终端的各种实施例可以包括蜂窝电话、具有无线通信功能的智能电话、具有无线通信功能的个人数字助理(PDA)、无线调制解调器、具有无线通信功能的便携式计算机、具有无线通信功能的拍摄设备(诸如数字相机)、具有无线通信功能的游戏设备、具有无线通信功能的用于存储和再现音乐的家用电器、能够执行无线互联网接入和浏览的互联网家用电器、以及具有其功能的集成组合的便携式单元或终端。此外,终端可以包括但不限于机器到机器(M2M)终端和机器类型通信(MTC)终端/设备。在本公开中,终端也可以被称为电子设备。

[0085] 在本公开中,电子设备可以具有嵌入其中的UICC,使得可以将简档下载并安装在其中。当电子设备没有嵌入式UICC时,可以将与电子设备物理分离的UICC插入到电子设备中并连接到电子设备。例如,UICC可以以卡类型插入到电子设备中。电子设备可以包括终端,并且终端可以包括UICC,该UICC被配置为使得可以将简档下载并安装在其中。不仅可以将UICC插入到终端中,而且UICC当与终端分离时可以插入其中,还可以插入并连接到终端。例如,被配置为使得简档可以被下载并安装在其中的UICC可以被称为eUICC。

[0086] 在本公开中,终端或电子设备可以包括安装在终端或电子设备中的软件或应用,以便控制UICC或eUICC。例如,安装在终端或电子设备中以便控制UICC或eUICC的软件或应用可以被称为本地简档助理(LPA)。

[0087] 如本文所使用的,“简档标识符”可以被称为简档ID、集成电路卡ID(ICCID)、匹配ID、事件ID、激活代码、激活代码令牌、命令代码、命令代码令牌或与ISD-P或简档域(PD)匹配的因素。简档ID可以指示每个简档的唯一ID。简档标识符可以包括能够对简档进行索引的简档供应服务器(SM-DP+)的地址。

[0088] 在本公开中,eUICC ID可以是嵌入在终端中的唯一ID,并且可以被称为EID。另外,如果eUICC具有预加载在其中的供应简档,则eUICC ID可以是供应简档的简档ID。另外,如果如实施例中那样终端和eUICC芯片未分离,则eUICC ID可以是终端ID。此外,eUICC ID可以指eUICC芯片的特定安全域。

[0089] 在本公开中,“简档容器”可以被称为简档域。简档容器可以是安全域。

[0090] 在本公开中,应用协议数据单元(APDU)可以是终端用于与eUICC互工作的消息。另外,APDU可以是PP或简档管理者(PM)用于与eUICC互工作的消息。

[0091] 在本公开中,简档供应凭证(PPC)可以是用于简档供应服务器和eUICC之间的相互认证、简档加密和签名的手段。PPC可以包括对称密钥、Rivest-Shamir-Adleman(RSA)证书和个人密钥、椭圆曲线密码(ECC)证书和个人密钥、根认证机构(根CA)和证书链中的至少一个。此外,如果存在多个简档供应服务器,则可以关于多个简档供应服务器在eUICC中存储或使用不同PPC。

[0092] 在本公开中,简档管理凭证(PMC)可以是用于简档管理服务器和eUICC之间的相互认证、传输数据加密和签名的手段。PMC可以包括对称密钥、RSA证书和个人密钥、ECC证书和个人密钥、根CA和证书链中的至少一个。另外,如果存在多个简档管理服务器,则可以关于多个简档管理服务器在eUICC中存储或使用不同PMC。

[0093] 在本公开中,ADI可以是应用标识符。该值可以是用于标识eUICC内的不同应用的标识符。

[0094] 在本公开中,术语“事件”可以用于表示简档下载、远程简档管理或用于以综合方式管理/处理简档或eUICC的其他指令。事件可以被称为远程SIM提供操作(或RSP操作)或事件记录。每个事件可以被称为包括与其对应的事件标识符(事件ID或eventID)、匹配标识符(匹配ID或matchingID)或存储事件的简档供应服务器(SM-DP+)或开放/中介服务器(SM-DS)的地址(FQDN、IP地址或URL)中的至少一个的数据。简档下载可以与简档安装互换使用。此外,术语“事件类型”可以用于指示特定事件是简档下载、远程简档管理(例如,删除、启用、禁用、替换或更新)还是用于管理/处理简档或eUICC的另一命令。事件类型可以被称为操作类型(或operationtype)、操作类(或operationclass)、事件请求类型、事件类或事件请求类。

[0095] 在本公开中,术语“简档包”可以与简档互换使用或用于表示特定简档的数据对象,并且可以被称为简档TLV或简档包TLV。如果通过使用加密参数对简档包进行加密,则可以将其称为受保护的简档包(PPP)或受保护的简档包TLV(PPP TLV)。当通过使用只能由特定eUICC解密的加密参数来加密简档包时,可以将其称为绑定简档包(BPP)或绑定简档包TLV(BPP TLV)。简档包TLV可以是以标签/长度/值(TLV)格式表达构成简档的信息的数据集。

[0096] 如本文所使用的,“本地简档管理(LPM)”可以被称为简档本地管理、本地管理、本地管理命令、本地命令、LPM包、简档本地管理包、本地管理包、本地管理命令包或本地命令

包。可以使用LPM以便通过安装在终端中的软件等来改变特定简档的状态(启用、禁用或删除),或者更新特定简档的内容(例如,简档元数据的简档昵称)。LPM可以包括一个或更多个本地管理命令,并且在这种情况下作为每个本地管理命令的目标的简档对于每个本地管理命令可以是相同的或不同的。

[0097] 如本文所使用的,“远程简档管理(RPM)”可以被称为简档远程管理、远程管理、远程管理命令、远程命令、RPM包、简档远程管理包、远程管理包、远程管理命令包或远程命令包。可以使用RPM以便改变特定简档的状态(启用、禁用或删除)或更新特定简档的内容(例如,简档昵称或简档元数据)。RPM可以包括一个或更多个远程管理命令,并且在这种情况下作为每个远程管理命令的目标的简档关于每个远程管理命令可以是相同的或不同的。

[0098] 如本文所使用的,术语“目标简档”可以表示作为本地管理命令或远程管理命令的目标的简档。

[0099] 如本文所使用的,“证书”或“数字证书”可以指用于基于包括一对公开密钥(PK)和秘密密钥(SK)的非对称密钥来相互认证的数字证书。每个证书可以包括一个公开密钥或多于一个的公开密钥、与每个公开密钥对应的公开密钥标识符(PKID)、颁发对应证书的证书颁发者(CI)的ID(证书颁发者ID)、以及数字签名。

[0100] 另外,证书颁发者可以被称为证书颁发者、证书颁发机构(CA)或证书认证机构。

[0101] 在本公开中,“公开密钥”和“公开密钥标识符”可以与以下项互换使用:特定公开密钥或包括所述公开密钥的证书;或特定公开密钥的部分或包括所述公开密钥的证书的部分;或特定公开密钥的运算结果(例如,哈希值)或包括所述公开密钥的证书的运算结果(例如,哈希值);或特定公开密钥的部分的运算结果(例如,哈希值)或包括所述公开密钥的证书的部分的运算结果(例如,哈希值);或存储数据的存储器。

[0102] 在本公开中,如果由证书颁发者颁发的证书(初级证书)用于颁发另一证书(次级证书),或者如果次级证书用于以互连方式颁发第三级或更高级证书,则证书之间的相关性可以被称为证书链或证书层级。用于发布初始证书的CI证书可以被称为证书根、最顶层证书、根CI、根CI证书、根CA或根CA证书。

[0103] 如本文所使用的,“移动运营商”可以指用于向终端提供通信服务的商业公司,并且可以以综合方式用于表示移动运营商的商业支持系统(BSS)、操作支持系统(OSS)、销售点(POS)终端和其他IT系统。此外,如本文使用的移动运营商不限于用于提供通信服务的特定商业公司,而是可以用于表示一个或更多个商业公司的群组或协会(或联盟),或者群组或协会的代表。另外,移动运营商还可以被称为运营商(OP或Op.)、移动网络运营商(MNO)、服务提供商(SP)或简档所有者(PO),并且每个移动运营商可以具有配置或分配给其的至少一个名称和/或对象标识符(OI)。如果移动运营商指一个或更多个商业公司的群组、协会或代表,则特定群组、协会或代表的名称或OID可以是由属于该群组或协会的所有商业公司共享的名称或OID,或者是与对应代表协作的所有商业的名称或OID。

[0104] 在本公开中,“版本”可以指由特定实体支持的规范或协议的版本,并且还可以表示为规范版本号(SVN)等。例如,“LPA版本(或LPA SVN)”可以用作指由终端内部的LPA支持的协议的版本的术语。例如,eUICC版本(或eUICC SVN)可以用作指由终端内的eUICC支持的协议的版本的术语。例如,设备版本(或设备SVN)可以用作指由终端内部的LPA支持的协议的版本和由eUICC支持的协议的版本中的至少一个值的术语。例如,服务器版本(或服务器

SVN)可以用作指由对应服务器支持的协议的版本的术语。例如,简档版本(或简档SVN)可以用作指由对应简档支持的协议的版本的术语。

[0105] 在本公开中,版本可以被表达为从指示对应版本的至少一个数字、界定每个数字的分隔符和指示对应数字描述版本的前缀中选择的至少一个的组合。例如,如果使用三个数字来分别描述版本的主要、次要和修订版本,则特定实体的版本可以通过使用分隔符“.”和前缀“v”来表达,诸如“v3.0.0”,或省略前缀的“3.0.0”。如有必要,数字“.”可以附加地省略,并且特定实体的版本可以仅由主版本指示。应当注意,使用三个数字、特定分隔符和前缀的版本描述的上述示例可以相同地扩展并应用于使用更多数字或其他分隔符和前缀的其他情况。

[0106] 如本文所使用的,关于两个版本的表述“第二版本在第一版本之前”可以被解释为描述第一版本的数字大于描述第二版本的数字的意思,或者由第一版本协议支持的部分或全部功能不被第二版本协议支持的意思。

[0107] 在本公开中,“AKA”可以指认证和密钥协商,并且可以指示用于接入3GPP和3GPP2网络的认证算法。

[0108] 在本公开中,“K”(K值)可以指存储在eUICC中的用于AKA认证算法的加密密钥。

[0109] 在本公开中,“OPc”可以是能够存储在eUICC中的用于AKA认证算法的参数值。

[0110] 在本公开中,“NAA”可以指存储在UICC中以便接入网络的网络接入应用程序,例如USIM或ISIM。NAA可以是网络接入模块。

[0111] 此外,在本公开的以下描述中,当并入本文的已知功能或配置的详细描述可能使本公开的主题相当不清楚时,将省略并入本文的已知功能或配置的详细描述。

[0112] 在下文中,将描述关于以下项的各种实施例:用于生成和管理能够远程管理简档的移动运营商的列表的方法和装置、用于在通信服务中将通信服务下载到终端、安装通信服务并连接通信的方法和装置、以及用于在通信系统中在线下载和安装简档的方法和装置。

[0113] 图1示出用于由根据实施例的终端通过使用终端中的已经加载了嵌入式简档的UICC来连接到移动通信网络的方法的示图。

[0114] 如图1所示,UICC 120可以被插入到终端110中。例如,UICC 120可以是可附接/可拆卸类型,或者可以预先嵌入在终端110中。

[0115] 已经将嵌入式简档加载在其中的UICC的嵌入式简档意味着其中嵌入了“接入信息”,其可以用于接入特定移动运营商。例如,接入信息可以是订户标识符(IMSI)以及与订户标识符一起认证网络所必需的K或Ki值。

[0116] 终端110可以使用UICC 120,以便与移动运营商的认证处理系统(例如,归属位置寄存器(HLR)或AuC)执行认证。例如,认证过程可以是AKA处理器。在认证成功之后,终端110可以通过使用移动通信系统的移动通信网络130来使用移动通信服务(例如,进行电话呼叫或使用移动数据)。

[0117] 图2示出根据实施例的终端从简档服务器接收远程管理命令并对其进行处理的正常过程的示例的示图。

[0118] 在图2中,终端250可以具有安装在其中的eUICC 252,并可以具有安装在其中的LPA,以便控制eUICC 252。另外,终端250或eUICC 252可以具有安装在其中的一个或更多个

简档。此外，每个安装的简档可以具有能够远程控制简档的一个或更多个简档服务器的描述。尽管在以下描述中将假设简档服务器是例如管理者简档服务器(管理SM-DP+)或SM-DP+，但是本公开的简档服务器不限于此。

[0119] 所描述的管理者简档服务器的列表可以包括每个管理者简档服务器的地址(以IP地址或FQDN的类型)或其对象标识符。尽管未在示图中示出，但是应移动运营商的请求而生成的远程简档管理命令可以在简档服务器260中待机。

[0120] 参考图2，在步骤201中，终端250和简档服务器260可以执行相互认证。步骤201可以包括基于服务器认证的TLS连接。此外，步骤201还可以包括发送和接收例如至少发起认证请求消息、发起认证响应消息和认证客户端请求消息的一个或更多个步骤。另外，步骤201可以是与步骤203的部分或全部集成的过程。

[0121] 在步骤203中，简档服务器260可以将远程简档管理命令发送到LPA 254。在步骤203中，简档服务器260可以使用例如至少一个远程管理命令和包括简档服务器260的数字签名的终端认证响应(认证客户端响应)消息。可以基于至少一个远程管理命令来计算简档服务器260的数字签名。

[0122] 将注意到，尽管该示图示出在步骤203中发送的仅一个“启用简档”远程管理命令的示例，但是可以如上所述发送多于一个的远程管理命令，并且除了“启用简档”远程管理命令之外，还可以发送各种类型的远程管理命令，诸如“禁用简档”和“删除简档”。

[0123] 在步骤205中，LPA 254可以将远程简档管理命令递送到eUICC 252。在步骤205中，LPA 254可以使用例如至少一个远程管理命令和包括简档服务器260的数字签名的远程管理输入请求(加载RPM包请求)消息。远程管理输入请求消息可以包括步骤203中的终端认证响应消息的部分或全部。

[0124] 在步骤207中，eUICC 252可以认证在步骤205中接收的简档服务器260的数字签名。可以基于在步骤205中接收的至少一个远程管理命令来计算数字签名的认证。在成功认证数字签名之后，eUICC 252可以执行步骤209。

[0125] 在步骤209中，关于在步骤205中接收的一个或更多个远程管理命令，eUICC 252可以识别发送了远程管理命令的简档服务器260是否被描述为每个远程管理命令的目标简档的管理者简档服务器。也就是说，远程管理命令可以以安装在eUICC中的不同简档为目标，并且可以基于远程管理命令内的简档ID(或ICCID)来标识对应的远程管理命令的目标简档。关于由被描述为管理者简档服务器的简档服务器260发送的远程管理命令的目标简档，eUICC 252可以执行步骤211。

[0126] 在步骤211中，eUICC 252可以执行在步骤205中接收的一个或更多个远程管理命令。如果接收到一个或更多个远程管理命令，则eUICC 252可以重复执行各个远程管理命令。在执行各个远程管理命令之后，eUICC 252可以生成远程管理输入结果(加载RPM包结果)。

[0127] 如果每个远程管理成功，则关于由eUICC 252接收的一个或更多个远程管理命令的远程管理输入结果可以包括至少一个字符串类型的“OK”或与其对应的数字串，并且如果每个远程管理失败，则可以包括至少一个字符串类型的指示失败原因的错误代码或与其对应的数字串。

[0128] 该示图示出在步骤205中接收到的远程管理命令是“启用简档”，并且eUICC 252已

经成功地启用目标简档并因此在步骤211中生成了结果“OK”的情况。

[0129] 在步骤213中，eUICC 252可以将远程管理输入结果作为回复发送到LPA254。在步骤213中，eUICC 252可以使用至少包括远程管理输入结果的远程管理输入响应(加载RPM包响应)消息。

[0130] 在步骤215中，LPA 254可以将远程管理输入结果(加载RPM包结果)递送到简档服务器260。在步骤215中，LPA 254可以使用例如处理通知消息。在步骤213中，处理通知消息可以包括远程管理输入响应消息的部分或全部。

[0131] 参考图2，如果在安装在终端250或eUICC 252中的特定简档中简档服务器260被描述为管理简档服务器，则简档服务器260可以将远程管理命令发送到终端250，以便远程控制目标简档。

[0132] 图3示出其中根据实施例的终端已经从简档服务器接收到远程管理命令，但是由于简档服务器未被描述为目标简档的管理者简档服务器(管理SM-DM+)而在远程管理中失败的一般过程的示例的示图，。

[0133] 在图3中，终端350和简档服务器360的描述与参考图2的描述相同，因此这里将不再重复。另外，步骤301至步骤307的描述与图2中的步骤201至步骤207的描述相同，因此这里将不再重复。

[0134] 在步骤309中，关于在步骤305中接收的一个或更多个远程管理命令，eUICC 352可以识别发送了远程管理命令的简档服务器360是否被描述为每个远程管理命令的目标简档的管理者简档服务器。关于由未被描述为管理者简档服务器的简档服务器360发送的远程管理命令的目标简档，eUICC 352可以执行步骤311。

[0135] 在步骤311中，eUICC 352可以生成远程管理输入结果(加载RPM包结果)。如果每个远程管理成功，则关于由eUICC 352接收的一个或更多个远程管理命令的远程管理输入结果可以包括至少一个字符串类型的“OK”或与其对应的数字串，并且如果每个远程管理失败，则包括至少一个字符串类型的指示失败原因的错误代码或与其对应的数字串。

[0136] 该示图示出在步骤305中接收的远程管理命令是“启用简档”，并且eUICC 352未能认证管理者简档服务器并因此在步骤309中生成错误代码“禁止管理SM-DP+(或disallowedManagingDp)”作为结果的情况。

[0137] 步骤313至步骤315的描述与图2中的步骤213至步骤215的描述相同，因此这里将不再重复。参考图3，通过使用安装在终端350或eUICC 352中的简档的管理者简档服务器列表，终端350可以区分具有远程管理对应简档的权限的简档服务器和没有权限的简档服务器，并且可以阻止没有权限的简档服务器进行远程管理，从而安全地保护简档。然而，缺点在于，在由不支持远程简档管理功能的简档服务器安装并因此没有在其中配置的管理者简档服务器列表的的简档的情况下，在通过简档更新生成管理者简档服务器列表之前，无法支持远程简档管理。

[0138] 图4A示出其中根据实施例的终端已经从简档服务器接收到远程管理命令，但是因为简档服务器未被描述为目标简档的管理者简档服务器而将远程管理命令切换为本地管理命令的终端操作过程的示例的示图。

[0139] 在图4A中，终端450可以具有安装在其中的eUICC 452，并且可以具有安装在其中的LPA 454以便控制eUICC 452。另外，终端450或eUICC 452可以具有安装在其中的一个或

更多个简档。另外，每个安装的简档可以具有能够远程控制简档的一个或更多个管理者简档服务器的描述，或者可以不具有其描述。没有对管理者简档服务器的描述的情况可以包括存在表示管理者简档服务器列表的数据对象但不存在其条目的情况，以及不存在表示管理者简档服务器列表的数据对象的情况。在本公开中，为了便于描述，前一种情况将被称为“空(empty)列表”，后一种情况将被称为“无效(null)列表”。当处理终端450的操作时，LPA 454可以区分空列表和无效列表。

[0140] 图4中的步骤401至步骤407的描述与图2中的步骤201至步骤207的描述相同，因此这里将不再重复。另外，图4中的步骤409至步骤413的描述与图3中的步骤309至步骤313的描述相同，因此这里将不再重复。

[0141] 在步骤415中，LPA 454可以检查由eUICC 452作为回复发送的远程管理输入结果(加载RPM包结果)。如果远程管理输入结果包括错误代码“禁止管理SM-DP+或disallowedManagingDP)”，则LPA 454可以检查目标简档的管理者简档服务器列表，以便确定错误代码的原因。

[0142] 为了检查管理者简档服务器列表，可以使用本地管理命令中的“获取简档信息”命令作为用于检索目标简档的简档元数据的操作。如果先前已经通过使用相同的命令检索了目标简档的简档元数据，然后将其高速缓存在临时存储器中，则可以利用临时存储器中的信息。根据检查目标简档的管理者简档服务器列表的结果，LPA 454可以如下操作：

[0143] (A)如果管理者简档服务器列表中已经描述了一个或更多个简档服务器LPA 454可以关于目标简档识别由于简档服务器460没有远程管理权而已经生成的错误代码“禁止管理SM-DP+(或disallowedManagingDp)”。在这种情况下，LPA 454可以在步骤417中将作为来自eUICC 452的回复的远程管理输入结果(加载RPM包结果)递送到简档服务器460，而不执行附加操作。

[0144] (B)如果管理者简档服务器列表为无效列表

[0145] LPA 454可以识别出因为目标简档不支持远程简档管理(例如，其中没有配置用于远程简档管理的管理者简档服务器列表的简档)而已经生成的错误代码“禁止管理SM-DP+(或disallowedManagingDp)”。在这种情况下，LPA454可以选择性地执行关于简档服务器460是否真实的附加认证。附加认证可以如以下方法列表(图中未示出)中那样执行，但不必然限于以下列表：

[0146] -没有单独的附加验证

[0147] -在步骤403中从简档服务器接收附加认证数据(令牌、签名、数字证书、位图、标志等)，并且LPA 454或eUICC 452进行认证

[0148] -在步骤403中使用除了终端认证响应之外的单独消息

[0149] -通过将目标简档的管理者简档服务器列表与单独存储在LPA 454或eUICC 452中的简档服务器的地址(FQDN的IP地址)进行比较，或者与对象标识符的列表进行比较，LPA 454或eUICC 452认证简档服务器460是否包括在对应列表中

[0150] -LPA 454或eUICC 452请求简档服务器460提供附加认证数据(令牌、签名、数字证书、位图、标志等)，并且LPA 454或eUICC 452认证从简档服务器460接收的数据作为回复

[0151] 如果附加认证成功，则LPA 454可以确定尽管目标简档不支持远程简档管理但简档服务器460具有远程管理权限，可以将远程管理命令切换为等同的本地管理命令(其不需

要管理者简档服务器认证)，并且可以处理所述本地管理命令。另外，可以生成处理结果数据。

[0152] 例如，命令“RPM启用简档”、“RPM禁用简档”、“RPM删除简档”和“RPM列表简档信息”可以分别切换为命令“本地启用简档”、“本地禁用简档”、“本地删除简档”和“本地获取简档信息”，然后执行。

[0153] (C)如果管理者简档服务器列表是空列表，则LPA 454可以执行操作(A)或执行操作(B)。

[0154] 步骤417的描述步骤415和与图2中的步骤215的描述相同，因此这里将不再重复。

[0155] 在步骤417中，LPA 454可以将远程管理输入结果和/或本地管理输入结果(本地管理结果)递送到简档服务器460。

[0156] 如果LPA 454已经将远程管理命令切换为等同的本地管理命令并随后处理所述本地管理命令，则LPA 454可以将本地管理输入结果切换为等同的远程管理输入结果并随后递送所述远程管理输入结果。在步骤417中，LPA 454可以使用例如处理通知消息。处理通知消息可以包括远程管理输入结果和/或本地管理输入结果的部分或全部。

[0157] 参考图4，终端450可以用等同的本地管理命令(其不需要与管理者简档服务器列表进行比较)替换关于不支持远程简档管理的简档(即，其中没有配置管理者简档服务器列表的简档)递送的远程管理命令，然后执行所述本地管理命令，从而支持对应简档的远程管理。另外，终端450可以另外认证尝试关于其中没有配置管理者简档服务器列表的简档进行远程管理的简档服务器，使得授权的简档服务器与未授权的简档服务器分开控制，从而安全地保护简档。

[0158] 同时，应当注意，尽管图4示出远程管理命令是启用命令的情况，但是本公开不限于对应的远程管理命令，并且同样可适用于各种远程管理命令，诸如禁止、删除和更新。

[0159] 还应注意，尽管图4中未示出，但如果需要，LPA 454可以在步骤403之后执行步骤415。例如，如果LPA 454已经识别出目标简档的管理者简档服务器列表是空列表或无效列表，则LPA 454可以立即将步骤403中包括的远程管理命令切换为本地管理命令并执行所述本地管理命令，而不与eUICC 452交换附加消息。这将在后面更详细地描述。

[0160] 作为另一示例，如果LPA 454已经通过远程管理命令的先前处理而识别出目标简档不支持远程管理命令，则LPA 454可以立即将步骤403中包括的远程管理命令切换为本地管理命令并执行所述本地管理命令，而不与eUICC 452交换附加消息。在这样的示例中，可以省略步骤405至步骤413。

[0161] 将参考图4B描述这种操作的实施例。

[0162] 另外，应当注意，尽管未在附图中示出，但是促使LPA454用本地管理替换远程管理的错误代码不必限于错误代码“禁止管理SM-DP+(或disallowedManagingDp)”，并且可以扩展到其他错误代码。

[0163] 例如，LPA 454可以响应于远程管理命令“简档所有者检查”而关于错误代码“简档所有者不匹配(或profileOwnerMismatch)”如在步骤415中选择性地执行简档服务器460的附加认证，可以用仅关于认证的简档服务器不需要简档所有者检查的本地管理替换需要简档所有者检查的远程管理，并且可以执行本地管理。

[0164] 图4B示出其中根据实施例的终端450已经从简档服务器460接收到远程管理命令，

但是由于简档服务器未被描述为目标简档的管理者简档服务器而执行将远程管理命令切换为本地管理命令的连续操作的终端操作过程的示例的示图。

[0165] 在图4B中,终端450和简档服务器460的描述与参考图4A的描述相同,因此在此将不再重复。另外,图4B中的步骤451至步骤467的描述与图4A中的步骤401至步骤417的描述相同,因此这里将不再重复。另外,图4B中的步骤469和步骤471的描述与图4A中的步骤401至步骤403的描述相同,因此这里将不再重复。

[0166] 由于LPA 454已经通过执行步骤455至465识别出目标简档不支持远程管理,因此LPF 454可以在步骤473中不向eUICC 452递送远程管理命令,并且可以如图4中的步骤415中那样操作。也就是说,LPA 454可以在不向eUICC 452递送远程管理命令的情况下执行本地简档管理。

[0167] 步骤475的描述与图4中的步骤417的描述相同,因此这里将不再重复。

[0168] 参考图4B,如果终端450接收到关于已经被识别为不支持远程简档管理的目标简档(即,其中没有配置管理者简档服务器列表的简档)的远程管理命令,则终端450不会非必要地将关于远程管理的远程管理命令递送到eUICC 452,可以立即用等同的本地管理命令(其不需要管理者简档服务器列表比较)替换所递送的远程管理命令,并且可以执行所述本地管理命令,从而减少eUICC 452和LPA 454的不必要的操作。

[0169] 图5示出其中根据实施例的终端550已经从简档服务器560接收到远程管理命令,但是LPA 554由于eUICC 552不支持远程简档管理而将远程管理命令切换为本地管理命令的终端操作过程的示例的示图。

[0170] 在图5中,终端550可以具有安装在其中的eUICC 552,并且可以具有安装在其中的LPA 554以便控制eUICC 552。另外,终端550或eUICC 552可以具有安装在其中的一个或更多个简档。此外,每个安装的简档可以具有能够远程控制简档的一个或更多个简档服务器的描述,或者可以不具有其描述。另外,eUICC 552可以不具有在其中实现的远程管理命令处理功能,使得eUICC 552无法执行远程管理命令。

[0171] 图5中的步骤501和步骤503的描述与图2中的步骤201和步骤203的描述相同,因此这里将不再重复。

[0172] 在步骤505中,LPA 554可以检查eUICC 552的能力。更具体地,LPA 554可以识别eUICC 252是否能够处理远程管理命令。步骤505可以在以下示例性方法中执行,但不必限于此,并且如果终端550已经识别出eUICC 552的能力,则可以省略步骤505。

[0173] -可以检查eUICC的规范版本号,以便如果规范版本号等于预定规范版本号(例如,v3.0.0)、高于预定规范版本号或不存在,则可以识别出远程管理命令能够被处理。如果eUICC的规范版本号低于预定规范版本号(v3.0.0),则可以识别出无法处理远程管理命令。

[0174] -可以检查eUICC RSP能力(或euiccRspCapability),以便如果在eUICC RSP能力中描述了RPM支持(或rpmSupport),则可以识别出远程管理命令能够被处理。如果不存在eUICC RSP能力,或者如果在eUICC RSP能力中未描述RPM支持,则可以识别出无法处理远程管理命令。

[0175] 另外,可以确定eUICC 552是否能够通过参考图4A和图4B描述的过程来处理远程管理命令。如果已经预先执行了这样的过程,则可以存储关于eUICC 552是否能够处理远程管理命令的信息,并且LPA可以在步骤505中检查该信息。可替代地,如果已经通过上述过程

识别出eUICC能力,则可以省略步骤505。

[0176] 如果在步骤505中确定eUICC 552无法处理远程管理命令,则LPA 554可以在步骤507中选择性地另外认证简档服务器260,可以将远程管理命令切换为等同的本地管理命令,并且可以处理所述本地管理命令。另外,可以生成处理结果数据。步骤507的更详细描述与图4中的步骤415的描述相同,因此这里将不再重复。

[0177] 另外,步骤509的描述与图4中的步骤417的描述相同,因此这里将不再重复。

[0178] 参考图5,如果确定安装在终端550中的eUICC 552不支持远程简档管理功能,则终端550可以将远程管理命令切换为等同的本地管理命令,然后对其进行处理,这不同于关于相同条件徒然地将远程管理命令(其无法被处理)递送到eUICC 552,因此远程管理失败的正常过程(对应于参考图8描述的以下过程)。

[0179] 还应当注意,图5的一些实施例与图4的一些实施例不是相互排斥的,并且可以组合实现其中的多于一个的实施例。例如,如果在图5的步骤505中确定eUICC 552无法处理远程管理命令,则LPA 554可以如在图4的步骤405中那样优先地将远程管理命令递送到eUICC 552,并且可以根据回复结果附加地如在图4的步骤413至415的操作中那样操作。将参考图9描述关于终端250的这种组合操作的一些实施例。

[0180] 同时,应当注意,终端550确定eUICC 552的功能并切换eUICC 552不支持的功能使得LPA 554处理该功能的操作不必限于将远程管理命令切换为本地管理命令的操作,并且也可适用于eUICC 552需要执行的其他操作。

[0181] 例如,如图6A至图6C所示,如果eUICC无法认证执行命令代码所必需的简档服务器的签名,则LPA可以将命令代码切换为激活代码,然后对其进行处理。这将参考图6A至图6C详细描述。

[0182] 图6A示出根据实施例的终端650通过特定应用程序成功地处理命令代码的终端操作过程的示例的示图。

[0183] 在图6A中,终端650可以具有安装在其中的eUICC 652,并且可以具有安装在其中的LPA 654以便控制eUICC 652。另外,终端650可以具有安装在其中的特定应用程序656(设备应用或设备app)。特定应用程序可能已经由特定移动运营商安装在终端中,使得用户订阅通信服务。特定应用程序可以将通过外部服务器等生成的命令代码递送到LPA 654,以便请求LPA 654在eUICC 652中安装简档或者管理简档。这样的功能可以被称为LPA应用可编程接口或LPA API。

[0184] 参考图6A,在步骤601中,应用程序656可以请求LPA 654启动LPA API。在步骤601中,应用程序可以使用例如“发起LPA API请求”消息。

[0185] 在步骤603中,LPA 654可以请求eUICC 652提供eUICC信息。在步骤603中,例如,可以使用“获得eUICC信息请求”消息。

[0186] 在步骤605中,eUICC 652可以将eUICC信息作为回复发送到LPA 654。在步骤605中,eUICC 652可以使用例如至少包括eUICC信息(euiccInfo2)的“获得eUICC信息响应”消息。

[0187] 在步骤607中,LPA 654可以请求eUICC 652提供随机字符串(随机质询)。质询(challenge)可以包括随机的16字节数字/字符串。在步骤607中,LPA可以使用例如“获得eUICC质询请求”消息。

[0188] 在步骤609中，eUICC 652可以生成字符串，并且可以将其作为回复发送到LPA 654。在步骤609中，eUICC 652可以使用例如至少包括由eUICC生成的字符串(euiccChallenge)的“获得eUICC质询响应”消息。

[0189] 在步骤611中，LPA 654可以将LPA API信息发送到应用程序656作为回复。在步骤611中，LPA 654可以使用例如至少包括euiccInfo2、euiccChallenge和deviceInfo的“发起LPAAPI响应”消息。

[0190] 在步骤613中，应用程序656可以生成命令代码。应用程序656可以与至少一个外部服务器(未示出)一起生成命令代码。应用程序656还可以在不与外部服务器互工作的情况下生成命令代码。命令代码可以至少包括例如一个或更多个激活代码，还可以包括基于激活代码生成的简档服务器的签名，并且还可以包括生成了该签名的简档服务器的至少一个数字证书。

[0191] 在步骤615中，应用程序655可以将命令代码递送到LPA 654。在步骤615中，LPA 654可以使用例如包括至少一个命令代码的“执行命令代码请求”消息。

[0192] 在步骤617中，LPA 654可以将命令代码递送到eUICC 652。在步骤617中，LPA 654可以使用例如包括至少一个命令代码的“验证命令代码请求”消息。

[0193] 在步骤619中，eUICC 652可以验证包括在命令代码中的简档服务器的签名。可以通过至少使用包括在命令代码中的激活代码和简档服务器的至少一个数字证书来执行签名的验证。

[0194] 在步骤621中，eUICC 652可以将验证命令代码的结果作为回复发送到LPA 654。在步骤621中，eUICC 652可以使用例如至少包括将验证命令代码的结果表示为数字串或字符串的结果值的“验证命令代码响应”消息。步骤621示出成功验证命令代码的结果的示例。

[0195] 在步骤623中，LPA 654可以将执行命令代码的结果作为回复发送到应用程序656。在步骤623中，LPA 654可以使用例如“执行命令代码响应”消息，该消息至少包括将执行命令代码的结果表示为数字串或字符串的结果值。

[0196] 在步骤625中，eUICC 652和LPA 654可以通过使用命令代码来新安装简档，或者可以管理已经安装的简档。步骤625可以通过包括图6A中未示出的至少一个简档服务器660来执行。步骤625可以是例如根据与图2中相同的过程来管理已经安装在终端250中的简档的过程。

[0197] 参考图6A，安装在终端中的应用程序656可以通过使用LPA API将命令代码递送到LPA 654，并且可以通过使用eUICC 652认证命令代码的有效性。为此，LPA 654和eUICC 652都会需要用于识别和解释命令代码的功能。

[0198] 图6B示出根据一些实施例的终端650无法通过特定应用程序处理命令代码的终端操作过程的示例的示图。

[0199] 图6B中的终端650、eUICC 652、LPA 654和应用程序656的描述与参考图6A进行的描述相同，因此这里将不再重复。另外，图6B中的步骤631至步骤647的描述与图6A中的步骤601至步骤617的描述相同，因此这里将不再重复。

[0200] 现在将参考图6B描述安装在终端中的应用程序656已经通过使用LPA API将命令代码递送到LPA 654，但是eUICC 652不具有用于认证命令代码的有效性的功能的情况。由于eUICC 652不具有用于认证命令代码的有效性的功能，因此LPA 654无法处理命令代码。

[0201] 因此,在步骤651中,eUICC 652可以将表示所接收的命令代码无法被处理的错误代码作为回复发送到LPA 654。例如,错误代码可以由指示“未找到参考数据”的字符串或数字串(或十六进制数字系统中的0x6a 0x88)表示。步骤651示出验证命令代码失败的结果的示例。

[0202] 在步骤653中,LPA 654可以将执行命令代码的结果作为回复发送到应用程序656。在步骤653中,LPA可以使用例如“执行命令代码响应”消息,该消息至少包括将执行命令代码的结果表示为数字串或字符串的结果值。步骤653示出执行命令代码失败的结果的示例。

[0203] 图6C示出终端操作过程的示例的示图,其中,当根据一些实施例的终端650通过特定应用程序处理命令代码时,LPA 654将命令代码切换为激活代码,然后处理激活代码。

[0204] 图6C中的终端650、eUICC 652、LPA 654和应用程序656的描述与参考图6A进行的描述相同,因此这里将不再重复。另外,图6C中的步骤661至步骤675的描述与图6A中的步骤601至步骤615的描述相同,因此这里将不再重复。

[0205] 在步骤677中,LPA 654可以检查eUICC 652的能力。更具体地,LPA 654可以识别eUICC 652是否能够验证命令代码。可以在以下示例性方法中执行这种确认,但不必受限于此,并且如果终端650已经识别出eUICC 652的能力,则可以省略步骤677。

[0206] -可以检查eUICC的规范版本号,以便如果规范版本号等于预定规范版本号(例如,v3.0.0)、高于预定规范版本号或者不存在,则识别出可以处理命令代码。如果eUICC的规范版本号低于预定规范版本号(v3.0.0),则可以识别出无法处理命令代码。

[0207] -可以检查eUICC RSP能力(或euiccRSPCapability),以便如果在RPM能力中描述了签名命令代码支持(或signedCommandCodeV3Support),则识别出可以处理命令代码。如果没有RSP能力,或者如果在RSP能力中没有描述签名命令代码支持,则可以识别出无法处理命令代码。

[0208] 可替代地,可以确定eUICC 652是否可以通过参考图6B所述的过程来处理命令代码。如果已经预先执行了这样的过程,则可以存储关于eUICC 652是否能够处理命令代码的信息,并且LPA可以在步骤677中检查该信息。可替代地,如果已经通过上述过程识别出eUICC能力,则可以省略步骤677。

[0209] 在步骤679中,LPA 654可以将命令代码切换为激活代码。更具体地,LPA 654可以在步骤679中以以下方式操作:

[0210] -LPA 654可以执行与如图6A的步骤619中所示eUICC 652认证包括在命令代码中的简档服务器的签名相同的操作。可以选择性地执行签名的这种认证。

[0211] -LPA 654可以提取(或确定)包括在命令代码中的激活代码。激活代码的提取可以是留下激活代码所必需的信息(例如,简档服务器的地址和简档标识符),排除包括在命令代码中但对于激活代码不必要的信息(例如,简档服务器的签名或数字证书)的操作。

[0212] 步骤683的描述与图7A中的步骤623的描述相同,因此这里将不再重复。在步骤685中,终端可以通过使用激活代码下载简档,或者可以接收远程简档管理并对其进行处理。

[0213] 参考图6C,安装在终端中的应用程序656可以通过使用LPA API将命令代码递送到LPA 654。LPA 654可以确定eUICC 652无法认证命令代码的有效性,可以从命令代码提取激活代码,可以从简档服务器接收与激活代码对应的简档下载或远程简档管理,并且可以处理该简档下载或远程简档管理。如本文所使用的,命令代码包括激活代码和添加到其上的

附加数据，并且附加数据可以是例如简档服务器的签名。根据图6C的实施例，与图6B的实施例相比，即使eUICC 652不具有用于认证命令代码的有效性的功能，LPA 654也可以从命令代码提取激活代码，可以从简档服务器接收与激活代码对应的简档下载或远程简档管理，并且可以处理该简档下载或远程简档管理。

[0214] 图7示出终端操作过程的示例的示图，其中，根据实施例的终端750已经从简档服务器760接收到远程管理命令，但是未能认证简档服务器760的签名，因此拒绝远程管理。

[0215] 在图7中，终端750和简档服务器760的描述与参考图2的描述相同，因此这里将不再重复。另外，图7中的步骤701至步骤707的描述与图2中的步骤201至步骤205的描述相同，因此这里将不再重复。

[0216] 在步骤707中，eUICC 752可以认证简档服务器760的数字签名。可以至少基于在步骤705中接收的一个或更多个远程管理命令来计算数字签名的认证。如果数字签名未能被认证，则eUICC 752可以执行步骤711。

[0217] 在步骤711中，eUICC 752可以生成远程管理输入结果(加载RPM包结果)。如果每个远程管理成功，则关于由eUICC 752接收的一个或更多个远程管理命令的远程管理输入结果可以包括至少一个字符串类型的“OK”或与其对应的数字串，并且如果每个远程管理失败，则包括至少一个字符串类型的指示失败原因的错误代码或与其对应的数字串。

[0218] 该示图示出在步骤705中接收的远程管理命令是“启用简档”，并且由于未能认证简档服务器760的数字签名，因此生成错误代码“无效签名(或invalidSignature)”的情况。

[0219] 步骤713至步骤715的描述与图2中的步骤713至步骤715的描述相同，因此这里将不再重复。

[0220] 参考图7，与图4相比，包括在远程管理输入结果中的错误代码“无效签名(或invalidSignature)”不是错误代码“禁止管理SM-DP+(或disallowedManagingDP)”，并且在步骤713之后，LPA 754可以相应地拒绝用本地管理替换远程管理。应当注意，促使LPA 754拒绝用本地管理替换远程管理的这种错误代码不必限于“无效签名(或invalidSignature)”，并且可以扩展到其他错误代码。

[0221] 图8示出正常操作过程的示例的示图，其中，根据实施例的终端850已经从简档服务器860接收到远程管理命令，但是由于eUICC 852不支持远程简档管理而无法进行远程管理。

[0222] 在图8中，终端850可以具有安装在其中的eUICC 852，并且可以具有安装在其中的LPA 854，以便控制eUICC 852。另外，终端850或eUICC 852可以具有安装在其中的一个或更多个简档。此外，每个安装的简档可以具有能够远程控制简档的一个或更多个简档服务器的描述，或者可以不具有其描述。另外，eUICC 852可以不具有在其中实现的远程管理命令处理功能，并且因此无法执行远程管理命令。

[0223] 图8中的步骤801至步骤805的描述与图2中的步骤201至步骤205的描述相同，因此这里将不再重复。

[0224] 在步骤807中，eUICC 852可以向LPA 854发送指示无法处理所接收的远程简档管理命令的错误代码作为回复。例如，错误代码可以表示为指示“未找到参考数据”的字符串或数字串(或十六进制数字系统中的0x6a 0x88)。

[0225] 在步骤809中，LPA 854可以将步骤807中的执行结果递送到简档服务器860。在步

骤809中,LPA可以使用例如处理通知消息。例如,处理通知消息可以被表示为指示“RPM不被支持”的字符串或数字串。

[0226] 参考图8,如果即使LPA 854可以处理远程简档管理命令,eUICC 852也不支持远程简档管理,则终端850无法处理从简档服务器860接收的远程管理命令。

[0227] 图9示出根据实施例的终端用本地管理命令替换远程管理命令的过程的示例的示图。

[0228] 参考图9,在步骤901中,终端可以开始操作。

[0229] 在步骤903中,终端可以从简档服务器接收远程管理命令。在步骤903中,例如,终端可以通过包括至少一个远程管理命令和简档服务器的数字签名的终端认证响应消息来接收远程管理命令。

[0230] 在步骤905中,终端可以确定是否能够执行远程管理命令。例如,终端可以确定eUICC是否支持远程管理命令的执行。步骤905中的确定过程的详细描述与图5中的步骤505的描述相同,因此这里将不再重复。如果终端无法执行远程管理命令,则终端可以执行步骤913。如果终端可以执行远程管理命令,则终端可以执行步骤907。

[0231] 在步骤907中,终端可以将远程管理命令递送到eUICC。在步骤907中,终端可以使用例如包括至少一个远程管理命令和简档服务器的数字签名的远程管理输入请求(加载RPM包请求)消息。远程管理输入请求消息可以包括步骤903中的终端认证响应消息的部分或全部。

[0232] 在步骤909中,终端可以从eUICC接收远程管理输入结果(加载RPM包结果)。在步骤909中,终端可以使用例如至少包括远程管理输入结果的远程管理输入响应(加载RPM包响应)消息。

[0233] 在步骤911中,终端可以检查远程管理输入结果的内容,并且可以确定远程管理输入结果是否包括特定远程管理错误代码(或预定远程管理错误代码)。特定远程管理错误代码可以是例如错误代码“禁止管理SM-DP+(或disallowedManagingDp)”、错误代码“简档所有者不匹配(或profileOwnerMismatch”)或终端已知的任何其他错误代码。

[0234] 如果远程管理输入结果不包括对应的远程管理错误代码,则终端可以执行步骤919。

[0235] 如果远程管理输入结果包括对应的远程管理错误代码,则终端可以执行步骤913。下面将描述其详细内容。

[0236] 在步骤913中,终端可以识别远程管理命令是否能够切换为本地管理命令。例如,终端可以检查目标简档的管理者简档服务器列表。可以通过使用存储在eUICC中的信息或者通过使用高速缓存在终端的高速缓存中的信息来检查管理者简档服务器列表。

[0237] 作为另一示例,终端可以附加地认证发送了远程管理命令的简档服务器。为此,终端可以识别发送了远程管理命令的简档服务器是否包括在由终端独立管理的简档服务器列表中;终端可以将字符串(质询)发送到发送了远程管理命令的简档服务器,并且可以响应于此而请求数字签名和/或数字证书;终端可以识别特定数据(例如,令牌)是否已经与远程管理命令一起递送;或者终端可以使用其他认证手段。上述示例不必然逐一使用,并且可以组合使用其中的多于一个的示例。另外,上述示例仅是附加认证的一个示例,并且也可以使用其他方法。

[0238] 如果远程管理命令无法切换为本地管理命令(例如,如果管理者简档服务器列表非空,和/或如果简档服务器的附加认证失败),则终端可以执行步骤919。

[0239] 如果远程管理命令可以切换为本地管理命令(例如,如果管理者简档服务器列表是无效列表,和/或如果简档服务器的附加认证成功),则终端可以执行步骤915。如果不清楚远程管理命令是否能够切换为本地管理命令(例如,如果管理者简档服务器列表是空列表,和/或如果执行两个或更多个认证的结果彼此不同),则终端可以选择性地执行步骤915或步骤919。

[0240] 在步骤915中,终端可以执行等同于远程管理命令的本地管理。为此,终端可以将本地管理命令递送到eUICC。步骤915的详细描述与图4中的步骤415的详细描述相同,因此这里将不再重复。

[0241] 在步骤917中,终端可以将本地管理输入结果(本地管理结果)切换为等同的远程管理输入结果(加载RPM包结果)。可以选择性地执行步骤917。步骤917的详细描述与图4中的步骤415的详细描述相同,因此这里将不再重复。

[0242] 在步骤919中,终端可以将远程管理输入结果或本地管理输入结果递送到简档服务器。在步骤919中,终端可以使用例如处理通知消息。处理通知消息可以包括远程管理输入结果或本地管理输入结果的部分或全部。

[0243] 终端可以结束该步骤,并且可以等待后续接收附加远程管理命令。

[0244] 图10示出根据一些实施例的终端用等同的第二版本功能(旧功能)替换无法由第二版本eUICC处理的第一版本eSIM功能(新功能)的过程的示例的示图。

[0245] 在本公开的以下描述中,关于第二版本在第一版本之前的情况,能够由第一版本eUICC处理的功能(eSIM功能)将被称为第一功能,并且能够由第二版本eUICC处理的功能将被称为第二功能。然而,实施例不限于此,并且可以使用各种术语,例如,新功能代替第一功能,以及旧功能代替第二功能。

[0246] 参考图10,终端可以开始操作。

[0247] 在步骤1003中,终端可以从简档服务器接收第一功能相关请求。也就是说,终端可以从安装在简档服务器或终端中的特定应用接收关于第一版本eSIM功能的执行请求。在步骤1003中,终端可以使用例如包括至少一个远程管理命令和简档服务器的数字签名的终端认证响应消息,或者包括激活代码的命令代码的“执行命令代码请求”消息。

[0248] 在步骤1005中,终端可以确定是否能够执行第一功能。例如,终端可以确定eUICC的规范版本号(SVN)或其RSP能力是否支持第一功能。步骤1005中的确定过程的详细描述与图5中的步骤505和图6C中的步骤677的确定过程的详细描述相同,因此这里将不再重复。如果终端无法执行第一功能,则终端可以执行步骤1013。如果终端可以执行远程管理命令,则终端可以执行步骤1007。

[0249] 在步骤1007中,终端可以向eUICC发送第一功能相关请求(或第一功能执行请求)。在步骤1007中,终端可以使用例如包括至少一个远程管理命令和简档服务器的数字签名的远程管理输入请求消息,或“验证命令代码请求”消息。

[0250] 在步骤1009中,终端可以从eUICC接收处理第一功能的结果。在步骤1009中,终端可以使用例如至少包括远程管理输入结果的远程管理输入响应消息或“验证命令代码响应”消息。

[0251] 在步骤1011中,终端可以检查处理第一功能的结果,并且可以确定是否包括特定错误代码。特定错误代码可以是例如错误代码“禁止管理SM-DP+(或disallowedManagingDp)”、错误代码“简档所有者不匹配(或profileOwnerMismatch”)、错误代码“未找到参考数据”(或十六进制数字系统中的0x6a 0x88)或终端已知的任何其他错误代码。

[0252] 如果处理结果不包括对应错误代码,则终端可以执行1019。如果处理结果包括对应错误代码,则终端可以执行1013。

[0253] 在步骤1013中,终端可以识别第一功能是否能够切换为第二功能。例如,终端可以检查目标简档的管理者简档服务器列表,或者可以检查eUICC的SVN或其RSP能力。可以通过使用存储在eUICC中的信息或者通过使用高速缓存在终端的高速缓存中的信息来检查该信息。

[0254] 作为另一示例,终端可以附加地认证发送了远程管理命令的简档服务器。为此,终端可以识别发送了远程管理命令的简档服务器是否包括在由终端独立管理的简档服务器列表中;终端可以将字符串(质询)发送到发送了远程管理命令的简档服务器,并且可以响应于此而请求数字签名和/或数字证书;终端可以识别特定数据(例如,令牌)是否已经与远程管理命令一起递送;或者终端可以使用其他认证手段。上述示例不必然逐一地使用,并且可以组合使用其中的多于一个示例。另外,上述示例仅是附加认证的一个示例,并且也可以使用其他方法。

[0255] 如果第一功能无法切换为第二功能,则终端可以执行步骤1019。如果第一功能能够切换为第二功能,则终端可以执行步骤1015。如果不清楚第一功能是否能够切换为第二功能,则终端可以选择性地执行步骤1015或步骤1019。

[0256] 在步骤1015中,终端可以处理等同于第一功能的第二功能。也就是说,终端可以将用于处理第二功能的第二功能相关信息递送到eUICC。步骤1015的详细描述与图4中的步骤415或图6C中的步骤679的详细描述相同,因此这里将不再重复。

[0257] 在步骤1017中,终端可以将处理第二功能的结果切换为处理第一功能的结果。可以选择性地执行步骤1017。步骤1017的详细描述与图4中的步骤415的详细描述相同,因此这里将不再重复。

[0258] 在步骤1019中,终端可以将第一功能处理结果和/或第二功能处理结果递送到简档服务器。在步骤1019中,终端可以使用处理通知消息。

[0259] 然后,终端可以结束操作并且可以等待后续接收附加远程管理命令。

[0260] 同时,如上所述,UICC是在被插入到移动通信终端等中的同时使用的智能卡,并且也被称为UICC卡。UICC可以包括用于接入移动通信运营商的网络的接入控制模块。接入控制模块的示例包括USIM、SIM和ISIM。包括USIM的UICC也被称为USIM卡。同样地,包括SIM模块的UICC也被称为SIM卡。

[0261] 在本公开的以下描述中,可以在正常意义上使用术语“SIM卡”,包括UICC卡、USIM卡和包括ISIM的UICC。也就是说,可以对USIM卡、ISIM卡或普通UICC卡进行针对SIM卡的相同技术应用。

[0262] UICC卡的物理形状和逻辑功能由称为ETSI(欧洲电信标准协会)的标准化组织定义,以便保持国际兼容性。就限定物理形状的形状因子而言,尺寸逐渐减小,包括最广泛使

用的迷你SIM、微型SIM和最近的纳米SIM。这对移动通信终端的紧凑性做出了很大贡献，但是预期尺寸小于纳米SIM的UICC卡的标准化是困难的，因为用户可能容易丢失UICC卡。此外，可附接/可拆卸UICC卡的特性需要用于在终端中安装可附接/可拆卸槽的空间。因此，预期任何进一步的紧凑度将是困难的。

[0263] SIM卡存储移动通信订户的个人信息，在接入移动通信网络时认证订户，并生成业务安全密钥，从而实现安全的移动通信使用。

[0264] SIM卡通常应特定移动通信运营商的请求被制造为用于对应运营商的专用卡，并且用于接入对应运营商的网络的认证信息(例如，USIM应用、IMSI、K值或OPc值)在卡被装运之前被加载到卡中。因此，所制造的SIM卡被交付给对应移动通信运营商，然后提供给订户，并且还可以通过使用诸如OTA的技术来管理(例如，安装、修改或删除)UICC内的应用。订户可以将UICC卡插入他/她自己的移动通信终端，从而使用对应移动通信运营商的网络和应用服务。当替换终端时，可以将UICC卡从现有终端移动/插入到新终端中，使得存储在UICC卡中的相同认证信息、移动通信电话号码、个人电话号码簿等可以在新终端中。

[0265] 然而，当移动通信终端用户想要从另一移动通信运营商接收服务时，SIM卡给他/她带来不便。也就是说，为了从移动通信运营商接收服务，移动通信终端用户需要不方便地物理获取SIM卡。例如，当他/她正在另一国家旅行时，需要获取本地SIM卡以接收本地移动通信服务，这是不方便的。漫游服务可以在一定程度上消除这种不便，但是存在服务相对昂贵的问题，并且如果相关通信运营商之间没有联系，则服务不可用。

[0266] 如果在SIM卡(即，SIM简档)中执行的运营商的订户认证模块被远程下载并安装在UICC卡中，则可以在一定程度上消除这种不便。也就是说，可以在用户期望的时间点将要使用的移动通信服务的SIM简档下载到UICC卡。可以在UICC卡中下载和安装多个SIM简档，并且可以仅选择和使用一个SIM。这样的UICC卡可以嵌入在终端中或者可以不嵌入在其中。

[0267] 同时，已经通过在制造移动通信终端时在移动通信终端中嵌入执行与UICC或SIM卡的功能类似的功能的安全模块来提出eUICC结构(无法容易地附接/拆卸的UICC)。这具有与由标准化组织ETSI定义的UICC的电气特性和逻辑结构相同的电气特性和逻辑结构，而物理形状因子和封装方法已经被修改为更有利于紧凑性，从而提供各种大小的eUICC芯片。这样的eUICC包括遵循机器对机器形状因子(MFF)1和MFF2形状因子的eUICC，并且还包括未被ETSI标准化但对于紧凑性更有利的芯片，诸如双扁平无引线(DFN)和晶片级芯片规模封装(WLCSP)方案。

[0268] 因此，在被嵌入终端中的同时使用的UICC被称为eUICC。通常，eUICC是指在被嵌入终端中的同时使用的UICC卡或UICC芯片，并且其被配置为使得能够远程下载和选择SIM模块。

[0269] 在本公开的以下描述中，被配置为使得能够远程下载和选择SIM模块的任何类型的UICC卡将作为整体被称为eUICC。也就是说，被配置为使得能够远程下载和选择SIM模块的UICC卡在下文中将被称为eUICC，而不管其是否嵌入终端中。此外，下载的SIM模块信息通常将被称为SIM简档、RSP SIM简档、eUICC简档，或者更简单地称为简档。另外，在本公开的以下描述中，其中加载有这种eUICC的终端将被称为eUICC终端或eSIM终端。

[0270] 如上所述，可以通过以下方法远程下载和安装SIM模块：

[0271] 根据第一方法，在其中存储有SIM简档的eUICC与远程简档服务器之间的相互认证

期间,只有具有与存储在eUICC中的秘密密钥相同的秘密密钥的远程服务器可以安装简档(操作1),启用安装的简档(操作2)或禁用安装的简档(操作3)。

[0272] 也就是说,根据第一方法,只有具有秘密密钥的“授权服务器”可以执行关于特定eUICC的简档管理(例如,操作1、操作2、操作3),并且可以对其中加载有eUICC的终端的简档安全地执行远程管理。

[0273] 根据第二方法,在其中存储有SIM简档的eUICC与远程简档服务器之间的认证期间,只有持有由存储在eUICC中的“可靠证书颁发者”颁发的证书并且可以用与证书对应的个人密钥进行签名的远程服务器可以安装(操作1)简档。

[0274] 第二方法的优点在于,只要服务器持有由可靠证书颁发者颁发的证书,任何服务器都可以在eUICC中安装SIM简档。例如,如果eUICC具有由特定组织管理并存储在其安全区域中的证书颁发者信息,并且如果终端制造商已经发布了其中加载有对应eUICC的终端,则想要将SIM简档下载到终端并由此提供通信服务的移动运营商可以操作其自己的远程简档服务器,该远程简档服务器具有由证书颁发者颁发并加载在其中的服务器证书,从而通过服务器向终端提供通信服务。相反,在第一方法的情况下,为了在特定eUICC终端中安装SIM简档,可以仅通过具有安装在eUICC中的秘密密钥的一个服务器下载简档。因此,不清楚谁操作服务器,从而限制了适销性。

[0275] 如在第二方法的情况下,基于证书的方法在制造和操作eSIM终端和远程服务器方面是有利的。因此,大多数运营商当前支持第二方法(通过远程服务器提供SIM简档),并且他们的数量正在快速增加。然而,由于任何服务器只要持有适当的证书就可以安装简档,因此可能违背用户的意图而安装简档。因此,在下载和安装任何简档的同时,用户在终端屏幕上的附加确认/协议过程是强制性的。也就是说,第二方法需要用户干预简档安装操作。

[0276] 第二方法在性能方面优于第一方法。参考第二方法,终端在应用进程(AP)期间以高速和优异的通信性能通过普通互联网IP网络以批处理模式接收加密的简档,然后将其安装在eUICC中。因此,下载/安装速度高,并且下载失败的可能性小。在第一方法的情况下,eUICC以OTA类型下载并安装简档(eUICC将加密的简档划分为多个部分,并通过调制解调器直接与服务器接收该多个部分,而不通过终端的AP)。速度低得多,并且下载失败的概率更高。

[0277] 然而,第二方法的局限性在于:如上所述,用户需要干预简档安装,从而使得难以关于大量终端远程地安装和管理SIM简档。

[0278] 因此,本公开提供一种方法和装置,其中,在终端中安装简档的过程中,代替由操纵终端的用户进行确认过程,1)终端用户或管理者远程地做出确认,或者2)服务器远程地自动确定简档安装内容的合法性,然后安装简档,从而关于一个或更多个终端高效地管理简档。

[0279] 在下文中,将定义本公开中使用的术语。

[0280] 如本文所使用的,“UICC”是在被插入移动通信终端的同时使用的智能卡,并且可以指被配置为存储移动通信订户的个人信息(诸如网络接入认证信息、电话号码簿和SMS)的芯片,使得当接入移动通信网络(例如,GSM、WDCMA或LTE)时,订户被认证,并且生成流量安全密钥,从而实现安全的移动通信使用。根据订户接入的移动通信网络的类型,UICC可以具有加载在其中的通信应用(例如,SIM、USIM或ISIM)。UICC还可以提供用于在其中加载各

种应用(例如,电子钱包、票务和电子护照)的更上层安全功能。

[0281] 如本文所使用的,“eUICC”是指嵌入终端中的芯片型安全模块,其无法插入终端/从终端拆卸(非“可附接/可拆卸类型”)。可以通过使用OTA技术来下载简档并将其安装在eUICC中。eUICC可以被称为UICC,其被配置为使得能够将简档下载并安装在其中。

[0282] 在本公开中,用于通过使用OTA技术下载简档并将其安装在eUICC中的方法也适用于可以插入终端和从终端拆卸的可附接/可拆卸UICC。也就是说,实施例也适用于被配置为使得可以通过使用OTA技术将简档下载并安装在其中的UICC。

[0283] 术语“UICC”在本公开中可以与“SIM”互换使用,并且术语“eUICC”可以与“eSIM”互换使用。

[0284] 如本文所使用的,“简档”可以指存储在UICC中并且以软件类型打包的应用、文件系统、认证密钥值等。

[0285] 如本文所使用的,“SIM简档”可以在与简档相同的意义上使用,或者可以指被包括在简档内部的SIM应用中并且以软件类型打包的信息。

[0286] 在本公开中,简档供应服务器(或远程简档供应服务器)可以包括生成SIM简档、通过使用证书和数字签名与eUICC执行相互认证、通过使用在相互认证期间商定的加密密钥来加密所生成的简档、或者将加密的简档提供给终端的功能,并且可以被称为SM-DP+。

[0287] 在本公开中,简档管理服务器(或远程简档管理服务器)可以包括生成远程简档管理命令、通过使用证书和数字签名与eUICC执行相互认证、或者通过使用在相互认证期间商定的MAC保护密钥使所生成的远程简档管理命令经受MAC保护的功能,并且可以被称为管理SM-DP+。

[0288] 如本文所使用的,简档供应服务器还可以并入简档管理服务器的功能。因此,下面描述的各种实施例中的简档供应服务器的操作也可以由简档管理服务器执行。同样,关于简档管理服务器描述的操作也可以由简档供应服务器执行。此外,简档供应服务器在并入简档管理服务器的功能时,也可以简称为简档服务器(或远程简档服务器)。

[0289] 如本文中所使用的术语“终端”可被称为移动站(MS)、用户设备、用户终端、无线终端、接入终端、终端、订户单元、订户站、无线设备、无线通信设备、无线发送/接收单元、移动节点、移动装置或其他术语。

[0290] 终端的各种实施例可以包括蜂窝电话、具有无线通信功能的智能电话、具有无线通信功能的个人数字助理(PDA)、无线调制解调器、具有无线通信功能的便携式计算机、具有无线通信功能的拍摄设备(诸如数字相机)、具有无线通信功能的游戏设备、具有无线通信功能的用于存储和再现音乐的家用电器、能够执行无线互联网接入和浏览的互联网家用电器、以及具有其功能的集成组合的便携式单元或终端。此外,终端可以包括但不限于M2M终端和MTC终端/设备。

[0291] 在本公开中,终端也可以被称为电子设备或简称为设备。除非另有说明,否则终端或设备是指其中加载或可以加载eUICC的终端。

[0292] 在本公开中,终端或设备可以包括安装在终端或电子设备中的软件或应用,以便控制UICC或eUICC。例如,软件或应用可以被称为LPA。

[0293] 在本公开中,终端或设备可以包括安装在终端或设备中的软件或应用,以便接近LPA并通过LPA控制UICC或eUICC。例如,软件或应用可以被称为服务app。服务app可以是独

立的应用或具有API类型。

[0294] 在本公开中，eUICC ID可以是嵌入在终端中的eUICC的唯一ID，并且可以被称为EID。

[0295] 在本公开中，术语“SIM简档”可以与简档包互换使用，可以用于表示特定简档的数据对象，并且可以被称为简档TLV或简档包TLV。如果通过使用加密参数对简档包进行加密，则可以将其称为受保护的简档包或受保护的简档包TLV。当通过使用只能由特定eUICC解密的加密参数来加密简档包时，可以将其称为绑定简档包或绑定简档包TLV。简档包TLV可以是以标签/长度/值(TLV)格式表达构成简档的信息的数据集。

[0296] 如本文所使用的，“远程简档管理”可以被称为简档远程管理、远程管理、远程管理命令、远程命令、远程简档管理包、简档远程管理包、远程管理包、远程管理命令包或远程命令包。可以使用RPM以便改变特定简档的状态(启用、禁用或删除)或更新特定简档的内容(例如，简档昵称或简档元数据)。

[0297] 此外，在本公开的以下描述中，当并入本文的已知功能或配置的详细描述可能使本公开的主题相当不清楚时，将省略并入本文的已知功能或配置的详细描述。

[0298] 在下文中，将参考附图描述所提出的实施例。

[0299] 图11A示出用于在本地操纵终端的同时下载和操纵SIM简档的方法的示图，并且图11B示出用于在本地操纵终端的同时下载和操纵SIM简档的方法的示图。

[0300] 参考图11A，在步骤1100中，eUICC终端通过用户通过终端的UI的输入来发起简档下载。

[0301] 因此，在步骤1105中，终端将eUICC质询值递送到简档供应服务器。

[0302] 然后，在步骤1110中，简档供应服务器可以通过使用与服务器的证书对应的个人密钥来计算关于包括eUICC质询值的信息的签名数据(或签名值)。服务器的证书可以包括椭圆曲线数字签名算法(ECDSA)证书，并且签名数据可以包括ECDSA签名数据。

[0303] 另外，在步骤1115中，简档供应服务器可以将由服务器生成的签名数据和证书递送到eUICC终端。

[0304] 然后，终端可以在步骤1120中认证证书和签名数据。

[0305] 如果认证通过，则eUICC终端可以在步骤1125中通过使用与存储在eUICC中的证书对应的个人密钥来计算eUICC签名数据。

[0306] 另外，在步骤1130中，eUICC终端可以向简档供应服务器提供eUICC签名数据和eUICC证书。

[0307] 此后，在步骤1135中，简档供应服务器可以认证eUICC证书和eUICC签名数据。

[0308] 如果认证结果成功，并且如果存在要下载到eUICC终端的简档，则在步骤1140中，简档服务器优先将简档元数据递送到eUICC终端。

[0309] eUICC终端通过终端的UI或通过经由近场通信(例如，BT、NFC、UWB或WiFi)直接连接到终端的另一终端的UI来显示所接收的简档元数据的全部或部分的信息，并且可以在用户检查UI的内容之后在步骤1145中继续简档安装。

[0310] 当确定继续简档安装时，eUICC终端在步骤1150中请求简档供应服务器提供简档。

[0311] 简档供应服务器在步骤1155中检查简档请求，并将包括简档元数据的简档下载到eUICC终端。

[0312] 此后，eUICC终端附加地认证步骤1155中的简档中的简档元数据是否与步骤1140中的简档元数据相同，然后将简档安装在eUICC中。

[0313] 图11B示出终端启用简档的过程。参考图11B，在图11A的过程之后，终端用户可以在步骤1170中通过终端的UI选择简档，以便输入“启用简档”。

[0314] eUICC终端可以随后在步骤1180中启用简档，并且可以通过使用简档内的接入信息(例如，IMSI或Ki)来接入移动通信网络。

[0315] 图12A示出根据本公开的用于通过远程管理服务器远程执行简档安装和简档启用的装置和方法的实施例，并且图12B示出根据本公开的用于通过远程管理服务器远程执行简档安装和简档启用的装置和方法的实施例。

[0316] 参考图12A，服务服务器(或远程管理服务器)可以在步骤1200中请求eUICC终端发起简档下载。服务服务器可以将要安装的简档的简档元数据信息的全部或部分递送到eUICC终端。另外，递送到eUICC终端的信息可以包括第二简档供应服务器信息、管理SM-DP+服务器信息或简档管理服务器信息中的至少一个。

[0317] 同时，在步骤1200之前，可以由eUICC终端的用户或由管理者预先在服务服务器中注册与eUICC终端对应的ID。ID可以是永久的或临时的。ID可以包括eUICC的ID(EID)、终端的IMFI、终端的序列ID或可用于识别终端的任何其他信息(ID)。另外，ID可以是可用于仅在终端和远程管理服务器之间识别终端的ID，或者是全球唯一的终端ID。

[0318] 另外，在步骤1200之前，eUICC终端可以在远程服务器中注册ID或与ID对应的值。这保证了当用户或管理者已经指定了特定eUICC终端或包括该eUICC终端的终端组时，可以将步骤1200中的简档发起请求递送到适当的eUICC终端。

[0319] 为了在步骤1200中将请求递送到适当的eUICC终端，eUICC终端还需要在远程管理服务器中注册EID或ID，并且稍后将参考图15描述与其相关的过程。

[0320] 同时，上述公开不仅适用于附图，而且适用于本公开的整个说明书。

[0321] 随后的步骤1210至1280可以与图11A中的步骤1105至1140相同或相似。这里将省略其详细描述。

[0322] 在步骤1245中，eUICC终端可以将在步骤1200中从服务服务器接收的简档元数据信息的全部或部分与在步骤1240中从简档供应服务器递送的简档元数据信息的全部或部分进行比较。如果两者匹配，则可以进行简档下载和安装过程，并且如果两者不匹配，则可以结束简档下载和安装过程。如果以这种方式远程安装简档，则可以通过附加地认证简档的有效性的步骤来高效地管理简档，并且可以提高简档安装的可靠性。同时，根据本公开的简档供应服务器可以被称为第一简档供应服务器以与第二简档供应服务器区分开。第一简档供应服务器是用于简档下载的服务器，并且可以包括上述SM-DP、SM-DP+等。第二简档供应服务器可以包括上述管理SM-DP+、管理者简档服务器等。

[0323] 简档元数据的部分可以是第二简档供应服务器信息、管理SM-DP+服务器信息或简档管理服务器信息。这可以同样应用于以下实施例。

[0324] 如果确定继续简档下载和安装，则eUICC终端在步骤1250中请求简档供应服务器提供简档。

[0325] 简档供应服务器在步骤1255中检查简档请求，并将包括简档元数据的简档下载到eUICC终端。

[0326] 此后,eUICC终端可以附加地认证步骤1255中的简档中的简档元数据是否与步骤1240中的简档元数据相同,并且可以在步骤1260中将简档安装在eUICC中。

[0327] 图12B示出根据实施例的用于由终端启用简档的方法的示图。

[0328] 参考图12B,在图12A的过程之后,在步骤1265中,服务服务器可以将能够启动在图12A中安装的SIM简档的简档递送到eUICC终端。图12A和图12B中所示的过程不必然连续执行,并且通过图12A的过程下载简档的过程和根据图12B的简档启用过程可以作为单独的过程执行。同样显而易见的是,如果已经下载了简档,则可以仅执行图12B的过程。

[0329] 启用命令发起可以直接表示仅通过对应的发起命令启用特定简档,但是在实施例中可以简单地指示eUICC质询被发送到管理SM-DP+的特定第二简档服务器或简档管理服务器,以便请求认证。

[0330] 步骤1270至1283中的eUICC终端和第二简档服务器之间的以下操作可以与图12A中的步骤1205至步骤1230相同或相似。

[0331] 在步骤1284中,第二简档服务器可以认证在步骤1200中接收的eUICC证书和eUICC签名数据。

[0332] 如果认证通过,则第二简档服务器可以准备要递送到eUICC终端的RPM命令或RPM包(如果存在的话)。

[0333] 在步骤1285中,第二简档服务器可以将RPM命令或RPM包递送到eUICC终端。

[0334] 在步骤1286中,eUICC终端认证所接收的RPM命令或RPM包,并且识别第二简档供应服务器的服务器信息是否与简档元数据内的信息匹配,该简档元数据包括在与RPM命令或RPM包中包括的RPM命令对应的简档中。

[0335] 如果两者匹配,则终端可以执行RPM命令。如果RPM命令指示启用特定简档,则终端可以在步骤1287中启用简档。

[0336] 因此,终端可以通过使用对应简档内的接入信息(IMSI或Ki信息)来接入移动通信网络。

[0337] 在启用可以通过第二简档供应服务器管理的简档之后,仅通过第二简档供应服务器禁用简档也是可能的。此外,eUICC终端的eUICC可以在给定时刻启用最多仅一个SIM简档,并且可以仅通过第二简档供应服务器启用/禁用安装的简档。

[0338] 图13A示出根据实施例的用于通过远程管理服务器远程执行简档安装和简档启用的装置和方法的另一实施例,并且图13B示出根据实施例的用于通过远程管理服务器远程执行简档安装和简档启用的装置和方法的另一实施例。

[0339] 参考图13A,服务服务器(远程管理服务器)可以在步骤1300中请求eUICC终端发起简档下载。

[0340] 随后的步骤1305至步骤1340可以与图12A中的步骤1205至步骤1240相同或相似。这里将省略其详细描述。

[0341] 在步骤1345中,终端可以将在步骤1340中从简档供应服务器接收的简档元数据信息的全部或部分递送到服务服务器。

[0342] 在步骤1350中,服务服务器可以将关于在步骤1345中接收的简档元数据的全部或部分的信息与服务服务器中预先配置的简档元数据的全部或部分进行比较,从而确认两者是否相同。特别地,预先配置的值可以包括关于第二简档供应服务器的信息,并且服务服务

器可以将预先配置的第二简档供应服务器信息与接收到的信息进行比较。

[0343] 在该实施例中,服务服务器将关于从终端接收的简档元数据的全部或部分的信息与服务服务器中预先配置的信息进行比较,使得在终端中仅安装具有在其中确认的适当的第二简档供应服务器信息的简档,并且仅允许第二简档供应服务器参与管理安装的简档的操作。在认证通过之后,进行以下过程。

[0344] 同时,如果认证未通过,则可以结束该过程,使得不安装对应的简档。

[0345] 如果认证通过,则在步骤1355中,服务服务器可以将结果发送到终端以通知认证成功。在接收到关于成功认证的响应之后,终端可以从步骤1360进行到步骤1370并安装简档。

[0346] 步骤1360和步骤1370之间的操作可以与图12A中的步骤1250-1260相同或相似。

[0347] 图13B示出根据实施例的用于由终端启用简档的方法的示图。

[0348] 参考图13B,在图13A的过程之后,服务服务器可以将安装在图13A中的SIM简档的简档启用发起递送到eUICC终端。图13A和图13B中所示的过程不必然连续执行,并且通过图13A的过程下载简档的过程和根据图13B的简档启用过程可以作为单独的过程执行。同样显而易见的是,如果已经下载了简档,则可以仅执行图13B的过程。

[0349] 启用命令发起可以直接表示仅通过对应的发起命令启用特定简档,但是在实施例中可以简单地指示eUICC质询被发送到管理SM-DP+的特定第二简档服务器或简档管理服务器,以便请求认证。

[0350] 步骤1380至步骤1385中的eUICC终端和第二简档服务器之间的以下操作可以与图12A中的步骤1205至步骤1230相同或相似。

[0351] 在步骤1386中,第二简档服务器可以认证在步骤1385中接收的eUICC证书和eUICC签名数据。

[0352] 如果认证通过,则第二简档服务器可以准备要递送到eUICC终端的RPM命令或RPM包(如果存在的话)。

[0353] 在步骤1387中,第二简档服务器可以将RPM命令或RPM包递送到eUICC终端。

[0354] 在步骤1388中,eUICC终端认证接收到的RPM命令或RPM包,并且确认第二简档供应服务器的服务器信息是否与简档元数据内的信息匹配,该简档元数据包括在与RPM命令或RPM包中包括的RPM命令对应的简档中。

[0355] 如果两者匹配,则终端可以执行RPM命令。如果RPM命令指示启用特定简档,则终端可以在步骤1389中启用简档。

[0356] 因此,终端可以通过使用对应简档内的接入信息(IMSI或Ki信息)来接入移动通信网络。

[0357] 在启用可以通过第二简档供应服务器管理的简档之后,仅通过第二简档供应服务器禁用简档也是可能的。此外,eUICC终端的eUICC可以在给定时刻启用最多仅一个SIM简档,并且可以仅通过第二简档供应服务器启用/禁用安装的简档。

[0358] 图14AA示出用于通过根据实施例的远程管理服务器远程执行简档安装和简档启用的装置和方法的另一实施例,图14AB示出用于通过根据实施例的远程管理服务器远程执行简档安装和简档启用的装置和方法的另一实施例,并且图14B示出用于通过根据实施例的远程管理服务器远程执行简档安装和简档启用的装置和方法的另一实施例。

[0359] 参考图14AA和图14AB,eUICC终端的管理者或用户可以通过管理终端接入服务服务器(或远程管理服务器),并且可以通过管理终端的UI输入简档下载发起请求。因此,在步骤1400中,管理终端可以将简档下载发起请求发送到服务服务器。

[0360] 从步骤1405到步骤1455的后续操作可以与图13A中的步骤1300到步骤1350相同或相似。这里将省略其详细描述。

[0361] 如果在步骤1455中认证成功,则服务服务器可以在步骤1460中向管理终端提供关于简档元数据的全部或部分的信息。因此,管理终端可以在步骤1465中确定是否进行简档安装。例如,eUICC终端的管理者或用户可以通过管理终端的UI检查元数据的部分或全部的内容或与其对应的内容(例如,图标),并且可以确定是否继续简档安装。可替代地,可以基于预存储在管理终端中的参考或规则来确定是否继续简档安装。

[0362] 在步骤1470中,管理终端可以将步骤1465中的确定结果(例如,指示是否继续简档安装的信息)递送到服务服务器。如果接收到的结果指示简档安装将继续,则服务服务器可以进行到下一过程,如果不是,则可以结束安装过程。

[0363] 如果要继续简档安装,则服务服务器和终端可以执行步骤1475到步骤1486。从步骤1475到步骤1486的过程可以与图13A中的从步骤1355到步骤1370的操作相同或相似。这里将省略其详细描述。

[0364] 图14B示出用于由根据实施例的终端启用简档的方法的示图。

[0365] 参考图14B,在图14A的过程之后,服务服务器可以将图14A中安装的SIM简档的简档启用发起递送到eUICC终端。图14B中的步骤1487至步骤1497可以与图13B中的步骤1375至步骤1389相同。

[0366] 图15示出根据实施例的可以与图12、图13和图14一起实现的更具体的操作的示图。

[0367] 参考图15,eUICC、LPA、连接控制app(与连接控制客户端可互换使用)和推送客户端可以是eUICC终端的组成元件。另外,连接控制app和推送客户端的组合或者单独的连接控制app可以被称为服务app。此外,连接控制服务器和推送服务器的组合或者单独的连接控制服务器可以被称为服务服务器(或远程管理服务器)。

[0368] 首先,将描述在参考图12描述的步骤1200之前在服务服务器中注册与eUICC对应的ID的处理。

[0369] 在步骤A中,eUICC终端可以在服务服务器中注册EID。更具体地,推送客户端可以维持与推送服务器的持久IP连接。推送服务器可以与连接控制服务器分离。

[0370] 推送客户端然后可以向连接控制客户端提供推送令牌。连接控制客户端可以请求LPA提供EID。然后,LPA可以将EID提供给连接控制客户端。

[0371] 连接控制客户端可以随后将从LPA接收的EID和推送令牌两者递送到连接控制服务器,从而注册EID。

[0372] 随着终端以这种方式在服务服务器中注册EID时,服务服务器可以向适当的终端发送简档发起请求。

[0373] 步骤B对应于以下步骤:在服务服务器执行图12A中的步骤1200、图12B中的步骤1265、图13A中的步骤1300、图13B中的步骤1375、图14A中的步骤1405和图14B中的步骤1487之前,服务服务器预先指示第一简档服务器或第二简档服务器准备简档下载或RPM下载,并

响应于此而接收匹配的ID。在图12A的步骤1230中，可以将匹配ID递送到第一简档服务器或第二简档服务器，以便识别第一简档服务器或第二简档服务器是否具有要提供给终端的简档或RPM。

[0374] 步骤C可以对应于图12A中的步骤1200、图12B中的步骤1265、图13A中的步骤1300、图13B中的步骤1375、图14B中的步骤1405和步骤14B中的步骤1487的整个过程，或其部分过程。

[0375] 在步骤C中，连接控制服务器可以初始向推送服务器提供推送令牌，以便向终端递送信息。推送服务器可以通过使用推送令牌将推送令牌递送到与步骤A中的推送令牌对应(或连接到该推送令牌)的推送客户端。

[0376] 然后，推送客户端可以将推送令牌递送到连接控制app，以便通过向连接控制服务器提供EID来询问连接控制app是否具有要处理的操作。例如，连接控制app可以通过检查动作请求来询问是否存在要处理的操作。

[0377] 响应于检查动作请求，连接控制服务器可以将初始化LPA API递送到连接控制客户端。

[0378] 然后，连接控制客户端可以将其递送到LPA，并且此后可以将匹配ID以及第一简档服务器或第二简档服务器的服务器地址递送到eUICC终端。匹配ID以及第一简档服务器或第二简档服务器的服务器地址可以是由SM-DP+2的签名所签名的值。

[0379] 图15中的第一简档服务器可以是图12至图14中的第一简档供应服务器或第二简档供应服务器。同样地，图15中的第二简档服务器可以与图12至图14中的第一简档供应服务器或第二简档供应服务器相同或分离。

[0380] 在步骤D之后是简档下载或RPM下载的过程。在简档或RPM下载完成之后，第一简档服务器可以将结果递送到连接控制服务器。

[0381] 尽管已经参考图12至图15描述了与一个eUICC终端相关的操作，但是可以通过与图12至图15中相同的过程来管理多个终端中的每一个。

[0382] 特别地，可以通过使用如图12或图13中的方案来有效地管理大规模终端。

[0383] 图16示出根据实施例的终端的配置的示图。

[0384] 如图16所示，终端可以包括收发器1610和至少一个处理器1620。另外，终端可以包括UICC 1630。例如，UICC 1630可以插入到终端中，或者可以嵌入在终端中。至少一个处理器1620还可以被称为控制器。

[0385] 根据实施例的收发器1610可以根据各种实施例利用简档服务器发送和接收信号、信息、数据等。

[0386] 例如，根据各种实施例的收发器1610可以从简档服务器接收至少包括远程管理命令的消息。

[0387] 根据实施例的收发器1610可以将包括远程管理输入结果的消息(处理通知)作为回复发送到简档服务器。

[0388] 同时，至少一个处理器1620是用于终端的整体控制的构成元件。如本文所使用的，处理器可以被定义为电路、专用集成电路、至少一个处理器或控制器。处理器1620可以根据如上所述的各种实施例控制终端的整体操作。

[0389] 例如，根据各种实施例的至少一个处理器1620可以确定接收到的远程管理命令是

否可以由UICC 1630处理,可以将远程管理命令输入到UICC 1630,可以识别简档服务器是否包括在UICC 1630中的管理者简档服务器列表中,可以在UICC 1630中执行远程管理,可以生成远程管理输入结果,可以在远程管理输入结果包括错误代码的情况下分析错误代码,可以将远程管理命令切换为本地管理命令,可以将本地管理命令输入到UICC 1630,可以在UICC 1630中执行本地管理,并且可以将本地管理输入结果(本地管理结果)切换为远程管理输入结果(加载RPM包结果)。

[0390] 另外,根据各种实施例的至少一个处理器1620可以控制收发器1610以便从简档服务器接收远程管理命令,可以处理远程管理命令,并且可以将远程管理输入结果发送到简档服务器。

[0391] 另外,根据本公开的处理器1620可以将从服务服务器接收的简档元数据与从简档供应服务器接收的元数据的全部或部分进行比较,从而认证服务服务器的简档下载发起请求。另外,响应于服务服务器的简档启用请求,处理器1620可以认证简档供应服务器的信息,从而启用简档。

[0392] 或者,处理器1620可以将简档元数据的全部或部分发送到服务服务器,使得服务服务器可以认证简档下载发起请求。

[0393] 处理器1620还可以控制本公开中描述的终端的其他操作。

[0394] 根据各种实施例的UICC 1630可以下载简档并且可以安装简档。UICC 1630还可以管理简档。

[0395] UICC 1630可以在处理器1620的控制下操作。可替代地,UICC 1630可以包括用于安装简档的处理器或控制器,或者可以具有安装在其中的应用。应用的部分也可以安装在处理器1620中。

[0396] 同时,在示出本公开的方法的附图中,描述的顺序不必然对应于执行的顺序。可以改变之前/之后的关系,或者可以并行进行执行。

[0397] 可替代地,在不脱离本公开的主旨的情况下,可以从示出本公开的方法的附图中省略一些组成元件,并且可以仅包括一些组成元件。

[0398] 另外,结合本公开的方法,在不脱离本公开的主旨的情况下,可以组合执行各个实施例中包括的部分或全部内容。

[0399] 同时,终端还可以包括存储器(未示出),并且可以存储用于终端的操作的数据,诸如基本程序、应用和配置信息。存储器可以包括从闪存型、硬盘型、多媒体卡微型、卡型存储器(例如,SD或XD存储器)、磁存储器、磁盘、光盘、随机存取存储器(RAM)、静态随机存取存储器(SRAM)、只读存储器(ROM)、可编程只读存储器(PROM)和电可擦除可编程只读存储器(EEPROM)中选择的至少一个存储介质。另外,处理器可以通过使用存储在存储器中的各种程序、内容、数据等来执行各种操作。

[0400] 图17示出根据实施例的简档服务器的配置的示图。

[0401] 参考图17,简档服务器可以包括收发器1710、控制器1720和存储器1730。在本公开中,控制器可以被定义为电路、专用集成电路或至少一个处理器。

[0402] 收发器1710可以与另一实体发送/接收信号。

[0403] 控制器1720可以控制根据本公开中提出的实施例的简档服务器的整体操作。例如,控制器1720可以控制各个块之间的信号流,使得根据上述流程图执行操作。

[0404] 存储器1730可以存储通过收发器1710发送/接收的信息和通过控制器1720生成的信息中的至少一个。

[0405] 图18示出根据实施例的服务服务器的配置的示图。

[0406] 参考图18,服务服务器可以包括收发器1810、控制器1820和存储器1830。在本公开中,控制器可以被定义为电路、专用集成电路或至少一个处理器。

[0407] 收发机1810可以与另一实体发送/接收信号。

[0408] 控制器1820可以控制根据本公开中提出的实施例的简档服务器的整体操作。例如,控制器1820可以控制各个块之间的信号流,使得根据上述流程图执行操作。

[0409] 存储器1830可以存储通过收发器1810发送/接收的信息和通过控制器1820生成的信息中的至少一个。

[0410] 在本公开的上述详细实施例中,根据所呈现的详细实施例,本公开中包括的组件以单数或复数表示。然而,选择单数形式或复数形式是为了便于适合于所呈现的情况的描述,并且本公开的各种实施例不限于其单个元件或多个元件。此外,说明书中表达的多个元件可以被配置为单个元件,或者说明书中的单个元件可以被配置为多个元件。

[0411] 虽然已经参考本公开的特定实施例示出和描述了本公开,但是本领域技术人员将理解,在不脱离本公开的范围的情况下,可以在其中进行形式和细节上的各种改变。因此,本公开的范围不应被限定为限于实施例,而应由所附权利要求及其等同物限定。

[0412] 其中使用的各种实施例和术语不是为了将本文公开的技术限制于特定实施方式的目的,而是应被理解为包括对应实施例的各种改变、等同物和/或替代方案。在描述附图时,可以使用类似的附图标记来表示类似的组成元件。单数表达可以包括复数表达,除非它们在上下文中明确不同。术语“A或B”、“A和/或B中的一个或更多个”、“A、B或C”或“A、B和/或C中的一个或更多个”可以包括它们的所有可能的组合。在本公开的各种实施例中使用的表述“第一”、“第二”、“所述第一”或“所述第二”可以修饰各种组件,而不管顺序和/或重要性如何,但不限制对应的组件。当元件(例如,第一元件)被称为“(功能地或通信地)连接”或“直接耦接”到另一元件(第二元件)时,该元件可以直接连接到另一元件或通过又一元件(例如,第三元件)连接到另一元件。

[0413] 如本文所使用的术语“模块”可以包括由硬件、软件或固件组成的单元,并且可以例如与术语“逻辑”、“逻辑块”、“组件”、“电路”等互换使用。“模块”可以是集成组件或用于执行一个或更多个功能的最小单元或其部分。例如,模块可以是专用集成电路(ASIC)。

[0414] 各种实施例可以被实现为机器(例如,计算机)可读存储介质(例如,包括存储在内部或外部存储器中的指令的软件(例如,程序))。机器是指能够从存储介质检索存储的指令并根据检索的指令进行操作的设备,并且可以包括根据各种实施例的终端。如果命令由处理器(例如,图11中的处理器1620)执行,则处理器可以在处理器的控制下直接或通过使用其他组成元件来执行与命令对应的功能。命令可以包括由编译器或解释器生成或执行的代码。

[0415] 机器可读存储介质可以以非暂时性存储介质的形式提供。这里,术语“非暂时性”仅意味着存储介质是有形的而不包括信号,而不管数据是半永久地还是暂时地存储在存储介质中。

[0416] 可以在被包括在计算机程序产品中的同时提供根据本文公开的各种实施例的方

法。计算机程序产品可以作为产品在卖方和买方之间交易。计算机程序产品可以以机器可读存储介质(例如,压缩盘只读存储器(CD-ROM))的形式分发,或者可以经由应用商店(例如,Play StoreTM)在线分发。在在线分发的情况下,计算机程序产品的至少部分可以至少临时存储在存储介质中,例如制造商的服务器、应用商店的服务器或中继服务器的存储器,或者可以临时生成。根据各种实施例的每个组成元件(例如,模块或程序)可以包括单个实体或多个实体,并且可以省略上述对应的子组成元件中的一些,或者在各种实施例中可以进一步包括其他子组成元件。可替代地或附加地,一些元件(例如,模块或程序)可以集成到单个元件中,并且集成的元件仍然可以以与集成对应元件之前相同或相似的方式执行由每个对应元件执行的功能。由根据各种实施例的模块、编程模块或其他元件执行的操作可以顺序地、并行地、重复地或以启发式方式执行。至少一些操作可以根据另一顺序来执行,可以被省略,或者可以进一步包括其他操作。

[0417] 尽管已经利用各种实施例描述了本公开,但是可以向本领域技术人员建议各种改变和修改。本公开旨在涵盖落入所附权利要求的范围内的这些改变和修改。

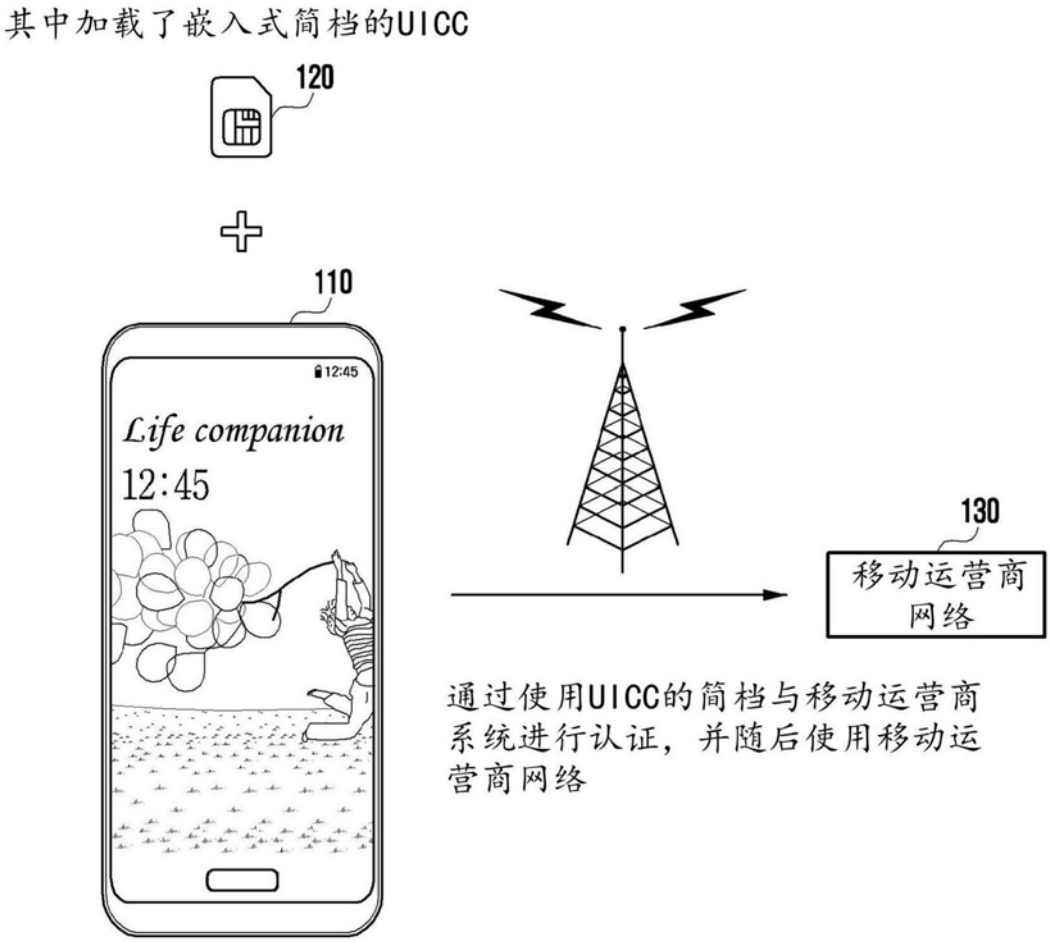

其中加载了嵌入式简档的UICC
120
110
12:45
Life companion
12:45
130
移动运营商网络
通过使用UICC的简档与移动运营商系统进行认证，并随后使用移动运营商网络

图1

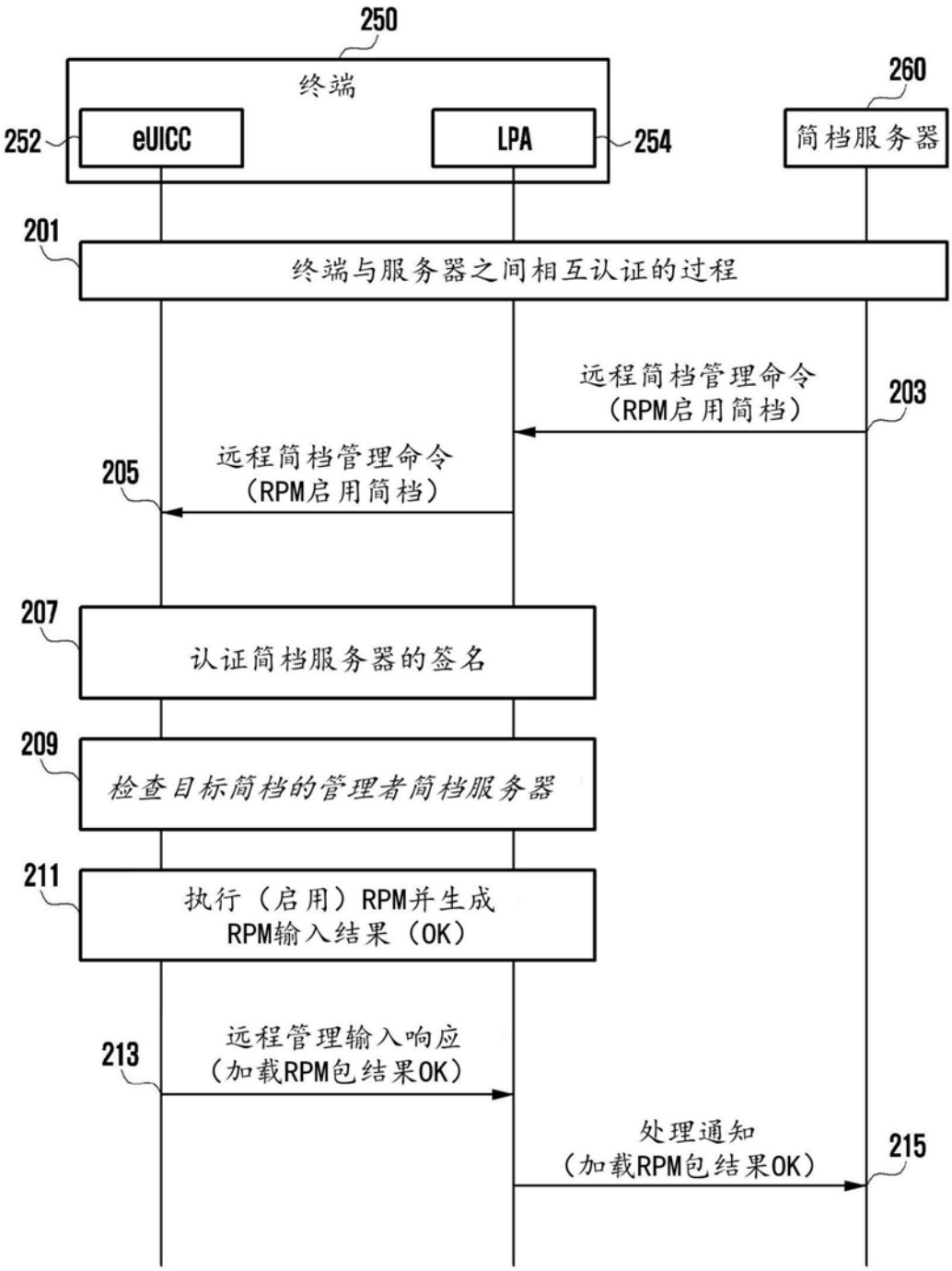

250
终端
252
eUICC
LPA
254
260
简档服务器
201
终端与服务器之间相互认证的过程
远程简档管理命令
（RPM启用简档）
203
205
远程简档管理命令
（RPM启用简档）
207
认证简档服务器的签名
209
检查目标简档的管理者简档服务器
211
执行（启用）RPM并生成
RPM输入结果（OK）
213
远程管理输入响应
（加载RPM包结果OK）
处理通知
（加载RPM包结果OK）
215

图2

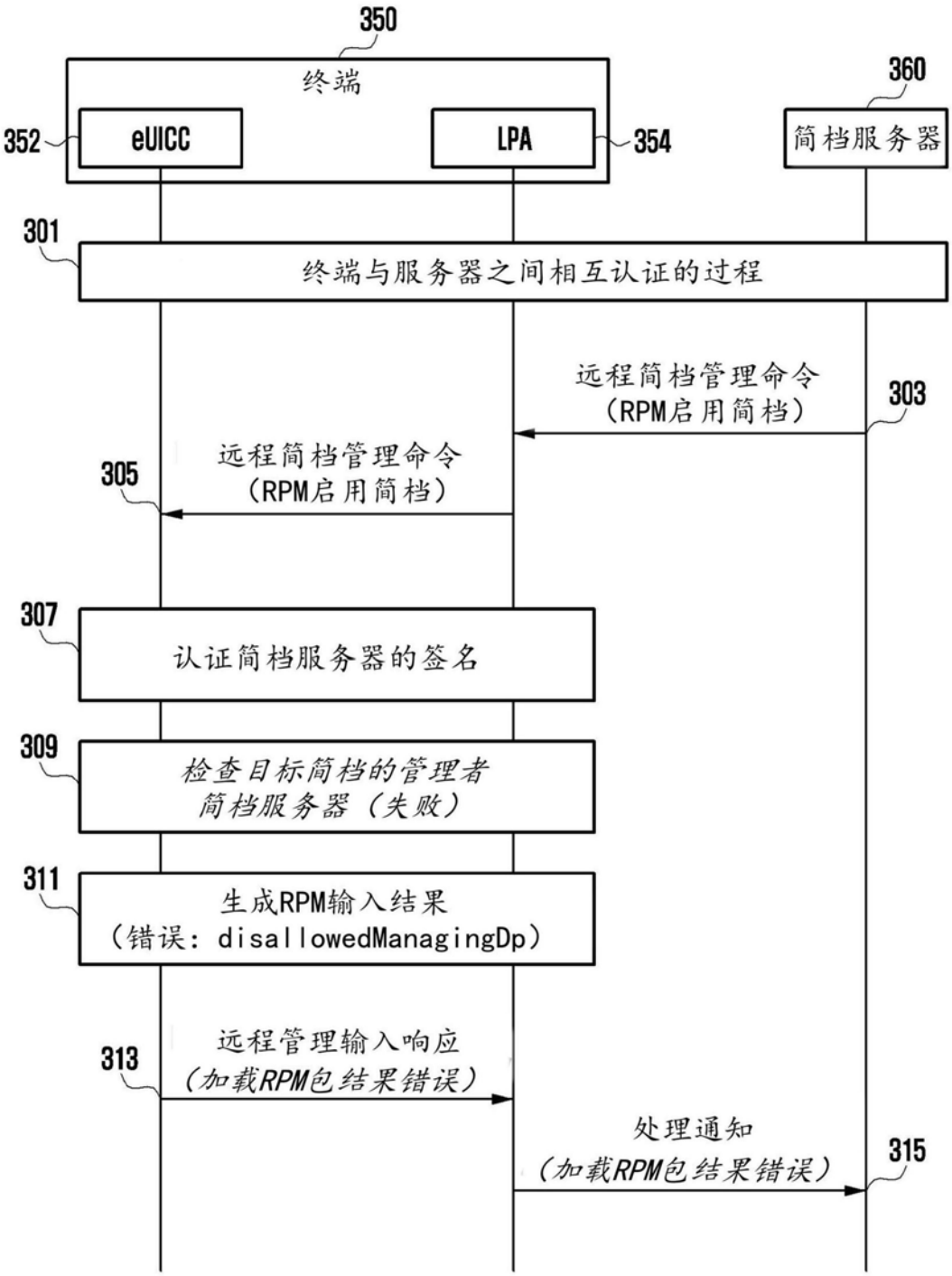

350
终端
352
eUICC
LPA
354
360
简档服务器
301
终端与服务器之间相互认证的过程
远程简档管理命令
(RPM启用简档)
303
远程简档管理命令
(RPM启用简档)
305
307
认证简档服务器的签名
309
检查目标简档的管理者
简档服务器（失败）
311
生成RPM输入结果
(错误：disallowedManagingDp)
远程管理输入响应
(加载RPM包结果错误)
313
处理通知
(加载RPM包结果错误)
315

图3

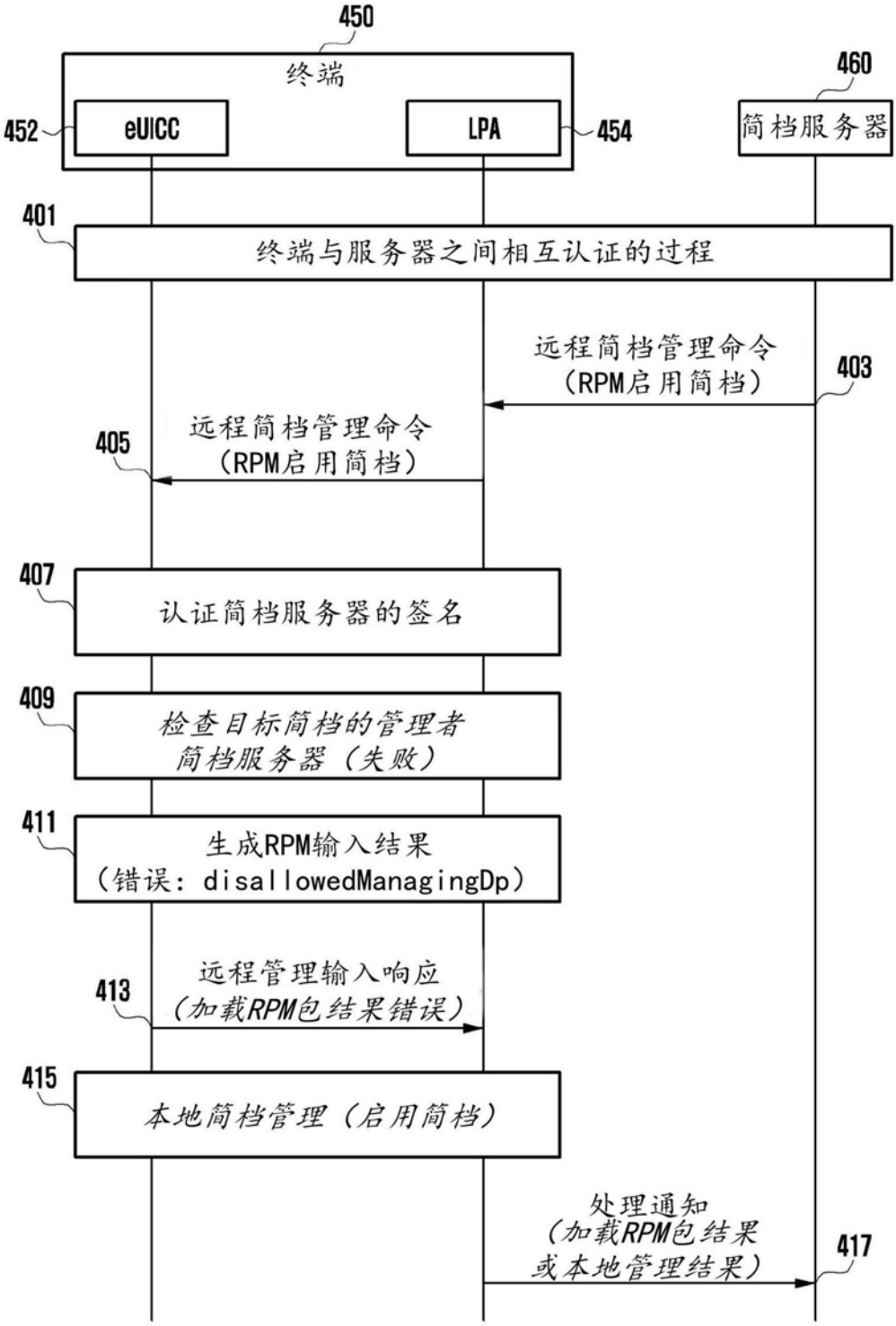

450
终端
452
eUICC
LPA
454
460
简档服务器
401
终端与服务器之间相互认证的过程
远程简档管理命令
(RPM启用简档)
403
405
远程简档管理命令
(RPM启用简档)
407
认证简档服务器的签名
409
检查目标简档的管理者
简档服务器 (失败)
411
生成RPM输入结果
(错误: disallowedManagingDp)
413
远程管理输入响应
(加载RPM包结果错误)
415
本地简档管理 (启用简档)
处理通知
(加载RPM包结果
或本地管理结果)
417

图4a

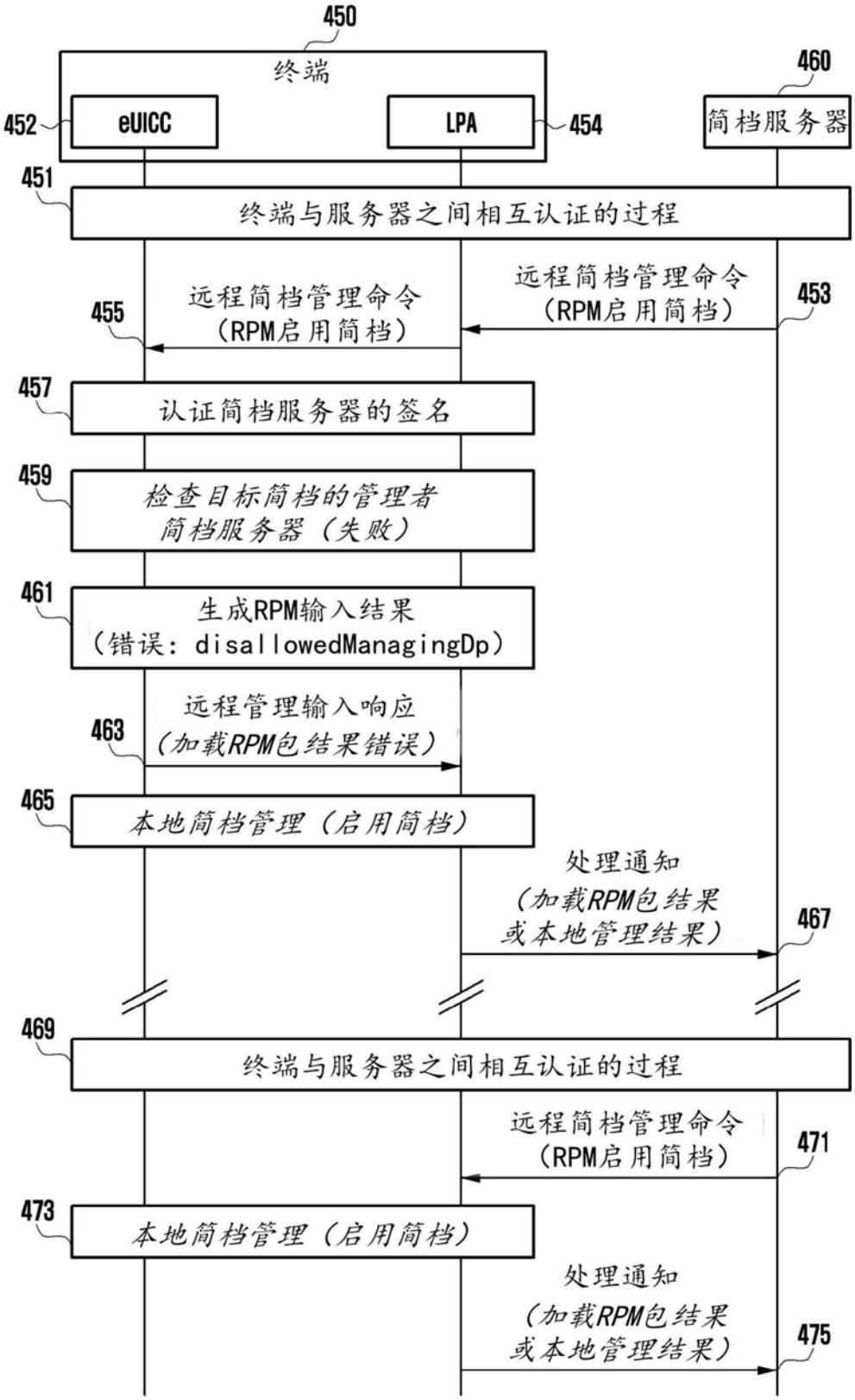

450
终端
452
eUICC
LPA
454
460
简档服务器
451
终端与服务器之间相互认证的过程
远程简档管理命令
(RPM启用简档)
455
远程简档管理命令
(RPM启用简档)
453
457
认证简档服务器的签名
459
检查目标简档的管理者
简档服务器（失败）
461
生成RPM输入结果
(错误：disallowedManagingDp)
远程管理输入响应
(加载RPM包结果错误)
463
465
本地简档管理（启用简档）
处理通知
(加载RPM包结果
或本地管理结果)
467
469
终端与服务器之间相互认证的过程
远程简档管理命令
(RPM启用简档)
471
473
本地简档管理（启用简档）
处理通知
(加载RPM包结果
或本地管理结果)
475

图4b

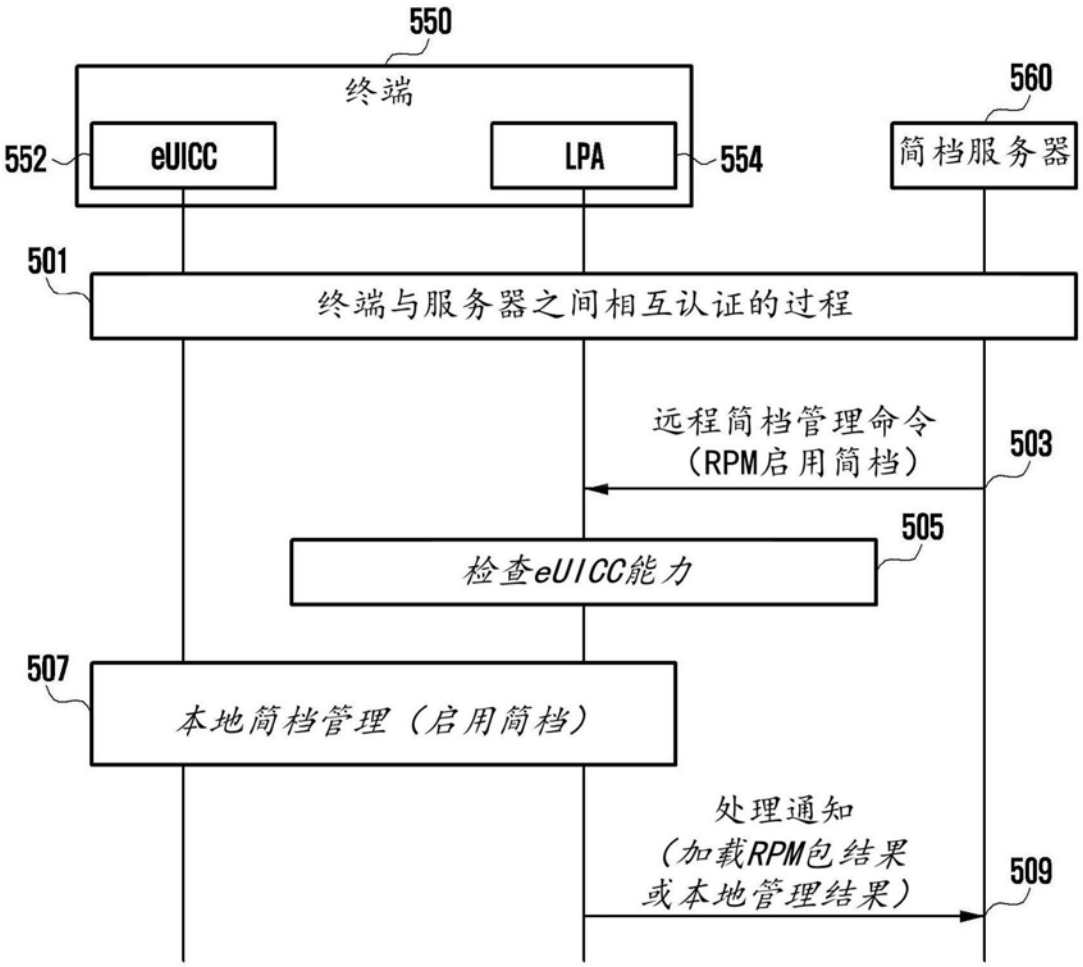

550
终端
552
eUICC
LPA
554
560
简档服务器
501
终端与服务器之间相互认证的过程
远程简档管理命令
（RPM启用简档）
503
505
检查eUICC能力
507
本地简档管理（启用简档）
处理通知
（加载RPM包结果
或本地管理结果）
509

图5

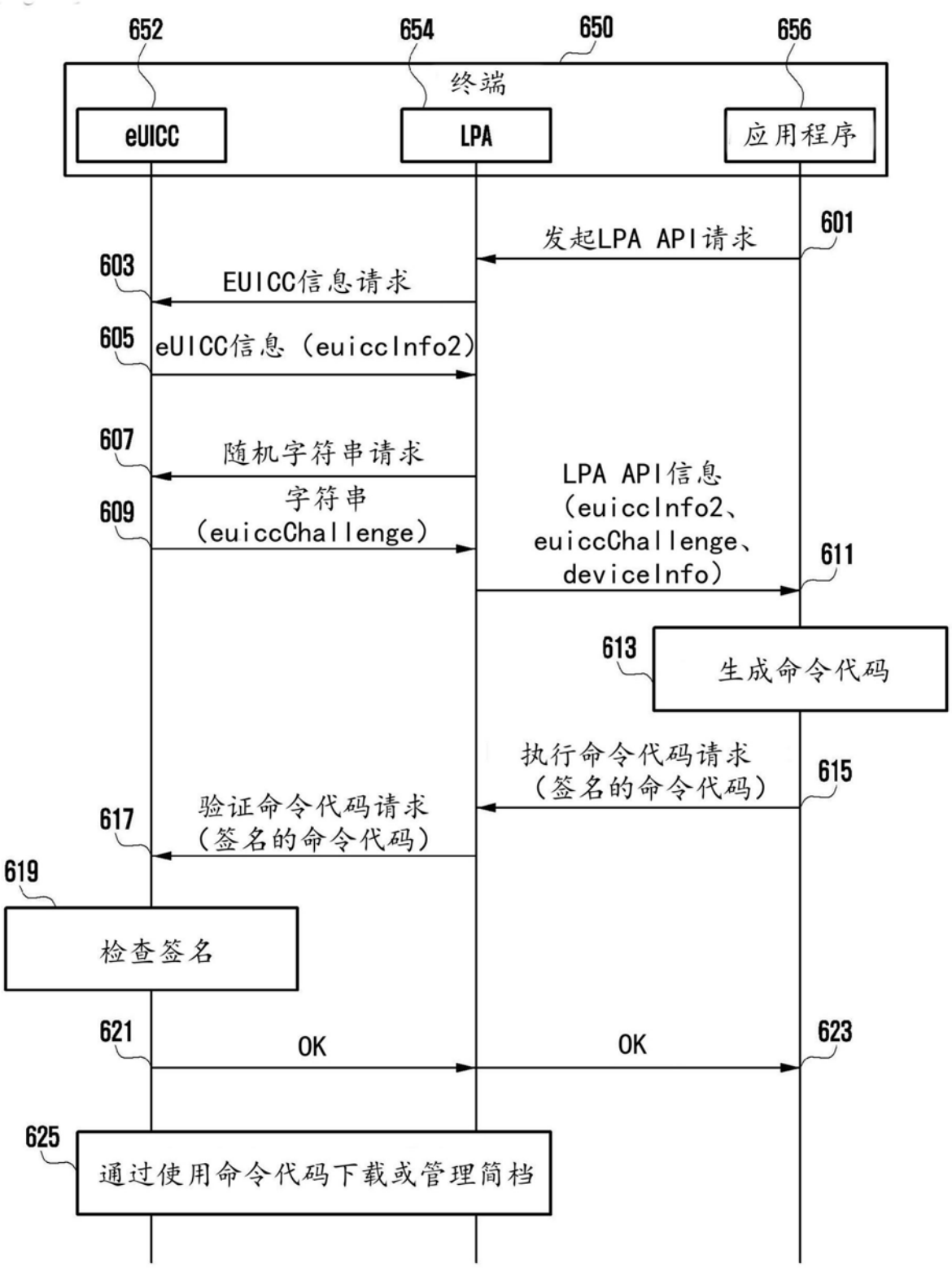

652
654
650
656
终端
eUICC
LPA
应用程序
601
发起LPA API请求
603
EUICC信息请求
605
eUICC信息（euiccInfo2）
607
随机字符串请求
609
字符串
（euiccChallenge）
LPA API信息
（euiccInfo2、
euiccChallenge、
deviceInfo）
611
613
生成命令代码
执行命令代码请求
（签名的命令代码）
615
617
验证命令代码请求
（签名的命令代码）
619
检查签名
621
OK
OK
623
625
通过使用命令代码下载或管理简档

图6a

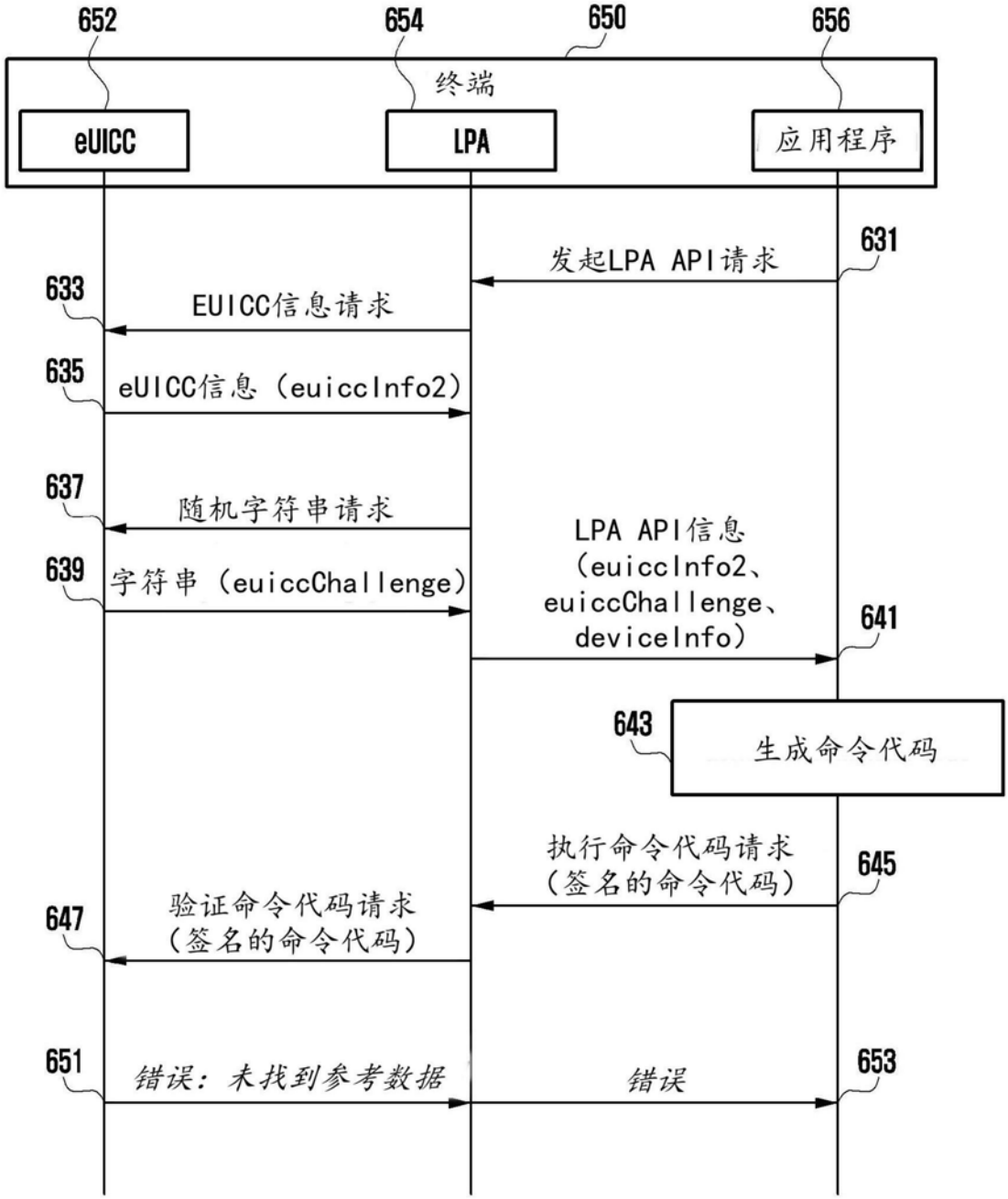

652
654
650
656
终端
eUICC
LPA
应用程序
631
发起LPA API请求
633
EUICC信息请求
635
eUICC信息（euiccInfo2）
637
随机字符串请求
639
字符串（euiccChallenge）
LPA API信息
（euiccInfo2、
euiccChallenge、
deviceInfo）
641
643
生成命令代码
执行命令代码请求
（签名的命令代码）
645
验证命令代码请求
（签名的命令代码）
647
651
错误：未找到参考数据
错误
653

图6b

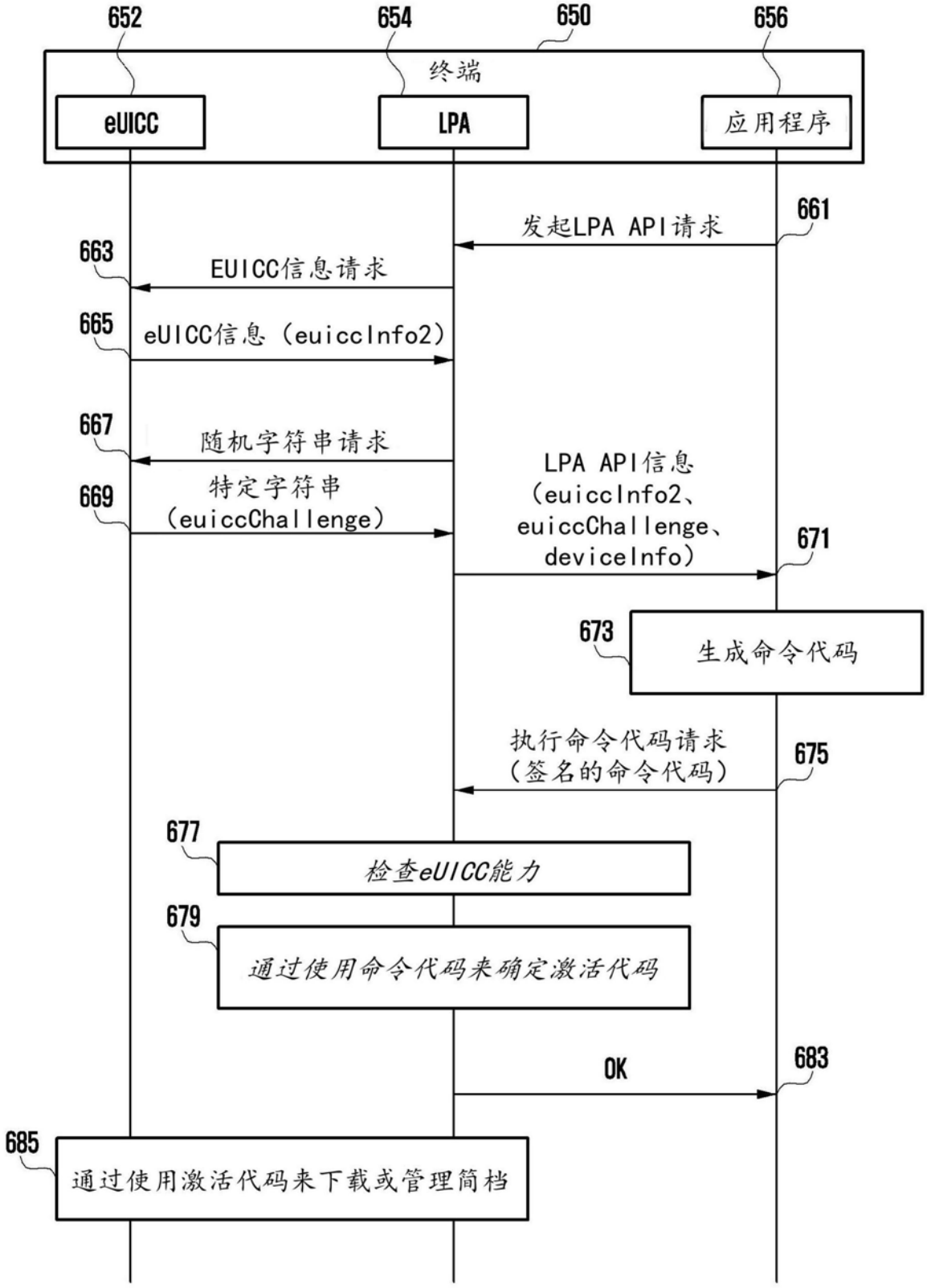

652
654
650
656
终端
eUICC
LPA
应用程序
661
发起LPA API请求
663
EUICC信息请求
665
eUICC信息（euiccInfo2）
667
随机字符串请求
669
特定字符串
（euiccChallenge）
LPA API信息
（euiccInfo2、
euiccChallenge、
deviceInfo）
671
673
生成命令代码
执行命令代码请求
（签名的命令代码）
675
677
检查eUICC能力
679
通过使用命令代码来确定激活代码
OK
683
685
通过使用激活代码来下载或管理简档

图6c

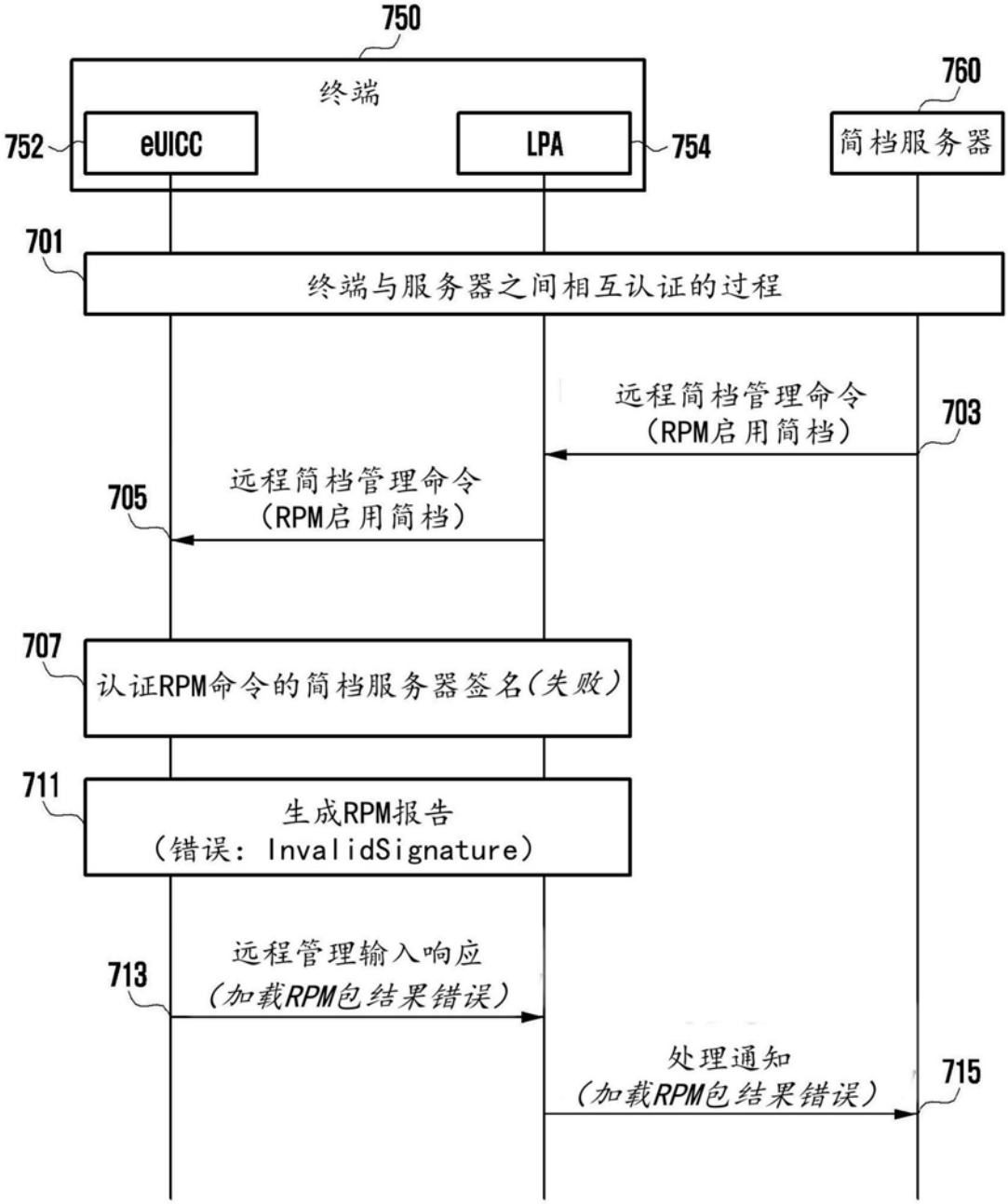

750
终端
752
eUICC
LPA
754
760
简档服务器
701
终端与服务器之间相互认证的过程
远程简档管理命令
(RPM启用简档)
703
705
远程简档管理命令
(RPM启用简档)
707
认证RPM命令的简档服务器签名(失败)
711
生成RPM报告
(错误: InvalidSignature)
713
远程管理输入响应
(加载RPM包结果错误)
处理通知
(加载RPM包结果错误)
715

图7

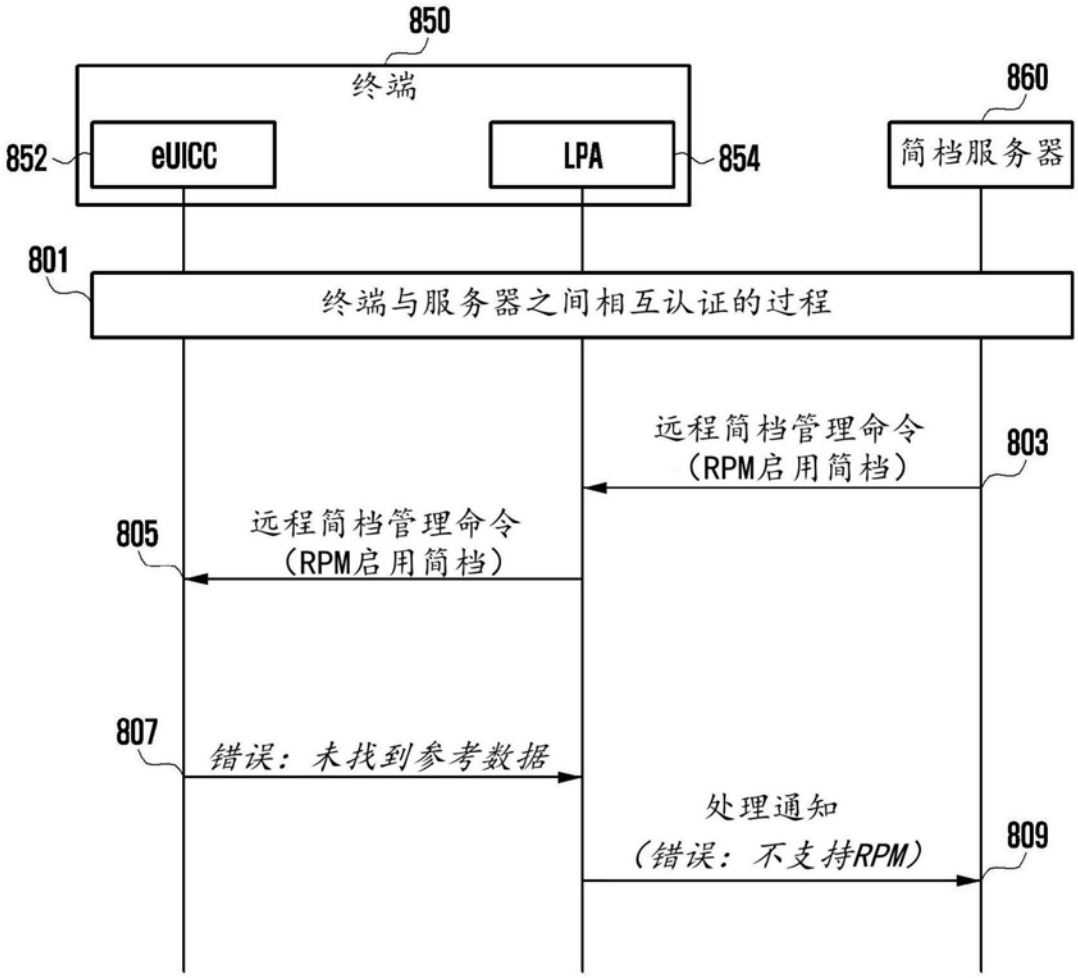

850
终端
852
eUICC
LPA
854
860
简档服务器
801
终端与服务器之间相互认证的过程
远程简档管理命令
(RPM启用简档)
803
805
远程简档管理命令
(RPM启用简档)
807
错误：未找到参考数据
处理通知
(错误：不支持RPM)
809

图8

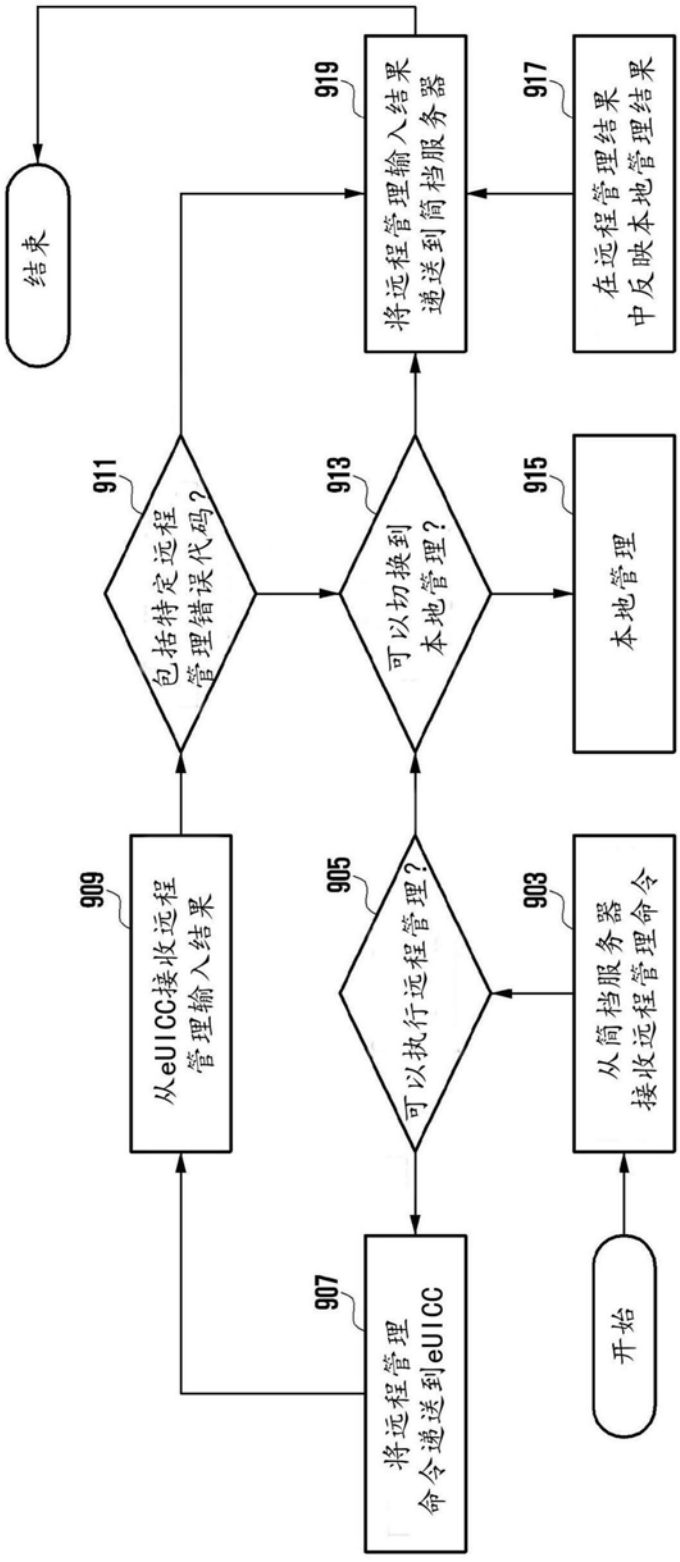

开始
从简档服务器
接收远程管理命令
903
可以执行远程管理?
905
将远程管理
命令递送到eUICC
907
从eUICC接收远程
管理输入结果
909
包括特定远程
管理错误代码?
911
可以切换到
本地管理?
913
本地管理
915
在远程管理结果
中反映本地管理结果
917
将远程管理输入结果
递送到简档服务器
919
结束

图9

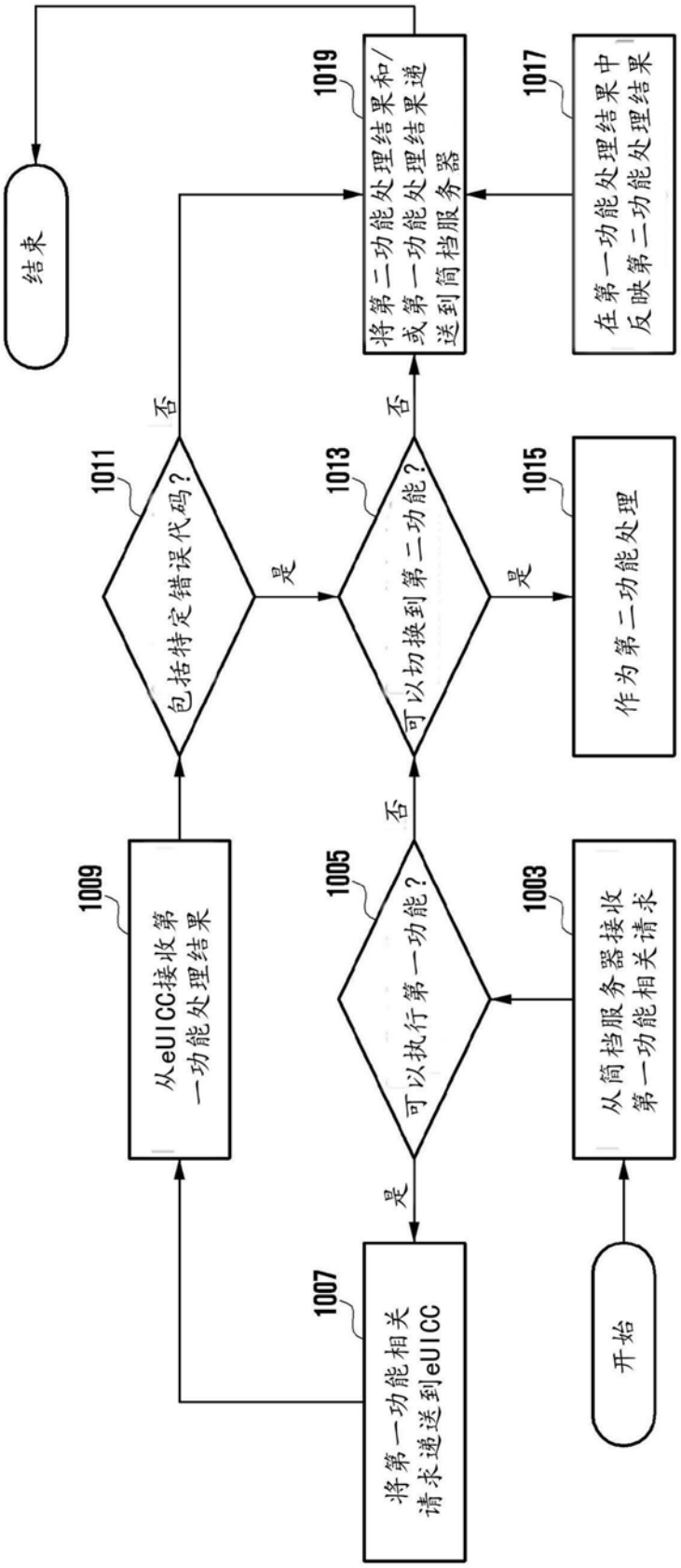

开始
从eUICC接收第一功能处理结果
从简档服务器接收第一功能相关请求
将第一功能相关请求递送到eUICC
可以执行第一功能？
从eUICC接收第一功能处理结果
作为第二功能处理
可以切换到第二功能？
在第一功能处理结果中反映第二功能处理结果
包括特定错误代码？
将第二功能处理结果和/或第一功能处理结果递送到简档服务器
结束
1003
1005
1007
1009
1011
1013
1015
1017
1019
是
否
是
否
是
否

图10

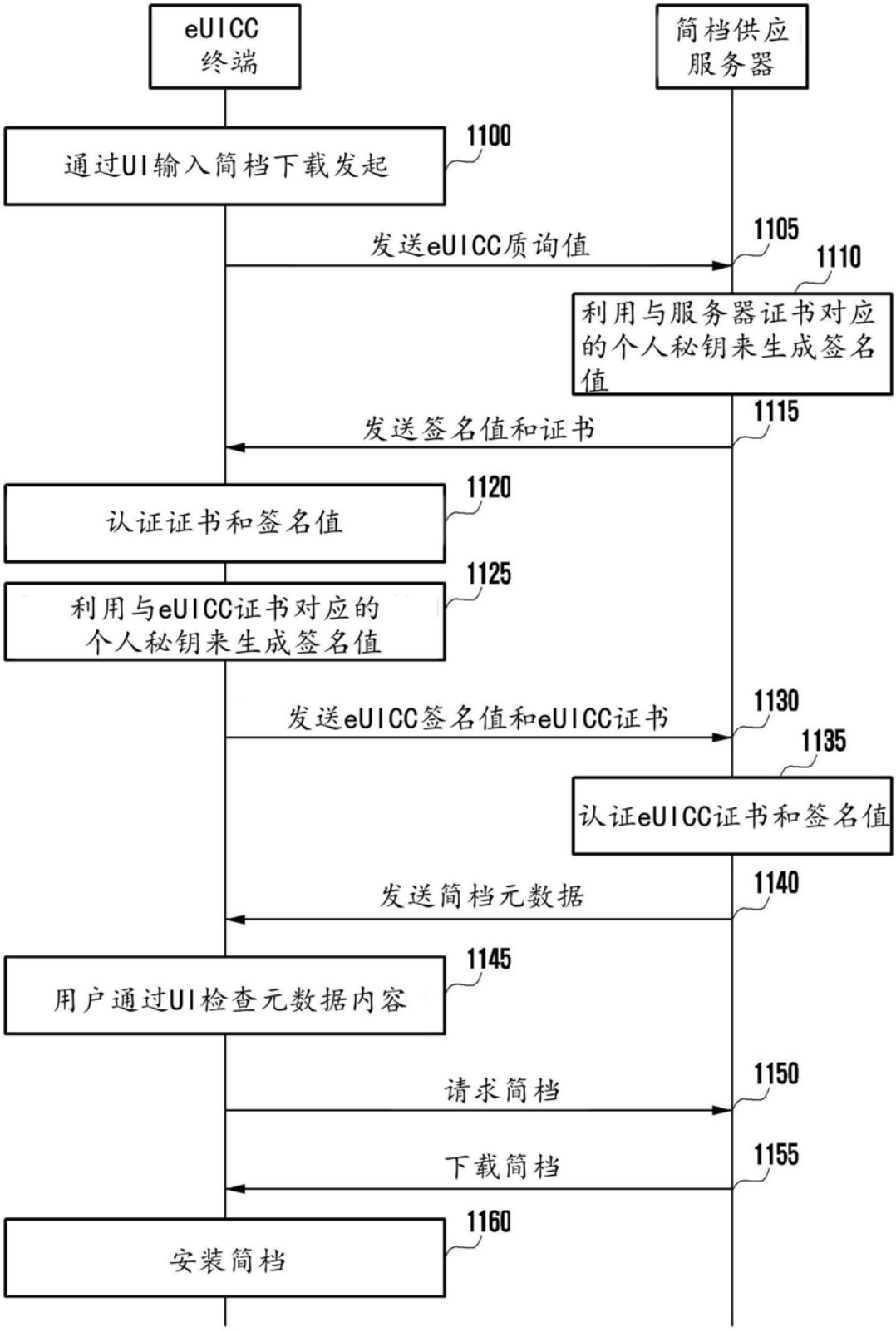

eUICC
终端
简档供应
服务器
1100
通过UI输入简档下载发起
1105
发送eUICC质询值
1110
利用与服务器证书对应的个人秘钥来生成签名值
1115
发送签名值和证书
1120
认证证书和签名值
1125
利用与eUICC证书对应的个人秘钥来生成签名值
1130
发送eUICC签名值和eUICC证书
1135
认证eUICC证书和签名值
1140
发送简档元数据
1145
用户通过UI检查元数据内容
1150
请求简档
1155
下载简档
1160
安装简档

图11a

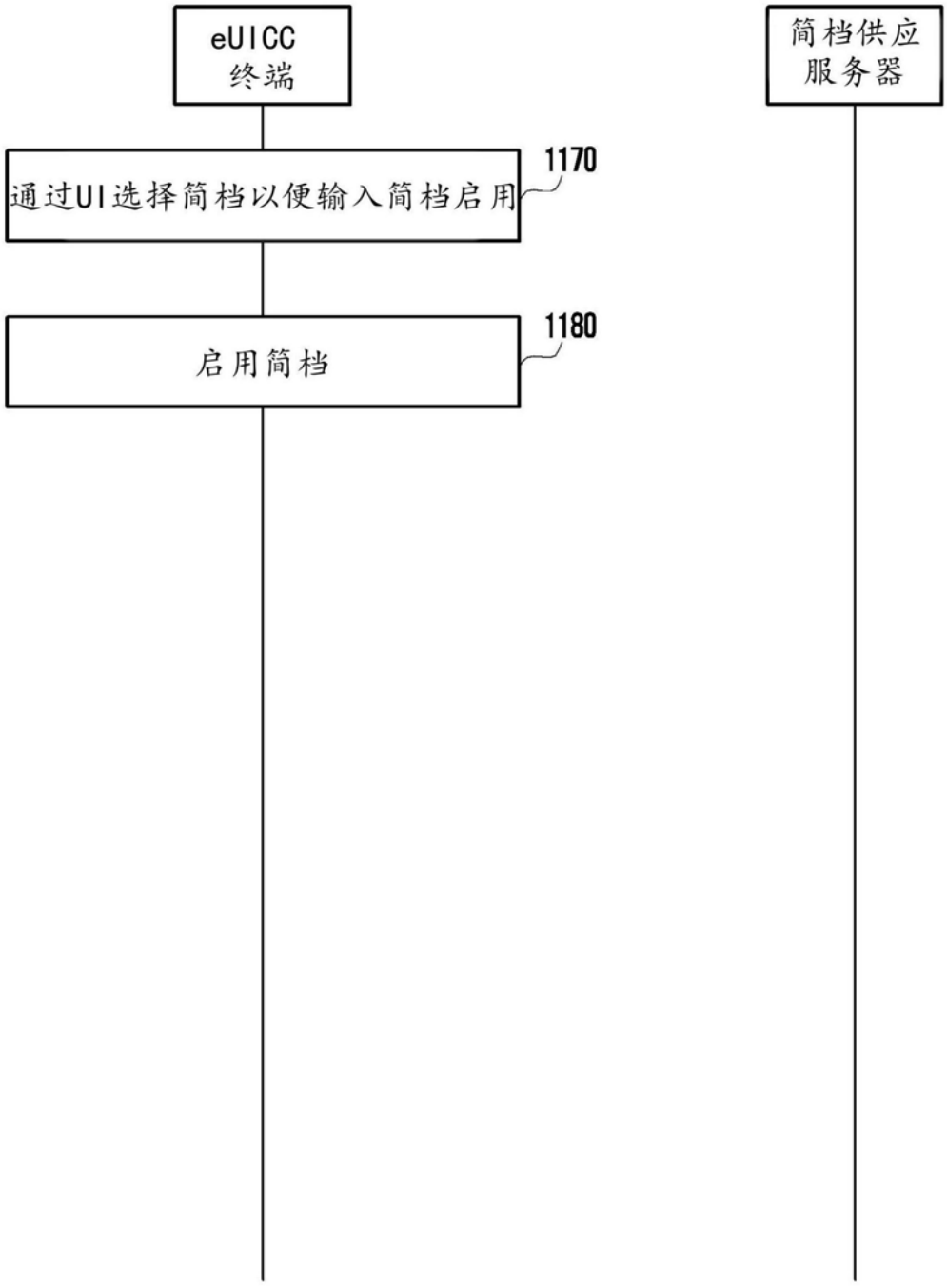


图11b

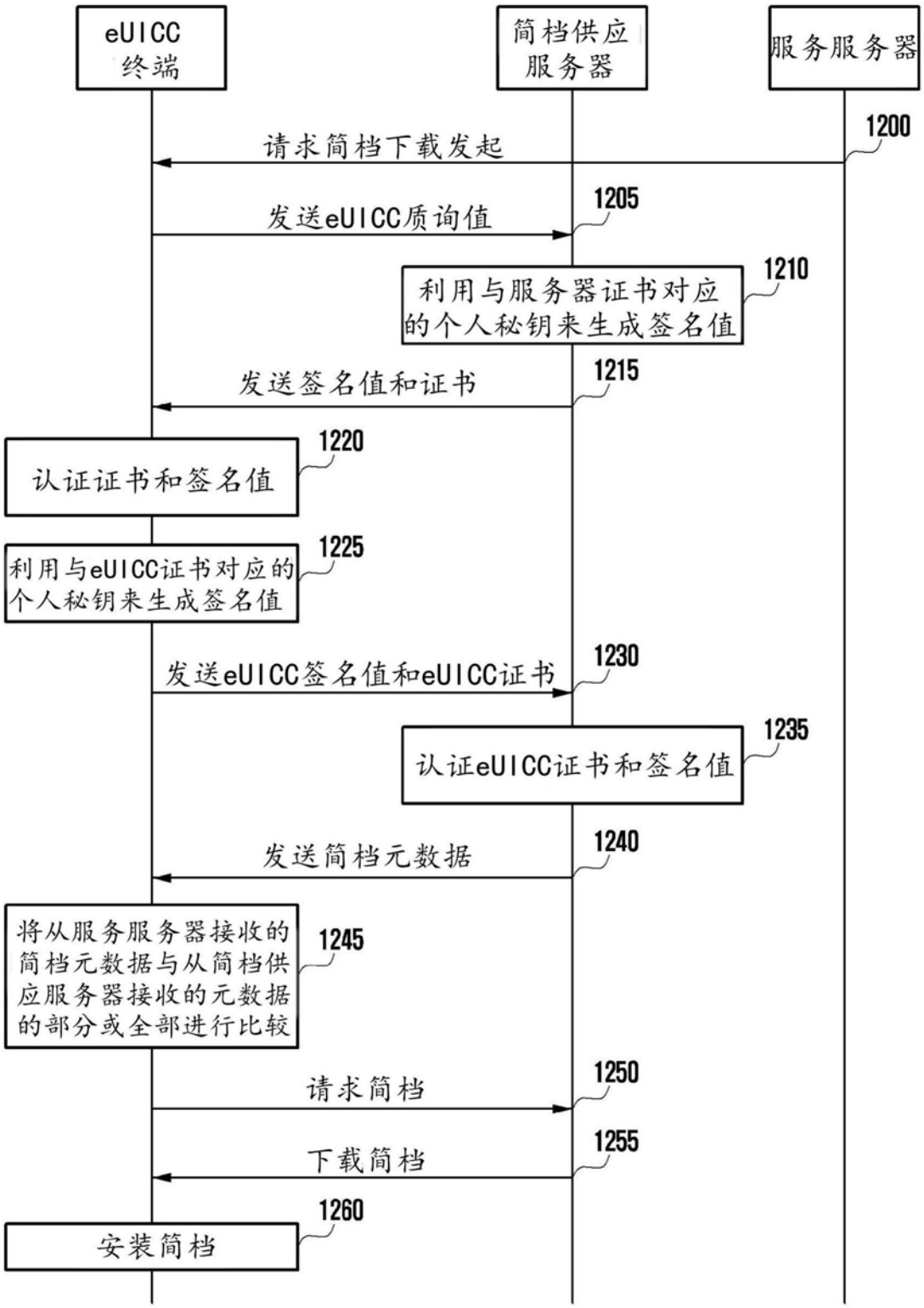

eUICC
终端
简档供应
服务器
服务服务器
1200
请求简档下载发起
1205
发送eUICC质询值
1210
利用与服务器证书对应
的个人秘钥来生成签名值
1215
发送签名值和证书
1220
认证证书和签名值
1225
利用与eUICC证书对应的
个人秘钥来生成签名值
1230
发送eUICC签名值和eUICC证书
1235
认证eUICC证书和签名值
1240
发送简档元数据
1245
将从服务服务器接收的
简档元数据与从简档供
应服务器接收的元数据
的部分或全部进行比较
1250
请求简档
1255
下载简档
1260
安装简档

图12a

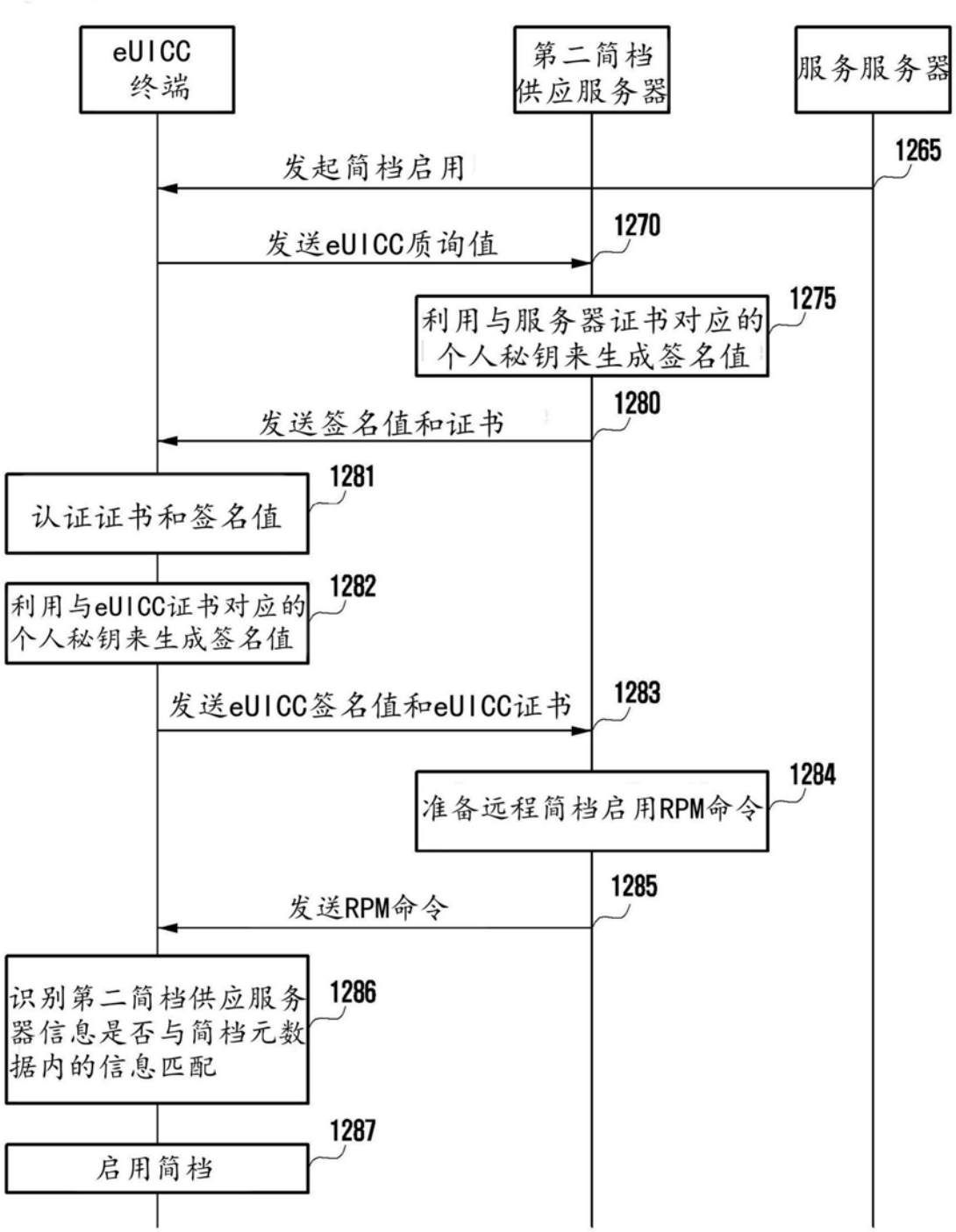

eUICC
终端
第二简档
供应服务器
服务服务器
1265
发起简档启用
1270
发送eUICC质询值
1275
利用与服务器证书对应的
个人秘钥来生成签名值
1280
发送签名值和证书
1281
认证证书和签名值
1282
利用与eUICC证书对应的
个人秘钥来生成签名值
发送eUICC签名值和eUICC证书
1283
1284
准备远程简档启用RPM命令
1285
发送RPM命令
1286
识别第二简档供应服务
器信息是否与简档元数
据内的信息匹配
1287
启用简档

图12b

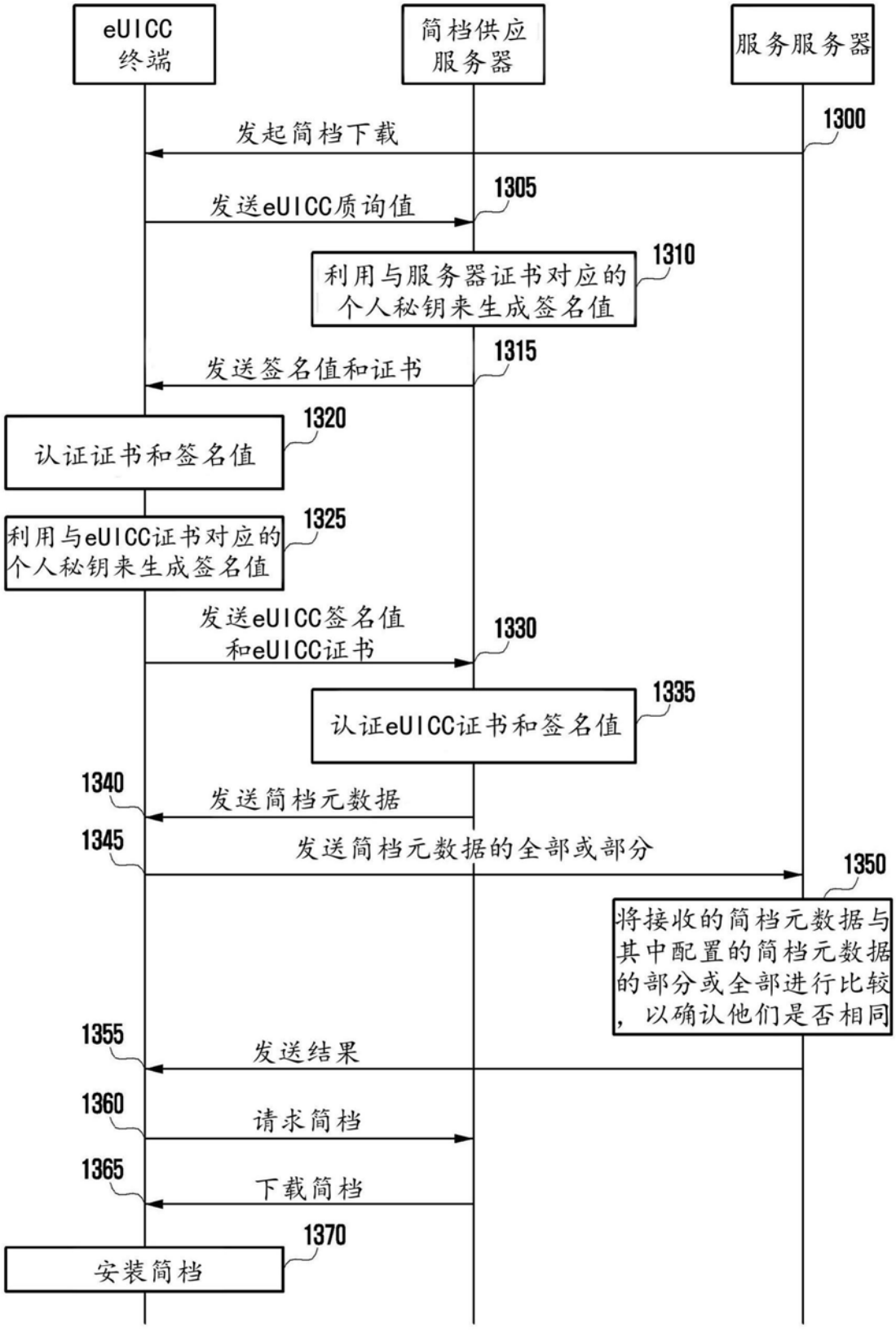

eUICC
终端
简档供应
服务器
服务服务器
1300
发起简档下载
1305
发送eUICC质询值
1310
利用与服务器证书对应的
个人秘钥来生成签名值
1315
发送签名值和证书
1320
认证证书和签名值
1325
利用与eUICC证书对应的
个人秘钥来生成签名值
发送eUICC签名值
和eUICC证书
1330
1335
认证eUICC证书和签名值
1340
发送简档元数据
1345
发送简档元数据的全部或部分
1350
将接收的简档元数据与
其中配置的简档元数据
的部分或全部进行比较
，以确认他们是否相同
1355
发送结果
1360
请求简档
1365
下载简档
1370
安装简档

图13a

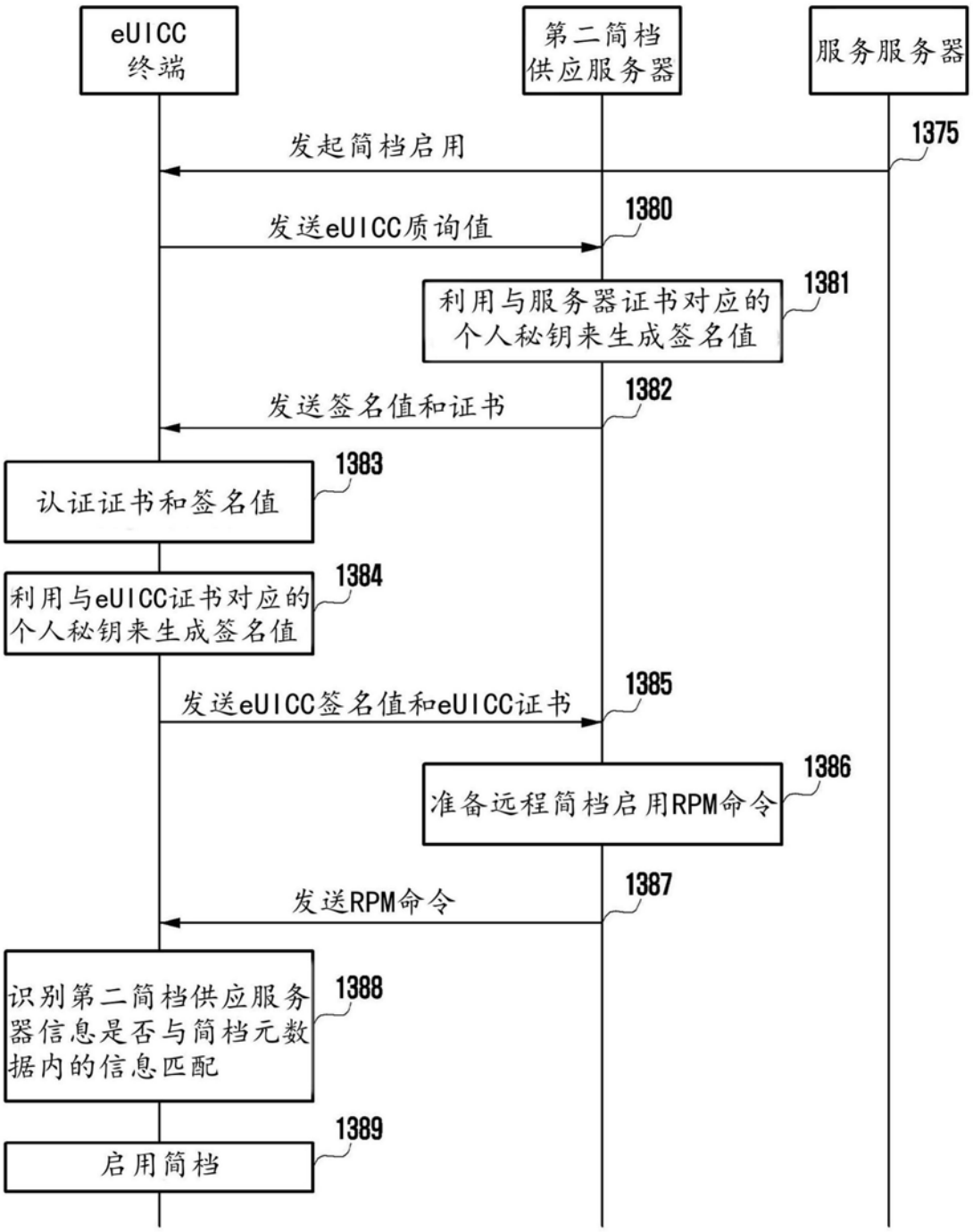

eUICC
终端
第二简档
供应服务器
服务服务器
1375
发起简档启用
1380
发送eUICC质询值
利用与服务器证书对应的
个人秘钥来生成签名值
1381
1382
发送签名值和证书
1383
认证证书和签名值
利用与eUICC证书对应的
个人秘钥来生成签名值
1384
1385
发送eUICC签名值和eUICC证书
准备远程简档启用RPM命令
1386
1387
发送RPM命令
识别第二简档供应服务
器信息是否与简档元数
据内的信息匹配
1388
1389
启用简档

图13b

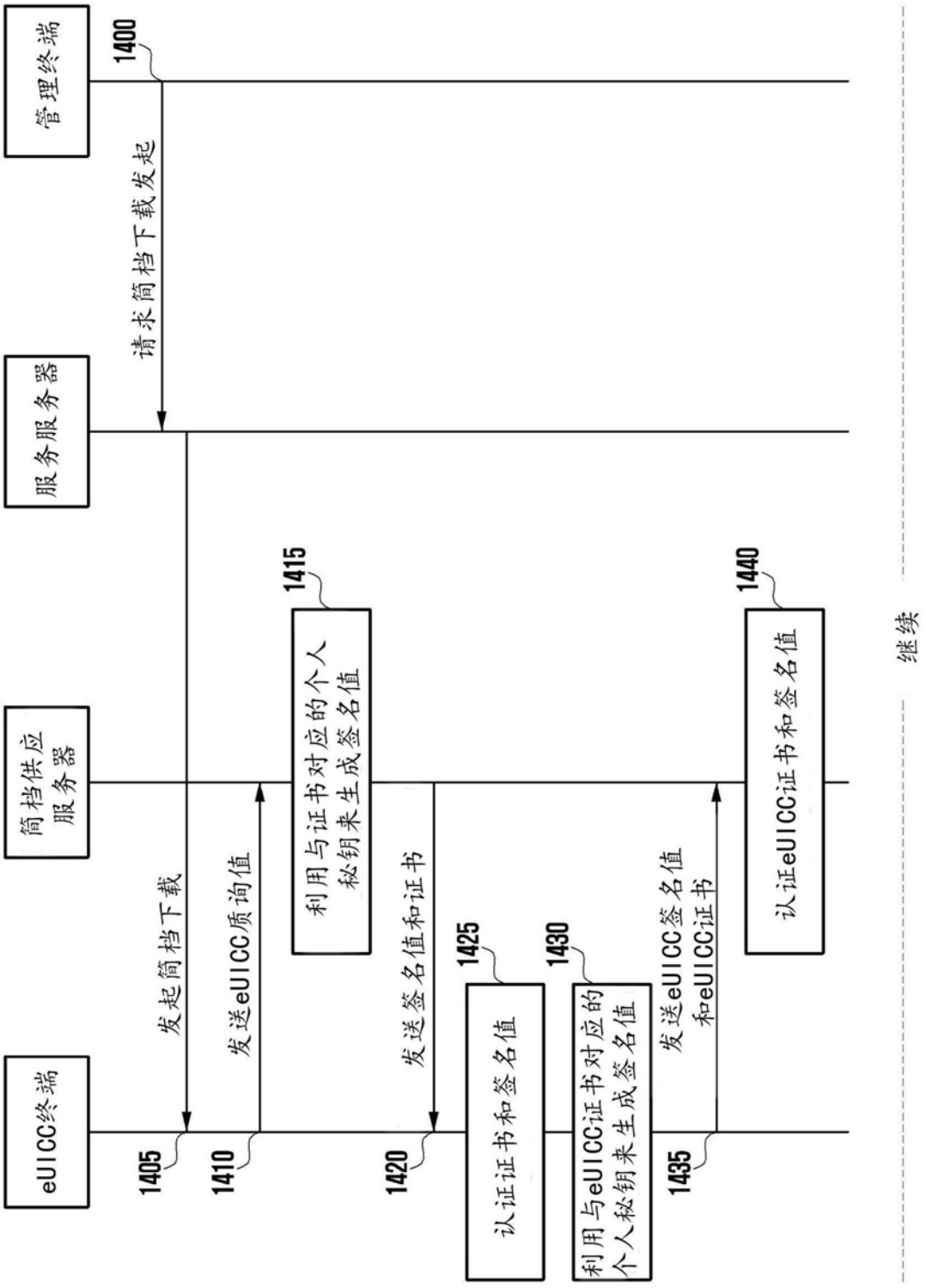

管理终端
1400
请求简档下载发起
服务服务器
简档供应服务器
1415
利用与证书对应的个人秘钥来生成签名值
1440
认证eUICC证书和签名值
继续
eUICC终端
发起简档下载
1405
发送eUICC质询值
1410
发送签名值和证书
1420
1425
认证证书和签名值
1430
利用与eUICC证书对应的个人秘钥来生成签名值
发送eUICC签名值和eUICC证书
1435

图14aa

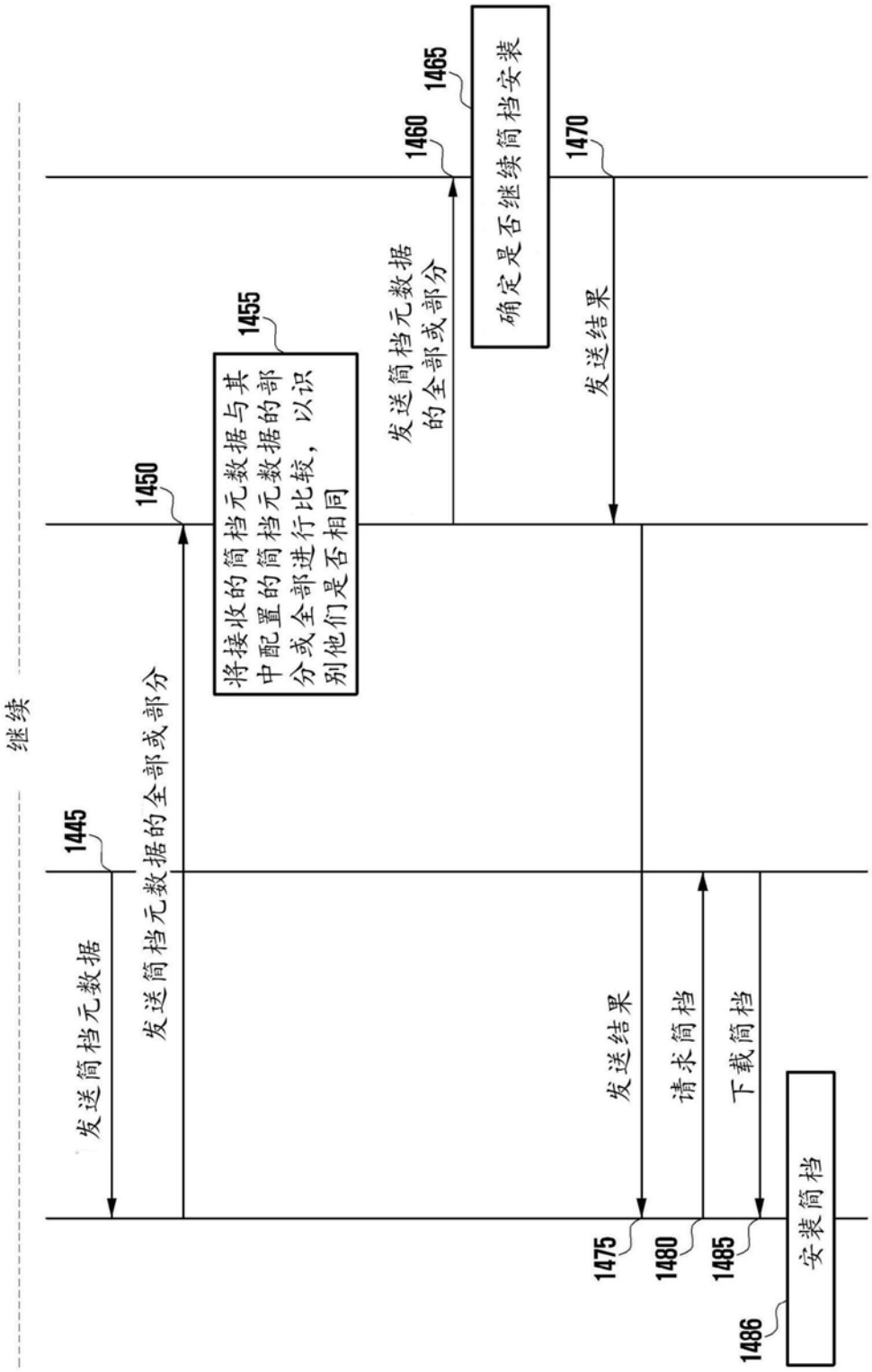

继续
1445
发送简档元数据
发送简档元数据的全部或部分
1450
将接收的简档元数据与其中配置的简档元数据的部分或全部进行比较，以识别他们是否相同
1455
发送简档元数据的全部或部分
1460
确定是否继续简档安装
1465
发送结果
1470
发送结果
1475
请求简档
1480
下载简档
1485
安装简档
1486

图14ab

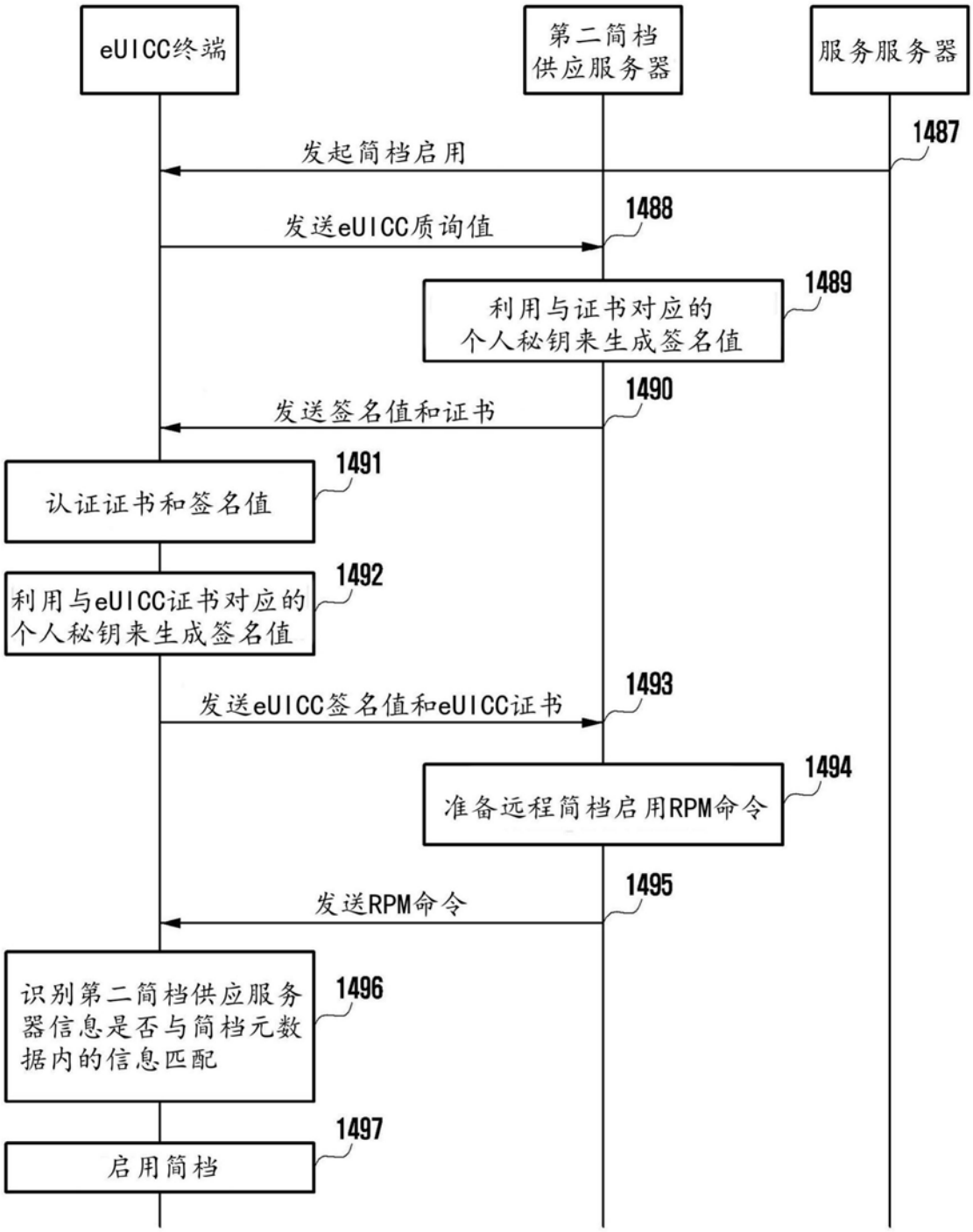

eUICC终端
第二简档供应服务器
服务服务器
1487
发起简档启用
1488
发送eUICC质询值
1489
利用与证书对应的个人秘钥来生成签名值
1490
发送签名值和证书
1491
认证证书和签名值
1492
利用与eUICC证书对应的个人秘钥来生成签名值
1493
发送eUICC签名值和eUICC证书
1494
准备远程简档启用RPM命令
1495
发送RPM命令
1496
识别第二简档供应服务器信息是否与简档元数据内的信息匹配
1497
启用简档

图14b

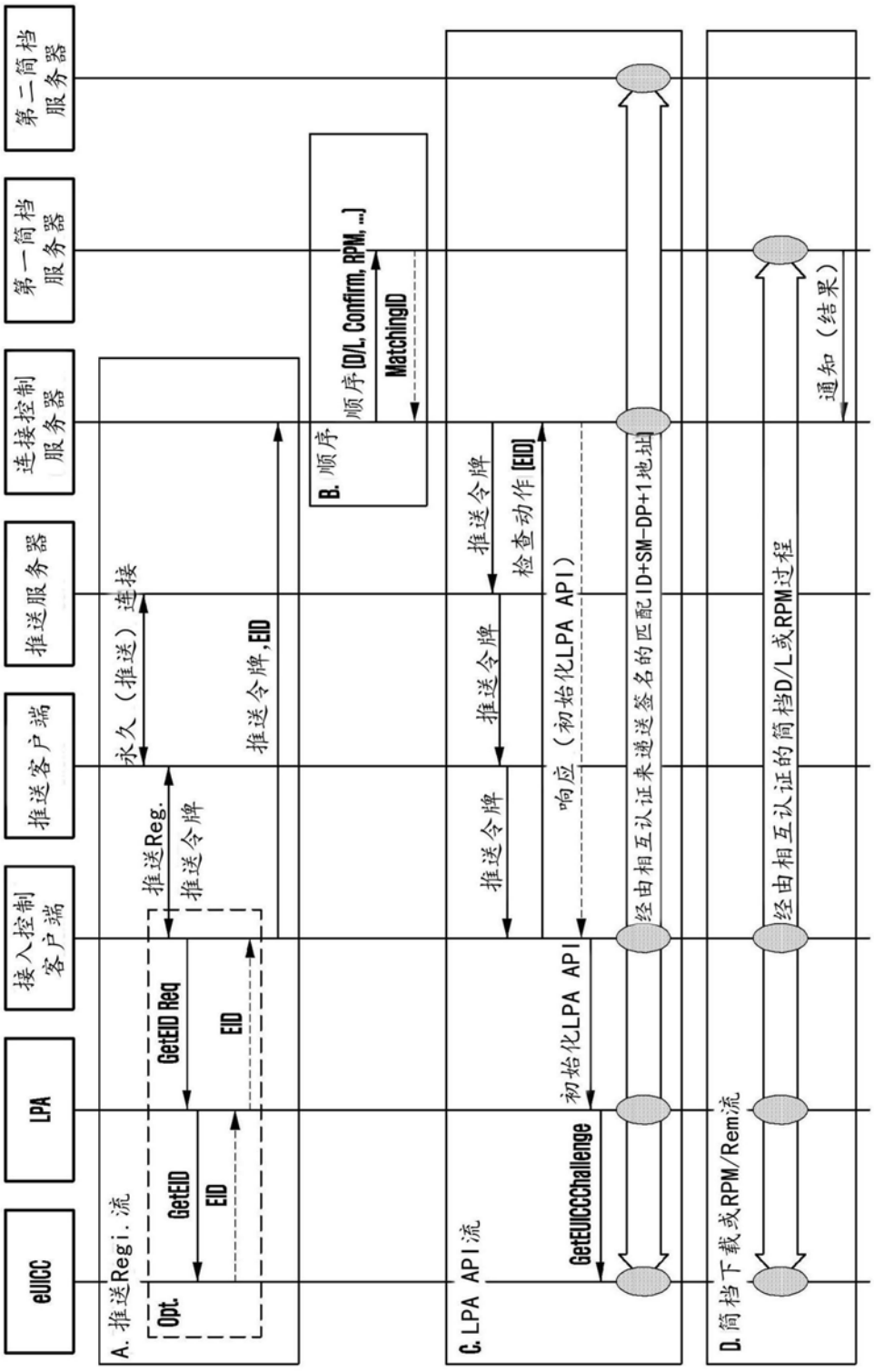

eUICC
LPA
接入控制客户端
推送客户端
推送服务器
连接控制服务器
第一简档服务器
第二简档服务器
A. 推送Regi.流
Opt.
GetEID
EID
GetEID Req
EID
推送Reg.
推送令牌
永久（推送）连接
推送令牌,EID
B. 顺序
顺序[D/L Confirm, RPM, ...]
MatchingID
C. LPA API流
初始化LPA API
GetEUICCChallenge
推送令牌
推送令牌
推送令牌
检查动作[EID]
响应（初始化LPA API）
经由相互认证来递送签名的匹配ID+SM-DP+1地址
D. 简档下载或RPM/Rem流
经由相互认证的简档D/L或RPM过程
通知（结果）

图15


1610
1620
1630
收发器
控制器
UICC

图16


1710
1720
1730
收发器
控制器
存储器

图17


1810
1820
1830
收发器
控制器
存储器

图18