(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 108040044 B
(45)授权公告日 2019.06.07

(21)申请号 201711283521.2

(22)申请日 2017.12.07

(65)同一申请的已公布的文献号
申请公布号 CN 108040044 A

(43)申请公布日 2018.05.15

(73)专利权人 恒宝股份有限公司
地址 212355 江苏省镇江市丹阳市横塘工业区

(72)发明人 何碧波

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/44(2013.01)

审查员 郑红萍

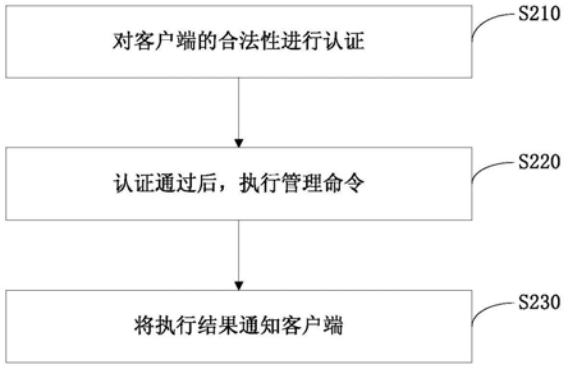
权利要求书1页 说明书6页 附图3页

(54)发明名称

一种实现eSIM卡安全认证的管理方法及系统

(57)摘要

本发明涉及移动通信领域，尤其涉及一种实现eSIM卡安全认证的管理方法及系统。所述方法包括：对客户端的合法性进行认证，认证通过后，执行管理命令，将执行结果通知所述客户端。采用本发明的技术方案，在设备中安装的LPA客户端，通过了认证或者规则检查后，才能得到访问eSIM卡中安全文件的许可，避免了未经许可直接操作eSIM卡带来的风险。



CN 108040044 B

1.一种实现eSIM卡安全认证的管理方法,其特征在于,包括:

对客户端的合法性进行认证;

认证通过后,执行管理命令;

将执行结果通知所述客户端;

所述对客户端的合法性认证具体包括:

eSIM卡使用持有由eSIM生产厂商签发的CA证书或EUM证书验证来自客户端认证请求中的客户端证书的合法性,从合法的客户端证书中提取公钥,验证认证请求中的签名值的正确性。

2.如权利要求1所述的管理方法,其特征在于,所述eSIM卡持有eSIM证书、EUM证书、eSIM私钥、CA证书和共享信息。

3.如权利要求2所述的管理方法,所述对客户端的合法性进行认证,具体包括:

验证来自所述客户端的认证请求,当认证请求合法时,生成临时非对称密钥,然后协商产生会话密钥,根据所述会话密钥建立安全通道。

4.如权利要求2所述的管理方法,其特征在于,所述eSIM卡中预置所述客户端的访问规则。

5.如权利要求4所述的管理方法,所述对客户端的合法性进行认证,具体包括:

接收来自所述客户端的唯一标识码和/或哈希值,读取eSIM卡中预置的所述访问规则,当检查所述客户端的唯一标识码和/或哈希值与所述访问规则中的唯一标识码和/或哈希值匹配时,认证客户端合法性通过。

6.一种eSIM卡,包括如下部件:

第一安全元件,对客户端的合法性进行认证;

处理元件,用于在所述第一安全元件对所述客户端的认证合法性通过后,执行管理命令,将执行结果通知客户端;

所述第一安全元件具体用于:eSIM卡使用持有由eSIM生产厂商签发的CA证书或EUM证书验证来自客户端认证请求中的客户端证书的合法性,从合法的客户端证书中提取公钥,验证认证请求中的签名值的正确性。

7.如权利要求6所述的eSIM卡,所述第一安全元件具体用于,验证来自所述客户端的认证请求,当认证请求合法时,生成临时非对称密钥,然后协商生成会话密钥,根据所述eSIM会话密钥建立安全通道。

8.如权利要求6所述的eSIM卡,所述第一安全元件还用于预置所述客户端的访问规则,所述访问规则包括访问eSIM卡的客户端应用的唯一标识码和/或哈希值。

9.一种实现eSIM卡安全认证的管理系统,其特征在于,包括:

如权利要求6-8之一所述的eSIM卡;

客户端,包括通信元件,用于在合法性认证通过后,向所述eSIM卡发送管理命令,并接收来自所述eSIM卡的执行结果。

10.如权利要求9所述的管理系统,其特征在于,

所述客户端还包括第二安全元件,用于认证来自所述eSIM卡的认证请求,还用于生成客户端会话密钥,使用所述客户端会话密钥建立安全通道。

一种实现eSIM卡安全认证的管理方法及系统

技术领域

[0001] 本发明涉及移动通信技术领域，尤其涉及一种实现eSIM卡安全认证的管理方法及系统。

背景技术

[0002] 在物联网领域，eSIM卡作为设备入网的关键元件，是设备提供接入运营商网络和进行身份认证媒介，同时，也给用户提供选择运营商以及服务的便利。用户通过设备操作系统里或手机中的LPA客户端(Local Profile Assistant，以下简称客户端)，不仅可以选择下载新的运营商的数据文件profile(profile包含文件系统、入网密钥参数、辅助安全域、应用等数据)，还可以对本地已有的数据文件profile进行激活、去激活和删除操作。LPA客户端在设备操作系统或手机中并不是唯一的，不同的运营商、卡商和第三方应用开发者都可以开发自己的LPA客户端。

[0003] 然而，现有的客户端与eSIM卡之间的数据交互却没有任何安全保障。客户端作为运行在设备操作系统上的一个应用软件，可以通过设备提供的硬件接口访问eSIM卡，但是设备提供的硬件接口，并没有认证客户端的合法性，只要客户端能安装在设备的操作系统中即可。因此，会产生如下问题：

[0004] (1)如果安装了多个来自不同运营商的客户端，如：联通客户端和移动客户端，联通客户端下载了数据文件profile之后，移动客户端可以无条件将该数据文件profile删除。

[0005] (2)如果安装了恶意客户端，则eSIM卡内的数据文件profile可以被该客户端无限制访问。

发明内容

[0006] 为克服现有技术中存在的不足，本发明提供了一种实现eSIM卡安全认证的管理方法。

[0007] 本发明采用的技术方案是：一种实现eSIM卡安全认证的管理方法，包括：

[0008] 对客户端的合法性进行认证；

[0009] 认证通过后，执行管理命令；

[0010] 将执行结果通知所述客户端。

[0011] 所述eSIM卡持有eSIM证书、EUM证书、eSIM私钥、CA证书和共享信息。

[0012] 所述对客户端的合法性进行认证，具体包括：

[0013] 验证来自所述客户端的认证请求，当认证请求合法时，生成临时非对称密钥，然后协商产生会话密钥，根据所述会话密钥建立安全通道。

[0014] 所述eSIM卡中预置所述客户端的访问规则。

[0015] 所述对客户端的合法性进行认证，具体包括：

[0016] 接收来自所述客户端的唯一标识码和哈希值，读取eSIM卡中预置的所述访问规

则，当检查所述客户端的唯一标识码和哈希值与所述访问规则中的唯一标识码和哈希值匹配时，认证客户端合法性通过。

[0017] 一种eSIM卡，包括如下部件：

[0018] 第一安全元件，对客户端的合法性进行认证；

[0019] 处理元件，用于在所述第一安全元件对所述客户端的认证合法性通过后，执行管理命令，将执行结果通知客户端。

[0020] 所述第一安全元件具体用于，验证来自所述客户端的认证请求，当认证请求合法时，生成临时非对称密钥，然后协商生成会话密钥，根据所述eSIM会话密钥建立安全通道。

[0021] 所述第一安全元件还用于预置所述客户端的访问规则，所述访问规则包括访问eSIM卡的客户端应用的唯一标识码和哈希值。

[0022] 本发明还提供一种实现eSIM卡安全认证的管理系统，包括：上述eSIM卡；

[0023] 客户端，包括通信元件，用于在合法性认证通过后，向所述eSIM卡发送管理命令，并接收来自所述eSIM卡的执行结果。

[0024] 所述客户端还包括第二安全元件，用于认证来自所述eSIM卡的认证请求，还用于生成客户端会话密钥，使用所述客户端会话密钥建立安全通道。

[0025] 本发明达到的有益效果是：采用本发明的技术方案，在设备中安装的LPA客户端在通过了认证或者规则检查后，才能得到访问eSIM卡中安全文件的许可，避免了未经许可直接操作eSIM卡的风险。

附图说明

[0026] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述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申请中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

[0027] 图1为现有技术操作系统模块交互示意图；

[0028] 图2为本发明实施例一提供的一种实现eSIM卡安全认证的管理方法流程图；

[0029] 图3为本发明提供的eSIM卡与客户端进行双向认证流程图；

[0030] 图4为本发明提供的一种认证客户端合法性的方法流程图；

[0031] 图5为本发明实施例二提供的一种实现eSIM卡安全认证的管理系统元件图。

具体实施方式

[0032] 本申请提供一种实现eSIM卡安全认证的管理方法及系统，实现在客户端与eSIM卡之间的安全认证。

[0033] 为了使本领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于本申请保护的范围。

[0034] 如图1所示，现有的运营商入网系统包括运营商服务器110、移动设备120、客户端130和eSIM卡140。具体的，在请求下载数据文件profile时，eSIM卡将持有证书通过客户端

传输给运营商服务器110,运营商服务器110和eSIM卡140完成双向认证,建立安全通道,保证数据文件profile下载过程的安全。然而,对profile的管理操作,没有所述双向认证和建立安全通道。显然,现有系统保障了运营商服务器110和eSIM卡140之间的profile下载的安全性,但是没有考虑eSIM卡与客户端之间的管理操作的安全性。

[0035] 为了解决现有的eSIM卡管理系统运营过程中eSIM卡与客户端之间的安全性问题,本发明提供了在eSIM卡与客户端之间进行管理操作的安全认证的方法,包括:认证方法和限制访问方式,通过以下实施例进行详细说明。

[0036] 实施例一

[0037] 下面结合附图2进一步介绍本申请的一种实现eSIM卡安全认证的管理方法,包括如下步骤:

[0038] 步骤S210:对客户端的合法性进行认证;

[0039] 本实施例中,对客户端的合法性进行认证具体通过下述两种方式之一进行认证,具体为:

[0040] 认证方法一、eSIM卡与客户端进行双向认证,认证通过后,生成会话密钥,建立安全通道,客户端合法性认证通过;

[0041] 发行eSIM卡时,eSIM卡中持有由eSIM生产厂商(EUM)签发的eSIM证书CERT_ESIM、eSIM私钥、EUM证书、CA证书,以及共享信息sharedinfo,所述共享信息包括生成的密钥类型、长度、eID等;

[0042] 在客户端中持有由CA机构或者eSIM生产厂商签发的客户端证书CERT_LPA、客户端私钥、CA证书或EUM证书以及共享信息sharedinfo。

[0043] 参见图3,具体的,eSIM卡与客户端进行双向认证包括如下子步骤:

[0044] 步骤S310:eSIM卡在收到来自客户端的认证请求后,验证认证请求是否合法,是则执行步骤S320,否则返回错误;

[0045] 客户端发起的认证请求为:

[0046] initAuthentication{

[0047] transactionID,

[0048] CERT_LPA,

[0049] signature1;}

[0050] 其中,transactionID为16字节的随机数、CERT_LPA为客户端持有的客户端证书、signature1为使用客户端证书的私钥对transactionID和客户端证书计算得到的签名值,保证传输过程中数据不被篡改。

[0051] 验证认证请求是否合法,具体包括:eSIM卡使用持有由eSIM生产厂商签发的CA证书或EUM证书验证认证请求中的客户端证书CERT_LPA的合法性,如果合法,则从合法的客户端证书中提取公钥,验证认证请求中的签名值signature1的正确性,如果正确,则执行步骤S320,否则返回错误;

[0052] 步骤S320:eSIM卡生成eSIM会话密钥,将认证结果返回至客户端;

[0053] eSIM卡生成一对临时非对称密钥,即临时公钥oneTimePublicKey和临时私钥oneTimePrivateKey,并根据临时私钥和客户端证书中的公钥使用预设算法生成eSIM会话密钥,优选的,预设算法为ECKA-EG算法,生成的eSIM会话密钥的源数据为:

[0054] generateSessionKey{

[0055] sharedinfo,

[0056] lpaPublicKey,

[0057] oneTimePrivateKey;}

[0058] 其中,sharedinfo为共享信息、lpaPublicKey为文件管理应用证书中的公钥、oneTimePrivateKey为临时私钥;

[0059] 使用临时私钥oneTimePrivateKey对transactionID、oneTimePublicKey以及eSIM证书签名得到签名结果,根据签名结果、认证请求中的随机数、临时公钥以及eSIM证书生成卡端发起的认证请求,认证请求为:

[0060] initAuthenticationResponse{

[0061] transactionID,

[0062] oneTimePublicKey,

[0063] CERT_ESIM,

[0064] signature2;}

[0065] 其中,transactionID为16字节的随机数,即所述客户端发起认证请求中的随机数、oneTimePublicKey为生成的临时公钥、CERT_ESIM为eSIM证书、signature2为eSIM证书的私钥对transactionID、oneTimePublicKey、CERT_ESIM的签名结果,这样能保证传输过程中数据不被篡改。

[0066] 步骤S330:客户端验证认证请求是否合法,是则执行步骤S340,否则返回错误;

[0067] 具体的,客户端使用持有的EUM证书验证认证结果中的eSIM证书是否合法,如果是,则从合法的eSIM证书中提取公钥,验证认证请求中的签名值的正确性,如果正确,则执行步骤S340,否则返回错误。

[0068] 步骤S340:客户端生成对称的客户端会话密钥,并使用生成的会话密钥建立安全通道;

[0069] 具体的,客户端根据临时公钥和客户端证书中的私钥使用预设算法生成对称的会话密钥,会话密钥为:

[0070] generateSessionKey{

[0071] sharedinfo,

[0072] lpaPrivateKey,

[0073] oneTimePublicKey;}

[0074] 其中,sharedinfo为共享信息,如生成的密钥类型、长度、eID等、lpaPrivateKey为客户端证书的私钥、oneTimePublicKey为认证请求中的临时公钥;

[0075] 优选的,预设算法为ECKA-EG算法,客户端和eSIM卡均采用相同的预设算法,能够确保客户端生成的会话密钥与eSIM卡生成的会话密钥完全相同,使用生成的会话密钥建立安全通道,客户端合法性认证完成。

[0076] 认证方法二、在eSIM卡中预置客户端的访问规则,当访问eSIM卡的客户端应用与预置在eSIM卡中的客户端的访问规则匹配时,客户端合法性认证通过。

[0077] eSIM卡出厂时预置其对应的客户端应用访问规则,所述访问规则内容为:需要访问的唯一标识码AID+哈希值;每个客户端都有预存的用于标识客户端合法身份的的唯一标

识码和哈希值。

[0078] 参见表1,移动终端中的客户端预存信息如下表所示:

[0079] 表1

[0080]

客户端	唯一标识码 AID	哈希值
移动运营商客户端	00 10 11 10 01 00 10 11	10 11 10 10 01 00 10 11 00 01 10 11 01 00……
联通运营商客户端	00 10 10 11 01 00 11 11	11 10 00 10 00 01 10 11

[0081]

		00 01 10 11 01 00……
电信运营商客户端	00 10 11 11 01 01 10 11	10 11 11 10 01 00 11 11 00 00 10 10 01 00……

[0082] 参见图4,认证客户端合法性的具体操作如下:

[0083] 步骤S410:客户端将客户端的唯一标识码和对应的哈希值发给操作系统,然后调用操作系统的硬件接口访问eSIM卡;

[0084] 步骤S420:操作系统的硬件接口打开eSIM逻辑通道,读取预置的客户端应用访问规则;

[0085] 步骤S430:操作系统判断来自客户端的唯一标识码和哈希值与来自eSIM卡的访问规则中预置的客户端唯一标识码和预置哈希值是否相同,是则认证客户端合法性通过,否则返回错误。

[0086] 继续回到图2,还包括:

[0087] 步骤S220:认证通过后,执行管理命令;

[0088] 管理命令包括激活、去激活和删除等管理指令,用以管理本地数据文件profile。

[0089] 本实施例中,当采用上述认证方法一进行客户端合法性认证时,则当认证通过后,eSIM卡通过建立好的安全通道接收客户端传输的管理命令,并执行该管理命令;当采用上述认证方法二进行客户端合法性认证时,则当认证通过后,eSIM卡通过操作系统中的硬件接口接收来自客户端的管理命令,并执行管理命令。

[0090] 步骤S230:将执行结果通知客户端,关闭eSIM逻辑通道。

[0091] 在上述第一种方式执行管理命令后,eSIM卡将执行结果返回客户端后,接收客户端返回的关闭eSIM逻辑通道请求,收到请求后,关闭eSIM逻辑通道。

[0092] 在上述第二种方式执行管理命令后,eSIM卡接收客户端发送的关闭eSIM逻辑通道命令,eSIM卡收到命令后,关闭eSIM逻辑通道。

[0093] 通过本发明的方法,在设备中安装的客户端,只有在通过认证或规则检查后,才能给授予访问eSIM卡中数据文件profile的许可,避免未经许可直接操作eSIM卡带来的风险。

[0094] 实施例二

[0095] 以上结合附图2、附图3和附图4介绍了实施例一中的eSIM卡安全认证的管理方法,以下结合附图5介绍eSIM卡安全认证的管理系统,包括eSIM卡510和客户端520;

[0096] eSIM卡510,包括如下部件:

[0097] 第一安全元件5101,对客户端的合法性进行认证;

[0098] 处理元件5102,用于打开在安全元件认证合法性通过后,执行管理命令并将执行结果通知客户端。

[0099] 客户端520,包括客户端通信元件5201,用于在合法性认证通过后,向eSIM卡510发送管理命令,并接收来自eSIM卡510的执行结果。

[0100] 其中第一安全元件5101具体用于,验证来自客户端520的认证请求,当认证请求合法时,生成临时非对称密钥,然后协商生成会话密钥,根据会话密钥建立安全通道。

[0101] 除此之外,第一安全元件5101还用于预置所述客户端的访问规则,所述访问规则包括访问eSIM卡的客户端应用的唯一标识码和哈希值。

[0102] 客户端520还包括第二安全元件5202,用于认证来自所述eSIM卡510的认证请求,还用于生成客户端会话密钥,使用所述客户端会话密钥建立安全通道。

[0103] 尽管已描述了本申请的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例作出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包含这些改动和变型在内。

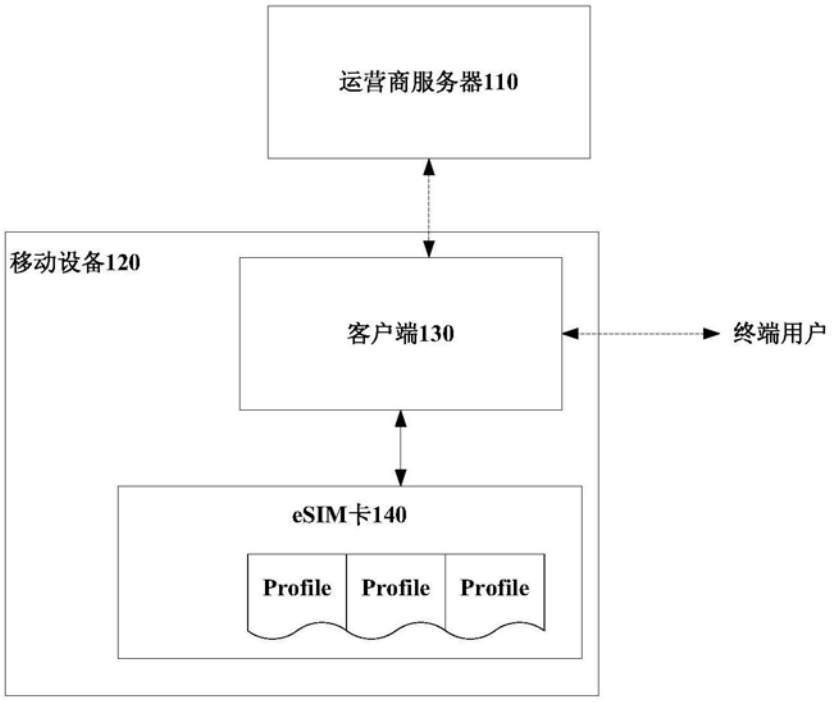

运营商服务器110
移动设备120
客户端130
终端用户
eSIM卡140
Profile
Profile
Profile

图1

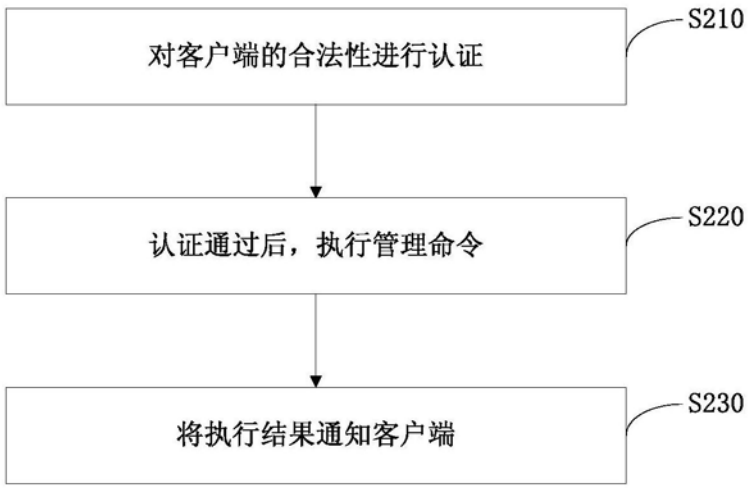

对客户端的合法性进行认证
S210
认证通过后，执行管理命令
S220
将执行结果通知客户端
S230

图2

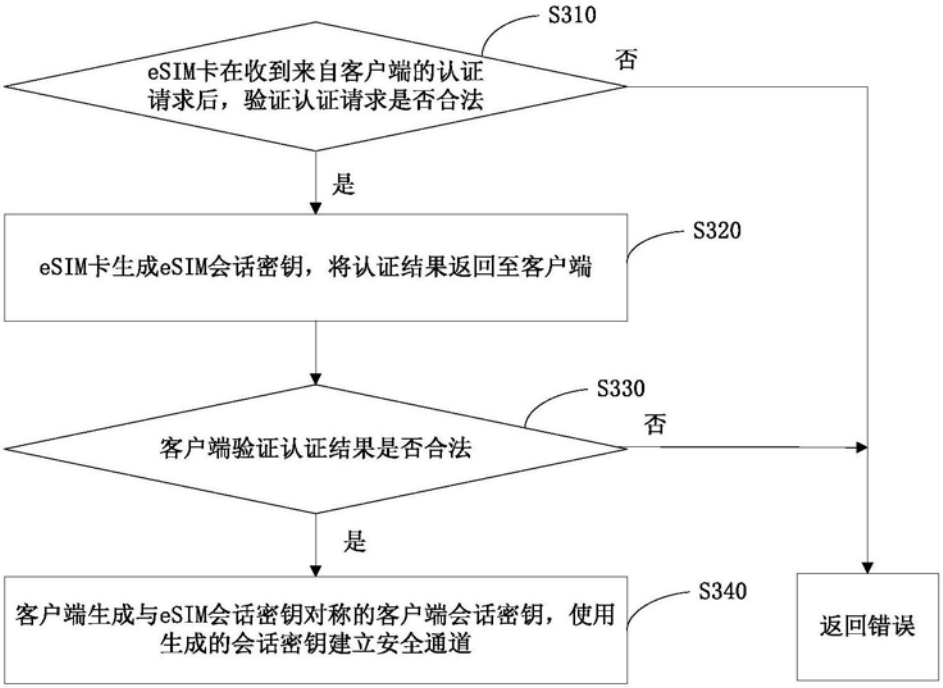

S310
eSIM卡在收到来自客户端的认证请求后，验证认证请求是否合法
否
是
S320
eSIM卡生成eSIM会话密钥，将认证结果返回至客户端
S330
客户端验证认证结果是否合法
否
是
S340
客户端生成与eSIM会话密钥对称的客户端会话密钥，使用生成的会话密钥建立安全通道
返回错误

图3

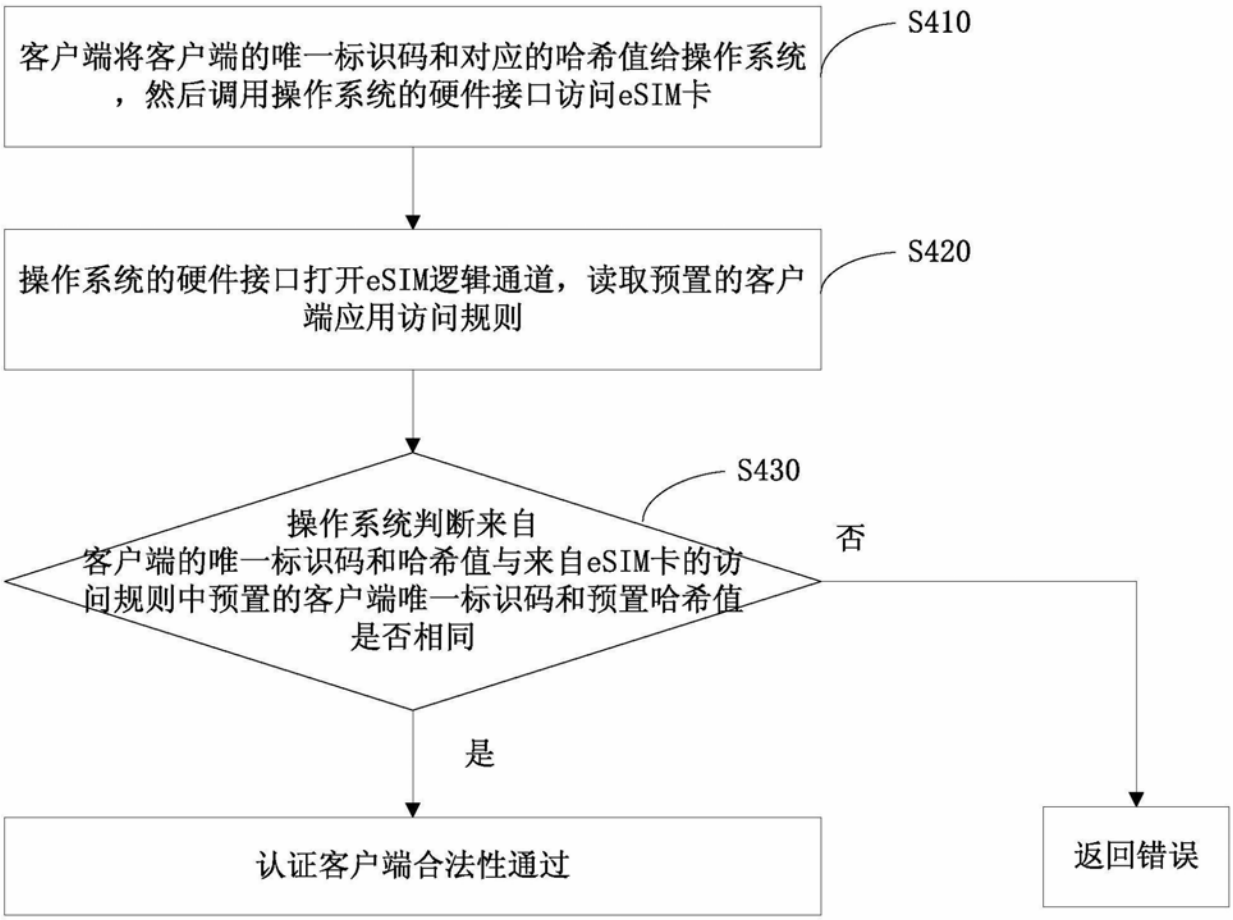

客户端将客户端的唯一标识码和对应的哈希值给操作系统，然后调用操作系统的硬件接口访问eSIM卡
S410
操作系统的硬件接口打开eSIM逻辑通道，读取预置的客户端应用访问规则
S420
操作系统判断来自客户端的唯一标识码和哈希值与来自eSIM卡的访问规则中预置的客户端唯一标识码和预置哈希值是否相同
S430
否
是
认证客户端合法性通过
返回错误

图4

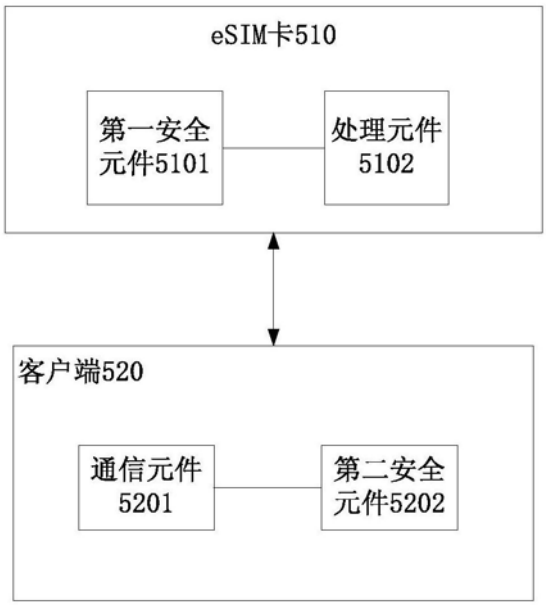

eSIM卡510
第一安全元件5101
处理元件5102
客户端520
通信元件5201
第二安全元件5202

图5