(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107925868 B
(45)授权公告日 2019.09.27

(21)申请号 201680044510.6

(22)申请日 2016.04.12

(65)同一申请的已公布的文献号
申请公布号 CN 107925868 A

(43)申请公布日 2018.04.17

(85)PCT国际申请进入国家阶段日
2018.02.05

(86)PCT国际申请的申请数据
PCT/CN2016/079097 2016.04.12

(87)PCT国际申请的公布数据
WO2017/177383 ZH 2017.10.19

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 程紫尧 龙水平 衣强 高林毅

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04W 8/20(2006.01)
H04W 12/06(2006.01)

(56)对比文件
CN 101296136 A,2008.10.29,
CN 104703170 A,2015.06.10,
CN 104852911 A,2015.08.19,
US 2014237101 A1,2014.08.21,

审查员 刘宁宁

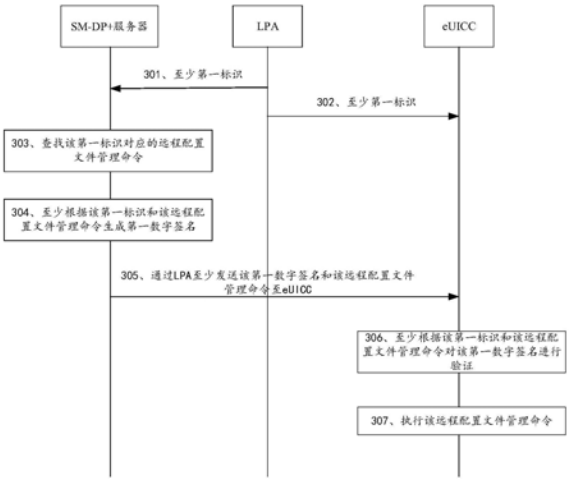
权利要求书6页 说明书19页 附图7页

(54)发明名称

一种远程管理方法及设备

(57)摘要

本发明实施例公开了一种远程管理方法及设备，其中方法包括：签约管理-数据准备SM-DP+服务器接收本地配置文件助手LPA发送的第一标识；所述SM-DP+服务器查找所述第一标识对应的远程配置文件管理命令；所述SM-DP+服务器至少根据所述第一标识和所述远程配置文件管理命令生成第一数字签名，并通过所述LPA至少发送所述第一数字签名和所述远程配置文件管理命令至嵌入式通用集成电路卡eUICC。可见，通过实施本发明实施例，SM-DP+服务器可至少发送第一数字签名和远程配置文件管理命令至eUICC，从而可使eUICC确定远程配置文件管理命令是否被非法设备篡改，并在确定远程配置文件管理命令未被非法设备篡改时才执行远程配置文件管理命令，从而提高了远程管理的安全性。



CN 107925868 B

1.一种远程管理方法,其特征在于,所述方法包括:

签约管理-数据准备SM-DP+服务器接收本地配置文件助手LPA发送的至少第一标识;

所述SM-DP+服务器查找所述第一标识对应的远程配置文件管理命令;

所述SM-DP+服务器至少根据所述第一标识和所述远程配置文件管理命令生成第一数字签名,并通过所述LPA至少发送所述第一数字签名和所述远程配置文件管理命令至嵌入式通用集成电路卡eUICC。

2.根据权利要求1所述的方法,其特征在于,所述签约管理-数据准备SM-DP+服务器接收本地配置文件助手LPA发送的第一标识之后,所述方法还包括:

所述SM-DP+服务器检查是否存储有与所述第一标识对应的事件;

若存储有与所述第一标识对应的事件,则当所述第一标识对应的事件为远程配置文件管理事件时,所述SM-DP+服务器不生成交互标识;

所述SM-DP+服务器查找所述第一标识对应的远程配置文件管理命令,包括:

当所述第一标识对应的事件为远程配置文件管理事件时,所述SM-DP+服务器查找所述第一标识对应的远程配置文件管理命令。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述SM-DP+服务器接收所述eUICC通过所述LPA至少发送的第二数字签名和所述eUICC的数字证书和eUICC制造商EUM的数字证书,所述第二数字签名是所述eUICC至少根据所述第一标识生成的;

所述SM-DP+服务器验证所述EUM的数字证书和所述eUICC的数字证书,并至少使用所述第一标识和所述eUICC的数字证书中的公钥对所述第二数字签名进行验证;

若对所述eUICC的数字证书、所述EUM的数字证书和所述第二数字签名均验证通过,则执行所述SM-DP+服务器查找所述第一标识对应的远程配置文件管理命令的步骤。

4.根据权利要求1～3任意一项所述的方法,其特征在于,所述SM-DP+服务器通过所述LPA至少发送所述第一数字签名和所述远程配置文件管理命令至嵌入式通用集成电路卡eUICC之后,所述方法还包括:

所述SM-DP+服务器接收到所述LPA发送的第一消息后,所述SM-DP+服务器向签约管理-发现服务SM-DS服务器发送第二消息,所述第二消息中至少包含所述SM-DP+服务器的地址、所述eUICC标识和所述第一标识,所述第二消息用于所述SM-DS服务器至少删除所述SM-DP+服务器发送的所述SM-DP+地址、所述eUICC标识和所述第一标识,所述第一消息至少包括所述第一标识和所述eUICC至少根据所述第一标识生成的数字签名。

5.一种远程管理方法,其特征在于,所述方法包括:

嵌入式通用集成电路卡eUICC接收本地配置文件助手LPA发送的至少第一标识;

所述eUICC接收所述LPA发送的至少第一数字签名和远程配置文件管理命令,所述第一数字签名为签约管理-数据准备SM-DP+服务器根据所述第一标识和所述远程配置文件管理命令生成的;

所述eUICC至少根据所述第一标识和所述远程配置文件管理命令对所述第一数字签名进行验证;

若对所述第一数字签名验证通过,则所述eUICC执行所述远程配置文件管理命令。

6.根据权利要求5所述的方法,其特征在于,所述嵌入式通用集成电路卡eUICC至少接

收本地配置文件助手LPA发送的第一标识之后,所述方法还包括:

所述eUICC至少根据所述第一标识生成第二数字签名;

所述eUICC通过所述LPA至少发送所述第二数字签名、所述eUICC的数字证书和eUICC制造商EUM的数字证书至所述SM-DP+服务器。

7.根据权利要求5所述的方法,其特征在于,所述eUICC对所述第一数字签名验证通过之后,所述eUICC执行所述远程配置文件管理命令之前,所述方法还包括:

若所述远程配置文件管理命令为目标命令,则所述eUICC发送第一消息至所述LPA,所述第一消息用于请求用户确认;

在接收到所述LPA返回的确认执行消息之后,所述eUICC执行所述远程配置文件管理命令。

8.根据权利要求5～7任意一项所述的方法,其特征在于,所述eUICC执行所述远程配置文件管理命令之后,所述方法还包括:

所述eUICC生成所述远程配置文件管理命令的远程配置文件管理结果,所述远程配置文件管理结果至少包括所述第一标识以及至少根据所述第一标识生成的第三数字签名;

所述eUICC发送至少包含所述第一标识和所述第三数字签名的所述远程配置文件管理结果至所述LPA。

9.一种远程管理方法,其特征在于,所述方法包括:

签约管理-发现服务SM-DS服务器接收签约管理-数据准备SM-DP+服务器发送的第一消息,所述第一消息至少包括嵌入式通用集成电路卡eUICC标识和第一标识;

所述SM-DS服务器对所述eUICC的身份认证通过后,所述SM-DS服务器生成令牌,所述令牌为至少根据所述第一标识、所述eUICC标识和所述SM-DS服务器的地址生成的数字签名;

所述SM-DS服务器发送第二消息至本地配置文件助手LPA,所述第二消息至少包括所述eUICC标识、所述第一标识、所述令牌、所述SM-DP+服务器的地址、所述SM-DS服务器的地址和所述SM-DS服务器的数字证书。

10.一种远程管理方法,其特征在于,所述方法包括:

签约管理-数据准备SM-DP+服务器接收本地配置文件助手LPA发送的第一消息,所述第一消息至少包括嵌入式通用集成电路卡eUICC标识、第一标识、令牌、SM-DS服务器的数字证书、所述SM-DS服务器的地址,所述令牌为所述SM-DS服务器至少根据所述第一标识、所述eUICC标识和所述SM-DS服务器的地址生成的数字签名;

所述SM-DP+服务器验证所述令牌;

若验证通过,则所述SM-DP+服务器检验所述SM-DS服务器的地址是否与所述第一标识对应的SM-DS服务器的地址相匹配,并且检验所述eUICC标识是否与所述第一标识对应的eUICC标识相匹配;

若所述SM-DS服务器的地址与所述第一标识对应的SM-DS服务器的地址相匹配,且所述eUICC标识与所述第一标识对应的eUICC标识相匹配,则所述SM-DP+服务器确定对所述eUICC的身份认证通过。

11.根据权利要求10所述的方法,其特征在于,所述第一消息还包括所述eUICC生成的随机数,所述SM-DP+服务器确定对所述eUICC的身份认证通过之后,所述方法还包括:

当所述第一标识对应的事件为远程配置文件管理事件时,所述SM-DP+服务器至少根据

所述随机数和所述第一标识对应的远程配置文件管理命令生成第一数字签名；

所述SM-DP+服务器通过所述LPA至少发送所述第一数字签名、所述远程配置文件管理命令和所述SM-DP+服务器的数字证书至所述eUICC。

12.根据权利要求10或11所述的方法，其特征在于，所述方法还包括：

所述SM-DP+服务器接收到所述LPA发送的第二消息后，所述SM-DP+服务器向签约管理-发现服务SM-DS服务器发送第三消息，所述第三消息中至少包含所述SM-DP+服务器的地址、所述eUICC标识和所述第一标识，所述第三消息用于所述SM-DS服务器至少删除所述SM-DP+服务器发送的所述SM-DP+服务器地址、所述eUICC标识和所述第一标识，所述第二消息至少包括结果代码以及至少根据所述结果代码生成的数字签名。

13.一种远程管理方法，其特征在于，所述方法包括：

嵌入式通用集成电路卡eUICC接收签约管理-数据准备SM-DP+服务器通过本地配置文件助手LPA发送的至少第一数字签名、远程配置文件管理命令和所述SM-DP+服务器的数字证书，所述第一数字签名为所述SM-DP+服务器至少根据随机数和所述远程配置文件管理命令生成，所述随机数为所述eUICC生成的；

所述eUICC验证所述SM-DP+服务器的数字证书，并至少使用所述随机数、所述SM-DP+服务器的数字证书中的公钥和所述远程配置文件管理命令对所述第一数字签名进行验证；

若对所述数字证书及第一数字签名验证通过，则执行所述远程配置文件管理命令。

14.根据权利要求13所述的方法，其特征在于，所述eUICC对所述数字证书及数字签名验证通过之后，所述eUICC执行所述远程配置文件管理命令之前，所述方法还包括：

若所述远程配置文件管理命令为目标命令，则所述eUICC发送第一消息至所述LPA，所述第一消息用于请求用户确认；

在接收到所述LPA返回的确认执行消息之后，所述eUICC执行所述远程配置文件管理命令。

15.根据权利要求13或14所述的方法，其特征在于，所述eUICC执行所述远程配置文件管理命令之后，所述方法还包括：

所述eUICC生成所述远程配置文件管理命令的远程配置文件管理结果，所述远程配置文件管理结果至少包括结果代码以及至少根据所述结果代码生成的数字签名；

所述eUICC发送至少包含所述结果代码以及至少根据所述结果代码生成的数字签名的所述远程配置文件管理结果至所述LPA。

16.一种签约管理-数据准备SM-DP+服务器，其特征在于，所述SM-DP+服务器包括：处理单元和通信单元，

所述处理单元，用于通过所述通信单元接收本地配置文件助手LPA发送的至少第一标识；

所述处理单元，还用于查找所述第一标识对应的远程配置文件管理命令；

所述处理单元，还用于根据至少所述第一标识和所述远程配置文件管理命令生成第一数字签名，并通过所述通信单元通过所述LPA至少发送所述第一数字签名和所述远程配置文件管理命令至嵌入式通用集成电路卡eUICC。

17.根据权利要求16所述的SM-DP+服务器，其特征在于，

所述处理单元，还用于在通过所述通信单元接收本地配置文件助手LPA发送的第一标

识之后，检查是否存储有与所述第一标识对应的事件；若存储有与所述第一标识对应的事件，则当所述第一标识对应的事件为远程配置文件管理事件时，所述处理单元不生成交互标识；

所述处理单元查找所述第一标识对应的远程配置文件管理命令的方式具体为：

当所述第一标识对应的事件为远程配置文件管理事件时，查找所述第一标识对应的远程配置文件管理命令。

18.根据权利要求16所述的SM-DP+服务器，其特征在于，

所述处理单元，还用于通过所述通信单元接收所述eUICC通过所述LPA至少发送的第二数字签名和所述eUICC的数字证书和eUICC制造商EUM的数字证书，所述第二数字签名是所述eUICC至少根据所述第一标识生成的；

所述处理单元，还用于验证所述EUM的数字证书和所述eUICC的数字证书，并至少使用所述第一标识和所述eUICC的数字证书中的公钥对所述第二数字签名进行验证；若对所述eUICC的数字证书、所述EUM的数字证书和所述第二数字签名均验证通过，则触发所述处理单元查找所述第一标识对应的远程配置文件管理命令。

19.根据权利要求16～18任意一项所述的SM-DP+服务器，其特征在于，

所述处理单元，还用于通过所述通信单元接收到所述LPA发送的第一消息后，通过所述通信单元向签约管理-发现服务SM-DS服务器发送第二消息，所述第二消息中至少包含所述SM-DP+服务器的地址、所述eUICC标识和所述第一标识，所述第二消息用于所述SM-DS服务器至少删除所述SM-DP+服务器发送的所述SM-DP+地址、所述eUICC标识和所述第一标识，所述第一消息至少包括所述第一标识和所述eUICC至少根据所述第一标识生成的数字签名。

20.一种嵌入式通用集成电路卡eUICC，其特征在于，所述eUICC包括：处理单元和通信单元，

所述处理单元，用于通过所述通信单元接收本地配置文件助手LPA发送的至少第一标识；

所述处理单元，还用于通过所述通信单元接收所述LPA发送的至少第一数字签名和远程配置文件管理命令，所述第一数字签名为签约管理-数据准备SM-DP+服务器根据所述第一标识和所述远程配置文件管理命令生成的；

所述处理单元，还用于至少根据所述第一标识和所述远程配置文件管理命令对所述第一数字签名进行验证；

所述处理单元，还用于当对所述第一数字签名验证通过时，执行所述远程配置文件管理命令。

21.根据权利要求20所述的eUICC，其特征在于，

所述处理单元，还用于在通过所述通信单元接收LPA发送的第一标识之后，至少根据所述第一标识生成第二数字签名；

所述处理单元，还用于通过所述通信单元通过所述LPA至少发送所述第二数字签名、所述eUICC的数字证书和eUICC制造商EUM的数字证书至所述SM-DP+服务器。

22.根据权利要求20所述的eUICC，其特征在于，

所述处理单元，还用于在对所述第一数字签名验证通过之后，在所述远程配置文件管理命令为目标命令时，通过所述通信单元发送第一消息至所述LPA，所述第一消息用于请求

用户确认；

所述处理单元执行所述远程配置文件管理命令的方式具体为：

在通过所述通信单元接收到所述LPA返回的确认执行消息之后，执行所述远程配置文件管理命令。

23.根据权利要求20～22任意一项所述的eUICC，其特征在于，

所述处理单元，还用于生成所述远程配置文件管理命令的远程配置文件管理结果，所述远程配置文件管理结果至少包括所述第一标识以及至少根据所述第一标识生成的第三数字签名；

所述处理单元，还用于通过所述通信单元发送至少包含所述第一标识和所述第三数字签名的所述远程配置文件管理结果至所述LPA。

24.一种签约管理-发现服务SM-DS服务器，其特征在于，所述SM-DS服务器包括：处理单元和通信单元，

所述处理单元，用于通过所述通信单元接收签约管理-数据准备SM-DP+服务器发送的第一消息，所述第一消息至少包括嵌入式通用集成电路卡eUICC标识和第一标识；

所述处理单元，还用于对所述eUICC的身份认证通过后，生成令牌，所述令牌为至少根据所述第一标识、所述eUICC标识和所述SM-DS服务器的地址生成的数字签名；

所述处理单元，还用于通过所述通信单元发送第二消息至本地配置文件助手LPA，所述第二消息至少包括所述eUICC标识、所述第一标识、所述令牌、所述SM-DP+服务器的地址、所述SM-DS服务器的地址和所述SM-DS服务器的数字证书。

25.一种签约管理-数据准备SM-DP+服务器，其特征在于，所述SM-DP+服务器包括：处理单元和通信单元，

所述处理单元，用于通过所述通信单元接收本地配置文件助手LPA发送的第一消息，所述第一消息至少包括嵌入式通用集成电路卡eUICC标识、第一标识、令牌、SM-DS服务器的数字证书、所述SM-DS服务器的地址，所述令牌为所述SM-DS服务器至少根据所述第一标识、所述eUICC标识和所述SM-DS服务器的地址生成的数字签名；

所述处理单元，还用于验证所述令牌；

所述处理单元，还用于在验证通过时，检验所述SM-DS服务器的地址是否与所述第一标识对应的SM-DS服务器的地址相匹配，并且检验所述eUICC标识是否与所述第一标识对应的eUICC标识相匹配；

所述处理单元，还用于在检验所述SM-DS服务器的地址与所述第一标识对应的SM-DS服务器的地址相匹配，且所述eUICC标识与所述第一标识对应的eUICC标识相匹配时，确定对所述eUICC的身份认证通过。

26.根据权利要求25所述的SM-DP+服务器，其特征在于，所述第一消息还包括所述eUICC生成的随机数，

所述处理单元，还用于在确定对所述eUICC的身份认证通过之后，当所述第一标识对应的事件为远程配置文件管理事件时，至少根据所述随机数和所述第一标识对应的远程配置文件管理命令生成第一数字签名；

所述SM-DP+服务器通过所述LPA至少发送所述第一数字签名、所述远程配置文件管理命令和所述SM-DP+服务器的数字证书至所述eUICC。

27.根据权利要求25或26所述的SM-DP+服务器，其特征在于，

所述处理单元，还用于在通过所述通信单元接收到所述LPA发送的第二消息后，通过所述通信单元向签约管理-发现服务SM-DS服务器发送第三消息，所述第三消息中至少包含所述SM-DP+服务器的地址、所述eUICC标识和所述第一标识，所述第三消息用于所述SM-DS服务器至少删除所述SM-DP+服务器发送的所述SM-DP+服务器地址、所述eUICC标识和所述第一标识，所述第二消息至少包括结果代码以及至少根据所述结果代码生成的数字签名。

28.一种嵌入式通用集成电路卡eUICC，其特征在于，所述eUICC包括：处理单元和通信单元，

所述处理单元，用于通过所述通信单元接收签约管理-数据准备SM-DP+服务器通过本地配置文件助手LPA发送的至少第一数字签名、远程配置文件管理命令和所述SM-DP+服务器的数字证书，所述第一数字签名为所述SM-DP+服务器至少根据随机数和所述远程配置文件管理命令生成，所述随机数为所述eUICC生成的；

所述处理单元，还用于验证所述SM-DP+服务器的数字证书，并至少使用所述随机数、所述SM-DP+服务器的数字证书中的公钥和所述远程配置文件管理命令对所述第一数字签名进行验证；

所述处理单元，还用于当对所述数字证书及第一数字签名验证通过时，执行所述远程配置文件管理命令。

29.根据权利要求28所述的eUICC，其特征在于，

所述处理单元，还用于所述数字证书及数字签名验证通过之后，当所述远程配置文件管理命令为目标命令时，通过所述通信单元发送第一消息至所述LPA，所述第一消息用于请求用户确认；

所述处理单元执行所述远程配置文件管理命令的方式具体为：

在通过所述通信单元接收到所述LPA返回的确认执行消息之后，所述eUICC执行所述远程配置文件管理命令。

30.根据权利要求28或29所述的eUICC，其特征在于，

所述处理单元，还用于在执行所述远程配置文件管理命令之后，生成所述远程配置文件管理命令的远程配置文件管理结果，所述远程配置文件管理结果至少包括结果代码以及至少根据所述结果代码生成的数字签名；

所述处理单元，还用于通过所述通信单元发送至少包含所述结果代码以及至少根据所述结果代码生成的数字签名的所述远程配置文件管理结果至所述LPA。

31.一种远程管理系统，其特征在于，包括如权利要求16至19中任一项所述的签约管理-数据准备SM-DP+服务器和如权利要求20至23中任一项所述的嵌入式通用集成电路卡eUICC，或者

所述远程管理系统包括如权利要求24所述的SM-DS服务器、如权利要求25至27中任一项所述的SM-DP+服务器和如权利要求28至30中任一项所述的eUICC。

一种远程管理方法及设备

技术领域

[0001] 本发明实施例通信技术领域，具体涉及一种远程管理方法及设备。

背景技术

[0002] 嵌入式通用集成电路卡(embedded Universal Integrated Circuit Card，eUICC)，也可称为嵌入式用户身份识别卡(embedded Subscriber Identity Module，eSIM)，eUICC可以通过插拔式或焊接式等放入到用户终端(如移动手机、平板电脑等)中。

[0003] 在实际应用中，eUICC安装通信运营商所提供的配置文件(profile)之后，就可接入通信运营商网络(如2G/3G/4G网络等)。通常通信运营商也会对eUICC中的配置文件进行远程管理，例如，激活eUICC中的配置文件、去激活eUICC中的配置文件、删除eUICC中的配置文件或审查eUICC的状态。

[0004] 图1是一种现有的远程管理的流程示意图，如图1所示，通常通信运营商对eUICC中的配置文件进行远程管理的流程可包括以下步骤：

[0005] 101、在通信运营商需要对eUICC中的配置文件进行远程管理时，通信运营商至少发送用于对该配置文件进行远程管理的远程配置文件管理命令(Remote profile Management Command)、eUICC标识(eUICC-ID，EID)、以及与该配置文件对应的签约管理-发现服务(Subscription Manager-Discovery Service，SM-DS)服务器的地址至签约管理-数据准备(Subscription Manager-Data Preparation，SM-DP+)服务器。

[0006] 102、SM-DP+服务器接收远程配置文件管理命令和SM-DS服务器的地址之后，生成远程配置文件管理命令对应的事件标识(该事件标识用于标识远程配置文件管理事件，该事件标识也可称为通知标识或告知标识)，并至少建立和储存该事件标识、远程配置文件管理命令、eUICC标识、SM-DP+服务器地址以及SM-DS服务器的地址之间的对应关系。

[0007] 103、SM-DP+服务器根据该SM-DS服务器的地址与该SM-DS服务器建立连接。

[0008] 104、SM-DP+服务器与该SM-DS服务器建立连接之后，至少将该事件标识、SM-DP+服务器的地址和eUICC标识注册在该SM-DS服务器中。

[0009] 105、用户终端中的本地配置文件助手(Local Profile Assistant，LPA)利用eUICC提供的该SM-DS服务器的地址与该SM-DS服务器建立连接。

[0010] 106、在LPA与SM-DS服务器建立连接之后，SM-DS服务器至少将事件标识、eUICC标识和SM-DP+服务器的地址发送给LPA。

[0011] 107、LPA根据SM-DP+服务器的地址与SM-DP+服务器建立连接。

[0012] 108、在LPA与SM-DP+服务器建立连接之后，LPA至少将事件标识发送至SM-DP+服务器。

[0013] 109、SM-DP+服务器接收事件标识之后，SM-DP+服务器将存储的与该事件标识对应的远程配置文件管理命令直接通过LPA发送至eUICC。

[0014] 110、eUICC接收该远程管理命令后，执行该远程配置文件管理命令。

[0015] 然而在实践中发现，SM-DP+服务器发送远程配置文件管理命令至eUICC的过程中，

则远程配置文件管理命令可被非法设备篡改，使eUICC执行被篡改的远程配置文件管理命令(如执行非法激活配置文件、非法去激活配置文件或非法删除配置文件等操作)。因此，上述远程管理的安全性不高。

发明内容

[0016] 本发明实施例公开了一种远程管理方法及设备，有利于提高远程管理的安全性。

[0017] 第一方面，本发明实施例公开了一种远程管理方法，该方法包括：

[0018] 签约管理-数据准备SM-DP+服务器接收本地配置文件助手LPA发送的第一标识；SM-DP+服务器查找第一标识对应的远程配置文件管理命令；SM-DP+服务器至少根据第一标识和远程配置文件管理命令生成第一数字签名，并通过LPA发送至少第一数字签名和远程配置文件管理命令至嵌入式通用集成电路卡eUICC。这样SM-DP+服务器至少发送第一数字签名和远程配置文件管理命令至eUICC之后，eUICC可至少根据第一数字签名和LPA发送给eUICC的该第一标识和SM-DP+的数字证书中的公钥对该第一数字签名进行验证，以确定远程配置文件管理命令是否被非法设备篡改，并在确定远程配置文件管理命令未被非法设备篡改时才执行远程配置文件管理命令，从而提高了远程管理的安全性。

[0019] 在一种可能的设计中，签约管理-数据准备SM-DP+服务器接收本地配置文件助手LPA发送的第一标识之后，还可检查是否存储有与第一标识对应的事件；若存储有与第一标识对应的事件，则当第一标识对应的事件为远程配置文件管理事件时，SM-DP+服务器不生成交互标识；SM-DP+服务器查找第一标识对应的远程配置文件管理命令，包括：当第一标识对应的事件为远程配置文件管理事件时，SM-DP+服务器查找第一标识对应的远程配置文件管理命令。交互标识即用于对交互进行标识的信息，通过在第一标识对应的事件为远程配置文件管理事件时，不生成交互标识，从而可使用已有的第一标识来替代交互标识，有利于减少参数的数量。

[0020] 在一种可能的设计中，SM-DP+服务器还可接收eUICC通过LPA至少发送的第二数字签名和eUICC的数字证书和eUICC制造商EUM的数字证书，该第二数字签名是eUICC至少根据第一标识生成的；SM-DP+服务器验证EUM的数字证书及eUICC的数字证书，并至少使用第一标识和eUICC的数字证书中的公钥对第二数字签名进行验证；若对EUM的数字证书、eUICC的数字证书和第二数字签名均验证通过，则执行SM-DP+服务器查找第一标识对应的远程配置文件管理命令的步骤。

[0021] 在一种可能的设计中，SM-DP+服务器通过LPA发送至少第一数字签名和远程配置文件管理命令至嵌入式通用集成电路卡eUICC之后，还可在接收到LPA发送的第一消息后，向签约管理-发现服务SM-DS服务器发送第二消息，该第二消息中至少包含SM-DP+服务器的地址、eUICC标识和第一标识，第二消息用于SM-DS服务器至少删除SM-DP+服务器发送的SM-DP+地址、eUICC标识和第一标识，该第一消息至少包括第一标识和eUICC根据第一标识生成的数字签名。这样在eUICC执行完远程配置文件管理命令之后，SM-DS服务器能够及时地删除其存储的该远程配置文件管理命令的信息(至少包括SM-DP+地址、eUICC标识和第一标识)，从而避免重复执行已完成的远程配置文件命令，并节省其存储空间。

[0022] 第二方面，本发明实施例提供了一种远程管理方法，该方法包括：嵌入式通用集成电路卡eUICC接收本地配置文件助手LPA发送的至少第一标识；eUICC接收LPA发送的至少第

一数字签名和远程配置文件管理命令，该第一数字签名为签约管理-数据准备SM-DP+服务器至少根据第一标识和远程配置文件管理命令生成的；eUICC至少根据第一标识和远程配置文件管理命令对第一数字签名进行验证；若对第一数字签名验证通过，则eUICC执行远程配置文件管理命令。这样若验证通过(说明该远程配置文件管理命令未被非法设备篡改)，eUICC才执行该远程配置文件管理命令。可见，提高了远程管理的安全性。

[0023] 在一种可能的设计中，嵌入式通用集成电路卡eUICC接收本地配置文件助手LPA发送的第一标识之后，还可至少根据第一标识生成第二数字签名；eUICC通过LPA至少发送第二数字签名、eUICC的数字证书和eUICC制造商EUM的数字证书至SM-DP+服务器。在实际应用中eUICC是根据交互标识来生成第二数字签名，这样用第一标识来替代交互标识的作用，减少了参数的数量，使参数变得更简洁化。

[0024] 在一种可能的设计中，eUICC对第一数字签名验证通过之后，在执行远程配置文件管理命令之前，若远程配置文件管理命令为目标命令，则eUICC还可发送第一消息至LPA，该第一消息用于请求用户确认；在接收到LPA返回的确认执行消息之后，eUICC执行远程配置文件管理命令。其中，该目标命令可包括但不限于激活配置文件的命令、去激活配置文件的命令或删除配置文件的命令。这样当需要对配置文件进行激活、去激活或删除时，向用户进行确认，能够有效地提高eUICC中配置文件信息的安全性，且能够使用户掌握远程设备对配置文件的操作情况。另外，对配置文件进行审查(Audit)时，无需用户确认。

[0025] 在一种可能的设计中，eUICC执行远程配置文件管理命令之后，还可生成远程配置文件管理命令的远程配置文件管理结果，该远程配置文件管理结果至少包括第一标识以及根据至少第一标识生成的第三数字签名；eUICC发送至少包含第一标识和第三数字签名的远程配置文件管理结果至LPA。这样在eUICC执行完远程配置文件管理命令之后，向LPA反馈远程配置文件管理结果，可使LPA告知SM-DP+服务器，以便SM-DP+服务器能够及时通知SM-DS服务器及时地删除其存储的该远程配置文件管理命令的信息(至少包括SM-DP+服务器地址、eUICC标识和第一标识)，从而避免重复执行已完成的远程配置文件命令，并节省SM-DS服务器的存储空间。

[0026] 第三方面，本发明实施例提供了一种远程管理方法，该方法包括：签约管理-发现服务SM-DS服务器接收签约管理-数据准备SM-DP+服务器发送的第一消息，该第一消息至少包括嵌入式通用集成电路卡eUICC标识和第一标识；SM-DS服务器对eUICC的身份认证通过后，SM-DS服务器生成令牌，该令牌为至少根据该第一标识、eUICC标识和SM-DS服务器的地址生成的数字签名；SM-DS服务器发送第二消息至本地配置文件助手LPA，该第二消息至少包括eUICC标识、第一标识、该令牌、SM-DP+服务器的地址、SM-DS服务器的地址和SM-DS服务器的数字证书。这样有利于简化SM-DP+服务器对eUICC进行身份验证过程中的交互流程，使整个操作流程更为精简。

[0027] 第四方面，本发明实施例提供了一种远程管理方法，该方法包括：签约管理-数据准备SM-DP+服务器接收本地配置文件助手LPA发送的第一消息，该第一消息至少包括嵌入式通用集成电路卡eUICC标识、第一标识、令牌、SM-DS服务器的数字证书、SM-DS服务器的地址，该令牌为SM-DS服务器至少该第一标识、根据eUICC标识和SM-DS服务器的地址生成的数字签名；SM-DP+服务器验证该令牌；若验证通过，则SM-DP+服务器检验SM-DS服务器的地址是否与第一标识对应的SM-DS服务器的地址相匹配，并且检验eUICC标识是否与第一标识对

应的eUICC标识相匹配;若SM-DS服务器的地址与第一标识对应的SM-DS服务器的地址相匹配,且eUICC标识与第一标识对应的eUICC标识相匹配,则SM-DP+服务器确定对eUICC的身份认证通过。这样有利于简化SM-DP+服务器对eUICC进行身份验证过程中的交互流程,使整个操作流程更为精简。

[0028] 在一种可能的设计中,第一消息还包括eUICC生成的随机数,SM-DP+服务器确定对eUICC的身份认证通过之后,当第一标识对应的事件为远程配置文件管理事件时,还可至少根据随机数和第一标识对应的远程配置文件管理命令生成第一数字签名;SM-DP+服务器通过LPA至少发送第一数字签名、远程配置文件管理命令和SM-DP+服务器的数字证书至eUICC。SM-DP+服务器通过至少根据远程配置文件管理命令和eUICC生成的随机数生成第一数字签名,eUICC只需对第一数字签名验证成功,就能确定对SM-DP+服务器的身份认证通过,且远程配置文件管理命令并未被非法设备篡改,从而简化了操作流程。且通过在确定远程配置文件管理命令并未被非法设备篡改之后,eUICC才执行远程配置文件管理命令也提高了远程配置文件管理的安全性。

[0029] 在一种可能的设计中,SM-DP+服务器接收到LPA发送的第二消息后,还可向签约管理-发现服务SM-DS服务器发送第三消息,该第三消息中至少包含SM-DP+服务器的地址、eUICC标识和第一标识,该第三消息用于SM-DS服务器至少删除SM-DP+服务器发送的SM-DP+服务器地址、eUICC标识和第一标识,该第二消息至少包括结果代码以及至少根据所述结果代码生成的数字签名。这样在eUICC执行完远程配置文件管理命令之后,SM-DS服务器能够及时地删除其存储的该远程配置文件管理命令的信息(至少包括SM-DP+地址、eUICC标识和第一标识),从而免重复执行已完成的远程配置文件命令,并节省其存储空间。

[0030] 第五方面,本发明实施例提供了一种远程管理方法,该方法包括:嵌入式通用集成电路卡eUICC接收签约管理-数据准备SM-DP+服务器通过本地配置文件助手LPA发送的至少包括第一数字签名、远程配置文件管理命令和SM-DP+服务器的数字证书的消息,该第一数字签名为SM-DP+服务器至少根据随机数和远程配置文件管理命令生成,该随机数为eUICC生成的;eUICC验证SM-DP+服务器的数字证书,并至少使用随机数、SM-DP+服务器的数字证书中的公钥和远程配置文件管理命令对第一数字签名进行验证;若对数字证书及第一数字签名验证通过,则执行远程配置文件管理命令。这样eUICC只需对第一数字签名验证成功,就能确定对SM-DP+服务器的身份验证通过,且远程配置文件管理命令并未被非法设备篡改,从而简化了操作流程。且通过在确定远程配置文件管理命令并未被非法设备篡改之后,eUICC才执行远程配置文件管理命令也提高了远程配置文件管理的安全性。

[0031] 在一种可能的设计中,eUICC对数字证书及数字签名验证通过之后,eUICC执行远程配置文件管理命令之前,若远程配置文件管理命令为目标命令,则eUICC还可发送第一消息至LPA,该第一消息用于请求用户确认;在接收到LPA返回的确认执行消息之后,eUICC执行远程配置文件管理命令。其中,该目标命令可包括但不限于激活配置文件的命令、去激活配置文件的命令或删除配置文件的命令。这样当需要对配置文件进行激活、去激活或删除时,向用户进行确认,能够有效地提高eUICC中配置文件信息的安全性,且能够使用户掌握远程设备对配置文件的操作情况。另外,对配置文件进行审查(Audit)时,无需用户确认。

[0032] 在一种可能的设计中,eUICC执行远程配置文件管理命令之后,还可生成远程配置文件管理命令的远程配置文件管理结果,该远程配置文件管理结果至少包括结果代码以及

至少根据该结果代码生成的数字签名;eUICC发送至少包含该结果代码以及至少根据该结果代码生成的数字签名的远程配置文件管理结果至LPA。这样在eUICC执行完远程配置文件管理命令之后,向LPA反馈远程配置文件管理结果,可使LPA告知SM-DP+服务器,以便SM-DP+服务器能够及时通知SM-DS服务器及时地删除其存储的该远程配置文件管理命令的信息(至少包括SM-DP+服务器地址、eUICC标识和第一标识),从而免重复执行已完成的远程配置文件命令,并节省SM-DS服务器的存储空间。

[0033] 第六方面,本发明实施例提供了一种签约管理-数据准备SM-DP+服务器,该SM-DP+服务器具有实现上述第一方面和第二方面设计中SM-DP+服务器行为的功能。该功能可以通过硬件实现,也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。该模块可以是软件和/或硬件。

[0034] 在一种可能的设计中,SM-DP+服务器的结构中包括处理器和收发器,该处理器被配置为支持SM-DP+服务器执行上述方法中相应的功能。该收发器用于支持SM-DP+服务器与其他网元之间的通信。SM-DP+服务器还可以包括存储器,该存储器用于与处理器耦合,其保存SM-DP+服务器必要的程序指令和数据。

[0035] 第七方面,本发明实施例提供了一种嵌入式通用集成电路卡eUICC,该eUICC具有实现上述第一方面和第二方面设计中eUICC行为的功能。该功能可以通过硬件实现,也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。该模块可以是软件和/或硬件。

[0036] 在一种可能的设计中,eUICC的结构中包括处理器和收发器,该处理器被配置为支持eUICC执行上述方法中相应的功能。该收发器用于支持eUICC与其他网元之间的通信。eUICC还可以包括存储器,该存储器用于与处理器耦合,其保存eUICC必要的程序指令和数据。

[0037] 第八方面,本发明实施例提供了一种签约管理-发现服务SM-DS服务器,该SM-DS服务器具有实现上述第三方面、第四方面和第五方面设计中SM-DS服务器行为的功能。该功能可以通过硬件实现,也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。该模块可以是软件和/或硬件。

[0038] 在一种可能的设计中,SM-DS服务器的结构中包括处理器和收发器,该处理器被配置为支持SM-DS服务器执行上述方法中相应的功能。该收发器用于支持SM-DS服务器与其他网元之间的通信。SM-DS服务器还可以包括存储器,该存储器用于与处理器耦合,其保存SM-DS服务器必要的程序指令和数据。

[0039] 第九方面,本发明实施例提供了一种签约管理-数据准备SM-DP+服务器,该SM-DP+服务器具有实现上述第三方面、第四方面和第五方面设计中SM-DP+服务器行为的功能。该功能可以通过硬件实现,也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。该模块可以是软件和/或硬件。

[0040] 在一种可能的设计中,SM-DP+服务器的结构中包括处理器和收发器,该处理器被配置为支持SM-DP+服务器执行上述方法中相应的功能。该收发器用于支持SM-DP+服务器与其他网元之间的通信。SM-DP+服务器还可以包括存储器,该存储器用于与处理器耦合,其保存SM-DP+服务器必要的程序指令和数据。

[0041] 第十方面,本发明实施例提供了一种嵌入式通用集成电路卡eUICC,该eUICC具有

实现上述第四方面和第五方面设计中eUICC行为的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。该模块可以是软件和/或硬件。

[0042] 在一种可能的设计中，eUICC的结构中包括处理器和收发器，该处理器被配置为支持eUICC执行上述方法中相应的功能。该收发器用于支持eUICC与其他网元之间的通信。eUICC还可以包括存储器，该存储器用于与处理器耦合，其保存eUICC必要的程序指令和数据。

[0043] 第十一方面，本发明实施例提供了一种计算机存储介质，用于储存为上述第六方面中SM-DP+服务器所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

[0044] 第十二方面，本发明实施例提供了一种计算机存储介质，用于储存为上述第七方面中eUICC所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

[0045] 第十三方面，本发明实施例提供了一种计算机存储介质，用于储存为上述第八方面中SM-DS服务器所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

[0046] 第十四方面，本发明实施例提供了一种计算机存储介质，用于储存为上述第九方面中SM-DP+服务器所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

[0047] 第十五方面，本发明实施例提供了一种计算机存储介质，用于储存为上述第十方面中eUICC所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

[0048] 相较于现有技术，本发明实施例中，SM-DP+服务器接收LPA发送的第一标识之后，将找到该第一标识对应的远程配置文件管理命令；SM-DP+服务器至少根据远程配置文件管理命令以及该第一标识生成第一数字签名，并通过LPA发送至少该第一数字签名和该远程配置文件管理命令至eUICC。从而eUICC在接收该第一数字签名和该远程配置文件管理命令之后，可至少根据LPA发送给eUICC的该第一标识和SM-DP+的数字证书中的公钥对该第一数字签名进行验证。若验证通过(说明该远程配置文件管理命令未被非法设备篡改)，eUICC才执行该远程配置文件管理命令。可见，通过本发明实施例，eUICC可确定远程配置文件管理命令是否被非法设备篡改，并在确定远程配置文件管理命令未被非法设备篡改时才执行远程配置文件管理命令，从而提高了远程管理的安全性。

[0049] 相较于现有技术，本发明实施例中，SM-DS服务器可至少根据eUICC标识和SM-DS服务器的地址生成令牌，并至少发送令牌至LPA；这样LPA就可发送该令牌至SM-DP+服务器；SM-DP+服务器接收LPA发送的该令牌之后，对令牌进行验证。在验证成功之后，若SM-DP+服务器验证SM-DS服务器的地址与第一标识对应的SM-DS服务器的地址相匹配，且eUICC标识与第一标识对应的eUICC标识相匹配，则SM-DP+服务器确定对eUICC的身份认证通过。可见，通过实施本发明实施例，简化了SM-DP+服务器对eUICC进行身份验证过程中的交互流程，使整个操作流程更为精简。

附图说明

[0050] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0051] 图1是本发明实施例公开的现有的远程管理的流程示意图；

[0052] 图2是本发明实施例公开的一种可能的系统架构图；

[0053] 图3是本发明实施例公开的一种远程管理方法的流程示意图；

[0054] 图4是本发明实施例公开的另一种远程管理方法的流程示意图；

[0055] 图5是本发明实施例公开的又一种远程管理方法的流程示意图；

[0056] 图6A是本发明实施例公开的一种SM-DP+服务器的结构示意图；

[0057] 图6B是本发明实施例公开的另一种SM-DP+服务器的结构示意图；

[0058] 图7A是本发明实施例公开的一种eUICC的的结构示意图；

[0059] 图7B是本发明实施例公开的另一种eUICC的结构示意图；

[0060] 图8A是本发明实施例公开的一种SM-DS服务器的结构示意图；

[0061] 图8B是本发明实施例公开的另一种SM-DS服务器的结构示意图。

具体实施方式

[0062] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0063] 本发明的说明书和权利要求书及上述附图中的术语“第一”和“第二”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备，没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0064] 在现有的远程管理过程中，SM-DP+服务器发送远程配置文件管理命令至eUICC时，远程配置文件管理命令可被非法设备篡改，进而使eUICC执行被篡改的远程配置文件管理命令(如执行非法激活配置文件、非法去激活配置文件或非法删除配置文件等操作)。因此，现有远程管理的安全性不高。

[0065] 为提高远程管理的安全性，本发明实施例公开了一种远程管理方法及设备。其中，方法和设备是基于同一发明构思的，由于方法及设备解决问题的原理相似，因此设备与方法的实施可以相互参见，重复之处不再赘述。

[0066] 为了清楚的描述本发明实施例的方案，下面结合附图2，对本发明实施例可能应用的业务场景和系统架构进行说明。

[0067] 请参见图2，图2是本发明实施例公开的一种可能的系统架构图。如图2所示，该系统架构包括：用户终端、SM-DP+服务器和SM-DS服务器。

[0068] 其中，用户终端可以包括移动手机、平板电脑、个人数字助理(Personal Digital Assistant，PDA)、电视、车载设备、机器到机器设备(Machine to Machine，M2M)、移动互联网设备(Mobile Intemet Device，MID)、智能穿戴设备(如智能手表、智能手环)等各类电子设备。用户终端内设置有eUICC和LPA，其中，LPA可部署于eUICC中，或也可与eUICC独立部署。

[0069] 可选的，LPA可包括本地签约下载(Local Profile Download，LPD)模块、本地用户

接口(Local User Interface,LUI)模块以及本地发现服务(Local Discovery Service,LDS)模块。通常,LPA在用户终端内部承担用户终端与eUICC之间交互的作用,LPD模块主要负责签约文件下载,LDS模块主要负责业务发现,LUI模块为用户提供UI界面。用户通过LPA可以管理下载到eUICC上的配置文件,如对配置文件进行激活、去激活、删除等操作。

[0070] 在图2所示的系统架构中,SM-DP+服务器可以通过LPA向eUICC发送远程配置文件管理命令,使eUICC执行远程配置文件管理命令,从而实现远程管理,远程配置文件管理包括激活配置文件、去激活配置文件、删除配置文件以及审查eUICC状态等。

[0071] SM-DS服务器的主要作用是提供一种机制让SM-DP+服务器与LPA联系,LPA可以从SM-DS服务器中获取SM-DP+服务器的地址,进而LPA就可以和SM-DP+服务器联系。其中,本文中的SM-DS服务器可以是具体的某一个SM-DS服务器,也可以是多级SM-DS服务器的统称。

[0072] 在图2所示的系统架构中,当通信运营商需要对配置文件进行远程操作(如下载配置文件至eUICC或对eUICC中的配置文件进行远程管理)时,通信运营商发送操作命令(如配置文件下载命令或远程配置文件管理命令)、eUICC标识(用于标识eUICC)以及与该配置文件对应的SM-DS服务器的地址至SM-DP+服务器。SM-DP+服务器接收操作命令、eUICC标识和SM-DS服务器的地址之后,生成与操作命令对应的事件标识,该标识也可称为通知标识或告知标识,该事件标识用于标识事件,其中,事件包括配置文件下载事件和远程配置文件管理事件。例如,若事件为配置文件下载事件,则生成配置文件下载的事件标识;若事件为远程配置文件管理事件,则生成远程配置文件管理的标识。SM-DP+服务器至少建立操作命令、事件标识、eUICC标识、SM-DP+服务器的地址和SM-DS服务器的地址之间的对应关系,并存储该对应关系。

[0073] 在图2所示的系统架构中,SM-DP+服务器生成与操作命令对应的事件标识之后,将根据SM-DS服务器的地址,至少发送事件标识、eUICC标识和SM-DP+服务器的地址至SM-DS服务器进行注册。

[0074] 在图2所示的系统架构中,eUICC中存储有SM-DS服务器的地址,LPA根据eUICC中提供的该SM-DS服务器的地址与SM-DS服务器进行连接。可选的,LPA与SM-DS服务器建立连接之后,SM-DS服务器和eUICC可通过LPA进行双向认证(即eUICC对SM-DS服务器的身份进行认证,SM-DS服务器对eUICC的身份进行认证)。在双向认证通过之后,SM-DS服务器至少发送SM-DP+服务器注册的事件标识、eUICC标识和SM-DP+服务器的地址至LPA。

[0075] 可以理解的是,本发明实施例描述的系统架构以及业务场景是为了更加清楚的说明本发明实施例的技术方案,并不构成对于本发明实施例提供的技术方案的限定,本领域普通技术人员可知,随着系统架构的演变和新业务场景的出现,本发明实施例提供的技术方案对于类似的技术问题,同样适用。

[0076] 下面将基于上面所述的本发明实施例涉及的共性方面,对本发明实施例进一步详细说明。

[0077] 请参见图3,图3是本发明实施例公开的一种远程管理方法的流程示意图。如图3所示,该远程管理方法可以包括301～307部分。

[0078] 301、LPA向SM-DP+服务器至少发送第一标识。

[0079] 本发明实施例中,该第一标识为事件标识。该第一标识为SM-DP+服务器注册在SM-DS服务器中的。在SM-DS服务器和eUICC双向认证之后,该第一标识被SM-DS服务器发送至

LPA。在SM-DS服务器和eUICC双向认证之后，SM-DS服务器还将发送SM-DP+服务器的地址至LPA。LPA接收至少SM-DP+服务器的地址和第一标识之后，根据SM-DP+服务器的地址与SM-DP+服务器进行连接，并在建立与SM-DP+服务器的连接之后向SM-DP+服务器至少发送第一标识。

[0080] 302、LPA向eUICC至少发送该第一标识。

[0081] 本发明实施例中，LPA至少发送第一标识至SM-DP+服务器之后，LPA至少发送该第一标识至eUICC。可选的，302部分与303部分的执行顺序不分先后，可先执行302部分，也可先执行303部分。

[0082] 303、SM-DP+服务器查找该第一标识对应的远程配置文件管理命令。

[0083] 本发明实施例中，SM-DP+服务器接收第一标识之后，若该第一标识为远程配置文件管理事件对应的事件标识，则SM-DP+服务器获取与该第一标识对应的远程配置文件管理命令。

[0084] 304、SM-DP+服务器至少根据该第一标识和该远程配置文件管理命令生成第一数字签名。

[0085] 本发明实施例中，SM-DP+服务器至少根据该第一标识和该远程配置文件管理命令生成第一数字签名的具体实施方式可以为：SM-DP+服务器至少根据该第一标识和该远程配置文件管理命令生成数据结构，再利用SM-DP+服务器的私钥根据该数据结构计算出第一数字签名。

[0086] 可选的，SM-DP+服务器可对第一标识和该远程配置文件管理命令进行哈希运算，得到一个信息摘要，再用SM-DP+服务器的私钥对该信息摘要进行加密以得到该第一数字签名。

[0087] 305、SM-DP+服务器通过LPA至少发送该第一数字签名和该远程配置文件管理命令至eUICC。

[0088] 本发明实施例中，SM-DP+服务器生成第一数字签名之后，将发送至少该第一数字签名和该远程配置文件管理命令至LPA，并由LPA发送至少该第一数字签名和该远程配置文件管理命令至eUICC。

[0089] 306、eUICC至少根据该第一标识和该远程配置文件管理命令对该第一数字签名进行验证。

[0090] 本发明实施例中，eUICC接收LPA发送的该第一标识、该远程配置文件管理命令和该第一数字签名之后，将至少使用该第一标识和该远程配置文件管理命令对该第一数字签名进行验证。

[0091] 可选的，eUICC至少使用该第一标识和该远程配置文件管理命令对该第一数字签名进行验证的具体实施方式可以为：eUICC利用之前接收到的SM-DP+服务器的数字证书的公钥对第一数字签名进行解密，得到信息摘要；再将第一标识和该远程配置文件管理命令进行哈希运算得到一个新的信息摘要；eUICC将解密得到的信息摘要和该新的信息摘要进行比较，若解密得到的信息摘要和该新的信息摘要一致，eUICC就确定对该第一数字签名验证通过，即该远程配置文件管理命令没有被篡改。

[0092] 307、eUICC执行该远程配置文件管理命令。

[0093] 本发明实施例中，若eUICC就确定对该第一数字签名验证通过，则eUICC执行该远

程配置文件管理命令。

[0094] 在图3所描述的方法中，SM-DP+服务器接收LPA发送的第一标识之后，将获取该第一标识对应的远程配置文件管理命令；SM-DP+服务器至少根据远程配置文件管理命令以及该第一标识生成第一数字签名，并通过LPA发送至少该第一数字签名和该远程配置文件管理命令至eUICC。从而eUICC在接收该第一数字签名和该远程配置文件管理命令之后，可至少根据LPA发送给eUICC的该第一标识和SM-DP+的数字证书中的公钥对该第一数字签名进行验证。若验证通过(说明该远程配置文件管理命令未被非法设备篡改)，eUICC才执行该远程配置文件管理命令。可见，通过实施图3所描述的实施例，eUICC可确定远程配置文件管理命令是否被非法设备篡改，并在确定远程配置文件管理命令未被非法设备篡改时才执行远程配置文件管理命令，从而提高了远程管理的安全性。

[0095] 请参见图4，图4是本发明实施例公开的另一种远程管理方法的流程示意图。如图4所示，该远程管理方法可以包括部分401～422部分。

[0096] 401、LPA向SM-DP+服务器至少发送第一标识和第一随机数。

[0097] 本发明实施例中，该第一随机数是eUICC发送给LPA的。在LPA接收到SM-DS服务器发送的SM-DP+服务器的地址、第一标识和eUICC标识之后，触发eUICC生成第一随机数。eUICC生成第一随机数之后发送第一随机数至LPA，LPA接收第一随机数之后，根据SM-DP+服务器的地址至少发送第一随机数和第一标识至SM-DP+服务器。其中，eUICC生成第一随机数之后会存储第一随机数。

[0098] 402、SM-DP+服务器检查是否存储有与第一标识对应的事件。

[0099] 本发明实施例中，该事件包括远程配置文件管理事件和配置文件下载事件。若SM-DP+服务器检查到存储有与第一标识对应的事件，则执行403部分。

[0100] 403、当第一标识对应的事件为远程配置文件管理事件时，SM-DP+服务器不生成交互标识。

[0101] 本发明实施例中，交互标识即用于对交互进行标识的信息，通过在第一标识对应的事件为远程配置文件管理事件时，不生成交互标识，从而可使用已有的事件标识来替代交互标识，有利于减少参数的数量。

[0102] 404、SM-DP+服务器生成第二随机数，并至少根据第二随机数和第一随机数生成第一数字签名。

[0103] 本发明实施例中，当SM-DP+服务器检查到存储有与第一标识对应的事件后，SM-DP+服务器生成第二随机数，并至少根据第二随机数和第一随机数生成第一数字签名。其中，SM-DP+服务器生成第二随机数之后，将存储第二随机数。

[0104] 本发明实施例中，SM-DP+服务器至少根据第二随机数和第一随机数生成第一数字签名的具体实施方式可以为：至少根据该第二随机数和第一随机数生成数据结构，再利用SM-DP+服务器的私钥根据该数据结构计算出第一数字签名。

[0105] 可选的，SM-DP+服务器根据至少第二随机数和第一随机数生成第一数字签名的具体实施方式可以为：SM-DP+服务器对至少第二随机数和第一随机数进行哈希运算，得到信息摘要，并使用SM-DP+服务器的私钥对该信息摘要进行加密，以得到第一数字签名。

[0106] 405、SM-DP+服务器至少发送第二随机数、第一数字签名和SM-DP+服务器的数字证书至LPA。

[0107] 406、LPA向eUICC至少发送该第一标识、第二随机数、第一数字签名和SM-DP+服务器的数字证书。

[0108] 407、eUICC对SM-DP+服务器的数字证书进行验证，并对第一数字签名进行验证。

[0109] 本发明实施例中，eUICC接收该第一标识、第二随机数、第一数字签名和SM-DP+服务器的数字证书之后，使用证书发布者(Ceritificate Issuer)的公钥对SM-DP+服务器的数字证书进行验证。对SM-DP+服务器的数字证书验证成功之后，eUICC获取SM-DP+服务器的数字证书中SM-DP+服务器的公钥，并至少使用SM-DP+服务器的公钥、第二随机数和自身存储的第一随机数对第一数字签名进行验证。

[0110] 可选的，eUICC至少使用SM-DP+服务器的公钥、第一随机数、第二随机数对第一数字签名进行验证的具体实施方式可以为：eUICC使用SM-DP+服务器的公钥对第一数字签名进行解密，以得到信息摘要；再至少根据第二随机数和eUICC存储的其之前生成的第一随机数进行哈希运算，得到一个新的信息摘要，将解密的信息摘要与该新的信息摘要进行对比，若一致，则确定第一数字签名验证通过。若确定第一数字签名验证通过，则执行408部分。

[0111] 408、eUICC至少根据该第一标识和该第二随机数生成第二数字签名。

[0112] 本发明实施例中，eUICC至少根据该第一标识和该第二随机数生成第二数字签名的具体实施方式可以为：至少根据该第一标识和该第二随机数生成数据结构，再利用eUICC的私钥根据该数据结构计算出第二数字签名。

[0113] 本发明实施例中，可选的，eUICC将第一标识和第二随机数进行哈希运算，得到一个信息摘要，再用eUICC的私钥对该信息摘要进行加密以得到该第二数字签名。

[0114] 409、eUICC通过LPA发送至少第二数字签名、eUICC的数字证书和eUICC制造商EUM的数字证书至SM-DP+服务器。

[0115] 本发明实施例中，eUICC生成第二数字签名之后，通过LPA发送至少第二数字签名、eUICC的数字证书和EUM的数字证书至SM-DP+服务器。

[0116] 410、SM-DP+服务器验证eUICC的数字证书和EUM的数字证书，并至少使用第一标识、第二随机数和eUICC的数字证书中的公钥对第二数字签名进行验证。

[0117] 本发明实施例中，SM-DP+服务器接收第二数字签名和eUICC的数字证书之后，证书发布者(Ceritificate Issuer)的公钥对EUM的数字证书进行验证，若验证成功，则确定对EUM的数字证书验证通过；SM-DP+服务器再利用EUM的数字证书中的公钥对eUICC的数字证书进行验证，若验证成功，则确定对eUICC的数字证书验证通过；在确定eUICC的数字证书验证通过之后，SM-DP+服务器至少使用第二随机数、eUICC的数字证书中的公钥以及第一标识对第二数字签名进行验证。

[0118] 可选的，SM-DP+服务器至少使用第二随机数、eUICC的数字证书中的公钥以及第一标识对第二数字签名进行验证的具体实施方式可以为：SM-DP+服务器使用eUICC的数字证书中的公钥对第二数字签名进行解密，得到信息摘要；再至少根据第一标识与SM-DP+服务器存储的其之前生成的第二随机数进行哈希运算，得到一个新的信息摘要；SM-DP+服务器将解密得到的信息摘要与该新的信息摘要进行对比，若一致，则SM-DP+服务器确定对第二数字签名验证通过。在对第二数字签名验证通过之后执行411部分。

[0119] 在实际应用中eUICC是根据交互标识来生成第二数字签名，相应地，SM-DP+服务器也根据该交互标识来验证第二数字签名。通过执行408～410部分，eUICC使用已存在的第一

标识来代替交互标识生成第二数字签名，相应地SM-DP+服务器根据自身存储的第一标识来验证第二数字签名，这样用第一标识来替代交互标识的作用，减少了参数的数量，使参数变得更简洁化。

[0120] 411、SM-DP+服务器查找第一标识对应的远程配置文件管理命令。

[0121] 412、SM-DP+服务器至少根据第一标识和远程配置文件管理命令生成第三数字签名。

[0122] 本发明实施例中，该第三数字签名即为图3所示的实施例中的第一数字签名。412部分与图3中的304部分相似，可参考图3中的304部分的描述，此处不作赘述。

[0123] 413、SM-DP+服务器通过LPA至少发送第三数字签名和远程配置文件管理命令至eUICC。

[0124] 本发明实施例中，413部分与图3中的305部分相似，可参考图3中的305部分的描述，此处不作赘述。

[0125] 414、eUICC至少根据该第一标识和该远程配置文件管理命令对该第三数字签名进行验证。

[0126] 本发明实施例中，414部分与图3中的306部分相似，可参考图3中的306部分的描述，此处不作赘述。

[0127] 415、eUICC发送第一消息至LPA。

[0128] 本发明实施例中，若eUICC确定对该第三数字签名验证通过，且远程配置文件管理命令为目标命令，则eUICC发送用于请求用户确认的第一消息至LPA。LPA接收第一消息之后，可通过LUI模块呈现用户确认。可选的，该目标命令可包括但不限于激活配置文件的命令、去激活配置文件的命令或删除配置文件的命令。

[0129] 416、LPA返回确认执行消息至eUICC。

[0130] 本发明实施例中，当LPA接收到用户输入的用于确认执行远程配置文件管理命令的指令时，LPA返回确认执行消息至eUICC。

[0131] 417、eUICC执行远程配置文件管理命令。

[0132] 本发明实施例中，eUICC接收到该确认执行消息之后，执行远程配置文件管理命令。

[0133] 通过执行415～417部分，当需要对配置文件进行激活、去激活或删除时，向用户进行确认，能够有效地提高eUICC中配置文件信息的安全性，且能够使用户掌握远程设备对配置文件的操作情况。

[0134] 418、eUICC生成远程配置文件管理命令的远程配置文件管理结果。

[0135] 本发明实施例中，eUICC执行完远程配置文件管理命令之后，生成远程配置文件管理命令的远程配置文件管理结果。该远程配置文件管理结果至少包括第一标识以及根据第一标识生成的第四数字签名。可选的，该远程配置文件管理结果还可包括结果代码、SM-DP+服务器的地址。可选的，该第四数字签名可以是根据第一标识、结果代码和SM-DP+服务器的地址生成的。

[0136] 419、eUICC发送至少包含第一标识和第四数字签名的远程配置文件管理结果至LPA。

[0137] 本发明实施例中，eUICC生成远程配置文件管理结果之后，发送至少包含第一标识

和第四数字签名的远程配置文件管理结果至LPA。可选的，若远程配置文件管理结果还包括结果代码和SM-DP+服务器的地址，eUICC还可发送结果代码和SM-DP+服务器的地址至LPA。

[0138] 420、LPA发送至少包括第一标识和第四数字签名的第二消息至SM-DP+服务器。

[0139] 本发明实施例中，LPA接收远程配置文件管理结果之后，发送第二消息至SM-DP+服务器，该第二消息至少包括远程配置文件管理结果中的第一标识和第四数字签名。

[0140] 可选的，若远程配置文件管理结果还包括结果代码和SM-DP+服务器的地址，第二消息还可包括结果代码和SM-DP+服务器的地址。

[0141] 421、SM-DP+服务器向SM-DS服务器发送第三消息。

[0142] 本发明实施例中，SM-DP+服务器接收到第二消息之后，SM-DS服务器发送第三消息至SM-DS服务器。该第三消息中至少包含SM-DP+服务器的地址、eUICC标识和第一标识，第三消息用于SM-DS服务器至少删除由SM-DP+服务器发送的SM-DP+服务器的地址、eUICC标识和第一标识。

[0143] 422、SM-DS服务器至少删除SM-DP+服务器发送的SM-DP+地址、eUICC标识和第一标识。

[0144] 本发明实施例中，SM-DS服务器接收第三消息之后，至少删除SM-DP+服务器发送的SM-DP+地址、eUICC标识和第一标识。

[0145] 通过执行418和422部分，在eUICC执行完远程配置文件管理命令之后，SM-DS服务器能够及时地删除其存储的至少SM-DP+地址、eUICC标识和第一标识，从而能够节省其存储空间。

[0146] 在图4所描述的方法中，SM-DP+服务器接收LPA发送的第一标识之后，将查找该第一标识对应的远程配置文件管理命令；SM-DP+服务器至少根据远程配置文件管理命令以及该第一标识生成第三数字签名，并通过LPA至少发送该第三数字签名和该远程配置文件管理命令至eUICC。从而eUICC在接收该第三数字签名和该远程配置文件管理命令之后，可至少根据LPA发送给eUICC的该第一标识和SM-DP+的数字证书中的公钥对该第三数字签名进行验证。若验证通过(说明该远程配置文件管理命令未被非法设备篡改)，eUICC才执行该远程配置文件管理命令。可见，通过实施图4所描述的方法，提高了远程管理的安全性。

[0147] 请参见图5，图5是本发明实施例公开的又一种远程管理方法的流程示意图。如图5所示，该远程管理方法可以包括501～511部分。

[0148] 501、SM-DS服务器接收SM-DP+服务器发送的第一消息。

[0149] 本发明实施例中，该第一消息至少包括eUICC标识和第一标识，可选的，该第一消息还可包括SM-DP+服务器的地址、eUICC信息1(eUICCinfo1)。

[0150] 502、SM-DS服务器对eUICC的身份认证通过后，SM-DS服务器生成令牌。

[0151] 本发明实施例中，该令牌为SM-DS服务器至少根据该第一标识、eUICC标识和SM-DS服务器的地址生成的数字签名。

[0152] 本发明实施例中，SM-DS服务器至少根据该第一标识、eUICC标识和SM-DS服务器的地址生成数字签名的具体实施方式可以为：SM-DS服务器至少根据该第一标识、eUICC标识和SM-DS服务器的地址生成数据结构，再利用SM-DP+服务器的私钥根据该数据结构计算出数字签名。

[0153] 可选的，SM-DS服务器至少根据该第一标识、eUICC标识和SM-DS服务器的地址生成

令牌的具体实施方式可以为:SM-DS服务器至少对该第一标识、eUICC标识和SM-DS服务器的地址进行哈希运算,得到一个信息摘要,再用SM-DS服务器的私钥对该信息摘要进行加密以得到该令牌。

[0154] 503、SM-DS服务器发送第二消息至LPA。

[0155] 本发明实施例中,该第二消息至少包括eUICC标识、第一标识、令牌、SM-DP+服务器的地址、SM-DS服务器的地址和SM-DS服务器的数字证书。

[0156] 504、LPA发送第三消息至SM-DP+服务器。

[0157] 本发明实施例中,LPA接收到第二消息之后,会发送第三消息至SM-DP+服务器。

[0158] 其中,该第三消息至少包括第二消息中的eUICC标识、第一标识、令牌、SM-DS服务器的数字证书和SM-DS服务器的地址。

[0159] 可选的,LPA接收到第二消息之后,还会触发eUICC生成随机数,eUICC生成随机数之后,返回随机数至LPA,该第三消息还可包括eUICC生成的该随机数。

[0160] 505、SM-DP+服务器验证令牌。

[0161] 本发明实施例中,SM-DP+服务器接收第三消息之后,至少根据eUICC标识、SM-DS服务器的数字证书和SM-DS服务器的地址对令牌进行验证。

[0162] 可选的,SM-DP+服务器验证令牌的具体实施方式可以为:SM-DP+服务器对SM-DS服务器的数字证书进行验证,验证成功之后,从SM-DS服务器的数字证书中得到SM-DS服务器的公钥;SM-DP+服务器使用SM-DS服务器的公钥对令牌进行解密,得到信息摘要;再将至少第三消息中的eUICC标识和SM-DS服务器的地址进行哈希运算得到一个新的信息摘要;SM-DP+服务器将解密得到的信息摘要和该新的信息摘要进行比较,若解密得到的信息摘要和该新的信息摘要一致,SM-DP+服务器就确定对令牌验证通过。

[0163] SM-DP+服务器确定对令牌验证通过之后,执行506部分。

[0164] 506、SM-DP+服务器检验SM-DS服务器的地址是否与第一标识对应的SM-DS服务器的地址相匹配,并且检验eUICC标识是否与第一标识对应的eUICC标识相匹配。

[0165] 本发明实施例中,SM-DP+服务器会检验第三消息中的SM-DS服务器的地址是否与第一标识对应的由通信运营商发送的SM-DS服务器的地址相匹配,并且检验第三消息中的eUICC标识是否与第一标识对应的由通信运营商发送的eUICC标识相匹配。

[0166] 若第三消息中的SM-DS服务器的地址与第一标识对应的由通信运营商发送的SM-DS服务器的地址相匹配,并且第三消息中的eUICC标识与第一标识对应的由通信运营商发送的eUICC标识相匹配,则执行507部分。

[0167] 507、SM-DP+服务器确定对eUICC的身份认证通过。

[0168] 在现有技术中,SM-DP+服务器对eUICC的身份进行验证时,SM-DP+服务器需要生成随机数,并通过LPA发送随机数至eUICC;eUICC根据该随机数生成数字签名,并通过LPA发送eUICC的数字证书和该数字签名至SM-DP+服务器进行验证;若SM-DP+服务器根据eUICC的数字证书中的公钥对该数字签名验证通过,则SM-DP+服务器确定对eUICC的身份验证通过。可见,在现有技术中,SM-DP+服务器对eUICC的身份进行验证时,SM-DP+服务器、LPA与eUICC之间会有很多信息交互,且交互流程非常繁琐。通过实施图5所示的501～507部分,SM-DS服务器生成令牌之后,通过LPA发送令牌至SM-DP+服务器,SM-DP+服务器根据令牌就可准确地对eUICC进行身份验证。可见,通过实施图5所示的501～507部分,简化了SM-DP+服务器对

eUICC进行身份验证过程中的交互流程，使整个操作流程更为精简。

[0169] 508、SM-DP+服务器至少根据随机数和第一标识对应的远程配置文件管理命令生成第一数字签名。

[0170] 本发明实施例中，当第一标识对应的事件为远程本地配置文件配置文件管理事件时，在SM-DP+服务器确定对eUICC的身份认证通过之后，SM-DP+服务器至少根据第三消息包括的随机数和第一标识对应的远程配置文件管理命令生成第一数字签名。

[0171] 本发明实施例中，SM-DP+服务器至少根据第三消息包括的随机数和第一标识对应的远程配置文件管理命令生成第一数字签名的具体实施方式可以为：SM-DP+服务器至少根据第三消息包括的随机数和第一标识对应的远程配置文件管理命令生成数据结构，再利用SM-DP+服务器的私钥根据该数据结构计算出第一数字签名。

[0172] 可选的，SM-DP+服务器至少根据第三消息包括的随机数和第一标识对应的远程配置文件管理命令生成第一数字签名的具体实施方式可以为：SM-DP+服务器至少对第三消息包括的随机数和第一标识对应的远程配置文件管理命令进行哈希运算，得到一个信息摘要，再用SM-DP+服务器的私钥对该信息摘要进行加密以得到该第一数字签名。

[0173] 509、SM-DP+服务器通过LPA至少发送第一数字签名、远程配置文件管理命令和SM-DP+服务器的数字证书至eUICC。

[0174] 510、eUICC验证SM-DP+服务器的数字证书，并至少使用该随机数、SM-DP+服务器的数字证书中的公钥和远程配置文件管理命令对第一数字签名进行验证。

[0175] 本发明实施例中，eUICC对SM-DP+服务器的数字证书验证通过之后，提取SM-DP+服务器的数字证书中的公钥，并至少使用该随机数、SM-DP+服务器的数字证书中的公钥和远程配置文件管理命令对第一数字签名进行验证。

[0176] 可选的，eUICC至少使用该随机数、SM-DP+服务器的数字证书中的公钥和远程配置文件管理命令对第一数字签名进行验证的具体实施方式可以为：eUICC使用SM-DP+服务器的数字证书中的公钥对第一数字签名进行解密，得到信息摘要；再至少将该随机数和该远程配置文件管理命令进行哈希运算得到一个新的信息摘要；eUICC将解密得到的信息摘要和该新的信息摘要进行比较，若解密得到的信息摘要和该新的信息摘要一致，eUICC就确定对该第一数字签名验证通过。

[0177] 若eUICC确定对该第一数字签名验证通过，则执行511部分。

[0178] 511、eUICC执行远程配置文件管理命令。

[0179] 通过实施图5所描述的508～511部分，SM-DP+服务器至少根据第一标识对应的远程配置文件管理命令和eUICC生成的随机数生成第一数字签名。并通过LPA发送至少第一数字签名、远程配置文件管理命令和SM-DP+服务器的数字证书至eUICC。eUICC对第一数字签名进行验证，验证通过后，eUICC确定对SM-DP+服务器的身份验证通过，且由于第一数字签名是至少根据远程配置文件管理命令生成的，因此，当对第一数字签名验证通过后，eUICC也可确定远程配置文件管理命令并未被非法设备篡改。因此，通过至少根据远程配置文件管理命令和eUICC生成的随机数生成第一数字签名，eUICC只需对第一数字签名验证成功，就能确定对SM-DP+服务器的身份验证通过，且远程配置文件管理命令并未被非法设备篡改，从而简化了操作流程。且通过在确定远程配置文件管理命令并未被非法设备篡改之后，eUICC才执行远程配置文件管理命令也提高了远程配置文件管理的安全性。

[0180] 作为一种可选的实施方式，eUICC对数字证书及数字签名验证通过之后，eUICC执行远程配置文件管理命令之前，eUICC还可执行以下步骤：

[0181] 11)若远程配置文件管理命令为目标命令，则eUICC发送第四消息至LPA，该第四消息用于请求用户确认；

[0182] 12)在接收到LPA返回的确认执行消息之后，eUICC执行远程配置文件管理命令。

[0183] 在该实施方式中，LPA接收第四消息之后，可通过LUI模块呈现用户确认。可选的，该目标命令可以为激活配置文件的命令、去激活配置文件的命令或删除配置文件的命令。

[0184] 通过实施该实施方式，当需要对配置文件进行激活、去激活或删除时，向用户进行确认，能够有效地提高eUICC中配置文件信息的安全性，且能够使用户掌握远程设备对配置文件的操作情况。

[0185] 作为一种可选的实施方式，eUICC执行远程配置文件管理命令之后，eUICC还可执行以下步骤：

[0186] 23)eUICC生成远程配置文件管理命令的远程配置文件管理结果，该远程配置文件管理结果至少包括结果代码以及至少根据该结果代码生成的数字签名；

[0187] 24)eUICC发送至少包含结果代码以及至少根据该结果代码生成的数字签名的远程配置文件管理结果至LPA。

[0188] 那么相应地，LPA接收eUICC发送的至少包含结果代码以及至少根据该结果代码生成的数字签名的远程配置文件管理结果之后，会发送至少包括结果代码以及至少根据该结果代码生成的数字签名的第五消息至SM-DP+服务器。

[0189] 那么相应地，SM-DP+服务器接收第五消息之后，SM-DP+服务器还可执行以下步骤：

[0190] 25)SM-DP+服务器向SM-DS服务器发送第六消息。

[0191] 26)SM-DS服务器至少删除SM-DP发送的SM-DP+地址、eUICC标识和第一标识。

[0192] 通过实施该实施方式，在eUICC执行完远程配置文件管理命令之后，SM-DS服务器能够及时地删除其存储的SM-DP+地址、eUICC标识和第一标识，从而能够节省其存储空间。

[0193] 上述主要从各个网元之间交互的角度对本发明实施例提供的方案进行了介绍。可以理解的是，各个网元，例如SM-DP+服务器、SM-DS服务器、LPA、eUICC等为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本发明能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0194] 本发明实施例可以根据上述方法示例对SM-DP+服务器、SM-DS服务器和eUICC等进行功能单元的划分，例如，可以对应各个功能划分各个功能单元，也可以将两个或两个以上的功能集成在一个处理单元中。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。需要说明的是，本发明实施例中对单元的划分是示意性的，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。

[0195] 在采用集成的单元的情况下，图6A示出了上述实施例中所涉及的SM-DP+服务器的一种可能的结构示意图。SM-DP+服务器600包括：处理单元602和通信单元603。处理单元602用于对SM-DP+服务器的动作进行控制管理，例如，处理单元602用于支持SM-DP+服务器执行

图3中的过程303、304和305，图4中的过程402～405、410～413和421，和/或用于本文所描述的技术的其它过程；或者，处理单元602用于支持SM-DP+服务器执行图5中的过程505～509，和/或用于本文所描述的技术的其它过程。通信单元603用于支持SM-DP+服务器与其他网络实体的通信，例如与图2中示出的功能模块或网络实体之间的通信。SM-DP+服务器还可以包括存储单元601，用于存储SM-DP+服务器的程序代码和数据。

[0196] 其中，处理单元602可以是处理器或控制器，例如可以是中央处理器(Central Processing Unit，CPU)，通用处理器，数字信号处理器(Digital Signal Processor，DSP)，专用集成电路(Application-Specific Integrated Circuit，ASIC)，现场可编程门阵列(Field Programmable Gate Array，FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本发明公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP和微处理器的组合等等。通信单元603可以是收发器、收发电路或通信接口等。存储单元601可以是存储器。

[0197] 当处理单元602为处理器，通信单元603为收发器，存储单元601为存储器时，本发明实施例所涉及的SM-DP+服务器可以为图6B所示的SM-DP+服务器。

[0198] 参阅图6B所示，该SM-DP+服务器610包括：处理器612、收发器613、存储器611以及总线614。其中，收发器613、处理器612以及存储器611通过总线614相互连接；总线614可以是外设部件互连标准(peripheral component interconnect，简称PCI)总线或扩展工业标准结构(extended industry standard architecture，简称EISA)总线等。所述总线614可以分为地址总线、数据总线、控制总线等。为便于表示，图6B中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0199] 在采用集成的单元的情况下，图7A示出了上述实施例中所涉及的eUICC的一种可能的结构示意图。eUICC700包括：处理单元702和通信单元703。处理单元702用于对eUICC的动作进行控制管理，例如，处理单元702用于支持eUICC执行图3中的过程306和307，图4中的过程414、415、417～419，和/或用于本文所描述的技术的其它过程；或者，处理单元702用于支持eUICC执行图5中的过程510和511，和/或用于本文所描述的技术的其它过程。通信单元703用于支持eUICC与其他网络实体的通信，例如与图2中示出的功能模块或网络实体之间的通信。eUICC还可以包括存储单元701，用于存储eUICC的程序代码和数据。

[0200] 其中，处理单元702可以是处理器或控制器，例如可以是中央处理器(Central Processing Unit，CPU)，通用处理器，数字信号处理器(Digital Signal Processor，DSP)，专用集成电路(Application-Specific Integrated Circuit，ASIC)，现场可编程门阵列(Field Programmable Gate Array，FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本发明公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP和微处理器的组合等等。通信单元703可以是收发器、收发电路或通信接口等。存储单元701可以是存储器。

[0201] 当处理单元702为处理器，通信单元703为收发器，存储单元701为存储器时，本发明实施例所涉及的eUICC可以为图7B所示的eUICC。

[0202] 参阅图7B所示，该eUICC710包括：处理器712、收发器713、存储器711以及总线714。

其中，收发器713、处理器712以及存储器711通过总线714相互连接；总线714可以是外设部件互连标准(peripheral component interconnect，简称PCI)总线或扩展工业标准结构(extended industry standard architecture，简称EISA)总线等。所述总线714可以分为地址总线、数据总线、控制总线等。为便于表示，图7B中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0203] 在采用集成的单元的情况下，图8A示出了上述实施例中所涉及的SM-DS服务器的一种可能的结构示意图。SM-DS服务器800包括：处理单元802和通信单元803。处理单元802用于对SM-DS服务器的动作进行控制管理，例如，处理单元802用于支持SM-DS服务器执行图5中的过程501～503，和/或用于本文所描述的技术的其它过程。通信单元803用于支持SM-DS服务器与其他网络实体的通信，例如与图2中示出的功能模块或网络实体之间的通信。SM-DS服务器还可以包括存储单元801，用于存储SM-DS服务器的程序代码和数据。

[0204] 其中，处理单元802可以是处理器或控制器，例如可以是中央处理器(Central Processing Unit，CPU)，通用处理器，数字信号处理器(Digital Signal Processor，DSP)，专用集成电路(Application-Specific Integrated Circuit，ASIC)，现场可编程门阵列(Field Programmable Gate Array，FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本发明公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP和微处理器的组合等等。通信单元803可以是收发器、收发电路或通信接口等。存储单元801可以是存储器。

[0205] 当处理单元802为处理器，通信单元803为收发器，存储单元801为存储器时，本发明实施例所涉及的SM-DS服务器可以为图8B所示的SM-DS服务器。

[0206] 参阅图8B所示，该SM-DS服务器810包括：处理器812、收发器813、存储器811以及总线814。其中，收发器813、处理器812以及存储器811通过总线814相互连接；总线814可以是外设部件互连标准(peripheral component interconnect，简称PCI)总线或扩展工业标准结构(extended industry standard architecture，简称EISA)总线等。所述总线814可以分为地址总线、数据总线、控制总线等。为便于表示，图8B中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0207] 需要说明的是，在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详细描述的部分，可以参见其他实施例的相关描述。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0208] 本发明实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

[0209] 本发明实施例终端中的模块可以根据实际需要进行合并、划分和删减。

[0210] 本发明实施例中所述模块，可以通过通用集成电路，例如CPU(Central Processing Unit，中央处理器)，或通过ASIC(Application Specific Integrated Circuit，专用集成电路)来实现。

[0211] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁

碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory,RAM)等。

[0212] 总之,以上所述仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

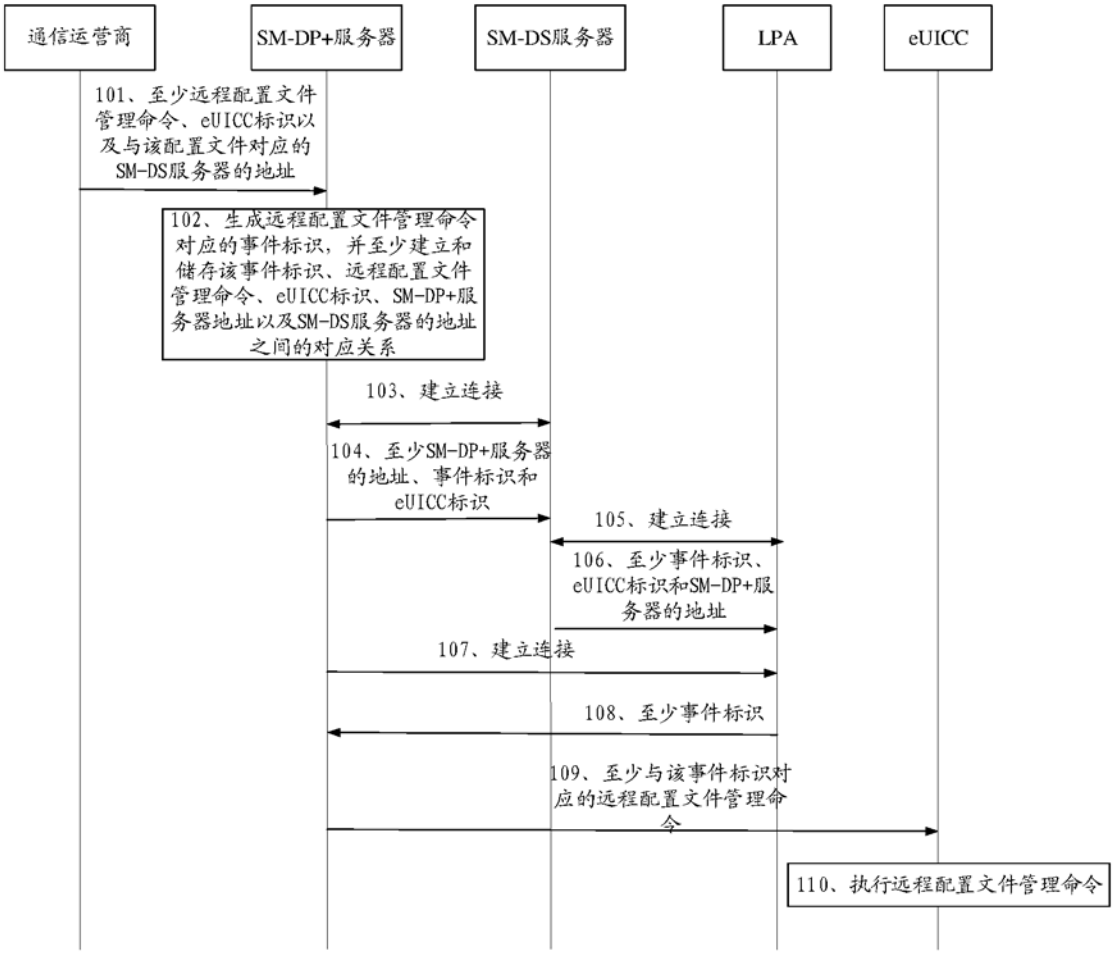

通信运营商
SM-DP+服务器
SM-DS服务器
LPA
eUICC
101、至少远程配置文件管理命令、eUICC标识以及与该配置文件对应的SM-DS服务器的地址
102、生成远程配置文件管理命令对应的事件标识，并至少建立和储存该事件标识、远程配置文件管理命令、eUICC标识、SM-DP+服务器地址以及SM-DS服务器的地址之间的对应关系
103、建立连接
104、至少SM-DP+服务器的地址、事件标识和eUICC标识
105、建立连接
106、至少事件标识、eUICC标识和SM-DP+服务器的地址
107、建立连接
108、至少事件标识
109、至少与该事件标识对应的远程配置文件管理命令
110、执行远程配置文件管理命令

图1

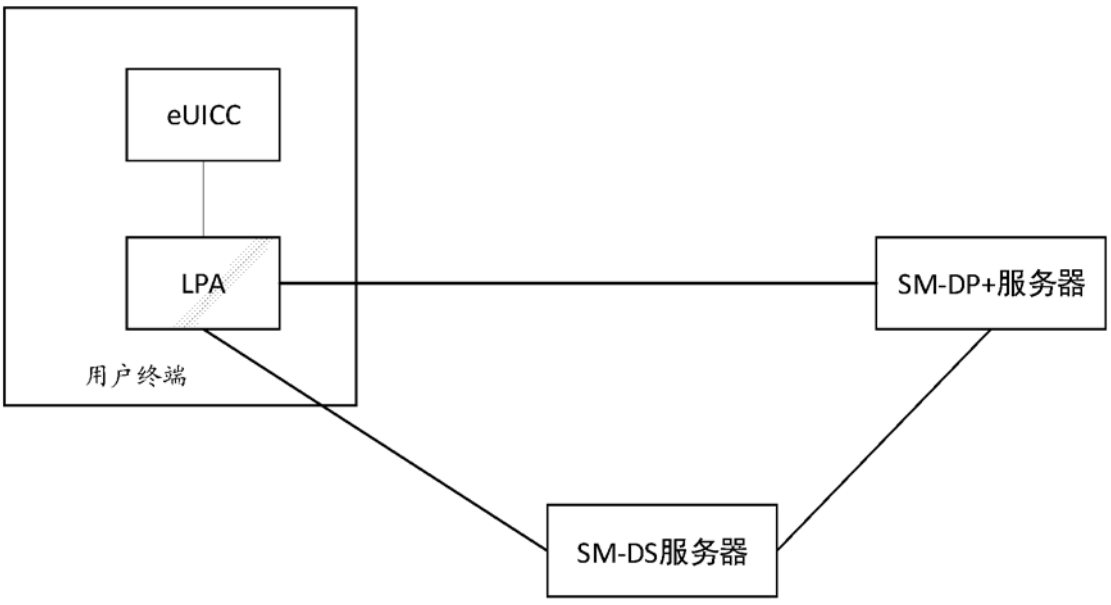

eUICC
LPA
用户终端
SM-DP+服务器
SM-DS服务器

图2

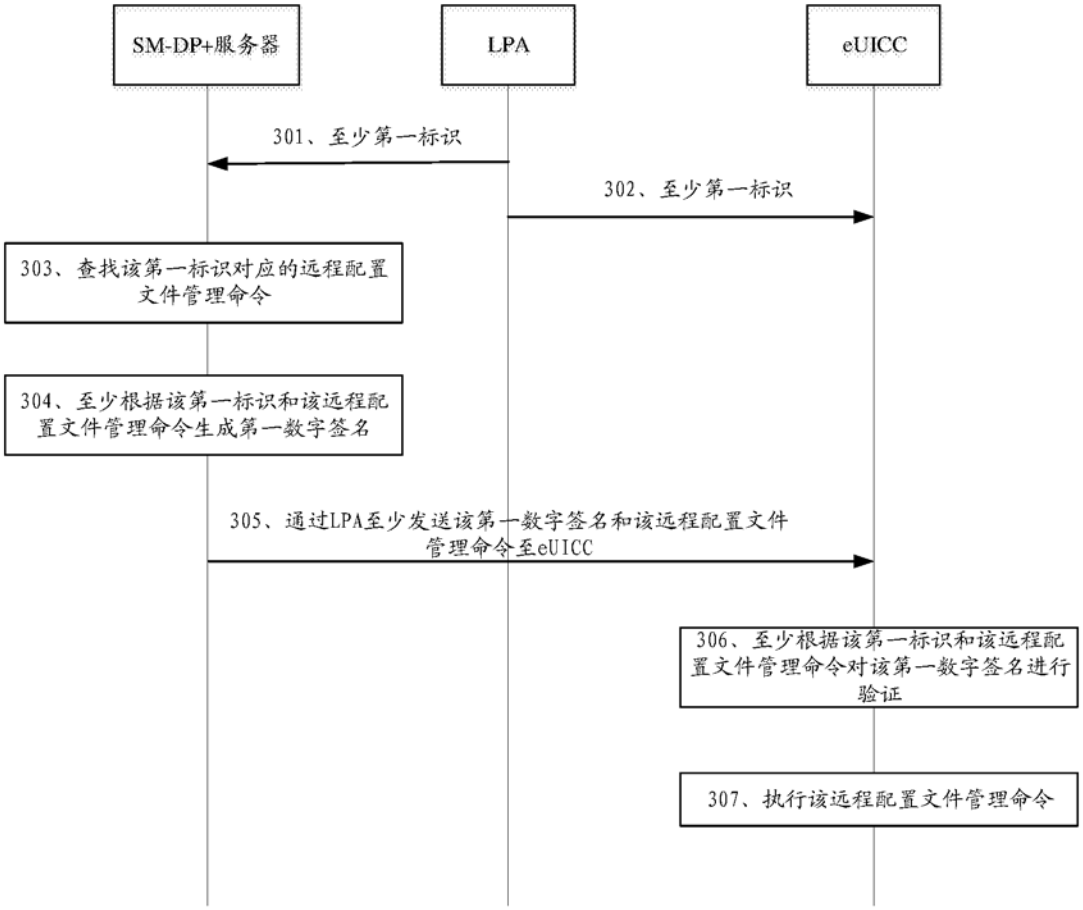

SM-DP+服务器
LPA
eUICC
301、至少第一标识
302、至少第一标识
303、查找该第一标识对应的远程配置文件管理命令
304、至少根据该第一标识和该远程配置文件管理命令生成第一数字签名
305、通过LPA至少发送该第一数字签名和该远程配置文件管理命令至eUICC
306、至少根据该第一标识和该远程配置文件管理命令对该第一数字签名进行验证
307、执行该远程配置文件管理命令

图3

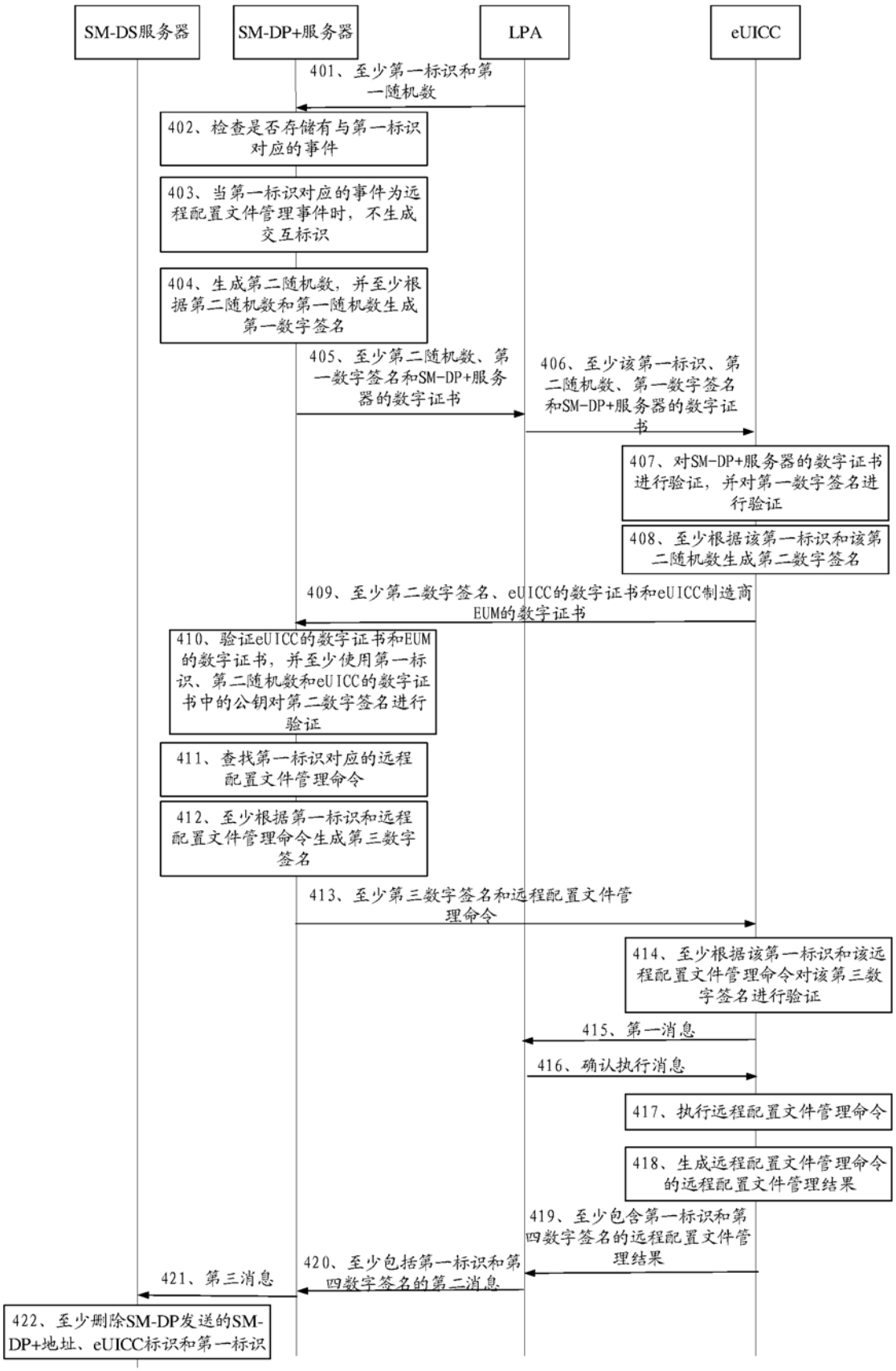

SM-DS服务器
SM-DP+服务器
LPA
eUICC
401、至少第一标识和第一随机数
402、检查是否存储有与第一标识对应的事件
403、当第一标识对应的事件为远程配置文件管理事件时，不生成交互标识
404、生成第二随机数，并至少根据第二随机数和第一随机数生成第一数字签名
405、至少第二随机数、第一数字签名和SM-DP+服务器的数字证书
406、至少该第一标识、第二随机数、第一数字签名和SM-DP+服务器的数字证书
407、对SM-DP+服务器的数字证书进行验证，并对第一数字签名进行验证
408、至少根据该第一标识和该第二随机数生成第二数字签名
409、至少第二数字签名、eUICC的数字证书和eUICC制造商EUM的数字证书
410、验证eUICC的数字证书和EUM的数字证书，并至少使用第一标识、第二随机数和eUICC的数字证书中的公钥对第二数字签名进行验证
411、查找第一标识对应的远程配置文件管理命令
412、至少根据第一标识和远程配置文件管理命令生成第三数字签名
413、至少第三数字签名和远程配置文件管理命令
414、至少根据该第一标识和该远程配置文件管理命令对该第三数字签名进行验证
415、第一消息
416、确认执行消息
417、执行远程配置文件管理命令
418、生成远程配置文件管理命令的远程配置文件管理结果
419、至少包含第一标识和第四数字签名的远程配置文件管理结果
420、至少包括第一标识和第四数字签名的第二消息
421、第三消息
422、至少删除SM-DP发送的SM-DP+地址、eUICC标识和第一标识

图4

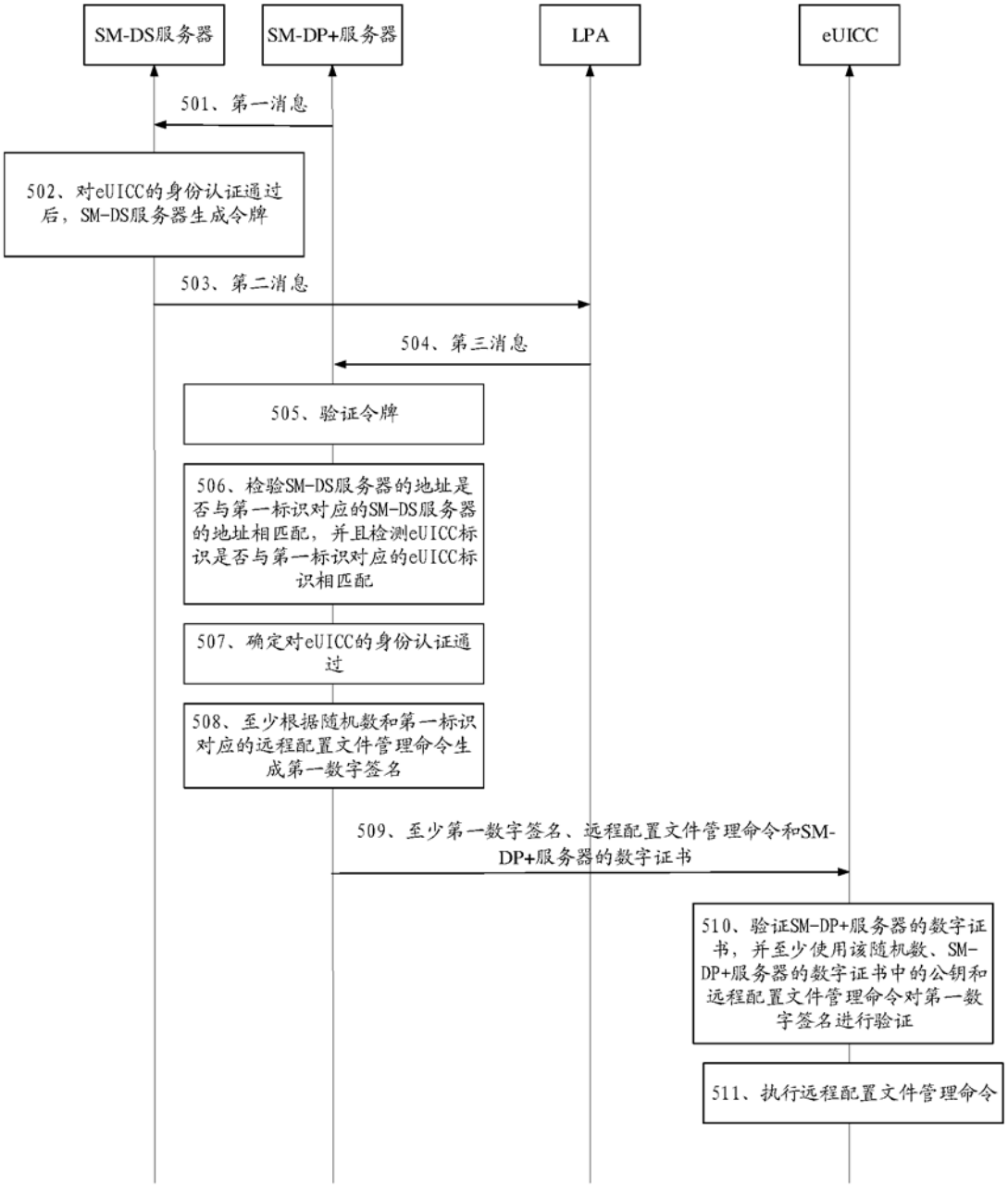

SM-DS服务器
SM-DP+服务器
LPA
eUICC
501、第一消息
502、对eUICC的身份认证通过后，SM-DS服务器生成令牌
503、第二消息
504、第三消息
505、验证令牌
506、检验SM-DS服务器的地址是否与第一标识对应的SM-DS服务器的地址相匹配，并且检测eUICC标识是否与第一标识对应的eUICC标识相匹配
507、确定对eUICC的身份认证通过
508、至少根据随机数和第一标识对应的远程配置文件管理命令生成第一数字签名
509、至少第一数字签名、远程配置文件管理命令和SM-DP+服务器的数字证书
510、验证SM-DP+服务器的数字证书，并至少使用该随机数、SM-DP+服务器的数字证书中的公钥和远程配置文件管理命令对第一数字签名进行验证
511、执行远程配置文件管理命令

图5

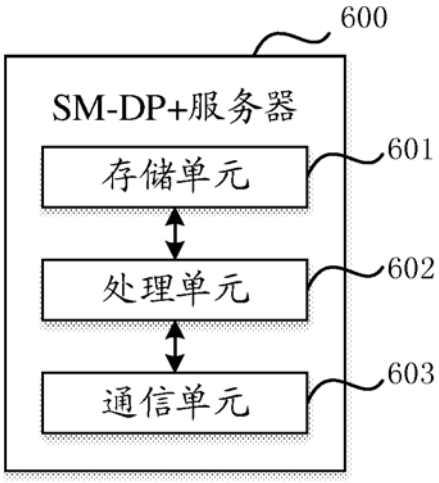

600
SM-DP+服务器
存储单元
601
处理单元
602
通信单元
603

图6A

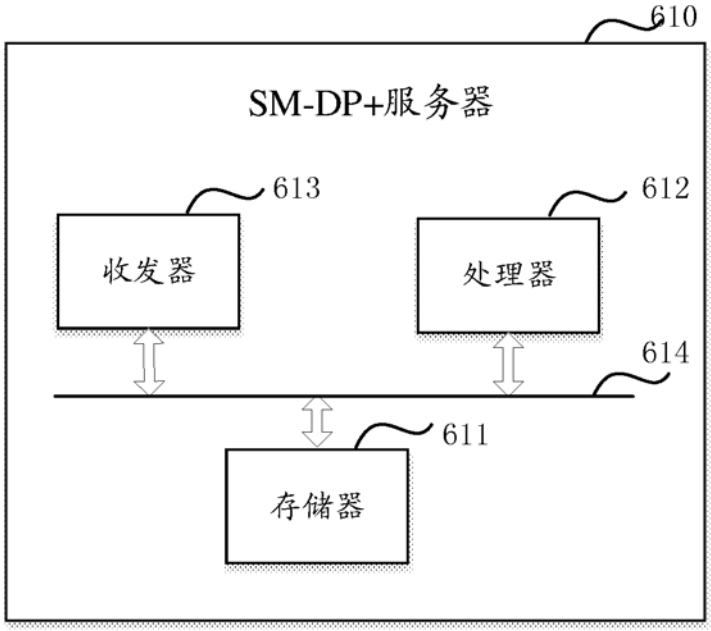

610
SM-DP+服务器
613
收发器
612
处理器
614
611
存储器

图6B

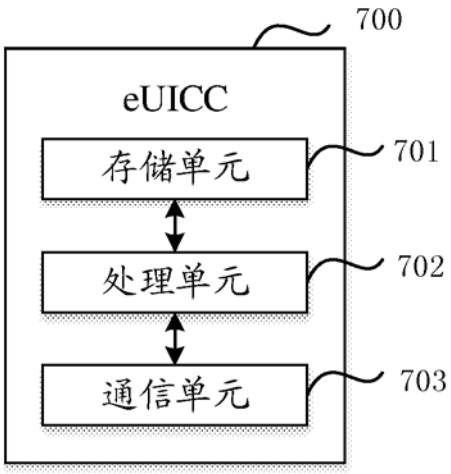

700
eUICC
存储单元
701
处理单元
702
通信单元
703

图7A

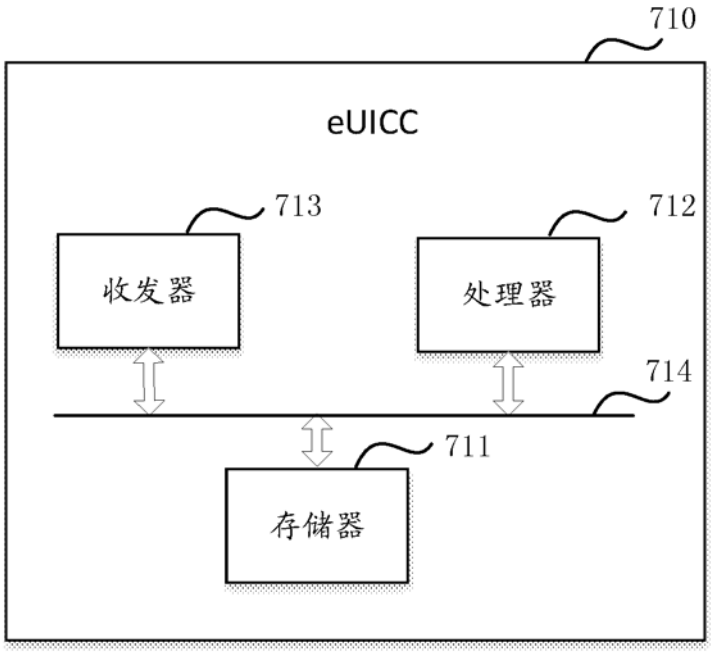

710
eUICC
713
收发器
712
处理器
714
711
存储器

图7B

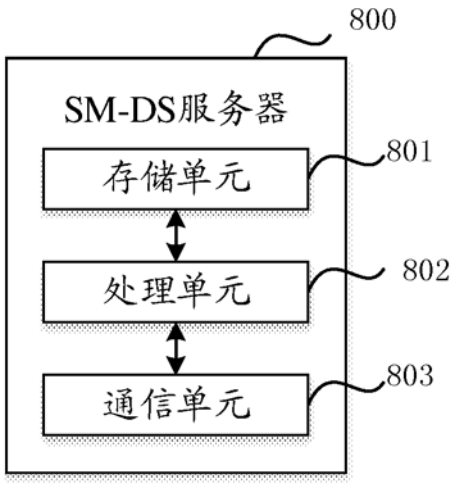

800
SM-DS服务器
存储单元
801
处理单元
802
通信单元
803

图8A

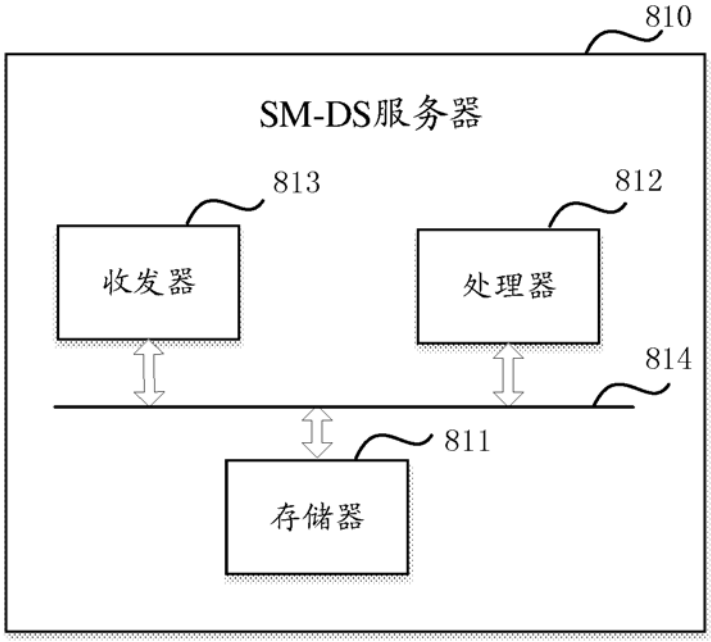

810
SM-DS服务器
813
收发器
812
处理器
814
811
存储器

图8B