(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 103974250 B
(45)授权公告日 2017.11.17

(21)申请号 201310037496.5

(22)申请日 2013.01.30

(65)同一申请的已公布的文献号
申请公布号 CN 103974250 A

(43)申请公布日 2014.08.06

(73)专利权人 华为终端有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地B区2号楼

(72)发明人 李永华 张国妍 宋琦 衣强 金辉

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳

(51)Int.Cl.
H04W 12/06(2009.01)

(56)对比文件
CN 102595400 A,2012.07.18,
WO 2012/076464 A1,2012.06.14,
CN 101123778 A,2008.02.13,

审查员 胡淼

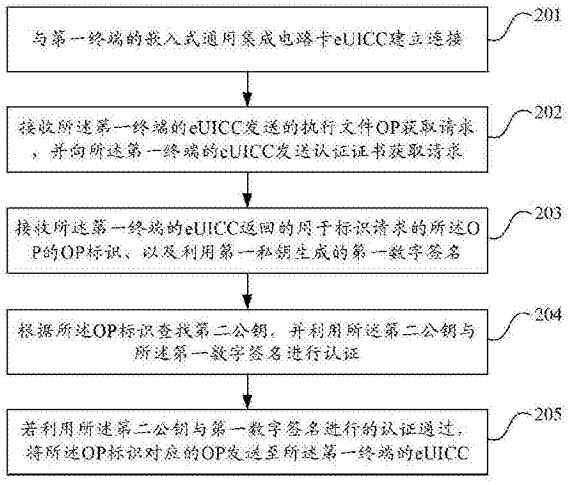
权利要求书6页 说明书20页 附图6页

(54)发明名称

配置方法和设备

(57)摘要

本发明提供一种配置方法和设备，其中方法包括：与第一终端的eUICC建立连接；接收第一终端的eUICC发送的OP获取请求，并向第一终端的eUICC发送认证证书获取请求；接收第一终端的eUICC返回的OP标识、以及利用第一私钥生成的数字签名，所述第一私钥是由第一终端的eUICC对从第一终端获取的第一密钥生成参数执行密钥生成算法后生成；获取第二公钥，并利用第二公钥与数字签名进行认证，第二公钥是从第二终端接收到并且是由第二终端的eUICC对从第二终端获取的第二密钥生成参数执行相同的密钥生成算法后生成；若认证通过，则将OP标识对应的OP发送至第一终端的eUICC。本发明提高了终端更换时的安全性。



CN 103974250 B

1.一种配置方法,其特征在于,包括:

与第一终端的嵌入式通用集成电路卡eUICC建立连接;

接收所述第一终端的eUICC发送的执行文件OP获取请求,向所述第一终端的eUICC发送认证证书获取请求;

接收所述第一终端的eUICC返回的标识请求的OP的OP标识、以及利用第一私钥生成的第一数字签名,所述第一私钥是由所述第一终端的eUICC对从所述第一终端获取的第一密钥生成参数执行密钥生成算法后生成;

根据所述OP标识查找第二公钥,并利用所述第二公钥与所述第一数字签名进行认证,所述第二公钥是从第二终端接收到,所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成;

若利用所述第二公钥与所述第一数字签名进行的认证通过,将所述OP发送至所述第一终端的eUICC。

2.根据权利要求1所述的方法,其特征在于,在与所述第一终端的嵌入式通用集成电路卡eUICC建立连接之前,还包括:

与所述第二终端的eUICC建立连接;

接收所述第二终端的eUICC发送的所述第二公钥、第二设备信息,所述第二设备信息用于标识所述第二终端;

记录所述第二公钥、向所述第二终端分配的所述OP标识以及所述第二设备信息之间的对应关系。

3.根据权利要求2所述的方法,其特征在于,在所述向所述第一终端的eUICC发送认证证书获取请求之前,还包括:

所述OP标识携带在所述OP获取请求中,还接收第一设备信息,所述第一设备信息用于标识所述第一终端;

根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系,查找到对应的所述第二设备信息;若判断所述第二设备信息与所述第一设备信息不同,则执行所述向所述第一终端的eUICC发送认证证书获取请求。

4.根据权利要求3所述的方法,其特征在于,在利用所述第二公钥与所述数字签名进行的认证通过之后,还包括:

记录所述OP标识与所述第一设备信息之间的对应关系。

5.根据权利要求2所述的方法,其特征在于,在记录所述第二公钥与所述OP标识之间的对应关系之后,还包括:

接收所述第二终端的eUICC发送的第二公钥修改请求;

根据所述第二公钥修改请求,向所述第二终端的eUICC发送第二认证信息获取请求;

接收所述第二终端的eUICC发送的第二认证信息,所述第二认证信息包括利用第三私钥生成的第二数字签名、以及所述OP标识;所述第三私钥是所述第二终端的eUICC对从所述第二终端获取的第三密钥生成参数执行所述密钥生成算法后生成;

利用所述第二公钥与所述第二数字签名进行认证,并在认证通过时,根据所述第二公钥修改请求对所述第二公钥进行修改。

6.根据权利要求2所述的方法,其特征在于,在记录所述第二公钥与所述OP标识之间的

对应关系之后，还包括：

接收所述第一终端的eUICC发送的第一公钥修改请求；

根据所述第一公钥修改请求，向所述第一终端的eUICC发送第一认证信息获取请求；

接收所述第一终端的eUICC发送的第一认证信息，所述第一认证信息包括利用第四私钥生成的第三数字签名、以及所述OP标识；所述第四私钥是所述第一终端的eUICC对从所述第一终端获取的第四密钥生成参数执行所述密钥生成算法后生成；

利用所述第二公钥与所述第三数字签名进行认证，并在认证通过时，根据所述第一公钥修改请求对所述第二公钥进行修改。

7.根据权利要求1所述的配置方法，其特征在于，所述将所述OP发送至所述第一终端的eUICC，包括：

通过所述第二公钥对所述OP加密，并将加密后的所述OP发送至所述第一终端的eUICC。

8.一种配置方法，其特征在于，包括：

嵌入式通用集成电路卡eUICC与远程管理平台建立连接，所述eUICC位于第一终端中；

所述eUICC向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求；

所述eUICC根据所述认证证书获取请求，从所述第一终端获取第一密钥生成参数，对所述第一密钥生成参数执行密钥生成算法生成第一私钥，利用所述第一私钥生成第一数字签名；还从所述第一终端获取用于标识请求的OP的OP标识，将所述OP标识和所述第一数字签名发送至所述远程管理平台；

所述eUICC接收所述远程管理平台发送的与所述OP标识对应的所述OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的；所述第二公钥是由所述远程管理平台从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成。

9.根据权利要求8所述的方法，其特征在于，在所述eUICC位于第一终端之前，当所述eUICC位于第二终端中时：

所述eUICC还接收所述远程管理平台发送的密钥生成指示；

所述eUICC根据所述密钥生成指示，从所述第二终端获取所述第二密钥生成参数、以及用于标识所述第二终端的第二设备信息；

所述eUICC根据所述第二密钥生成参数执行所述密钥生成算法得到密钥对，所述密钥对包括所述第二公钥和第二私钥，并将所述第二公钥和所述第二设备信息发送至所述远程管理平台，以使得所述远程管理平台记录所述第二公钥、向所述第二终端分配的所述OP标识以及所述第二设备信息之间的对应关系。

10.根据权利要求9所述的方法，其特征在于，还包括：

所述eUICC将第一设备信息发送至所述远程管理平台，所述第一设备信息用于标识所述第一终端；以使得所述远程管理平台根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系查找到对应的所述第二设备信息，并在确定所述第二设备信息与所述第一设备信息不同时发送所述认证证书获取请求。

11.根据权利要求9所述的方法，其特征在于，所述eUICC位于所述第二终端中时，在所

述将第二设备信息发送至所述远程管理平台之后，还包括：

向所述远程管理平台发送第二公钥修改请求，并接收所述远程管理平台根据所述第二公钥修改请求返回的第二认证信息获取请求；

根据所述第二认证信息获取请求，从所述第二终端获取第三密钥生成参数，并执行所述密钥生成算法得到第三私钥，利用所述第三私钥生成第二数字签名；还从所述第二终端获取所述OP标识；

将所述第二数字签名和所述OP标识发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第二数字签名认证通过后，根据所述第二公钥修改请求对所述第二公钥进行修改。

12.根据权利要求10所述的方法，其特征在于，所述eUICC位于所述第一终端中时，在所述将第一设备信息发送至所述远程管理平台之后，还包括：

向所述远程管理平台发送第一公钥修改请求，并接收所述远程管理平台根据所述第一公钥修改请求返回的第一认证信息获取请求；

根据所述第一认证信息获取请求，从所述第一终端获取第四密钥生成参数，并执行所述密钥生成算法得到第四私钥，利用所述第四私钥生成第三数字签名；还从所述第一终端获取所述OP标识；

将所述第三数字签名、所述OP标识和所述第一设备信息发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第三数字签名认证通过后，根据所述第一公钥修改请求对所述第二公钥进行修改。

13.根据权利要求8所述的方法，其特征在于，所述eUICC位于所述第一终端中，在接收所述远程管理平台发送的所述OP之后，还包括：

利用生成的所述第一私钥，对从所述远程管理平台接收的所述OP进行解密；

将所述第一私钥删除。

14.一种远程管理平台，其特征在于，包括：

通信连接单元，用于与第一终端的嵌入式通用集成电路卡eUICC建立连接；

信息获取单元，用于接收所述第一终端的eUICC发送的执行文件OP获取请求，向所述第一终端的eUICC发送认证证书获取请求；接收所述第一终端的eUICC返回的标识请求的OP的OP标识、以及利用第一私钥生成的第一数字签名，所述第一私钥是由所述第一终端的eUICC对从所述第一终端获取的第一密钥生成参数执行密钥生成算法后生成；

身份验证单元，用于根据所述OP标识查找第二公钥，并利用所述第二公钥与所述第一数字签名进行认证，所述第二公钥是从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成；

文件管理单元，用于在所述身份验证单元利用所述第二公钥与所述第一数字签名进行的认证通过时，将所述OP发送至所述第一终端的eUICC。

15.根据权利要求14所述的远程管理平台，其特征在于，

所述通信连接单元，还用于与所述第二终端的eUICC建立连接；

所述信息获取单元，还用于接收所述第二终端的eUICC发送的所述第二公钥、第二设备信息，所述第二设备信息用于标识所述第二终端；

所述文件管理单元，还用于记录所述第二公钥、向所述第二终端分配的所述OP标识以及所述第二设备信息之间的对应关系。

16.根据权利要求15所述的远程管理平台，其特征在于，

所述信息获取单元，所接收的所述OP标识携带在所述OP获取请求中，还用于接收所述第一终端的eUICC返回的第一设备信息，所述第一设备信息用于标识所述第一终端；

所述身份验证单元，还用于根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系，查找到对应的所述第二设备信息；若判断所述第二设备信息与所述第一设备信息不同，则指示所述信息获取单元执行所述向所述第一终端的eUICC发送认证证书获取请求。

17.根据权利要求16所述的远程管理平台，其特征在于，

所述文件管理单元，还用于记录所述OP标识与所述第一设备信息之间的对应关系，并删除所述第二设备信息。

18.根据权利要求15所述的远程管理平台，其特征在于，

所述信息获取单元，还用于接收第二终端的eUICC发送的第二公钥修改请求；根据所述第二公钥修改请求，向所述第二终端的eUICC发送第二认证信息获取请求；以及，接收所述第二终端的eUICC发送的第二认证信息，所述第二认证信息包括利用第三私钥生成的第二数字签名、以及所述OP标识；所述第三私钥是所述第二终端的eUICC对从所述第二终端获取的第三密钥生成参数执行所述密钥生成算法后生成；

所述身份认证单元，还用于利用所述第二公钥与所述第二数字签名进行认证通过时，根据所述第二公钥修改请求对所述第二公钥进行修改。

19.根据权利要求15所述的远程管理平台，其特征在于，

所述信息获取单元，还用于接收第一终端的eUICC发送的第一公钥修改请求；根据所述第一公钥修改请求，向所述第一终端的eUICC发送第一认证信息获取请求；以及，接收所述第一终端的eUICC发送的第一认证信息，所述第一认证信息包括利用第四私钥生成的第三数字签名、以及所述OP标识；所述第四私钥是所述第一终端的eUICC对从所述第一终端获取的第四密钥生成参数执行所述密钥生成算法后生成；

所述身份认证单元，还用于利用所述第二公钥与所述第三数字签名进行认证通过时，根据所述第一公钥修改请求对所述第二公钥进行修改。

20.根据权利要求14所述的远程管理平台，其特征在于，

所述文件管理单元，具体用于通过所述第二公钥对所述OP加密，并将加密后的所述OP发送至所述第一终端的eUICC。

21.一种嵌入式通用集成电路卡eUICC，其特征在于，包括：

通信连接单元，用于在所述eUICC位于第一终端中时，与远程管理平台建立连接；

信息管理单元，用于向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求；还从所述第一终端获取用于标识请求的所述OP的OP标识，并将身份认证单元生成的第一数字签名以及所述OP标识发送至所述远程管理平台；

身份认证单元，用于根据所述认证证书获取请求，从所述第一终端获取第一密钥生成参数，对所述第一密钥生成参数执行密钥生成算法生成第一私钥，利用所述第一私钥生成第一数字签名；

文件管理单元，用于接收所述远程管理平台发送的与所述OP标识对应的OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的；所述第二公钥是由所述远程管理平台从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成。

22.根据权利要求21所述的eUICC，其特征在于，

所述信息管理单元，还用于在所述eUICC位于第一终端之前，当所述eUICC位于第二终端中时，接收所述远程管理平台发送的密钥生成指示，从所述第二终端获取所述第二密钥生成参数、以及用于标识所述第二终端的第二设备信息；以及，将所述身份认证单元生成的所述第二公钥、所述第二设备信息发送至所述远程管理平台；

所述身份认证单元，还用于根据所述第二密钥生成参数执行所述密钥生成算法得到密钥对，所述密钥对包括所述第二公钥和第二私钥。

23.根据权利要求22所述的eUICC，其特征在于，

所述信息管理单元，还用于当所述eUICC位于所述第一终端中时，将所述OP标识携带在所述OP获取请求中发送至所述远程管理平台；还将第一设备信息发送至所述远程管理平台，所述第一设备信息用于标识所述第一终端，以使得所述远程管理平台根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系查找到对应的所述第二设备信息，并在确定所述第二设备信息与所述第一设备信息不同时发送所述认证证书获取请求。

24.根据权利要求22所述的eUICC，其特征在于，

所述信息管理单元，还用于当所述eUICC位于所述第二终端中时，在所述将第二设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第二公钥修改请求，并接收所述远程管理平台根据所述第二公钥修改请求返回的第二认证信息获取请求；以及，根据所述远程管理平台返回的所述第二认证信息获取请求，从第二终端获取所述OP标识；还用于将所述OP标识和所述身份认证单元生成的第二数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第二数字签名认证通过后，根据所述第二公钥修改请求对所述第二公钥进行修改；

所述身份认证单元，还用于根据所述第二认证信息获取请求，从所述第二终端获取第三密钥生成参数，并执行所述密钥生成算法生成第三私钥，利用所述第三私钥生成所述第二数字签名。

25.根据权利要求23所述的eUICC，其特征在于，

所述信息管理单元，还用于当所述eUICC位于所述第一终端中时，在所述将第一设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第一公钥修改请求，并接收所述远程管理平台根据所述第一公钥修改请求返回的第一认证信息获取请求；以及，根据所述远程管理平台返回的所述第一认证信息获取请求，从第一终端获取所述OP标识；还用于将所述OP标识和所述身份认证单元生成的第三数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第三数字签名认证通过后，根据所述第一公钥修改请求对所述第二公钥进行修改；

所述身份认证单元，还用于根据所述第一认证信息获取请求，从所述第一终端获取第四密钥生成参数，并执行所述密钥生成算法生成第四私钥，利用所述第四私钥生成所述第

三数字签名。

26.根据权利要求21所述的eUICC,其特征在于,

所述文件管理单元,还用于当所述eUICC位于所述第一终端中时,利用所述身份认证单元生成的所述第一私钥,对从所述远程管理平台接收的所述OP进行解密;

所述身份认证单元,还用于将所述第一私钥删除。

配置方法和设备

技术领域

[0001] 本发明涉及通信技术，尤其涉及一种配置方法和设备。

背景技术

[0002] 用户在使用终端(例如，手机)的过程中，可能会由于各种原因需要更换终端，例如终端损坏、终端被盗窃等，用户也可能会主动更换终端。对于使用通用集成电路卡(Universal Integrated Circuit Card，简称：UICC)的终端来说，由于运营商的文件(例如，执行文件(Operational Profile，简称：OP))封装在UICC中，用户在更换终端时只需要将第二终端使用的UICC插入到第一终端，即可利用所述OP继续使用运营商的网络。但是，对于使用嵌入式集成电路卡(Embedded Universal Integrated Circuit Card，简称：eUICC)的终端来说，由于每个终端的eUICC是嵌入到终端中的，而且运营商的文件(例如，OP)不再封装到eUICC中，用户在更换终端时，第一终端的eUICC必须重新向运营商的签约管理实体(Subscription Manager，简称：SM)请求OP并在该第一终端的eUICC上激活，才能继续使用运营商的网络；该签约管理实体可以称为远程管理平台。

[0003] 对于使用eUICC的终端，在终端更换过程中可能存在如下的安全隐患：例如，用户A与C运营商具有签约关系，该用户A为C运营商的合法用户，C运营商为用户A分配了用于使用C运营商网络的一些信息，可以称作认证信息；用户A在更换终端时，需要在再次请求OP时携带上述运营商分配的认证信息，C运营商就会根据该认证信息为用户A的新终端的eUICC下发OP。但是，假设存在未与C运营商签约的用户B，用户B可能会以某种方式获知了C运营商为用户A分配的认证信息，并利用该信息向C运营商请求OP；此时C运营商将无法识别出用户B为非合法用户，也会向用户B的终端下发OP，造成非合法用户非法使用C运营商的网络。

发明内容

[0004] 本发明提供一种配置方法和设备，以提高终端更换时的安全性。

[0005] 第一方面，提供一种配置方法，包括：

[0006] 与第一终端的嵌入式通用集成电路卡eUICC建立连接；

[0007] 接收所述第一终端的eUICC发送的执行文件OP获取请求，向所述第一终端的eUICC发送认证证书获取请求；

[0008] 接收所述第一终端的eUICC返回的标识请求的OP的OP标识、以及利用第一私钥生成的第一数字签名，所述第一私钥是由所述第一终端的eUICC对从所述第一终端获取的第一密钥生成参数执行密钥生成算法后生成；

[0009] 根据所述OP标识查找第二公钥，并利用所述第二公钥与所述第一数字签名进行认证，所述第二公钥是从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成；

[0010] 若利用所述第二公钥与所述第一数字签名进行的认证通过，将所述OP发送至所述第一终端的eUICC。

[0011] 结合第一方面，在第一种可能的实现方式中，在与所述第一终端的嵌入式通用集成电路卡eUICC建立连接之前，还包括：与所述第二终端的eUICC建立连接；接收所述第二终端的eUICC发送的所述第二公钥、第二设备信息，所述第二设备信息用于标识所述第二终端；记录所述第二公钥、向所述第二终端分配的所述OP标识以及所述第二设备信息之间的对应关系。

[0012] 结合第一方面、或者第一方面的第一种可能的实现方式，在所述向所述第一终端的eUICC发送认证证书获取请求之前，还包括：所述OP标识携带在所述OP获取请求中，还接收第一设备信息，所述第一设备信息用于标识所述第一终端；根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系，查找到对应的所述第二设备信息；若判断所述第二设备信息与所述第一设备信息不同，则执行所述向所述第一终端的eUICC发送认证证书获取请求。

[0013] 结合第一方面的第二种可能的实现方式，在第三种可能的实现方式中，在利用所述第二公钥与所述数字签名进行的认证通过之后，还包括：记录所述OP标识与所述第一设备信息之间的对应关系。

[0014] 结合第一方面的第一种可能的实现方式，在第四种可能的实现方式中，在记录所述第二公钥与所述OP标识之间的对应关系之后，还包括：接收所述第二终端的eUICC发送的第二公钥修改请求；根据所述第二公钥修改请求，向所述第二终端的eUICC发送第二认证信息获取请求；接收所述第二终端的eUICC发送的第二认证信息，所述第二认证信息包括利用第三私钥生成的第二数字签名、以及所述OP标识；所述第三私钥是所述第二终端的eUICC对从所述第二终端获取的第三密钥生成参数执行所述密钥生成算法后生成；利用所述第二公钥与所述第二数字签名进行认证，并在认证通过时，根据所述第二公钥修改请求对所述第二公钥进行修改。

[0015] 结合第一方面的第一种可能的实现方式，在第五种可能的实现方式中，在记录所述第二公钥与所述OP标识之间的对应关系之后，还包括：接收所述第一终端的eUICC发送的第一公钥修改请求；根据所述第一公钥修改请求，向所述第一终端的eUICC发送第一认证信息获取请求；接收所述第一终端的eUICC发送的第一认证信息，所述第一认证信息包括利用第四私钥生成的第三数字签名、以及所述OP标识；所述第四私钥是所述第一终端的eUICC对从所述第一终端获取的第四密钥生成参数执行所述密钥生成算法后生成；利用所述第二公钥与所述第三数字签名进行认证，并在认证通过时，根据所述第一公钥修改请求对所述第二公钥进行修改。

[0016] 结合第一方面，在第六种可能的实现方式中，所述将所述OP发送至所述第一终端的eUICC，包括：通过所述第二公钥对所述OP加密，并将加密后的所述OP发送至所述第一终端的eUICC。

[0017] 第二方面，提供一种配置方法，包括：

[0018] 嵌入式通用集成电路卡eUICC与远程管理平台建立连接，所述eUICC位于第一终端中；

[0019] 所述eUICC向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求；

[0020] 所述eUICC根据所述认证证书获取请求，从所述第一终端获取第一密钥生成参数，

对所述第一密钥生成参数执行密钥生成算法生成第一私钥，利用所述第一私钥生成第一数字签名；还从所述第一终端获取用于标识请求的OP的OP标识，将所述OP标识和所述第一数字签名发送至所述远程管理平台；

[0021] 所述eUICC接收所述远程管理平台发送的与所述OP标识对应的所述OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的；所述第二公钥是由所述远程管理平台从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成。

[0022] 结合第二方面，在第一种可能的实现方式中，在所述eUICC位于第一终端之前，当所述eUICC位于第二终端中时：所述eUICC还接收所述远程管理平台发送的密钥生成指示；所述eUICC根据所述密钥生成指示，从所述第二终端获取所述第二密钥生成参数、以及用于标识所述第二终端的第二设备信息；所述eUICC根据所述第二密钥生成参数执行所述密钥生成算法得到密钥对，所述密钥对包括所述第二公钥和第二私钥，并将所述第二公钥和所述第二设备信息发送至所述远程管理平台，以使得所述远程管理平台记录所述第二公钥、向所述第二终端分配的所述OP标识以及所述第二设备信息之间的对应关系。

[0023] 结合第二方面、或者第二方面的第一种可能的实现方式，在第二种可能的实现方式中，还包括：所述eUICC将第一设备信息发送至所述远程管理平台，所述第一设备信息用于标识所述第一终端；以使得所述远程管理平台根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系查找到对应的所述第二设备信息，并在确定所述第二设备信息与所述第一设备信息不同时发送所述认证证书获取请求。

[0024] 结合第二方面的第一种可能的实现方式，在第三种可能的实现方式中，所述eUICC位于所述第二终端中时，在所述将第二设备信息发送至所述远程管理平台之后，还包括：向所述远程管理平台发送第二公钥修改请求，并接收所述远程管理平台根据所述第二公钥修改请求返回的第二认证信息获取请求；根据所述第二认证信息获取请求，从所述第二终端获取第三密钥生成参数，并执行所述密钥生成算法得到第三私钥，利用所述第三私钥生成所述第二数字签名；还从所述第二终端获取所述OP标识；将所述第二数字签名和所述OP标识发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第二数字签名认证通过后，根据所述第二公钥修改请求对所述第二公钥进行修改。

[0025] 结合第二方面的第二种可能的实现方式，在第四种可能的实现方式中，所述eUICC位于所述第一终端中时，在所述将第一设备信息发送至所述远程管理平台之后，还包括：向所述远程管理平台发送第一公钥修改请求，并接收所述远程管理平台根据所述第一公钥修改请求返回的第一认证信息获取请求；根据所述第一认证信息获取请求，从所述第一终端获取第四密钥生成参数，并执行所述密钥生成算法得到第四私钥，利用所述第四私钥生成第三数字签名；还从所述第一终端获取所述OP标识；将所述第三数字签名、所述OP标识和所述第一设备信息发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第三数字签名认证通过后，根据所述第一公钥修改请求对所述第二公钥进行修改。

[0026] 结合第二方面，在第五种可能的实现方式中，所述eUICC位于所述第一终端中，在接收所述远程管理平台发送的所述OP之后，还包括：利用生成的所述密钥对中的所述第一私钥，对从所述远程管理平台接收的所述OP进行解密；将所述第一私钥删除。

[0027] 第三方面，提供一种远程管理平台，包括：

[0028] 通信连接单元，用于与第一终端的嵌入式通用集成电路卡eUICC建立连接；

[0029] 信息获取单元，用于接收所述第一终端的eUICC发送的执行文件OP获取请求，向所述第一终端的eUICC发送认证证书获取请求；接收所述第一终端的eUICC返回的标识请求的OP的OP标识、以及利用第一私钥生成的第一数字签名，所述第一私钥是由所述第一终端的eUICC对从所述第一终端获取的第一密钥生成参数执行密钥生成算法后生成；

[0030] 身份验证单元，用于根据所述OP标识查找第二公钥，并利用所述第二公钥与所述第一数字签名进行认证，所述第二公钥是从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成；

[0031] 文件管理单元，用于在所述身份验证单元利用所述第二公钥与所述第一数字签名进行的认证通过时，将所述OP发送至所述第一终端的eUICC。

[0032] 结合第三方面，在第一种可能的实现方式中，所述通信连接单元，还用于与所述第二终端的eUICC建立连接；所述信息获取单元，还用于接收所述第二终端的eUICC发送的所述第二公钥、第二设备信息，所述第二设备信息用于标识所述第二终端；所述文件管理单元，还用于记录所述第二公钥、向所述第二终端分配的所述OP标识以及所述第二设备信息之间的对应关系。

[0033] 结合第三方面、或者第三方面的第一种可能的实现方式，在第二种可能的实现方式中，所述信息获取单元，所接收的所述OP标识携带在所述OP获取请求中，还用于接收所述第一终端的eUICC返回的第一设备信息，所述第一设备信息用于标识所述第一终端；所述身份验证单元，还用于根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系，查找到对应的所述第二设备信息；若判断所述第二设备信息与所述第一设备信息不同，则指示所述信息获取单元执行所述向所述第一终端的eUICC发送认证证书获取请求。

[0034] 结合第三方面的第二种可能的实现方式，在第三种可能的实现方式中，所述文件管理单元，还用于记录所述OP标识与所述第一设备信息之间的对应关系，并删除所述第二设备信息。

[0035] 结合第三方面的第二种可能的实现方式，在第四种可能的实现方式中，所述信息获取单元，还用于接收第二终端的eUICC发送的第二公钥修改请求；根据所述第二公钥修改请求，向所述第二终端的eUICC发送第二认证信息获取请求；以及，接收所述第二终端的eUICC发送的第二认证信息，所述第二认证信息包括利用第三私钥生成的第二数字签名、以及所述OP标识；所述第三私钥是所述第二终端的eUICC对从所述第二终端获取的第三密钥生成参数执行所述密钥生成算法后生成；所述身份认证单元，还用于利用所述第二公钥与所述第二数字签名进行认证通过时，根据所述第二公钥修改请求对所述第二公钥进行修改。

[0036] 结合第三方面的第一种可能的实现方式，在第五种可能的实现方式中，所述信息获取单元，还用于接收第一终端的eUICC发送的第一公钥修改请求；根据所述第一公钥修改请求，向所述第一终端的eUICC发送第一认证信息获取请求；以及，接收所述第一终端的eUICC发送的第一认证信息，所述第一认证信息包括利用第四私钥生成的第三数字签名、以及所述OP标识；所述第四私钥是所述第一终端的eUICC对从所述第一终端获取的第四密钥

生成参数执行所述密钥生成算法后生成；所述身份认证单元，还用于利用所述第二公钥与所述第三数字签名进行认证通过时，根据所述第一公钥修改请求对所述第二公钥进行修改。

[0037] 结合第三方面，在第六种可能的实现方式中，所述文件管理单元，具体用于通过所述第二公钥对所述OP加密，并将加密后的所述OP发送至所述第一终端的eUICC。

[0038] 第四方面，提供一种嵌入式通用集成电路卡eUICC，包括：

[0039] 通信连接单元，用于在所述eUICC位于第一终端中时，与远程管理平台建立连接；

[0040] 信息管理单元，用于向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求；还从所述第一终端获取用于标识请求的所述OP的OP标识，并将身份认证单元生成的所述第一数字签名以及所述OP标识发送至所述远程管理平台；

[0041] 身份认证单元，用于根据所述认证证书获取请求，从所述第一终端获取第一密钥生成参数，对所述第一密钥生成参数执行密钥生成算法生成第一私钥，利用所述第一私钥生成第一数字签名；

[0042] 文件管理单元，用于接收所述远程管理平台发送的与所述OP标识对应的OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的；所述第二公钥是由所述远程管理平台从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成。

[0043] 结合第四方面，在第一种可能的实现方式中，所述信息管理单元，还用于在所述eUICC位于第一终端之前，当所述eUICC位于第二终端中时，接收所述远程管理平台发送的密钥生成指示，从所述第二终端获取所述第二密钥生成参数、以及用于标识所述第二终端的第二设备信息；以及，将所述身份认证单元生成的所述第二公钥、所述第二设备信息发送至所述远程管理平台；所述身份认证单元，还用于根据所述第二密钥生成参数执行所述密钥生成算法得到密钥对，所述密钥对包括所述第二公钥和第二私钥。

[0044] 结合第四方面、或者第四方面的第一种可能的实现方式，在第二种可能的实现方式中，所述信息管理单元，还用于当所述eUICC位于所述第一终端中时，将所述OP标识携带在所述OP获取请求中发送至所述远程管理平台；还将所述第一设备信息发送至所述远程管理平台，所述第一设备信息用于标识所述第一终端，以使得所述远程管理平台根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系查找到对应的所述第二设备信息，并在确定所述第二设备信息与所述第一设备信息不同时发送所述认证证书获取请求。

[0045] 结合第四方面的第一种可能的实现方式，在第三种可能的实现方式中，所述信息管理单元，还用于当所述eUICC位于所述第二终端中时，在所述将第二设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第二公钥修改请求，并接收所述远程管理平台根据所述第二公钥修改请求返回的第二认证信息获取请求；以及，根据所述远程管理平台返回的所述第二认证信息获取请求，从第二终端获取所述OP标识；还用于将所述OP标识和所述身份认证单元生成的所述第二数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第二数字签名认证通过后，根据所述第二公钥修改请求对所述第二公钥进行修改；所述身份认证单元，还用于根据所述第二认证信息获取请求，

从所述第二终端获取第三密钥生成参数，并执行所述密钥生成算法生成第三私钥，利用所述第三私钥生成所述第二数字签名。

[0046] 结合第四方面的第二种可能的实现方式，在第四种可能的实现方式中，所述信息管理单元，还用于当所述eUICC位于所述第一终端中时，在所述将第一设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第一公钥修改请求，并接收所述远程管理平台根据所述第一公钥修改请求返回的第一认证信息获取请求；以及，根据所述远程管理平台返回的所述第一认证信息获取请求，从第一终端获取所述OP标识；还用于将所述OP标识和所述身份认证单元生成的所述第三数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第三数字签名认证通过后，根据所述第一公钥修改请求对所述第二公钥进行修改；所述身份认证单元，还用于根据所述第一认证信息获取请求，从所述第一终端获取第四密钥生成参数，并执行所述密钥生成算法生成第四私钥，利用所述第四私钥生成所述第三数字签名。

[0047] 结合第四方面，在第五种可能的实现方式中，所述文件管理单元，还用于当所述eUICC位于所述第一终端中时，利用所述身份认证单元生成的所述第一私钥，对从所述远程管理平台接收的所述OP进行解密；所述身份认证单元，还用于将所述第一私钥删除。

[0048] 本发明提供的配置方法和设备的技术效果是：通过将根据从第二终端获取的密钥生成参数执行密钥生成算法得到的第二公钥，与根据从第一终端获取的密钥生成参数执行相同的密钥生成算法得到的第一私钥生成的数字签名进行认证，若认证通过则表明从第二终端获取的密钥生成参数与从第一终端获取的密钥生成参数相同，也即是表明第一终端和第二终端对应的是相同的用户，则将OP发送至第一终端的eUICC，从而避免了第一终端和第二终端对应的是不同用户的情况的发生，提高了终端更换时的安全性。

附图说明

[0049] 图1为本发明配置方法实施例的系统应用图；

[0050] 图2为本发明配置方法一实施例的流程示意图；

[0051] 图3为本发明配置方法另一实施例的流程示意图；

[0052] 图4为本发明配置方法又一实施例的第二终端处理信令图；

[0053] 图5为本发明配置方法又一实施例的第一终端处理信令图；

[0054] 图6为本发明配置方法又一实施例的公钥修改处理信令图；

[0055] 图7为本发明远程管理平台实施例的结构示意图；

[0056] 图8为本发明远程管理平台实施例的实体结构示意图；

[0057] 图9为本发明嵌入式通用集成电路卡eUICC实施例的结构示意图；

[0058] 图10为本发明嵌入式通用集成电路卡eUICC实施例的实体结构示意图。

具体实施方式

[0059] 首先对本发明实施例中涉及到的一些概念进行说明：本发明实施例针对的是安装有eUICC的第二终端(user equipment，简称：UE)和第一终端进行更换的过程进行说明，在该UE更换的过程中，涉及到了运营商侧的远程管理平台和UE，需要两者共同完成UE的更换处理。可以结合参见图1，图1为本发明配置方法实施例的系统应用图，该图中示出了eUICC、

UE、远程管理平台等之间的联系；其中，

[0060] eUICC：该eUICC不同于传统的通用集成电路卡(Universal Integrated Circuit Card，简称：UICC)，传统的UICC是运营商定制的，出厂时包含了运营商的相关信息，一旦出厂后，运营商信息不可变更；而eUICC是嵌入在UE中的UICC，该eUICC可以通过下载MNO(英文全称Mobile Network Operator，中文翻译为移动网络运营商)的相关数据例如执行文件OP的方式来更换MNO，只要下载某个MNO对应的执行文件OP，就可以通过该OP接入MNO的网络。在更换终端时，第一终端上的eUICC也需要重新向运营商请求OP并激活，才能继续使用MNO的网络。

[0061] eUICC与UE：该eUICC是嵌入式安装在UE中的，但是该eUICC不具有射频功能，其不能与外部设备进行信号的收发；比如，在连接MNO的网络时，是由eUICC指示UE使用OP接入MNO的网络；又例如，eUICC要获取某个MNO的OP，也是指示UE去向该MNO的远程管理平台发送OP请求的；因此，在后续的本发明实施例中提到的eUICC接入某MNO、与eUICC指示UE利用OP接入MNO，两者表达的意思实质上是相同的。

[0062] 远程管理平台：负责移动网络运营商MNO侧的签约管理；比如，eUICC要想接入某个MNO，需要获取并安装该MNO的执行文件OP，而该OP就是由远程管理平台负责准备并下发至eUICC的，即eUICC需要从远程管理平台下载该MNO的OP，才能使用该OP接入MNO的网络。

[0063] 该远程管理平台包括SM-SR和SM-DP；

[0064] SM-DP：执行文件OP是由该SM-DP负责分配的，用于OP的数据准备，该SM-DP具体可以根据eUICC的请求，为eUICC分配对应的OP，使得eUICC可以使用该OP接入该OP所属的MNO的网络；

[0065] SM-SR：eUICC不会直接与SM-DP通信，相关的请求都是发送至SM-SR，由SM-SR转发至SM-DP的，即该SM-SR负责文件的路由功能；例如，eUICC发送的OP请求是发送至SM-SR，再由SM-SR转发至SM-DP的；该SM-SR还可以将SM-DP分配的OP转发至eUICC。

[0066] 在上述说明的基础上，下面对本发明实施例的配置方法进行说明，其中，所述的配置方法指的是当安装eUICC的第二终端要更换为第一终端时，第一终端如何从MNO侧的远程管理平台重新请求OP，以及远程管理平台如何将OP发送至第一终端的eUICC的过程。

[0067] 实施例一

[0068] 图2为本发明配置方法一实施例的流程示意图，该方法是由远程管理平台执行，如图2所示，该方法可以包括：

[0069] 201、与第一终端的嵌入式通用集成电路卡eUICC建立连接；

[0070] 其中，远程管理平台即运营商侧的签约管理实体(Subscription Manager，简称：SM)，该SM与终端UE中的eUICC建立连接的过程，可以按照现有的连接流程执行，例如，eUICC可以通过其上的预备文件(Provisioning Profile，简称：PP)中的网络连接应用(Network Access Application，简称：NAA)连接某个可用网络，再通过该可用网络连接SM。

[0071] 所述的第一终端指的是，例如，用户的原终端损坏或不再使用，又新买了一个终端，则原终端称为第二终端，新买的终端称为第一终端，在本实施例中，用户要使用该第一终端重新接入运营商网络，并且仍然使用之前运营商分配的OP，本实施例中，该第一终端即是要向运营商的SM重新请求所述OP并激活。

[0072] 202、接收所述第一终端的eUICC发送的执行文件OP获取请求，并向所述第一终端

的eUICC发送认证证书获取请求；

[0073] 其中，本实施例的远程管理平台在接收到第一终端的eUICC发送的OP获取请求后，远程管理平台若判断出该OP获取请求是用户更换的终端发出的OP获取请，则不会根据该请求立即向第一终端返回OP，而是向第一终端的eUICC发送认证证书获取请求，需要对第一终端进行身份认证，认证通过后再下发OP。

[0074] 所述的远程管理平台判断第一终端是否是用户更换后的终端或者是用户更换前的原始终端，具体实施中可以采用多种方法，例如，远程管理平台可以请求第一终端提供其设备信息(可以称为第一设备信息)，并判断是否已经存储该设备信息，若存储则表明该第一终端是用户更换后的终端，否则表明该第一终端是用户更换前的原始终端。

[0075] 203、接收所述第一终端的eUICC返回的用于标识请求的所述OP的OP标识、以及利用第一私钥生成的第一数字签名；

[0076] 其中，第一终端的eUICC在接收到远程管理平台发送的认证证书获取请求之后，将从第一终端获取OP标识，该OP标识是远程管理平台分配给之前的第二终端的OP对应的OP标识，第一终端的eUICC将该OP标识返回给远程管理平台，是用于使得远程管理平台将该OP标识对应的之前分配的OP发送至该第一终端的eUICC。例如，该OP标识可以是终端所属的用户的电话号码，用户可以向第一终端输入该电话号码，第一终端将该号码发送至eUICC。

[0077] 此外，第一终端的eUICC还向远程管理平台发送利用第一私钥生成的第一数字签名；该第一私钥是由第一终端的eUICC从第一终端获取第一密钥生成参数，并利用该第一密钥生成参数执行密钥生成算法后生成。例如，所述的密钥生成算法可以是RSA(RSA公钥加密算法，是1977年由Ron Rivest、Adi Shamirh和LenAdleman在美国麻省理工学院开发的，RSA取名来自这三名开发者的名字)密钥生成算法，所述的第一密钥生成参数可以是某个阿拉伯数字(比如，256434)，或者是比较复杂的阿拉伯数字“12345”或者英文字母“abcd”等；所述的从第一终端获取第一密钥生成参数可以是第一终端的用户按动该第一终端的数字键输入所述第一密钥生成参数，该第一终端的用户是与运营商签约的合法用户。

[0078] 204、根据所述OP标识查找第二公钥，并利用所述第二公钥与所述第一数字签名进行认证；

[0079] 其中，所述第二公钥是远程管理平台从第二终端接收到，并且所述第二公钥是由第二终端的eUICC从第二终端获取第二密钥生成参数，对所述第二密钥生成参数执行密钥生成算法后生成。在第二终端的eUICC将第二公钥发送至远程管理平台之后，远程管理平台才为第二终端的eUICC发送分配的OP，并设定该OP对应的OP标识，所以远程管理平台侧在接收到第一终端发送的OP标识之前已经预先存储了上述的OP、OP标识以及第二公钥之间的对应关系的，远程管理平台能够根据从第一终端获取到的OP标识查找到对应的第二公钥。

[0080] 所述第二终端的eUICC采用的密钥生成算法与第一终端的eUICC采用的密钥生成算法是相同的，例如都是采用RSA算法；所述的第二终端的eUICC从第二终端获取第二密钥生成参数的方式也与第一终端的eUICC相同，例如都是通过用户按动终端上的功能键输入。

[0081] 205、若利用所述第二公钥与所述第一数字签名进行的认证通过，将所述OP标识对应的OP发送至所述第一终端的eUICC；

[0082] 其中，将所述第二公钥与第一数字签名进行认证，是利用不对称的密钥体系，将第二终端的eUICC生成的第二公钥，与第一终端的eUICC生成的第一私钥得到的第一数字签名

进行认证。例如，采用第二公钥对所述第一数字签名进行解密，判断是否能够正确解密；如果能够正确解密，则表明认证通过。

[0083] 所述的第二公钥是第二终端的eUICC利用从第二终端获取的第二密钥生成参数执行密钥生成算法后生成，所述的第一私钥是第一终端的eUICC利用从第一终端获取的第一密钥生成参数执行相同的密钥生成算法后生成；如果从第二终端获取的第二密钥生成参数与从第一终端获取的第一密钥生成参数相同，则认证就会通过。而密钥生成参数的获取方式都是终端所属的用户按动终端上的功能键输入的，比如，用户按动手机上的键盘输入阿拉伯数字“12345”或者英文字母“abcd”等，因此，如果第一终端获取的第一密钥生成参数与第二终端获取的第二密钥生成参数如果相同，则表明第一终端和第二终端对应的是同一个用户，比如都是运营商的合法签约用户(即用户A)。如果有另外一个非合法用户B想要使用第一终端接入运营商网络，则该非合法用户B是不能够知道用户A设定的密钥生成参数的，其在输入密钥生成参数时与用户A在第二终端输入的密钥生成参数不同，则运营商的远程管理平台就会认证失败，不会向该非合法用户B的终端发送OP，从而保证了终端更换时的安全性。

[0084] 实施例二

[0085] 图3为本发明配置方法另一实施例的流程示意图，该方法是由第一终端的eUICC执行，如图3所示，该方法可以包括：

[0086] 301、与远程管理平台建立连接；

[0087] 302、向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求；

[0088] 其中，第一终端的eUICC在与远程管理平台建立连接后，就会向该平台发送OP获取请求；本实施例中，远程管理平台在接收到第一终端的eUICC发送的该OP获取请求后，就会向第一终端的eUICC发送认证证书获取请求，请求验证第一终端的身份。

[0089] 需要说明的是，从远程管理平台侧，判断发送OP获取请求的某个终端是用户更换之后的新终端还是更换之前的旧终端，可以有多种方式；例如，在该平台与某个终端建立连接后，如果在接收到终端发送的OP获取请求之前，预先接收到了该终端发送的公钥，然后再接收到终端发送的OP获取请求，则表明该终端是第二终端，是首次为该终端所属的用户建立签约关系，首次为该用户使用的终端上的eUICC分配OP，则平台在接收到OP获取请求后，就会直接发送OP至第二终端。但是，如果平台在接收到终端发送的OP获取请求之前，没有接收到所述的公钥，而是在建立连接后直接接收到OP获取请求，则可以认为该终端是签约用户的第一终端，用户在执行终端的更换，此时，平台就需要验证第一终端的身份，主要是验证该第一终端所属的用户是否与第二终端是同一个用户，以防止非签约用户的非法使用，在验证通过后再向第一终端下发之前分配给第二终端的OP。

[0090] 又例如，还可以按照上面已经提到的，通过判断是否已经存储有该终端的设备信息，来判断该终端是户更换之后的新终端还是更换之前的旧终端。

[0091] 303、根据所述认证证书获取请求，从第一终端获取第一密钥生成参数，对所述第一密钥生成参数执行密钥生成算法生成第一私钥，利用所述第一私钥生成第一数字签名；还从所述第一终端获取用于标识请求的所述OP的OP标识，将所述OP标识和所述第一数字签名发送至所述远程管理平台；

[0092] 其中，第一终端的eUICC在接收到远程管理平台发送的认证证书获取请求后，将开始获取一些用于认证的信息；例如，从第一终端获取第一密钥生成参数，对该第一密钥生成参数执行密钥生成算法生成密钥对，该密钥对包括第一公钥和第一私钥，并利用所述第一私钥生成第一数字签名；以及获取OP标识，并将该OP标识和第一数字签名一并发送至远程管理平台。所述的第一数字签名是用于远程管理平台验证第一终端身份的，所述的OP标识是用于查找第二公钥，以及在认证通过后查找要发送的OP的。

[0093] 304、接收所述远程管理平台发送的与所述OP标识对应的OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的；

[0094] 其中，第一终端的eUICC接收远程管理平台发送的用第二公钥加密的OP，所述OP是利用第二公钥加密的；该平台是在利用第二公钥和第一数字签名认证通过后发送的。所述第二公钥是由所述远程管理平台从第二终端接收到，并且是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成；所述认证通过表明从所述第二终端获取的第二密钥生成参数与从所述第一终端获取的第一密钥生成参数相同。

[0095] 实施例三

[0096] 为了使得对配置方法的说明更加清楚，本实施例将按照终端更换时的具体实施过程，分别对第二终端和第一终端要执行的处理流程进行详细描述；所述的第二终端是用户在更换终端之前使用的终端，所述的第一终端是用户在更换终端之后使用的终端。其中，在下面的各流程的描述中，各步骤之间的执行顺序并不局限于此，在具体实施时可以根据实际情况进行变更。

[0097] 图4为本发明配置方法又一实施例的第二终端处理信令图，该图4主要描述用户在使用之前的第二终端时需要做哪些处理；其中，远程管理平台即为SM，在如下的描述中将以SM来说明；并且，该SM包括SM-SR和SM-DP，在流程的描述中将直接以SM来说明，本领域技术可以理解，实际上是由SM-SR将相关的消息在UE和SM-DP之间进行转发的，主要是由SM-DP执行对相关消息的处理。如图4所示，包括：

[0098] 401、第二终端激活eUICC的PP文件中的应用NAA；

[0099] 其中，用户购买当前的第二终端时，激活该第二终端中的eUICC，选择默认的profile(即预备文件PP#0)，激活PP#0中的默认应用NAA0。

[0100] 402、第二终端的eUICC通过NAA连接网络；

[0101] 其中，NAA0能够自动搜索可接入的网络并连接该网络，使得当前第二终端的eUICC通过NAA0连接该网络。

[0102] 403、第二终端的eUICC与SM建立连接；

[0103] 经过上面的几个步骤，当前第二终端的eUICC通过已连接的网络连接到SM。

[0104] 404、第二终端的eUICC向SM发送OP获取请求；

[0105] 405、SM向第二终端的eUICC返回OP获取请求确认；

[0106] 406、第二终端的eUICC请求第二终端提供密钥生成参数；

[0107] 其中，所述的第二终端的eUICC在接收到上述SM返回的OP获取请求确认后，相当于获得了密钥生成指示，将开始执行密钥生成算法，请求第二终端提供密钥生成参数。

[0108] 其中，该密钥生成参数可以称为第二密钥生成参数。

[0109] 407、第二终端提供密钥生成参数至eUICC；

[0110] 其中，所述的第二密钥生成参数是在执行密钥生成算法获取密钥对时所需要的参数；其可以是一个或多个阿拉伯数字，该阿拉伯数字是用户通过第二终端输入的；例如，可以是用户按动第二终端上的数字键输入，或者也可以在一个符号集内设计一个对应关系，某个符号对应某个数字，将用户在符号集范围内输入的参数转化为阿拉伯数字。

[0111] 用户应当记住自己输入的第二密钥生成参数，因为在后续更换终端时，第一终端上也需要用户输入与该第二密钥生成参数相同的第一密钥生成参数，第一终端才能通过SM的认证，第一终端的eUICC才能获取到OP。

[0112] 408、第二终端的eUICC根据所述第二密钥生成参数执行密钥生成算法得到密钥对，包括第二公钥和第二私钥；

[0113] 409、第二终端的eUICC将第二公钥和第二设备信息发送至SM，(携带第二设备信息)；

[0114] 其中，所述的第二设备信息的获取过程是：第二终端的eUICC请求第二终端提供第二设备信息，所述第二设备信息用于标识所述第二终端；例如，该第二设备信息可以是国际移动设备身份码(International Mobile Equipment Identity，简称：IMEI)信息。第二终端将第二设备信息发送给eUICC。

[0115] 可选的，具体实施中，第二设备信息也可以通过某个单独的消息发送至SM。

[0116] 410、SM记录第二公钥与所述第二设备信息之间的对应关系；

[0117] 其中，SM在接收到第二终端的eUICC发送的第二公钥与第二设备信息后，在SM-DP上存储该第二公钥和第二设备信息，并记录两者的对应关系，在设备信息不变的条件下，可以利用该第二设备信息查找到对应的第二公钥。

[0118] 411、SM将OP发送给第二终端的eUICC；

[0119] 其中，SM向第二终端的eUICC发送OP时，还分配所述OP对应的OP标识(该OP标识即OP ID List)，该OP标识例如是用户的一个或多个电话号码。该SM在将OP发送给第二终端的eUICC时，可以是使用在410中获取到的第二公钥对OP进行加密，以保证OP的安全传输。

[0120] 412、第二终端的eUICC安装并激活收到的OP；

[0121] 其中，第二终端的eUICC在接收到SM发送的OP时，将利用在407中生成的第二私钥对所述OP进行解密；并在解密后安装OP，激活OP#1。

[0122] 413、第二终端的eUICC通过OP连接到运营商MNO的网络；

[0123] 其中，第二终端的eUICC可以是通过OP#1上的NAA#1连接到移动网络运营商(Mobile Network Operator，简称：MNO)的网络。

[0124] 414、第二终端的eUICC将第二私钥删除；

[0125] 其中，第二终端的eUICC在使用第二私钥解密OP后，将彻底删除该第二私钥信息，以防止当前的第二终端被盗用带来的安全隐患问题；比如，如果当前的第二终端被盗用，并且没有删除第二私钥，则盗用者就可能利用该第二私钥生成数字签名，这样SM侧就会对被盗用的第二终端认证通过，导致非合法用户通过该被盗终端使用运营商网络。

[0126] 415、SM记录第二公钥、OP、OP标识以及第二设备信息之间的对应关系；

[0127] 其中，当前的第二终端在接入运营商的网络后，SM-DP在其服务器上对应第二终端

信息的存储单元上，存储OP以及OP标识信息及其对应关系；并且，SM还存储之前接收到的第二公钥、第二设备信息与所述的OP以及OP标识之间的对应关系，SM在与第二终端的eUICC之间在进行通信交互时，会携带OP标识、设备信息、或者eUICC标识信息等，所以SM是能够获知接收到的第二公钥、第二设备信息与OP以及OP标识均是对应于同一个终端的。

[0128] 图5为本发明配置方法又一实施例的第一终端处理信令图，该图5主要描述用户在使用第一终端时需要做哪些处理，第一终端如何重新从SM获取到OP；需要说明的是：第一终端的eUICC与第二终端的eUICC是同一个eUICC。如图5所示，包括：

[0129] 501、第一终端激活eUICC的PP文件中的应用NAA；

[0130] 502、第一终端的eUICC通过NAA连接可用网络；

[0131] 503、第一终端的eUICC与SM建立连接；

[0132] 504、第一终端的eUICC请求第一终端提供OP标识；

[0133] 其中，所述的OP标识是SM之前为第二终端的eUICC分配的OP对应的标识，例如是用户的电话号码；

[0134] 505、第一终端将OP标识发送至eUICC；

[0135] 506、第一终端的eUICC向SM发送OP获取请求，携带OP标识和第一设备信息；

[0136] 其中，所述的第一设备信息的获取是，在第一终端与SM建立连接后，SM可以请求第一终端的eUICC提供第一终端的设备信息；第一终端的eUICC请求第一终端提供用于标识第一终端的第一设备信息；例如，所述的第一设备信息是IMEI信息。第一终端将第一设备信息发送给eUICC。

[0137] 当然，可选的，具体实施中，该第一设备信息也可以单独发送至SM。

[0138] 需要说明的是，该步骤与图4所示中的410步骤是完全不同的，本实施例的OP获取请求在发送时，还同时发送了OP标识和第一设备信息，而在410中并没有携带这些信息

[0139] 507、SM向第一终端的eUICC发送认证证书获取请求；

[0140] 其中，SM在接收到上述的OP标识和第一设备信息后，将根据OP标识、以及之前存储的OP标识与第二设备信息之间的对应关系，查找到对应的第二设备信息。如果该第二设备信息与接收到的第一设备信息不同，则表明第一终端是新终端即用户更换后的终端，则SM执行向第一终端的eUICC发送认证证书获取请求，以对该第一终端的身份进行认证，实际上是要认证更换前的第二终端与该第一终端是否是同一个用户，以避免非合法用户的使用。

[0141] 508、第一终端的eUICC自动运行密钥生成算法；

[0142] 其中，如上面图4所述的，第二终端执行密钥生成算法可以是接收到用户的触发后执行，而本实施例的第一终端处理中，eUICC可以在接收到SM发送的认证证书获取请求后，根据该请求自动运行密钥生成算法。

[0143] 例如，所述的密钥生成算法是RSA算法。

[0144] 509、第一终端的eUICC请求第一终端提供密钥生成参数，该参数是用于生成密钥对所使用的；

[0145] 该密钥生成参数可以称为第一密钥生成参数；

[0146] 510、第一终端提供密钥生成参数至eUICC；

[0147] 其中，该第一终端提供第一密钥生成参数的方式与第二终端是相同的，例如，都是由用户按动终端上的功能键进行阿拉伯数字的输入；如果第一终端和第二终端对应的是同

一个用户，则第一终端提供的第一密钥生成参数和第二终端提供的第二密钥生成参数是相同的，如果第一终端和第二终端对应的不是同一个用户，则通常第一终端的用户是不知道第二终端用户设定的密钥生成参数的，第一终端提供的第一密钥生成参数和第二终端提供的第二密钥生成参数不相同。

[0148] 511、第一终端的eUICC根据所述第一密钥生成参数执行密钥生成算法后生成密钥对，包括第一公钥和第一私钥；

[0149] 其中，第一终端和第二终端采用的密钥生成算法是相同的，例如都是RSA算法；如果第一终端和第二终端的密钥生成参数相同，则执行密钥生成算法得到的密钥对也是相同的，即所述的密钥对第一公钥和第一私钥，与上面的密钥对第二公钥和第二私钥实际上是相同的，本发明实施例只是以第一、第二来区分该密钥对是由不同的终端或者在不同的流程中生成。如果第一终端和第二终端的密钥生成参数不同，则执行密钥生成算法后生成的密钥对也是不同的。

[0150] 512、第一终端的eUICC利用第一私钥生成数字签名；

[0151] 其中，第一终端的eUICC利用509中得到的第一私钥生成第一数字签名。

[0152] 513、第一终端的eUICC将第一数字签名发送至SM；

[0153] 514、SM根据OP标识查找第二公钥，并利用第二公钥与第一数字签名进行认证；

[0154] 其中，所述的第二公钥是SM在图4所示的实施例中，从第二终端接收到的，并且是由第二终端的eUICC对从第二终端获取的第二密钥生成参数执行与第一终端相同的密钥生成算法后生成。若利用第二公钥与第一数字签名进行认证通过，则表明从所述第二终端获取的第二密钥生成参数与从所述第一终端获取的第一密钥生成参数相同，也即表明新第二终端对应的是同一个用户；否则，表明从所述第二终端获取的第二密钥生成参数与从所述第一终端获取的第一密钥生成参数不同，也即表明第一终端和第二终端对应的不是同一个用户。

[0155] 如果认证成功，则继续执行517；否则，如果认证失败，可以重复505-516步骤，给第一终端3次认证机会，假如三次机会之后仍然认证失败，则SM可以向第一终端的eUICC返回认证失败消息，拒绝向其提供请求的OP。

[0156] 515、SM通知MNO停止和第二终端的签约关系；

[0157] 其中，相当于告知MNO用户不再使用第二终端，为用户分配的OP也不再是与第二终端的第二设备信息对应。

[0158] 516、MNO向SM发送与第二终端停止签约关系的确认消息；

[0159] 517、MNO停止与第二终端的签约关系；

[0160] 518、SM将记录OP标识与第一设备信息之间的对应关系，并删除第二设备信息；

[0161] 其中，由于用户进行了终端的更换，SM中的SM-DP也需要将之前记录的第二设备信息替换为第一设备信息；实际上此时SM中存储的是第一设备信息、第二公钥、OP和OP标识之间的对应关系。

[0162] 519、SM将OP标识对应的OP发送至第一终端的eUICC；

[0163] 其中，SM在发送OP时，可以利用从第二终端获取的第二公钥加密该OP，以保证OP传输过程中的安全性。

[0164] 520、第一终端的eUICC利用第一私钥解密OP；

[0165] 其中，第一终端的eUICC可以利用509中生成的第一私钥解密OP。

[0166] 521、第一终端的eUICC安装并激活OP；

[0167] 522、第一终端的eUICC通过OP连接到运营商MNO的网络；

[0168] 523、第一终端的eUICC将第一私钥删除；

[0169] 其中，第一终端的eUICC在接入网络成功后，将彻底删除第一私钥，以防止终端被盗用带来的安全隐患问题。

[0170] 此外，SM侧存储的公钥也是能够修改的，图6为本发明配置方法又一实施例的公钥修改处理信令图，该图6主要描述用户在使用第一终端时如果要修改SM存储的公钥，需要做哪些处理；如图6所示，包括：

[0171] 601、第一终端的eUICC接收到公钥修改指示；

[0172] 具体实施时，例如可以在第一终端上设置一个用于用户选择触发的选项“公钥修改”，如果用户选择该选项，表明用户想要进行公钥修改，终端可以向第一终端的eUICC发送公钥修改指示。

[0173] 602、第一终端的eUICC向SM发送第一公钥修改请求；

[0174] 603、SM向第一终端的eUICC发送第一认证信息获取请求；

[0175] 其中，SM在接收到第一公钥修改请求时，得知用户想要修改公钥，则SM将向第一终端的eUICC发送第一认证信息获取请求，需要首先对第一终端进行认证。

[0176] 604、第一终端的eUICC执行密钥生成算法；

[0177] 其中，第一终端的eUICC在接收到SM发送的第一认证信息获取请求时，将自动运行密钥生成算法例如RSA算法。

[0178] 605、第一终端的eUICC请求第一终端提供密钥生成参数；

[0179] 其中，该密钥生成参数可以称为第四密钥生成参数；第一终端的eUICC在执行密钥生成算法的过程中，会需要获取用于生成密钥对的第四密钥生成参数。

[0180] 606、第一终端提供密钥生成参数至eUICC；

[0181] 其中，密钥生成参数的提供方式与前述的方式相同，不再赘述；并且这里获取的密钥生成参数与第一终端在修改公钥前提供的参数相同。

[0182] 607、第一终端的eUICC执行密钥生成算法得到密钥对；

[0183] 其中，所生成的密钥对包括第四公钥和第四私钥；

[0184] 同理，这里的“第四”只是用于表示该密钥对是在与之前不同的流程中生成的。

[0185] 608、第一终端的eUICC利用第四私钥生成第三数字签名；

[0186] 609、第一终端的eUICC请求第一终端提供OP标识；

[0187] 610、第一终端提供OP标识至eUICC；

[0188] 611、第一终端的eUICC将第三数字签名、OP标识发送至SM，可以携带第一设备信息；

[0189] 其中，第一设备信息的获取是，第一终端的eUICC请求第一终端提供用于标识第一终端的第一设备信息；第一终端将第一设备信息发送给eUICC。

[0190] 612、SM通过第二公钥与所述第三数字签名进行认证；

[0191] 其中，SM可以通过OP标识查找到对应的第二公钥，并利用第二公钥来验证第三数字签名，以检验第一终端的合法性。其中，所述的第二公钥与OP、OP标识和第一设备信息都

是具有对应关系的。

[0192] 具体实施中，也可以给第一终端3次认证机会，如果第一终端认证失败，则重复执行603-612。如果认证通过，则继续执行613，否则，SM可以拒绝第一终端的公钥修改请求，向第一终端的eUICC返回认证失败消息。

[0193] 613、SM与第一终端交互进行第二公钥的修改；

[0194] 其中，SM根据所述第一公钥修改请求对所述第二公钥进行修改，具体的公钥修改过程，例如是，用户在第一终端输入期望更改为的新密钥生成参数，第一终端的eUICC利用新密钥生成参数执行密钥生成算法生成新公钥，并将新公钥发送至SM，SM将接收到的新公钥进行存储。

[0195] 上述的公钥修改的流程也同样适用于旧终端(即第二终端)，第二终端修改公钥的方式与上述相同，不再赘述。比如，在记录所述第二公钥与所述第二设备信息之间的对应关系之后，接收所述第二终端的eUICC发送的第二公钥修改请求；根据所述第二公钥修改请求，向所述第二终端的eUICC发送第二认证信息获取请求；接收所述第二终端的eUICC发送的第二认证信息，所述第二认证信息包括利用第三私钥生成的第二数字签名、以及用于标识所述第二终端的第二设备信息；所述第三私钥是所述第二终端的eUICC对从所述第二终端获取的第三密钥生成参数执行所述密钥生成算法后生成；利用所述第二公钥与所述第二数字签名进行认证，并在认证通过时，根据所述第二公钥修改请求对所述第二公钥进行修改。

[0196] 需要说明的是，如果上述修改公钥的过程，是在终端已经执行了前面描述的接收SM分配的OP、激活并安装OP，连接到运营商网络、删除私钥等之后执行的，则此时修改公钥后，为了安全性考虑，在修改公钥的处理流程中再次生成的私钥，应该被删除；如果上述修改公钥的过程进行时，上述的终端接收SM分配的OP、激活并安装OP等过程还未执行，则终端中存储私钥不能被删除，因为还需要用于后续接收到的OP的解密。

[0197] 实施例四

[0198] 图7为本发明远程管理平台实施例的结构示意图，该远程管理平台可以是SM，并且如下所述的远程管理平台中的各功能单元，通常可以是在SM中的SM-DP中设置，或者是由SM-DP和SM-SR共同实现该功能单元。

[0199] 如图7所示，本实施例的远程管理平台包括：通信连接单元71、信息获取单元72、身份验证单元73和文件管理单元74；其中，

[0200] 通信连接单元71，用于与第一终端的eUICC建立连接；

[0201] 信息获取单元72，用于接收所述第一终端的eUICC发送的执行文件OP获取请求，向所述第一终端的eUICC发送认证证书获取请求；接收所述第一终端的eUICC返回的标识请求的OP的OP标识、以及利用第一私钥生成的第一数字签名，所述第一私钥是由所述第一终端的eUICC对从所述第一终端获取的第一密钥生成参数执行密钥生成算法后生成；

[0202] 身份验证单元73，用于根据所述OP标识查找第二公钥，并利用所述第二公钥与所述第一数字签名进行认证，所述第二公钥是从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成；；

[0203] 文件管理单元74，用于在所述身份验证单元利用所述第二公钥与所述第一数字签

名进行的认证通过时，将所述OP发送至所述第一终端的eUICC。

[0204] 进一步的，所述通信连接单元71，还用于与所述第二终端的eUICC建立连接；

[0205] 所述信息获取单元72，还用于接收所述第二终端的eUICC发送的所述第二公钥、第二设备信息，所述第二设备信息用于标识所述第二终端；

[0206] 所述文件管理单元74，还用于记录所述第二公钥、向所述第二终端分配的OP标识以及所述第二设备信息之间的对应关系。

[0207] 进一步的，所述信息获取单元72，所接收的所述OP标识携带在所述OP获取请求中，还用于接收所述第一终端的eUICC返回的第一设备信息，所述第一设备信息用于标识所述第一终端；

[0208] 所述身份验证单元73，还用于根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系，查找到对应的所述第二设备信息；若判断所述第二设备信息与所述第一设备信息不同，则指示所述信息获取单元执行所述向所述第一终端的eUICC发送认证证书获取请求。

[0209] 进一步的，所述文件管理单元74，还用于记录所述OP标识与所述第一设备信息之间的对应关系，并删除所述第二设备信息。

[0210] 进一步的，所述信息获取单元72，还用于接收第二终端的eUICC发送的第二公钥修改请求；根据所述第二公钥修改请求，向所述第二终端的eUICC发送第二认证信息获取请求；以及，接收所述第二终端的eUICC发送的第二认证信息，所述第二认证信息包括利用所述第三私钥生成的第二数字签名、以及OP标识；所述第三私钥是所述第二终端的eUICC对从所述第二终端获取的第三密钥生成参数执行所述密钥生成算法后生成；

[0211] 所述身份认证单元73，还用于利用所述第二公钥与所述第二数字签名进行认证通过时，根据所述第二公钥修改请求对所述第二公钥进行修改。

[0212] 进一步的，所述信息获取单元72，还用于接收第一终端的eUICC发送的第一公钥修改请求；根据所述第一公钥修改请求，向所述第一终端的eUICC发送第一认证信息获取请求；以及，接收所述第一终端的eUICC发送的第一认证信息，所述第一认证信息包括利用第四私钥生成的第三数字签名、以及OP标识；所述第四私钥是所述第一终端的eUICC对从所述第一终端获取的第四密钥生成参数执行所述密钥生成算法后生成；

[0213] 所述身份认证单元73，还用于利用所述第二公钥与所述第三数字签名进行认证通过时，根据所述第一公钥修改请求对所述第二公钥进行修改。

[0214] 进一步的，所述文件管理单元74，具体用于通过所述第二公钥对所述OP加密，并将加密后的所述OP发送至所述第一终端的eUICC。

[0215] 图8为本发明远程管理平台实施例的实体结构示意图，如图8所示，该远程管理平台包括：处理器81和存储器82；

[0216] 所述存储器82，用于存储第二公钥，所述第二公钥是从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成；

[0217] 所述处理器81，用于与第一终端的嵌入式通用集成电路卡eUICC建立连接；接收所述第一终端的eUICC发送的执行文件OP获取请求，向所述第一终端的eUICC发送认证证书获取请求；接收所述第一终端的eUICC返回的用于标识请求的所述OP的OP标识、以及利用第一

私钥生成的第一数字签名，所述第一私钥是由所述第一终端的eUICC对从所述第一终端获取的第一密钥生成参数执行密钥生成算法后生成；根据所述OP标识查找第二公钥，并利用所述第二公钥与所述第一数字签名进行认证；在认证通过时，将所述OP发送至所述第一终端的eUICC。

[0218] 进一步的，所述处理器81，还用于与所述第二终端的eUICC建立连接；接收所述第二终端的eUICC发送的所述第二公钥、第二设备信息，所述第二设备信息用于标识所述第二终端；以及记录所述第二公钥、向所述第二终端分配的OP标识以及所述第二设备信息之间的对应关系。

[0219] 进一步的，所述处理器81，还用于所接收的所述OP标识携带在所述OP获取请求中，还用于接收所述第一终端的eUICC返回的第一设备信息，所述第一设备信息用于标识所述第一终端；根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系，查找到对应的所述第二设备信息；若判断所述第二设备信息与所述第一设备信息不同，则指示所述信息获取单元执行所述向所述第一终端的eUICC发送认证证书获取请求。

[0220] 进一步的，所述处理器81，还用于所述OP标识与所述第一设备信息之间的对应关系，并删除所述第二设备信息。

[0221] 进一步的，所述处理器81，还用于接收第二终端的eUICC发送的第二公钥修改请求；根据所述第二公钥修改请求，向所述第二终端的eUICC发送第二认证信息获取请求；以及，接收所述第二终端的eUICC发送的第二认证信息，所述第二认证信息包括利用第三私钥生成的第二数字签名、以及OP标识；所述第三私钥是所述第二终端的eUICC对从所述第二终端获取的第三密钥生成参数执行所述密钥生成算法后生成；利用所述第二公钥与所述第二数字签名进行认证通过时，根据所述第二公钥修改请求对所述第二公钥进行修改。

[0222] 进一步的，所述处理器81，还用于接收第一终端的eUICC发送的第一公钥修改请求；根据所述第一公钥修改请求，向所述第一终端的eUICC发送第一认证信息获取请求；以及，接收所述第一终端的eUICC发送的第一认证信息，所述第一认证信息包括利用第四私钥生成的第三数字签名、以及OP标识；所述第四私钥是所述第一终端的eUICC对从所述第一终端获取的第四密钥生成参数执行所述密钥生成算法后生成；利用所述第二公钥与所述第三数字签名进行认证通过时，根据第一公钥修改请求对所述第二公钥进行修改。

[0223] 进一步的，所述处理器81，还用于通过所述第二公钥对所述OP加密，并将加密后的所述OP发送至所述第一终端的eUICC。

[0224] 实施例五

[0225] 图9为本发明嵌入式通用集成电路卡eUICC实施例的结构示意图，如图9所示，该eUICC可以包括：通信连接单元91、信息管理单元92、身份认证单元93和文件管理单元94；其中，

[0226] 通信连接单元91，用于在所述eUICC位于第一终端中时，与远程管理平台建立连接；

[0227] 信息管理单元92，用于向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求；还从所述第一终端获取用于标识请求的所述OP的OP标识，并将身份认证单元生成的所述第一数字签名以及所述OP标识发送至所述远程管理平台；

[0228] 身份认证单元93，用于根据所述认证证书获取请求，从所述第一终端获取第一密钥生成参数，对所述第一密钥生成参数执行密钥生成算法生成第一私钥，利用所述第一私钥生成第一数字签名；

[0229] 文件管理单元94，用于接收所述远程管理平台发送的与所述OP标识对应的OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的；所述第二公钥是由所述远程管理平台从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的与所述第一密钥生成参数相同的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成。

[0230] 进一步的，所述信息管理单元92，还用于在所述eUICC位于第一终端之前，当所述eUICC位于第二终端中时，接收所述远程管理平台发送的密钥生成指示，从所述第二终端获取所述第二密钥生成参数、以及用于标识所述第二终端的第二设备信息；以及，将所述身份认证单元生成的所述第二公钥、所述第二设备信息发送至所述远程管理平台；

[0231] 所述身份认证单元93，还用于根据所述第二密钥生成参数执行所述密钥生成算法得到密钥对，所述密钥对包括所述第二公钥和第二私钥。

[0232] 进一步的，所述信息管理单元92，还用于当所述eUICC位于所述第二终端中时，将所述OP标识携带在所述OP获取请求中发送至所述远程管理平台；还将所述第一设备信息发送至所述远程管理平台，所述第一设备信息用于标识所述第一终端，以使得所述远程管理平台根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系查找到对应的所述第二设备信息，并在确定所述第二设备信息与所述第一设备信息不同时发送所述认证证书获取请求。

[0233] 进一步的，所述信息管理单元92，还用于当所述eUICC位于所述第二终端中时，在所述将第二设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第二公钥修改请求，并接收所述远程管理平台根据所述第二公钥修改请求返回的第二认证信息获取请求；以及，根据所述远程管理平台返回的所述第二认证信息获取请求，从第二终端获取OP标识；还用于将所述OP标识和所述身份认证单元生成的所述第二数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第二数字签名认证通过后，根据所述第二公钥修改请求对所述第二公钥进行修改；

[0234] 所述身份认证单元93，还用于根据所述第二认证信息获取请求，从所述第二终端获取第三密钥生成参数，并执行所述密钥生成算法生成第三私钥，利用所述第三私钥生成所述第二数字签名。

[0235] 进一步的，所述信息管理单元92，还用于当所述eUICC位于所述第一终端中时，在所述将第一设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第一公钥修改请求，并接收所述远程管理平台根据所述第一公钥修改请求返回的第一认证信息获取请求；以及，根据所述远程管理平台返回的所述第一认证信息获取请求，从第一终端获取OP标识；还用于将所述OP标识和所述身份认证单元生成的所述第三数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第三数字签名认证通过后，根据所述第一公钥修改请求对所述第二公钥进行修改；

[0236] 所述身份认证单元93，还用于根据所述第一认证信息获取请求，从所述第一终端获取第四密钥生成参数，并执行所述密钥生成算法生成第四私钥，利用所述第四私钥生成

所述第三数字签名。

[0237] 进一步的，所述文件管理单元94，还用于当所述eUICC位于所述第一终端中时，利用所述身份认证单元生成的第一私钥，对从所述远程管理平台接收的所述OP进行解密；

[0238] 所述身份认证单元93，还用于将所述第一私钥删除。

[0239] 图10为本发明嵌入式通用集成电路卡eUICC实施例的实体结构示意图，如图10所示，该eUICC包括：处理器1001和存储器1002；

[0240] 所述处理器1001，用于在所述eUICC位于第一终端中时，与远程管理平台建立连接；向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求；还从所述第一终端获取用于标识请求的所述OP的OP标识，并将身份认证单元生成的所述第一数字签名以及所述OP标识发送至所述远程管理平台；根据所述认证证书获取请求，从第一终端获取第一密钥生成参数，对所述第一密钥生成参数执行密钥生成算法生成第一私钥，利用所述第一私钥生成第一数字签名；接收所述远程管理平台发送的与所述OP标识对应的OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的；所述第二公钥是由所述远程管理平台从第二终端接收到，所述第二公钥是由所述第二终端的eUICC对从所述第二终端获取的第二密钥生成参数执行与所述第一终端相同的密钥生成算法后生成；

[0241] 所述存储器1002，用于存储所述OP。

[0242] 进一步的，所述处理器1001，还用于在所述eUICC位于第一终端之前，当所述eUICC位于第二终端中时，接收所述远程管理平台发送的密钥生成指示，从所述第二终端获取所述第二密钥生成参数、以及用于标识所述第二终端的第二设备信息；以及，将所述身份认证单元生成的所述第二公钥、所述第二设备信息发送至所述远程管理平台；根据所述第二密钥生成参数执行所述密钥生成算法得到密钥对，所述密钥对包括所述第二公钥和第二私钥。

[0243] 进一步的，所述处理器1001，还用于当所述eUICC位于所述第二终端中时，将所述OP标识携带在所述OP获取请求中发送至所述远程管理平台；还将所述第一设备信息发送至所述远程管理平台，所述第一设备信息用于标识所述第一终端，以使得所述远程管理平台根据所述OP标识、以及所述OP标识与所述第二设备信息之间的对应关系查找到对应的所述第二设备信息，并在确定所述第二设备信息与第一设备信息不同时发送所述认证证书获取请求。

[0244] 进一步的，所述处理器1001，还用于当所述eUICC位于所述第二终端中时，在所述将第二设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第二公钥修改请求，并接收所述远程管理平台根据所述第二公钥修改请求返回的第二认证信息获取请求；以及，根据所述远程管理平台返回的所述第二认证信息获取请求，从第二终端获取OP标识；还用于将所述OP标识和所述身份认证单元生成的所述第二数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第二数字签名认证通过后，根据所述第二公钥修改请求对所述第二公钥进行修改；根据所述第二认证信息获取请求，从所述第二终端获取第三密钥生成参数，并执行所述密钥生成算法生成第三私钥，利用所述第三私钥生成所述第二数字签名。

[0245] 进一步的，所述处理器1001，还用于当所述eUICC位于所述第一终端中时，在所述

将第一设备信息发送至所述远程管理平台之后，向所述远程管理平台发送第一公钥修改请求，并接收所述远程管理平台根据所述第一公钥修改请求返回的第一认证信息获取请求；以及，根据所述远程管理平台返回的所述第一认证信息获取请求，从第一终端获取OP标识；还用于将所述OP标识和所述身份认证单元生成的所述第三数字签名发送至所述远程管理平台，以使得所述远程管理平台在利用所述第二公钥与所述第三数字签名认证通过后，根据所述第一公钥修改请求对所述第二公钥进行修改；根据所述第一认证信息获取请求，从所述第一终端获取第四密钥生成参数，并执行所述密钥生成算法生成第四私钥，利用所述第四私钥生成所述第三数字签名。

[0246] 进一步的，所述处理器1001，还用于当所述eUICC位于所述第一终端中时，利用生成的第一私钥，对从所述远程管理平台接收的所述OP进行解密；将所述第一私钥删除。

[0247] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0248] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

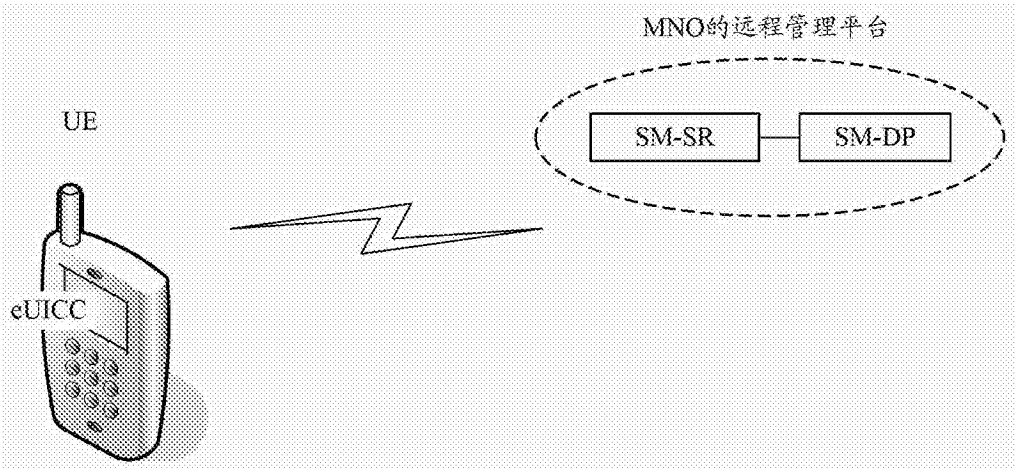

MNO的远程管理平台
UE
SM-SR
SM-DP
eUICC

图1

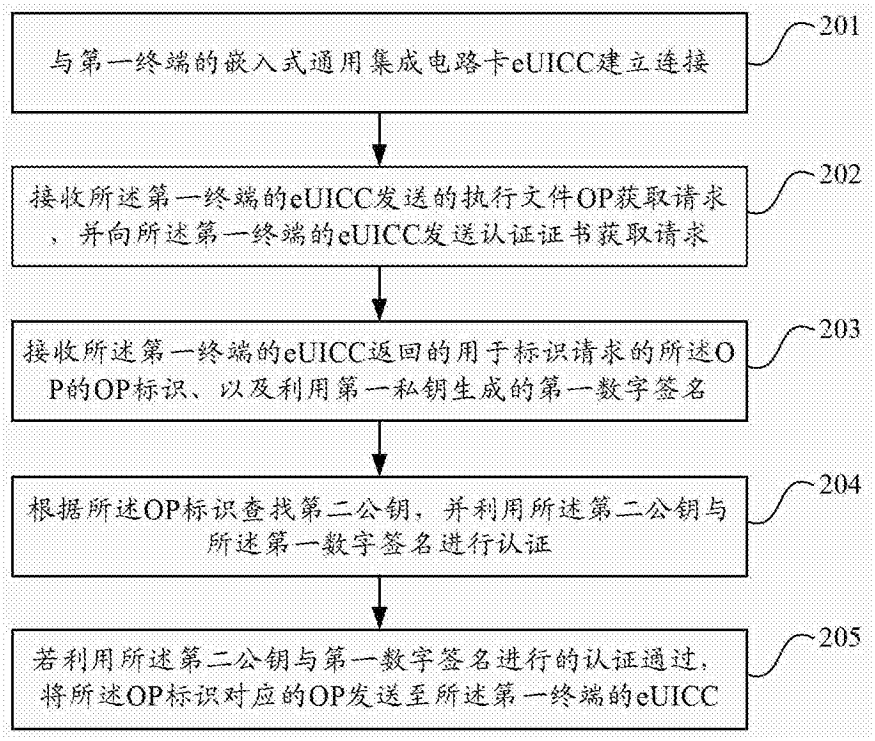

与第一终端的嵌入式通用集成电路卡eUICC建立连接
201
接收所述第一终端的eUICC发送的执行文件OP获取请求，并向所述第一终端的eUICC发送认证证书获取请求
202
接收所述第一终端的eUICC返回的用于标识请求的所述OP的OP标识、以及利用第一私钥生成的第一数字签名
203
根据所述OP标识查找第二公钥，并利用所述第二公钥与所述第一数字签名进行认证
204
若利用所述第二公钥与第一数字签名进行的认证通过，将所述OP标识对应的OP发送至所述第一终端的eUICC
205

图2

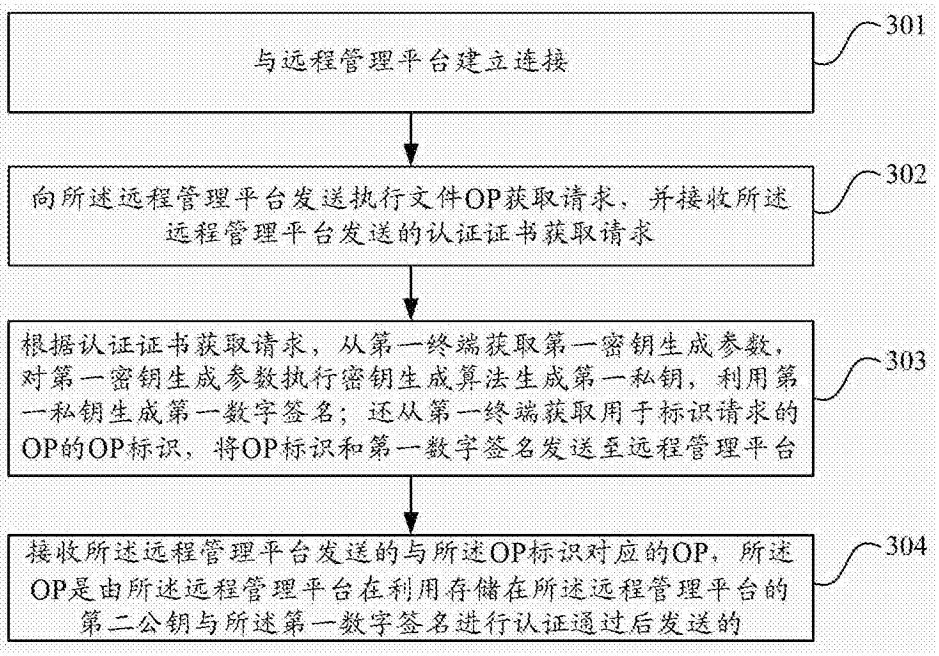

与远程管理平台建立连接
301
向所述远程管理平台发送执行文件OP获取请求，并接收所述远程管理平台发送的认证证书获取请求
302
根据认证证书获取请求，从第一终端获取第一密钥生成参数，对第一密钥生成参数执行密钥生成算法生成第一私钥，利用第一私钥生成第一数字签名；还从第一终端获取用于标识请求的OP的OP标识，将OP标识和第一数字签名发送至远程管理平台
303
接收所述远程管理平台发送的与所述OP标识对应的OP，所述OP是由所述远程管理平台在利用存储在所述远程管理平台的第二公钥与所述第一数字签名进行认证通过后发送的
304

图3

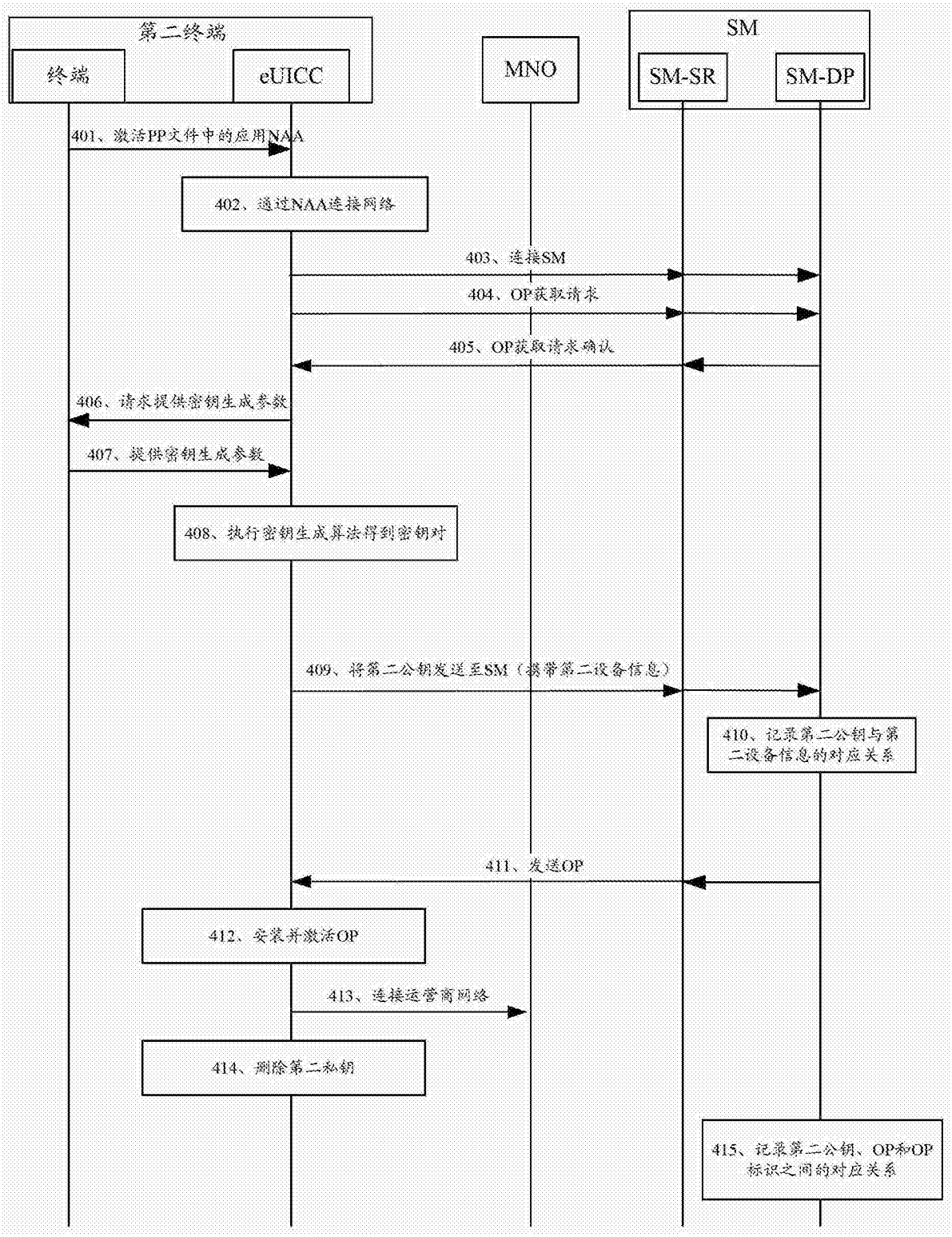

第二终端
终端
eUICC
MNO
SM
SM-SR
SM-DP
401、激活PP文件中的应用NAA
402、通过NAA连接网络
403、连接SM
404、OP获取请求
405、OP获取请求确认
406、请求提供密钥生成参数
407、提供密钥生成参数
408、执行密钥生成算法得到密钥对
409、将第二公钥发送至SM（携带第二设备信息）
410、记录第二公钥与第二设备信息的对应关系
411、发送OP
412、安装并激活OP
413、连接运营商网络
414、删除第二私钥
415、记录第二公钥、OP和OP标识之间的对应关系

图4

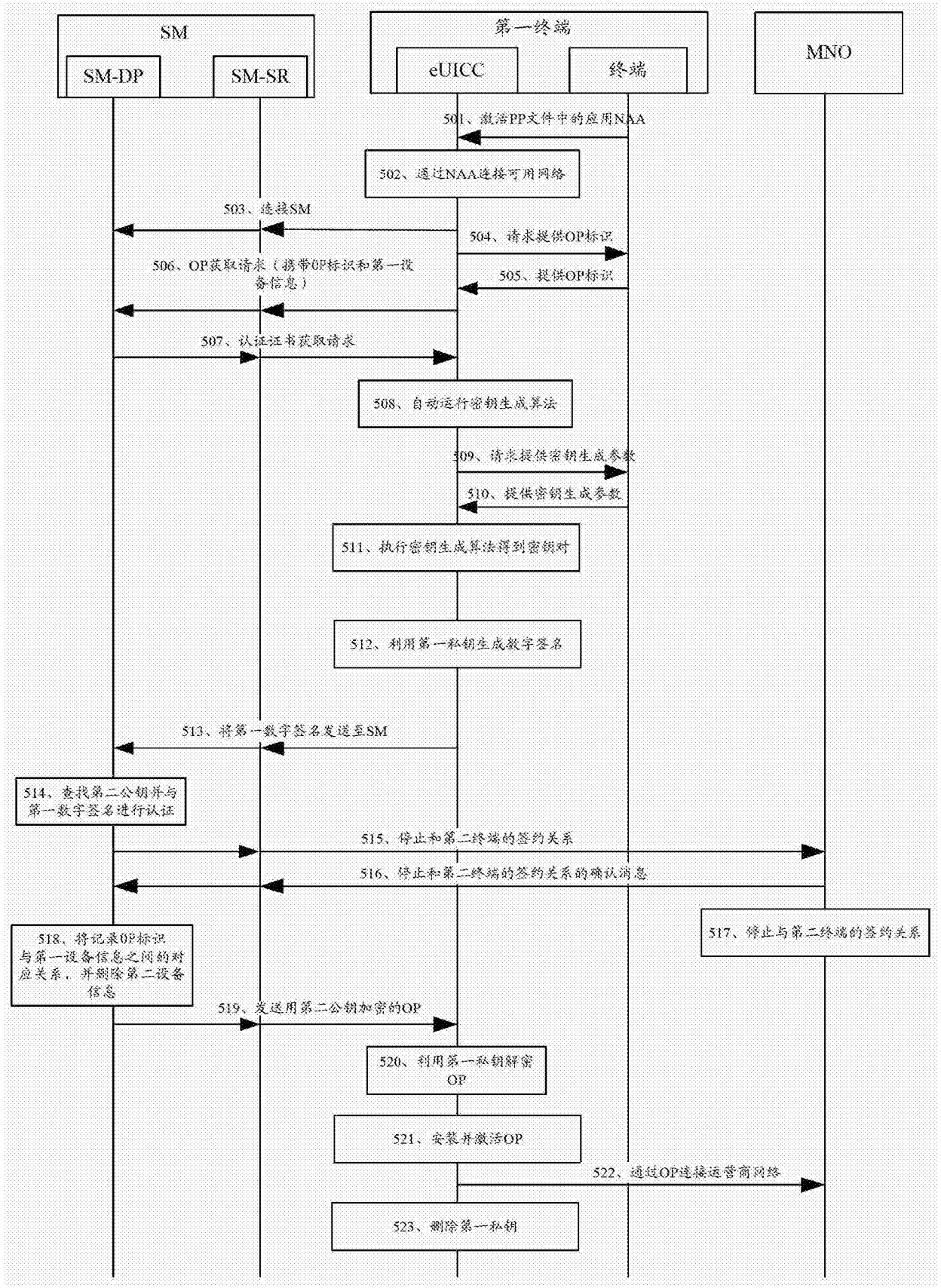

SM
SM-DP
SM-SR
第一终端
eUICC
终端
MNO
501、激活PP文件中的应用NAA
502、通过NAA连接可用网络
503、连接SM
504、请求提供OP标识
505、提供OP标识
506、OP获取请求（携带OP标识和第一设备信息）
507、认证证书获取请求
508、自动运行密钥生成算法
509、请求提供密钥生成参数
510、提供密钥生成参数
511、执行密钥生成算法得到密钥对
512、利用第一私钥生成数字签名
513、将第一数字签名发送至SM
514、查找第二公钥并与第一数字签名进行认证
515、停止和第二终端的签约关系
516、停止和第二终端的签约关系的确认消息
517、停止与第二终端的签约关系
518、将记录OP标识与第一设备信息之间的对应关系，并删除第二设备信息
519、发送用第二公钥加密的OP
520、利用第一私钥解密OP
521、安装并激活OP
522、通过OP连接运营商网络
523、删除第一私钥

图5

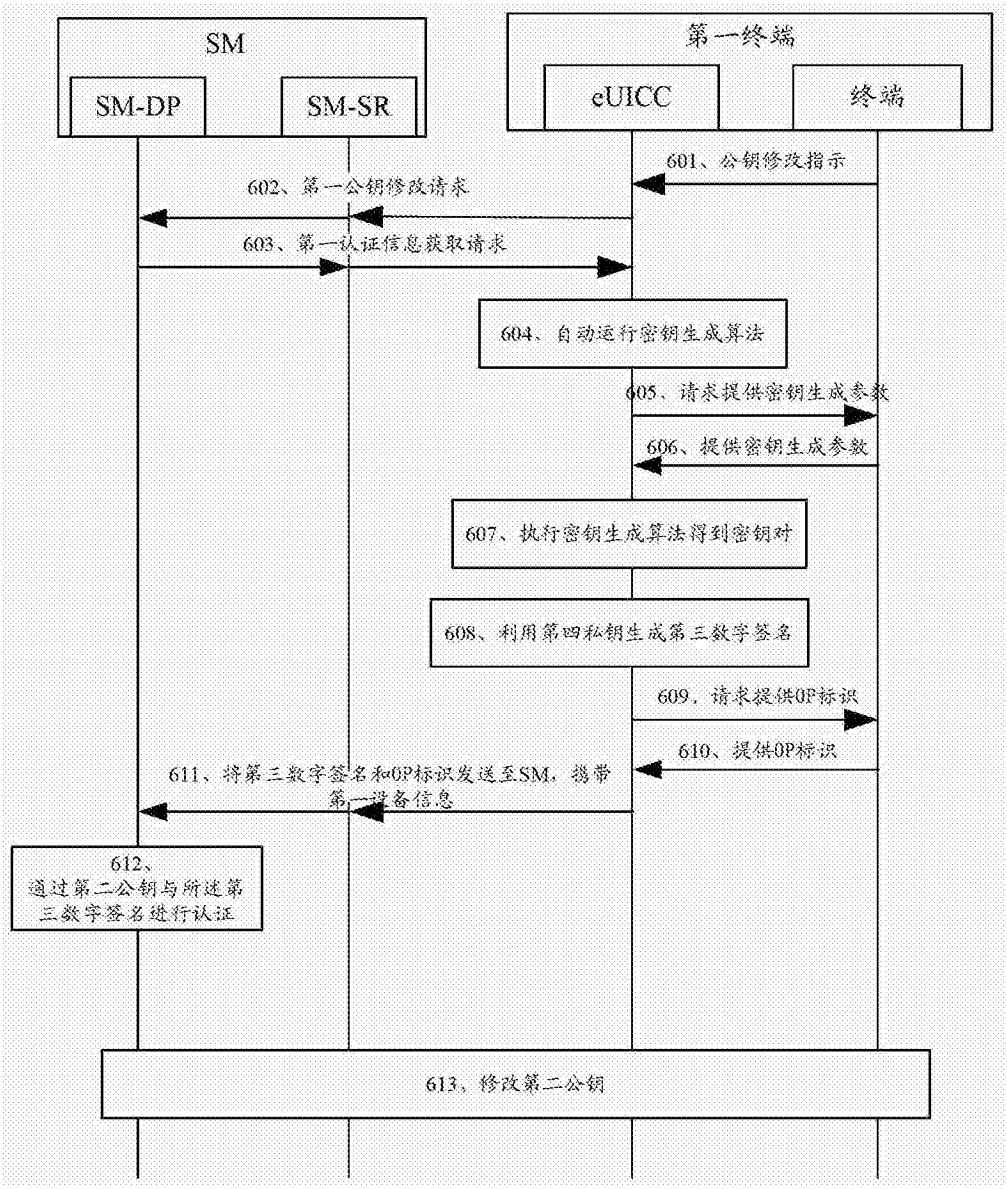

SM
SM-DP
SM-SR
第一终端
eUICC
终端
601、公钥修改指示
602、第一公钥修改请求
603、第一认证信息获取请求
604、自动运行密钥生成算法
605、请求提供密钥生成参数
606、提供密钥生成参数
607、执行密钥生成算法得到密钥对
608、利用第四私钥生成第三数字签名
609、请求提供OP标识
610、提供OP标识
611、将第三数字签名和OP标识发送至SM，携带第一设备信息
612、通过第二公钥与所述第三数字签名进行认证
613、修改第二公钥

图6

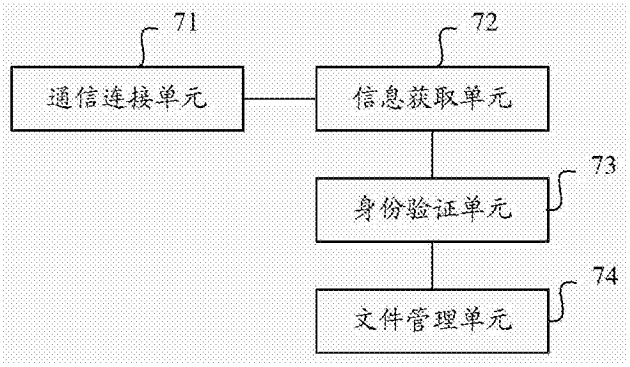

71
72
通信连接单元
信息获取单元
73
身份验证单元
74
文件管理单元

图7

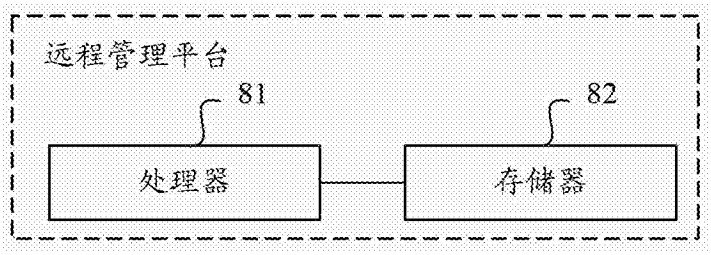

远程管理平台
81
82
处理器
存储器

图8

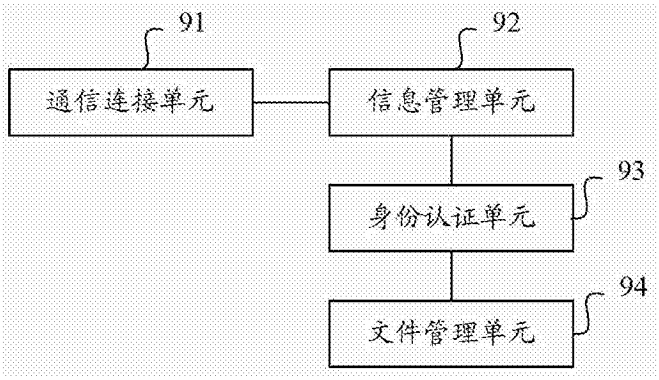

91
92
通信连接单元
信息管理单元
93
身份认证单元
94
文件管理单元

图9

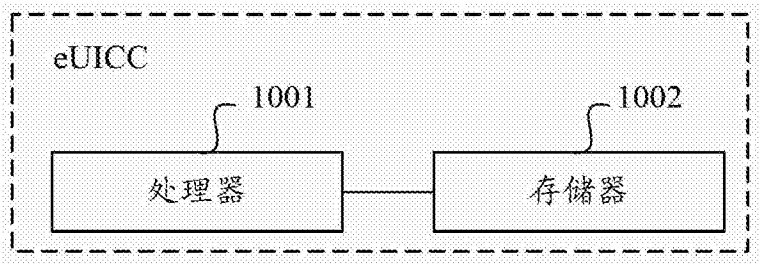

eUICC
1001
1002
处理器
存储器

图10