(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 109547464 B
(45)授权公告日 2021.12.10

(21)申请号 201811542660.7
(22)申请日 2011.10.28
(65)同一申请的已公布的文献号
申请公布号 CN 109547464 A
(43)申请公布日 2019.03.29
(30)优先权数据
61/407,866 2010.10.28 US
13/080,521 2011.04.05 US
(62)分案原申请数据
201110462171.2 2011.10.28
(73)专利权人 苹果公司
地址 美国加利福尼亚
(72)发明人 S·V·谢尔 J·冯豪克
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 李玲
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 4/50(2018.01)
H04W 4/60(2018.01)
H04W 8/18(2009.01)
H04W 12/069(2021.01)
(56)对比文件
WO 2004017565 A1,2004.02.26
WO 03077572 A1,2003.09.18
WO 2010102259 A2,2010.09.10
CN 1701295 A,2005.11.23
CN 101032126 A,2007.09.05
CN 1767438 A,2006.05.03
US 2005108171 A1,2005.05.19
US 2009305671 A1,2009.12.10
审查员 张宁

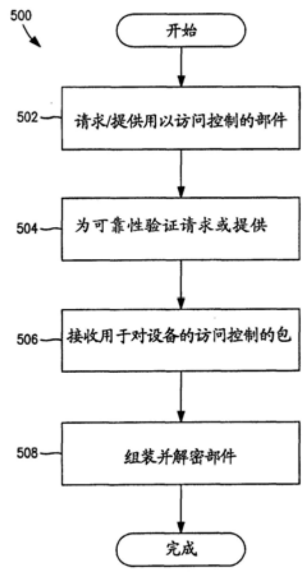
权利要求书2页 说明书12页 附图9页

(54)发明名称

用于存储和执行访问控制客户端的方法及装置

(57)摘要

本申请涉及用于存储和执行访问控制客户端的方法及装置。公开了在将使用访问控制实体的主设备被部署后用于安全提供所述访问控制实体(例如电子或虚拟订户身份模块(eSIM)部件)的方法和装置。在一个实施例中,无线(例如,蜂窝)用户装备被给予唯一设备密钥和签名证书,其可以被用于为“实地”用户装备提供更新或新的eSIM。基于使用设备密钥的安全证书传输,用户装备可以信任实质上由未知第三方eSIM卖方递送的eSIM。在另一方面,操作系统(OS)被分为多个分区或“沙盒”。在操作期间,用户设备可以激活并执行在与当前无线网络相对应的沙盒中的操作系统。在连接网络时接收的个性化包仅应用于那个沙盒。类似地,当加载eSIM时,OS只需要装载当前运行时环境所必须的软件的列表。不使用的软件能被随后激活。



CN 109547464 B

1.一种由电子通用集成电路卡eUICC执行的方法,所述方法包括:

识别访问控制客户端和相关联的补丁,以用于在所述eUICC的存储器中包括的多个安全分区中的一个安全分区内执行,其中所述多个安全分区中的每个安全分区包括相应的访问控制客户端;

验证所述访问控制客户端和所述相关联的补丁;以及

在成功验证所述访问控制客户端和所述相关联的补丁之后:

使得与所述访问控制客户端相关联的操作系统OS在和其中包括所述访问控制客户端的所述安全分区对应的限制范围内执行,其中所述OS在被执行时执行所述访问控制客户端。

2.根据权利要求1所述的方法,其中所述访问控制客户端包括电子订户身份模块eSIM,并且所述eSIM是物理SIM的虚拟化。

3.根据权利要求1所述的方法,其中验证所述访问控制客户端和所述相关联的补丁包括通过验证证书来核查完整性。

4.根据权利要求1所述的方法,其中在所述eUICC的重置之后执行所述方法。

5.根据权利要求1所述的方法,其中所述访问控制客户端和与其中包括所述eUICC的移动设备相关联的缺省移动网络运营商MNO对应。

6.根据权利要求1所述的方法,其中,其中包括所述访问控制客户端的所述安全分区存储至少一个附加访问控制客户端。

7.根据权利要求1所述的方法,其中执行所述访问控制客户端使得其中包括所述eUICC的移动设备能够向和所述访问控制客户端对应的移动网络运营商MNO登记。

8.一种电子通用集成电路卡eUICC,包括:

至少一个存储器,所述至少一个存储器包括多个安全分区,其中所述多个安全分区中的每个安全分区包括相应的访问控制客户端;以及

至少一个处理器,所述至少一个处理器被配置为使得所述eUICC执行包括如下操作的步骤:

识别访问控制客户端和相关联的补丁,以用于在所述多个安全分区中的一个安全分区内执行;

验证所述访问控制客户端和所述相关联的补丁;以及

在成功验证所述访问控制客户端和所述相关联的补丁之后:

使得与所述访问控制客户端相关联的操作系统OS在和其中包括所述访问控制客户端的所述安全分区对应的限制范围内执行,

其中所述OS在被执行时执行所述访问控制客户端。

9.根据权利要求8所述的eUICC,其中所述访问控制客户端包括电子订户身份模块eSIM,并且所述eSIM是物理SIM的虚拟化。

10.根据权利要求8所述的eUICC,其中验证所述访问控制客户端和所述相关联的补丁包括通过验证证书来核查完整性。

11.根据权利要求8所述的eUICC,其中所述eUICC在所述eUICC的重置之后执行所述步骤。

12.根据权利要求8所述的eUICC,其中所述访问控制客户端和与其中包括所述eUICC的

移动设备相关联的缺省移动网络运营商MNO对应。

13.根据权利要求8所述的eUICC,其中,其中包括所述访问控制客户端的所述安全分区存储至少一个附加访问控制客户端。

14.根据权利要求8所述的eUICC,其中执行所述访问控制客户端使得其中包括所述eUICC的移动设备能够向和所述访问控制客户端对应的移动网络运营商MNO登记。

15.一种移动设备,包括:

至少一个存储器;

至少一个处理器;

至少一个无线接口;以及

电子通用集成电路卡eUICC,所述eUICC包括:

存储器,所述存储器存储多个访问控制客户端,其中所述多个访问控制客户端中的每个访问控制客户端被包括在相应的安全分区中,以及

处理器,所述处理器被配置为使得所述eUICC执行包括如下的步骤:

识别访问控制客户端和相关联的补丁,以用于在包括所述访问控制客户端的安全分区内执行,其中与所述访问控制客户端相关联的补丁包括被配置为管理所述访问控制客户端的操作系统OS,

验证所述访问控制客户端和所述相关联的补丁,以及

在验证所述访问控制客户端和所述OS之后:

使得所述OS在和所述安全分区对应的限制范围内执行,

其中所述OS在被执行时使得所述访问控制客户端被执行。

16.根据权利要求15所述的移动设备,其中所述访问控制客户端包括电子订户身份模块eSIM,并且所述eSIM是物理SIM的虚拟化。

17.根据权利要求15所述的移动设备,其中验证所述访问控制客户端和所述相关联的补丁包括通过验证证书来核查完整性。

18.根据权利要求15所述的移动设备,其中所述步骤在所述eUICC的重置之后被执行。

19.根据权利要求15所述的移动设备,其中所述访问控制客户端和与所述移动设备相关联的缺省移动网络运营商MNO对应。

20.根据权利要求15所述的移动设备,其中执行所述访问控制客户端使得所述移动设备能够使用所述至少一个无线接口来向和所述访问控制客户端对应的移动网络运营商MNO登记。

用于存储和执行访问控制客户端的方法及装置

[0001] 本申请是申请日为2011年10月28日、申请号为201110462171.2、发明名称为“用于存储和执行访问控制客户端的方法及装置”的发明专利申请的分案申请。

[0002] 优先权和相关申请

[0003] 本申请要求于2011年4月5日提交的、题为“METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS”的美国专利申请第13/080521号的优先权，该美国专利申请则要求于2010年10月28日提交的、题为“METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS”的美国临时专利申请第61/407866号的优先权。前述申请分别通过引用全文结合于此。

[0004] 本申请还涉及：于2011年4月5日提交的、题为“APPARATUS AND METHODS FOR CONTROLLING DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS”的美国专利申请第13/080558号，于2010年11月22日提交的、题为“WIRELESS NETWORK AUTHENTICATION APPARATUS AND METHODS”的美国专利申请申请第12/952082号，于2010年11月22日提交的、题为“APPARATUS AND METHODS FOR PROVISIONING SUBSCRIBER IDENTITY DATA IN A WIRELESS NETWORK”的美国专利申请第12/952089号，于2010年12月28日提交的、题为“VIRTUAL SUBSCRIBER IDENTITY MODULE DISTRIBUTION SYSTEM”的美国专利申请第12/980232号，以及于2009年1月13日提交的、题为“POSTPONED CARRIER CONFIGURATION”的美国专利申请第12/353227号，以及于2011年4月5日提交的、题为“APPARATUS AND METHODS FOR STORING ELECTRONIC ACCESS CLIENTS”的美国临时专利申请第61/472109号，于2011年4月5日提交的、题为“APPARATUS AND METHODS FOR DISTRIBUTING AND STORING ELECTRONIC ACCESS CLIENTS”美国临时专利申请第61/472115号，于2010年10月28日提交的、题为“METHODS AND APPARATUS FOR ACCESS CONTROL CLIENT ASSISTED ROAMING”的美国临时专利申请第61/407858号，于2010年10月28日提交、题为“MANAGEMENT SYSTEMS FOR MULTIPLE ACCESS CONTROL ENTITIES”的美国临时专利申请第61/407861号(现在的于2011年4月4日提交的相同标题的美国专利申请第13/079614号)，于2010年10月28日提交的、题为“METHODS AND APPARATUS FOR DELIVERING ELECTRONIC IDENTIFICATION COMPONENTS OVER A WIRELESS NETWORK”的美国临时专利申请第61/407862号，于2010年10月29日提交的、题为“ACCESS DATA PROVISIONING SERVICE”的美国临时申请第61/408504号(现在的于2011年4月1日提交的、题为“ACCESS DATA PROVISIONING APPARATUS AND METHODS”的美国专利申请第13/078811号)，于2010年11月3日提交的、题为“METHODS AND APPARATUS FOR ACCESS DATA RECOVERY FROM A MALFUNCTIONING DEVICE”的美国临时专利申请第61/409891号，2010年11月4日提交的、题为“SIMULACRUM OF PHYSICAL SECURITY DEVICE AND METHODS”的美国临时专利申请第61/410298号(现在的于2011年4月5日提交的相同标题的美国专利申请第13/080533号)，以及于2010年11月12日提交的、题为“APPARATUS AND METHODS FOR RECORDATION OF DEVICE HISTORY ACROSS MULTIPLE SOFTWARE EMULATION”的美国临时专利申请第61/413317号，前述的申请分别通过引用全文结合于此。

技术领域

[0005] 本发明一般地涉及无线通信和数据网络领域。更具体地，在一个示例性的方面，本发明针对用于访问控制实体或客户端的安全修改、存储和执行的方法和装置。

背景技术

[0006] 在很多现有的无线通信系统中要求访问控制以进行安全通信。例如，一个简单的访问控制方案包括：(i)验证通信方的身份，及(ii)授予与经验证身份相称的访问等级。在一个示例性蜂窝系统(例如，通用移动电信系统(UMTS))的情境中，访问控制由访问控制客户端管理，该访问控制客户端被称作在物理的通用集成电路卡(UICC)上执行的通用订户身份模块(USIM)。该USIM访问控制客户端向UMTS蜂窝网络认证所述用户。在成功认证后，订户被允许访问蜂窝网络，在下文使用中，术语“访问控制客户端”通常指代逻辑实体，具体化为硬件或软件，适用于控制第一设备对网络的访问。访问控制客户端的普通示例包括上述的USIM、CDMA订户识别模块(CSIM)、IP多媒体服务身份模块(ISIM)、订户身份模块(SIM)、可移除用户身份模块(RUIM)等。

[0007] 传统地，USIM(或更一般的“SIM”)执行公知的认证和密钥协商(AKA)规程，该规程验证并解密可应用的数据和程序以保证安全初始化。特别地，USIM必须包括：(i)成功回答远程询问来向网络运营商证明其身份，并且(ii)发出验证网络身份的询问。

[0008] 但是，现有的SIM解决方案有许多弱点和不足。首先，SIM软件被硬编码到物理UICC卡介质；所述订户需要新UICC来更换SIM操作。这对MNO和用户两者都是有害的；例如，如果认证过程被“破坏”(例如，经由恶意“黑客”活动)，则必须向订户发出新的UICC，而这个过程时耗时且昂贵的。此外，出于随后将在此更详细描述的原因，物理SIM仅认可单个受信实体；特别地，被配置来与其通信的移动网络运营商(MNO)。于是，除了经由设备和MNO之间的现有受信关系之外，当前不存在用于引入部署后编程的方法。例如，希望提供新的或更新SIM软件的第三方SIM开发商既受到物理SIM卡介质的不变性的限制，又受到他们无法在其自身和订户SIM之间建立受信关系的限制。这个控制“瓶颈”极大地限制了SIM卖方所提供的数量和容量。

[0009] 相应地，需要新的解决方案来允许对部署后的SIM的分配和修改。理想地，这样的解决方案使得移动设备在位于“实地”(部署后)的情况下仍能接收并实现对SIM操作的改变。进一步地，改进的方法和装置可以支持其他期望特征，尤其是对多个SIM简档的支持、灵活操作、更新等。

[0010] 但是更通常地，需要改进的方法和装置来进行访问控制客户端的安全修改、存储和执行。需要修改访问控制客户端操作的技术来支持这些特征，例如，多个订户访问简档、安全设备更新、订户服务供应的可选方法等。进一步地，由于访问控制的敏感性和暗地使用及服务偷窃的可能性，执行这个修改的安全方法是主要考虑的内容。

发明内容

[0011] 本发明通过提供改进的用于安全修改、存储和执行访问控制客户端的装置和方法来满足前述需求。

[0012] 本发明第一方面公开了一种无线装置。在一个实施例中，所述装置包括：一个或多

个无线链路,适于经由访问控制客户端与至少一个网络进行通信;安全元件,被配置为存储访问控制客户端;到安全元件的接口,所述接口具有加密密钥和与其相关联的资格证书;处理器,以及与所述处理器进行数据通信的存储设备,所述存储设备包括计算机可执行指令。至少所述计算机可执行指令的至少一个子集被进一步分区成一个或多个分段。

[0013] 在一个变形中,所述计算机可执行指令在由处理器执行时:经由所述接口为特定于所述至少一个网络的访问控制客户端发送对一个或多个部件的请求,所述请求包括资格证书和加密密钥;接收一个或多个所请求的部件,所述一个或多个部件与第二资格证书相关联;验证第二资格证书;响应于第二资格证书的成功检验,加载所述访问控制客户端。

[0014] 在本发明的第二方面,公开了一种相互认证的方法。在一个实施例中,所述方法包括:请求一个或多个部件,所述请求与第一资格证书相关联;接收一个或多个部件以及第二资格证书;如果所述第二资格证书有效,则加载所述一个或多个部件,其中所述第一和第二资格证书是由受信实体发出。

[0015] 在本发明的第三方面,公开了一种执行访问控制客户端的方法。在一个实施例中,所述方法包括,执行第一引导操作系统,所述引导操作系统选择安全分区,所述安全分区只与一个访问控制客户端相关联;验证所述安全分区,安全分区包括一个公用操作系统和一个访问控制客户端;以及执行公用操作系统,所述公用操作系统加载所述一个访问控制客户端。所述访问控制客户端被配置为用网络(例如外部的蜂窝网络)进行认证。

[0016] 在本发明的第四方面,公开了一种移动设备。在一个实施例中,所述移动设备被配置为通过引导OS架构来请求、接收和利用虚拟或电子SIM数据结构。

[0017] 在本发明的第五方面,公开了一种计算机可读装置。在一个实施例中,所述装置包括运行有至少一个计算机程序的存储介质,所述至少一个计算机程序被配置为通过引导OS来接收、处理和提供用于虚拟或电子SIM的请求。

[0018] 在本发明的第六方面,公开了一种向用户分配虚拟或电子SIM的系统。在一个实施例中,所述系统包括支持经诸如因特网、MAN或WLAN等网络来递送eSIM的、可用于递送操作系统部件的装置。

[0019] 通过参考附图和如下给出的对示例性实施例的详细描述,本领域技术人员可以立即获知本发明的其他特征和优点。

附图说明

[0020] 图1图解地例示了一个使用现有USIM的示例性认证与密钥协商(AKA)规程。

[0021] 图2是例示了根据本发明的用于向软件实体(例如,用户装备(UE)、第三方软件卖方、SIM卖方等)指定设备密钥对的一个方法实施例的逻辑流程图。

[0022] 图3图解地例示了根据本发明一个实施例用于在UE和软件卖方之间安全递送实时部件的示例性交易。

[0023] 图4图解地例示了根据本发明用于安全执行eSIM的一个方法实施例。

[0024] 图4A图解地例示了根据本发明的引导OS、eUICC和eSIM架构的一个实施例。

[0025] 图5是例示了安全修改和存储用于访问控制客户端的部件的一个一般性方法实施例的逻辑流程图,。

[0026] 图6是例示了根据本发明的安全执行用于访问控制客户端的部件的一个一般性方

法实施例的逻辑流程图，。

[0027] 图7是用于实施本发明各方法的示例性装置的框图。

[0028] 图8是根据一些实施例的无线装置的功能性框图。

[0029] 所有附图©版权2010苹果公司。保留所有权利。

具体实施方式

[0030] 现在将附图进行参考，贯穿附图，相同的数字表示相同的部分。

[0031] 综述

[0032] 本发明尤其提供使得用户装备和任何受信第三方实体能够彼此验证的安全方法和装置。本发明还公开了使得任何第三方实体即使在用户装备已被部署后仍然可以变为受信的方法和装置。例如，移动设备(例如，UMTS UE)可以识别第三方eSIM(例如，虚拟或电子SIM——此后称为“eSIM”)卖主，并发起受信对话以购买、获取或更新其eSIM。类似地，所述第三方eSIM卖主可以验证UE是受信设备，并安全地编码其eSIM以供递送。所述受信对话基于唯一的设备密钥和资格证书；如在此后所描述的，在一个示例性实施例中，所述设备密钥基于公钥/私钥密码术。

[0033] 本发明的各个方面涉及访问控制客户端(整体或部分)的安全接收。由于访问控制材料对网络运营商的敏感特性，现有解决方案已经偏好于使用物理卡形态因素。但是，本发明有利地提供对虚拟化或电子访问控制客户端(例如，eSIM)的安全发送，从而避免了对物理卡的需求及其关联限制。

[0034] 进一步地，不像现有解决方案，本发明能够递送访问控制客户端材料而无需预先存在的访问控制客户端，由此大大增强了用户灵活性和使用感受。

[0035] 在本发明的再一方面，设备(例如，移动用户设备)可以激活并执行多个存储的访问控制客户端(例如，eSIM)中的一个。具体地，在加载eSIM时，操作系统(OS)只需要加载当前运行时环境所必须的软件的列表。这种“沙盒”效应确保能够在同一个设备中利用多个eSIM，而不会存在对其他eSIM的不恰当访问。

[0036] 示例性实施例的详细描述

[0037] 现在详细描述本发明的示例性实施例和各个方面。虽然这些实施例和方面主要是在GSM、GPRS/EDGE、或UMTS蜂窝网络的订户身份模块(SIM)的情境中讨论的，但是本领域技术人员可以理解本发明并不限于此。事实上，本发明的多个方面可以被用于任何能够从安全修改、存储和执行访问控制实体或客户端中受益的无线网络(无论是蜂窝或其他)。

[0038] 同样应该认识到当在此使用术语“订户身份模块”时，这个术语绝不必须蕴含或要求 (i)由订户自身使用(即，本发明可由订户或非订户实施)；(ii)单个个体的身份(即，本发明可以被一群个体使用，例如家庭，或如企业之类的无形或虚构的实体)；或(iii)任何有形“模块”装备或硬件。

[0039] 现有技术的订户身份模块(SIM)操作

[0040] 在现有UMTS蜂窝网络的情境中，用户装备(UE)包括移动设备和通用订户身份模块(USIM)。所述USIM是从物理的通用集成电路卡(UICC)存储和执行的逻辑软件实体。所述USIM中存储有各种信息，例如订户信息，以及用于向网络运营商进行认证从而获得无线网络服务的密钥和算法。USIM软件基于Java Card™编程语言。Java Card是Java™编程语言的

一个已被修改用于嵌入式"卡"类型设备(例如前述UICC)的子集。

[0041] 通常,UICC在被分配给订户之前已编程有USIM;这种预编程或"个性化"特定于每个网络运营商。例如,在部署前,USIM与国际移动订户身份(IMSI)、唯一的集成电路卡标识符(ICC-ID)以及专门的认证密钥(K)相关联。网络运营商将所述关联存储在网络认证中心(AuC)的寄存器中。在个性化之后,该UICC被分配给用户。

[0042] 现在参考图1,详细例示了使用前述的现有USIM的一个示例性认证和密钥协商(AKA)规程。在常规认证规程期间,UE从USIM获得国际移动订户身份(IMSI)。UE将所述IMSI传递给网络运营商或者被访问核心网络的服务网络(SN)。SN将所述认证请求转发给本网(Home Network,HN)的AuC。所述HN将接收到的IMSI与AuC的寄存器相比较并获得合适的K。所述HN生成随机数(RAND)并通过一个算法使用K签署该随机数以创建期望响应(XRES)。HN使用各种算法进一步生成用于索引和完整性保护的密钥索引(CK)和完整性密钥(IK),以及认证令牌(AUTN)。所述HN向所述SN发送由RAND、XRES、CK和AUTN组成的认证向量。所述SN存储所述认证向量,只用于单次认证过程。所述SN将RAND和AUTN传递给UE。

[0043] 一旦UE接收到RAND和AUTN,USIM验证接收到的AUTN是否有效。如果有效,UE则使用该接收到的RAND并通过使用存储的K和与生成XRES相同的算法来计算该UE自身的响应(RES)。UE将RES传递回SN。SN将XRES与该接收到的RES相比较,并且如果匹配,SN则授权UE使用运营商的无线网络服务。

[0044] 典型操作

[0045] 现在参照一个示例性的实现来讨论本发明的各个方面。在本发明示例性实施例的上下文中,代替使用现有技术中的物理的UICC,所述UICC被仿真为虚拟或电子实体,例如软件应用,其在此后被称作电子通用集成电路卡(eUICC),并且被包括在UE中的安全元件(例如,安全微处理器或存储设备)内。该eUICC能够存储并管理多个SIM元件,这些元件在此后被称作电子订户身份模块(eSIM)。每个eSIM是典型USIM的软件仿真,并且包括模拟编程和与此相关联的用户数据。该eUICC基于eSIM的ICC-ID来选择eSIM。一旦eUICC选择了期望的一个或多个eSIM,所述UE可以发起认证规程以从eSIM的对应网络运营商获取无线网络服务。进一步地,每个eSIM应用通常包括访问控制客户端,例如前述的USIM、CSIM、ISIM、SIM、RUIM等。可以理解每个eSIM都与一个用户账号相关联,这样一个"eSIM"可以广泛地包括多个访问控制客户端(例如,一个用户可能具有一个USIM以及一个与同一eSIM账户相关联的SIM)。

[0046] 正如前面提到的,上述的现有USIM规程要求使用预先共享的密钥来向核心网(例如,前述的本网(HN)、服务网络(SN)和认证中心(AuC)等)进行认证。因此,由于预先共享的密钥必须被严格保护,USIM规程需要用于网络运营商的"封闭"系统。相反,本发明提供了让eUICC和任何第三方实体能够彼此信任的安全方法,并且使得即使在用户装备被部署之后,任何第三方实体仍然能够变为受信。

[0047] 相应地,本发明在某些方面具有复杂得多的安全需求,但是也有利地提供了大得多的灵活性。进一步地,本领域技术人员将会理解虽然本发明的各个方面都从使用"虚拟"软件结构(例如,eUICC、eSIM)中受益,但是这些益处不限于这些虚拟实施例。事实上,在此讨论的原理同样适用于对尤其是在物理卡介质、专用安全硬件等中具体化的访问控制客户端的安全修改、存储和执行。

[0048] 建立受信通信

[0049] 图2例示了用于为软件实体(例如,eUICC、第三方软件卖方、SIM卖方等)指定设备密钥对的示例性方法。在步骤202,加密公钥/私钥对(例如,Rivest、Shamir和Adleman(RSA)算法)被指定给软件实体,并被存储在所述软件实体的被物理保护的安全元件中;例如,UE中的eUICC,第三方软件卖方的安全数据库。例如,eUICC由受信第三方编程;或者可选地,可以在第一次被制造/激活时内部生成公钥/私钥对。

[0050] 简言之,公钥/私钥对是基于秘密的私钥以及可公开的公钥。公钥/私钥方案是被考虑为“不对称的”,因为用于加密和解密的密钥是不同的,因此加密器和解密器并不共享同一密钥。相反,“对称”密钥方案使用同一密钥(或经简单转换的密钥)来进行加密和解密。Rivest、Shamir和Adleman(RSA)算法是一种被广泛用于现有技术中的公钥/私钥对密码术,但是可以理解本发明并不限制于该RSA算法。

[0051] 公/私密码方案能被用于加密消息,和/或生成签名。特别地,消息能由私钥加密,并由公钥解密,从而保证消息在传输中不被改变。类似地,用私钥生成的签名能用公钥验证,从而保证生成签名的实体的合法性。在这两种使用中,私钥是保密的,而公钥则被自由分配。

[0052] 在步骤204,发行针对该公钥/私钥对的资格证书。例如,通过为eUICC密钥发布“资格”证书,受信实体证实eUICC的可靠性和私钥的保密性。该公钥/私钥对现在是eUICC的设备密钥对。

[0053] 在一个实施例中,资格证书包括收集的数据,所述数据包括但不限于:(i)发证机构的身份信息,(ii)设备的识别信息,(iii)描述发证算法的元数据,和/或(iv)适当的公钥。这些部件可以进一步由背书资格人的私钥所签署。在一个实施例中,在正常操作期间,这个数字签名被接收方检验从而验证内容是安全的并且没有被篡改过。

[0054] 因为设备密钥对是不对称的,所以公钥可以被发布,而不会危及私钥的完整性。因此,设备密钥和证书可以被用于保护和验证在前不知道的多方(例如,eUICC和第三方)之间的通信。考虑如下用于在eUICC和软件卖方(在图3中示出)之间安全递送运行时部件的示例性交易。

[0055] 在图3的步骤302,eUICC请求来自第三方eSIM卖方的eSIM。虽然在以下示例描述了eSIM应用的安全传递,但是运行时环境应用的其他常见示例可以包括补丁,全功能操作系统等。

[0056] 在步骤304,第三方eSIM卖方从资格证书取还与eUICC对应的设备公钥,例如,所述资格证书可以从数据库,由eUICC查询等方式获得。特别注意的是,eUICC的对应私钥在这个过程中有利地从不暴露给第三方eSIM卖方。

[0057] 在步骤305,第三方eSIM卖方验证资格证书。在一个示例性实施例中,资格证书由受信实体(例如,在此的受让人,Apple™)唯一地签署的。一旦第三方eSIM卖方验证了该资格证书,则第三方eSIM卖方随后能够确认该eUICC被受信实体(例如,Apple™)和联盟所信任,并且是安全的。

[0058] 在步骤306,eSIM运行时环境被加密并在随后针对与所述UE对应的具体eUICC由第三方软件卖方签署。在替换实施例中,eSIM运行时环境首先被签署,然后被加密。在一个示例性情况下,卖方使用其自身的卖方非对称签名密钥和RSA公钥/私钥,以及证书链来签署

所述eSIM,并使用短暂或临时的对称密钥来加密eSIM。临时对称密钥在准备用于eUICC的包时被随机生成。

[0059] 在步骤308,被签署并加密的eSIM运行时环境被第三方eSIM卖方分成多个包以供递送(例如,经无线接口等)。例如,被签署并加密的eSIM被分成大小与通信链路质量相适应的包(封包的递送支持本领域已知的多种期望的纠错方案)。

[0060] 在步骤310,短暂的对称密钥被安全传输到eUICC,例如通过使用恰当的eUICC公钥来加密该对称密钥。卖方证书可被明文传送,或可选择地被加密。通常,卖方证书不被加密以减少接收机的处理负担(但这不是对系统的要求,加密也可以在所有情况下或者可选择地被使用,被选择地应用)。

[0061] 在步骤312,eUICC验证卖方证书。应该注意使用卖方的签名公钥对卖方证书的成功验证为eUICC提供了签名不是伪造的证明。

[0062] 在某些情况下,卖方证书可以进一步包括由外部受信实体(例如,MNO等)签署的签名。如果卖方证书有效,则UE随后使用它的(eUICC的)私钥来解密该短暂的对称密钥。前述交换的成功完成保证了在eUICC和第三方实体之间的路径是安全的,并通过公用的短暂对称密钥来加密以供进一步的数据交易。

[0063] 因此在步骤314,大量的加密包能被eUICC安全地接收、重新组装和解密。在这个具体示例中,eUICC下载用于eSIM的包。

[0064] 在一个实施例中,卖方证书、密钥和加密包被一起传输。替换实施例则使用其他范例;例如,发送证书和密钥,先建立安全连接,然后发起经所述安全连接的加密包传输。

[0065] 本发明的示例性实施例将eSIM视为独立于eUICC的实体。因此,在没有现有eSIM的益处的情况下,并且即使在用户装备已被部署之后,eUICC仍能建立到第三方实体的安全连接。示例性的eUICC确保了eSIM的安全传递,从而直接使得第三方eSIM卖方能够向移动设备分配eSIM,而不需要像之前那样依赖于现有的SIM AKA规程。

[0066] 更直接地,设备具有与和任何单个eSIM(以及发布该eSIM的MNO)相关联的对称密钥相分离且有区别的非对称设备密钥对。在eSIM和eUICC之间的这种区别性对设备操作系统的复杂性具有相当的影响。

[0067] <u>安全分区的执行</u>

[0068] 正如前面所提到的,现有的用于物理UICC的解决方案包括单个USIM实体;然而,本领域技术人员将会认识到本发明的各个方面很容易适合存储和执行多个访问控制客户端简档。因此,在本发明的另一个实施例中,eUICC必须确定网络和eSIM双方的有效性。由于前面任务的复杂性,现有技术的SIM结构不再满足初始化。代替地,在本发明的一个示例性实施例中,引导操作系统(OS)加载“公用的”或“常驻的”操作系统;公用OS加载恰当的eSIM,并且加载的eSIM可以执行前述的认证和密钥协商(AKA)规程。

[0069] 特别地,本发明的引导OS在一个实现中负责密码验证,解密,以及公用OS的加载,以及与激活的eSIM相关联的所有补丁。引导OS在虚拟化的软件eUICC上执行;因此,eSIM和关联的公用OS是“沙盒化的”;它们只访问可通过eUICC使其有效的适当的补丁。例如,在一个示例性实施例中,eUICC只是使得补丁能够共享与eSIM相同的签署者。

[0070] 现在参考图4,描述了一个用于安全地执行分区eSIM的示例性方法。

[0071] 在步骤402,eUICC在芯片重置时启动引导OS。在步骤404,引导OS分析补丁的授权

列表来启动运行时环境。例如，引导OS可以识别缺省网络及其关联补丁。这些补丁中的至少一个是公用OS，其他补丁包括激活的eSIM，以及与eSIM相关联的任何附加补丁。

[0072] 在步骤406，引导OS验证补丁的完整性，例如，通过分析证书，或其他方式。例如，在一个实施例中，受信实体(例如，记录的受让人)可以发布证书，或者以其他方式起到签名链的信任根的功能。如果补丁被恰当地签署，则所述引导OS就能够执行补丁。只有与合适的eSIM对应的经验证补丁才被加载(其他补丁可以被存储，但是不在“沙盒”中执行)。

[0073] 在步骤408，引导OS启动公用OS。公用OS提供eSIM和其余硬件之间的接口。所述公用OS通常提供模仿专用于特定eSIM的UICC的输入和输出功能。通常，这包括诸如文件输入和输出(IO)等之类的功能。

[0074] 然后，在步骤410，公用OS可以执行合适的eSIM。

[0075] 图4例示了在引导OS 452、公用OS 454和eSIM 456之间的软件关系。最值得注意地，在示例性的实施例中(如图4和4A所描述的)，不同的eSIM简档在它们自己的公用OS中操作。通过将不同eSIM简档的运行时环境分隔到彼此不同的沙盒中，前述实施例有利地保持了对先代SIM架构的兼容，但同时好利用了本发明的益处。通常，通过保证每个eSIM在它们自己的环境中执行，现有SIM软件能被直接虚拟化。此外，沙盒保证了其他eSIMs的存在不会导致不良的交互，这是支持广泛大量第三方eSIM卖方(例如，其可能具有独家的协议和能力等)的必须要求。

[0076] 如前面注意到的，前述讨论主要以基于SIM的网络技术和特征为基础。因此，现将呈现对用于实现本发明的一个或多个方面的一般性方法和装置的示例性实施例的描述。

[0077] 方法

[0078] 现在参考图5，例示了用于安全修改和存储用于访问控制客户端的部件的一般性方法500的一个实施例。

[0079] 在步骤502，用于访问控制客户端的一个或多个部件被请求或提供。在一个示例性实施例中，该一个或多个部件整体或部分包括：(i)公用操作系统，(ii)至少一个eSIM，和/或(iii)与eSIM相关联的一个或多个个性化补丁。在其他的技术实现中，所述包可与CDMA订户识别模块(CSIM)、IP多媒体服务身份模块(ISIM)、订户身份模块(SIM)，可移除用户身份模块(ISIM)等相关联。本领域普通技术人员根据本公开可以认识到领域内多种类似结构的近乎无限的排列，并且对这里所呈现的适应这些类似结构和排列的方法和装置的修改完全在获知本公开的本领域普通技术人员的能力范围内。

[0080] 在一个实施例中，一个或多个部件由设备或与设备相关的用户请求或“拉出”；即，由发出了肯定通信或请求的设备/用户请求或“拉出”。在替换实施例中，一个或多个部件被指定或“推送”到设备；即，没有前述通信或请求，而是根据某些其他准则或方案，例如，周期性地，基于一个事件的发生等。可以对一个或多个部件的存在进行广告，或以其他方式进行广播，或将其存储到可被访问或搜索的储存库内。

[0081] 在其他实施例中，一个或多个部件由一个或多个与上下文有关的事件(例如，设备进入特定区域、超出特定的使用等)询问或以其他方式触发。

[0082] 所述请求或提供也可以包括由受信方发起的签名或证书。在其他替换实现中，所述请求或提供包括加密尝试。在再一些变形中，请求或提供包括确定可靠性的途径(例如，基于密码认证的用户接口等)。

[0083] 所述请求或提供也可以包括交易密钥。在这类变形中,交易密钥是短暂密钥。也可以使用其他的永久交易密钥;例如,对多个交易会话,多个用户等,该密钥可以是相同的。在其他变形中,交易密钥是对称密钥,或作为替换是非对称密钥。

[0084] 在步骤504,请求或提供被验证其可靠性。在一个实施例中,由受信方发起的签名或证书被检验是否有效。在某些情况下,这需要与受信方的外部接触。作为替换,签名或证书的有效性可以是自明的,或者以其他方式可由验证其发现的,不需要诉诸于受信方。其他方案则可依赖于订户输入;例如用户名和密钥登陆,或简单的肯定应答方案等。

[0085] 成功的验证也可以被配置为需要一个或多个尝试应答交换。在一些变形中,验证可以是单向的(例如,只是交易方中的一个被验证),或双向的(例如,交易双方都必须成功)。在其他的方案中,验证是不同频道信号传输的(例如,经由另一个通信路径)或经由订户协助来执行。

[0086] 成功的验证导致对安全交易必要的一个或多个参数的协商。例如,在一个实施例中,建立了一个或多个交易密钥。在一些变形中,交易密钥在验证后生成。在替换变形中,交易密钥在验证之前就被提议或生成,并在随后被有条件地使用。

[0087] 然后,在步骤506,设备接收与访问控制客户端相关联的一个或多个包。包可以通过交易密钥来进一步加密以保证安全传输。在一个变形中,包被非对称地加密;即,使用公钥对包加密。在其他变形中,使用事先协商好的共享密钥对包进行对称加密。作为替换,使用可识别的签名来签署包。相关领域中已知的包的可验证递送的大量其他解决方案可以与本发明并存地使用。

[0088] 在步骤508,设备组装包,并解密一个或多个部件。在一个示例性实施例中,一个或多个部件与合适的公用操作系统相关联。例如,前面所提及的,补丁可以包括至少一个eSIM,和/或与如前所述的一个或多个eSIM相关联的个性化补丁。在步骤508的结尾,一个或多个部件已被成功并安全地转移至目标设备。

[0089] 现参考图6,例示了一种为用于访问控制客户端的部件进行安全执行的一般性方法600的示例性实施例。

[0090] 在步骤602,识别访问控制客户端和一个或多个关联补丁。在一个示例性实施例中,访问控制客户端和一个或多个关联补丁由操作系统选出。在一个实现中,操作系统进一步从简单的引导操作系统中被引导。

[0091] 在一个配置下,引导操作系统保持多个安全分区,其中每个分区与其他分区相区别,且由内存分区执行的软件不能访问其他不相关分区或被其他不相关分区访问。例如,一个示例性的设备执行简单的引导OS;所述简单的引导OS在单个的“沙盒”分区中加载并执行公用OS及其关联eSIM,以及补丁。

[0092] 本发明的各个实施例根据一个或多个分类来对可用部件和补丁的整个清单进行分离。在这类变形中,根据公共签署者或受信源来关联部件和补丁。例如,在一种场景下,简单引导OS可以只允许公用OS和由相同eSIM卖方签名的eSIMs用以执行。在其他变形中,部件和补丁可以根据用户选择或不同的信任等级来进行关联。例如,各个部件可以从不同的协作实体(例如,受信的eSIM卖方,和受信的网络个性化等)散布。

[0093] 在方法600的步骤604,访问控制客户端及其关联补丁被验证其操作。在一个实施例中,访问控制客户端及其关联补丁被检验其完整性;即,它们没有被篡改或以其他方式变

更。用于这类完整性检验的常用方法包括校验和、加密散列或残余等。验证补丁可靠性的其他方案可以包括证书验证、状态验证等。

[0094] 在步骤606,经验证的访问控制客户端被执行。一旦成功加载和执行,访问控制客户端为关联网络执行最初的访问控制过程。例如,经验证的eSIM能够执行认证和密钥协商规程。

[0095] 示例性的移动装置

[0096] 现参考图7,例示了用于实现本发明的方法的示例性装置700。

[0097] 图7的示例性UE装置是具有处理器子系统702的无线设备,所述处理器子系统702例如是数字信号处理器、微处理器、现场可编程门阵列、或是安装在一个或多个基底上的多个处理部件。所述处理子系统也可以包括内部高速缓冲存储器。处理子系统与包括存储器的存储器子系统704相连,所述存储器例如可以包括SRAM、闪存和SDRAM部件。所述存储器子系统可以实施一个或多个DMA类型硬件,从而如本领域周知的那样使得数据访问更加便利。存储器子系统包括可以被处理器子系统执行的计算机可执行指令。

[0098] 在本发明的一个示例性实施例中,所述设备可以包括一个或多个无线接口(706),适于连接至一个或多个无线网络。通过实施合适的天线和调制解调器子系统,所述多个无线接口可以支持不同的无线技术,例如GSM、CDMA、UMTS、LTE/LTE-A、WiMAX、WLAN、蓝牙等。

[0099] 用户接口子系统708包括任何数量的已知I/O,包括但不限于:键盘、触摸屏(例如,多点触摸接口)、LCD显示器、背光、扬声器、和/或麦克风。但是,应该认识到在某些应用中,可以排除这些部件中的一个或多个。例如PCMCIA卡类型客户端的实施例可以不使用用户接口(因为它们可以附载到与其物理和/或电气耦合的主装置的用户接口)。

[0100] 在该例示的实施例中,所述设备包括安全元件710,后者包括并操作eUICC应用。所述eUICC能够存储并访问多个用于与网络运营商进行认证的访问控制客户端。所述安全元件可以根据处理器子系统的请求而被存储器子系统访问。

[0101] 在一个示例性实施例中,所述安全元件至少包括可分区的存储器,所述可分区的存储器适于包括一个或多个访问控制客户端及其关联补丁。每个分区保持与其他分区相区别,并且从所述存储器分区执行的软件不能访问其他无关的分区或被其他无关的分区访问。

[0102] 所述安全元件也包括安全领域已知类型的所谓“安全微处理器”或SM。

[0103] 进一步地,示例性实施例的各种实现方式包括当执行时会启动简单引导操作系统(OS)的指令。所述引导操作系统进一步被配置为从安全元件选择至少一个分区,并用其加载适当的访问控制客户端。在各种实现中,访问控制客户端可以被进一步提供有与受信签署者相关联的一个或多个证书。所述引导OS可以在执行访问控制客户端之前验证所述证书。

[0104] 进一步地,在一个实施例中,所述安全元件保有所存储的访问控制客户端的列表或清单。所述清单可以包括所存储的访问控制客户端的当前状态的信息;这类信息可以包括可用性、完整性、有效性、先前经历的错误等。所述清单可以进一步被链接或耦合到用户接口,从而使得用户能够选择可用的访问控制客户端。

[0105] 参考回图7,安全元件710能够接收并存储用于一个或多个访问控制客户端的部件来与网络运营商进行认证。在一个示例性实施例中,安全元件具有关联的设备密钥和资格

证书。这个设备密钥被用于保护并验证在以前不知道的多方(例如,UE和第三方)之间的通信。

[0106] 在这类变形中,所述设备密钥是非对称公钥/私钥对中的私钥。对应公钥可以被自由地分配,而不会危及私钥的完整性。例如,设备可以被指定(或内部生成)RSA公钥/私钥;所述公钥对部署后的通信可用。

[0107] 进一步地,在某些变形中,所述资格证书是与受信实体相关联的唯一签署的数字签名。在一个示例性的情景中,所述资格证书可以由第三方实体验证,并提供示例性装置的完整性的证明。

[0108] 虽然前述的用于编程安全元件的方法和装置是关于RSA密钥对而例示的,但是本领域普通技术人员很容易理解其他认证方案可以类似地替代。例如,在其他变形中,设备密钥可以是共享密钥,其中共享密钥的分配被高度地保护。再一些实施例还可以基于证书而不是密码交换。

[0109] 根据一些实施例,附图8示出了根据上述本发明的原理配置的无线装置800的功能性框图。所述无线装置的功能性框图可以通过硬件、软件或硬件和软件的结合来执行本发明的原理。本领域技术人员可以理解图8所描述的功能块可被组合或被分成子块来实现如上所述的本发明的原理。因此,在此的描述可以支持在此描述的功能块的任何可能的结合或分离或进一步限定。

[0110] 如图8所示,无线设备800包括一个或多个无线链路802、安全元件804、安全元件的接口808以及处理器810。所述一个或多个无线链接802适于与至少一个网络(未示出)通信。安全元件804被配置为存储访问控制客户端806。所述接口808具有加密密钥和与其关联的第一证书。所述处理器810具有发送单元812、接收单元814、验证单元816和存储单元818。

[0111] 在一个实施例中,发送单元812经由所述接口为特定于所述至少一个网络的访问控制客户端发送对一个或多个部件的请求。接收单元814接收一个或多个所请求的部件和第二证书。验证单元816验证第二证书,并且响应于所述第二证书的成功校验,存储单元818将访问控制客户端存储到安全元件。

[0112] 在一些实施例中,处理器810被配置为:经由接口为特定于所述至少一个网络的访问控制客户端发送对一个或多个部件的请求(例如,用发送单元812);接收一个或多个所请求的部件和第二证书(例如,用接收单元814);验证第二证书(例如,用验证单元816),并且响应于所述第二证书的成功校验将访问控制客户端存储到安全元件(例如,用存储单元818)。

[0113] 在一些实施例中,访问控制客户端806包括一个或多个电子订户身份模块(eSIMs)822。安全元件804包括电子通用集成电路卡(eUICC)824,并且一个或多个eSIM中的每一个都与一个国际移动用户标识符(IMSI)相关联。每个eSIM进一步被配置为至少部分基于认证与密钥协商(AKA)建立与蜂窝网络的安全连接。

[0114] 在一些实施例中,至少一个网络包括全球移动通信标准(GSM)网络。

[0115] 在一些实施例中,至少一个网络包括通用移动电信系统(UMTS)网络。

[0116] 在一些实施例中,至少一个网络包括码分多址访问2000(CDMA 2000)网络。

[0117] 在一些实施例中,所述请求包括第一资格证书。

[0118] 在一些实施例中,加密密钥被唯一地与第一资格证书相关联。

[0119] 在一些实施例中，加密密钥具有可以被公开分配的非对称对应密钥。

[0120] 在一些实施例中，非对称对应密钥确保了到无线装置的安全传输。

[0121] 在一些实施例中，一个或多个部件包括已使用会话密钥加密的访问控制客户端，并且第一和第二证书分别包括第一和第二资格证书。

[0122] 在一些实施例中，所述会话密钥是随机生成的。

[0123] 将会认识到虽然本发明在某些方面按照方法的一定顺序或步骤描述，但是这些描述只是本发明的更广泛方法的例示，并可以根据特定应用的需要而被修改。某些步骤在某些情况下并不是必须实施或是可选择的。另外，某些步骤或功能可以被添加到公开的实施例，或改变两个或两个以上步骤执行的顺序。所有这样的变形都涵盖在此处公开和声明的本发明中。

[0124] 虽然以上的详细描述业已示出、描述和指出了本发明应用到各个实施例中的新颖特征，但是可以理解本领域技术人员可以做出多种对所示出的设备或过程形式和细节上的省略、替换和改变而不背离本发明。前述的描述是现在能想到的执行本发明的最佳模式。这些描述绝不意味着限制，而应该被视作本发明的一般性原理的例示。本发明的范围应参考权利要求来确定。

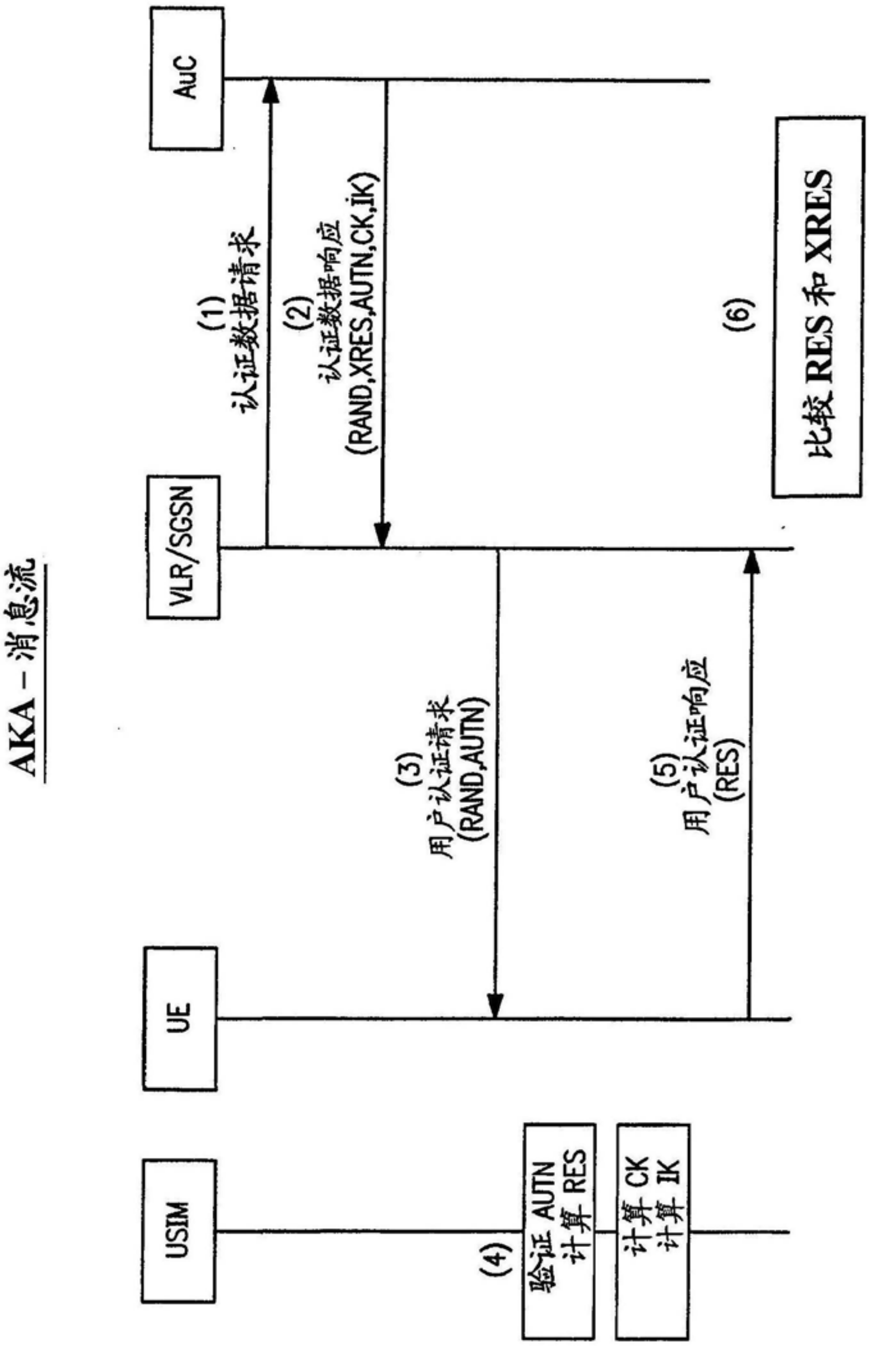

AKA－消息流
USIM
UE
VLR/SGSN
AuC
(1)
认证数据请求
(2)
认证数据响应
(RAND,XRES,AUTN,CK,IK)
(3)
用户认证请求
(RAND,AUTN)
(4)
验证 AUTN
计算 RES
计算 CK
计算 IK
(5)
用户认证响应
(RES)
(6)
比较 RES 和 XRES

图1(现有技术)

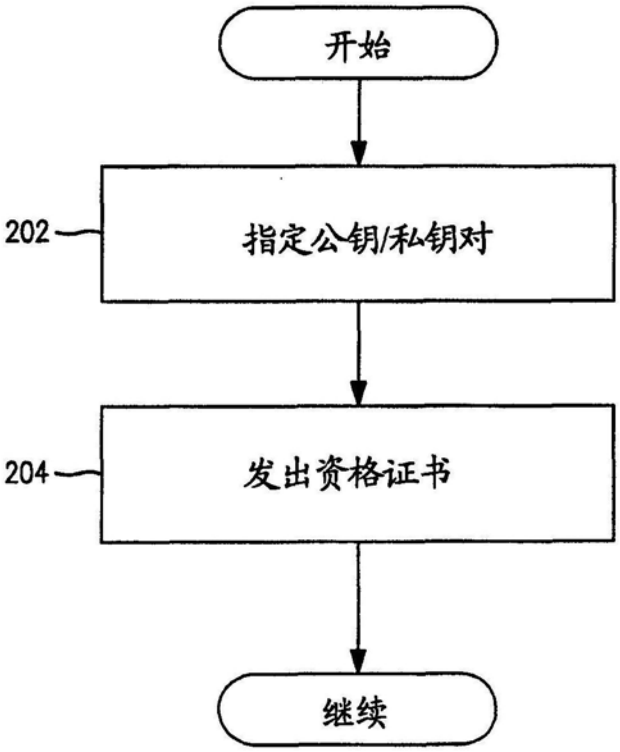


图2

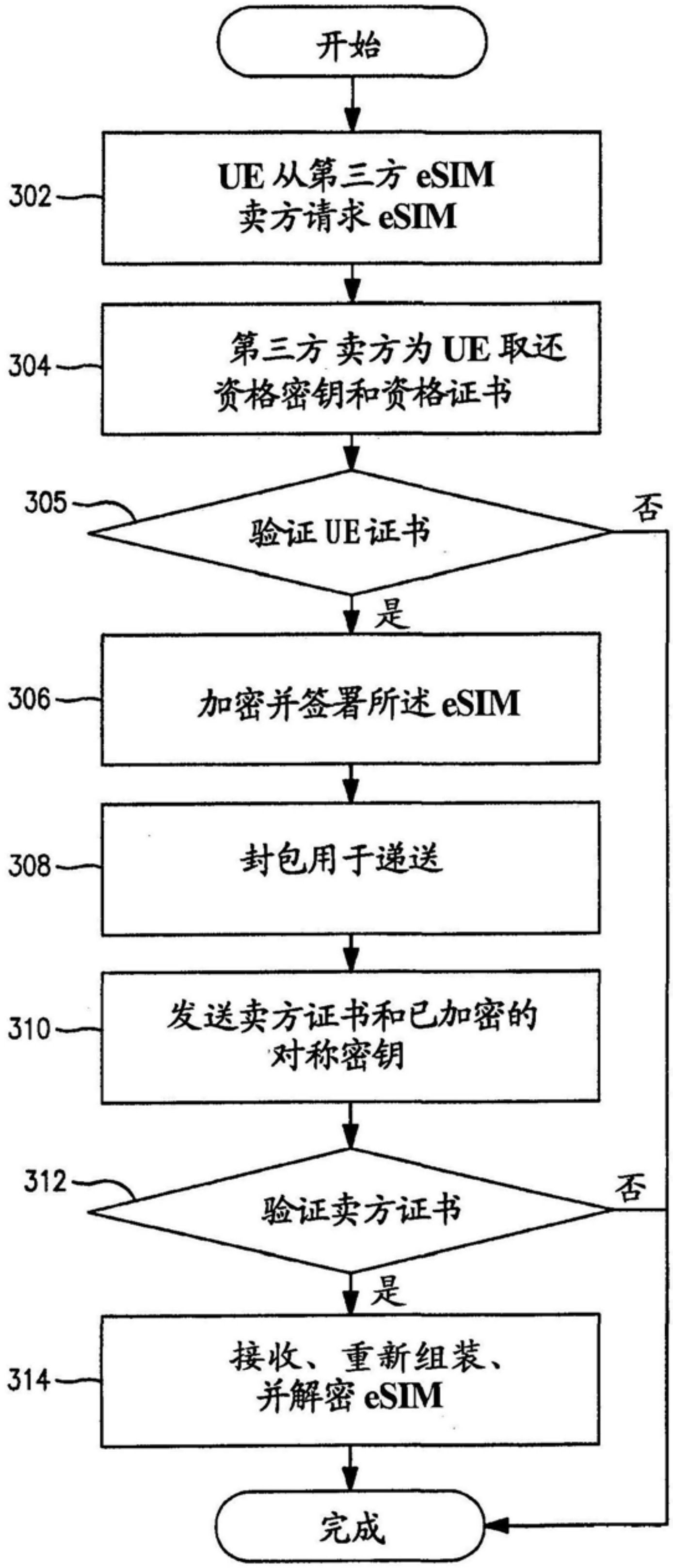

开始
302
UE从第三方eSIM卖方请求eSIM
304
第三方卖方为UE取还资格密钥和资格证书
305
验证UE证书
否
是
306
加密并签署所述eSIM
308
封包用于递送
310
发送卖方证书和已加密的对称密钥
312
验证卖方证书
否
是
314
接收、重新组装、并解密eSIM
完成

图3

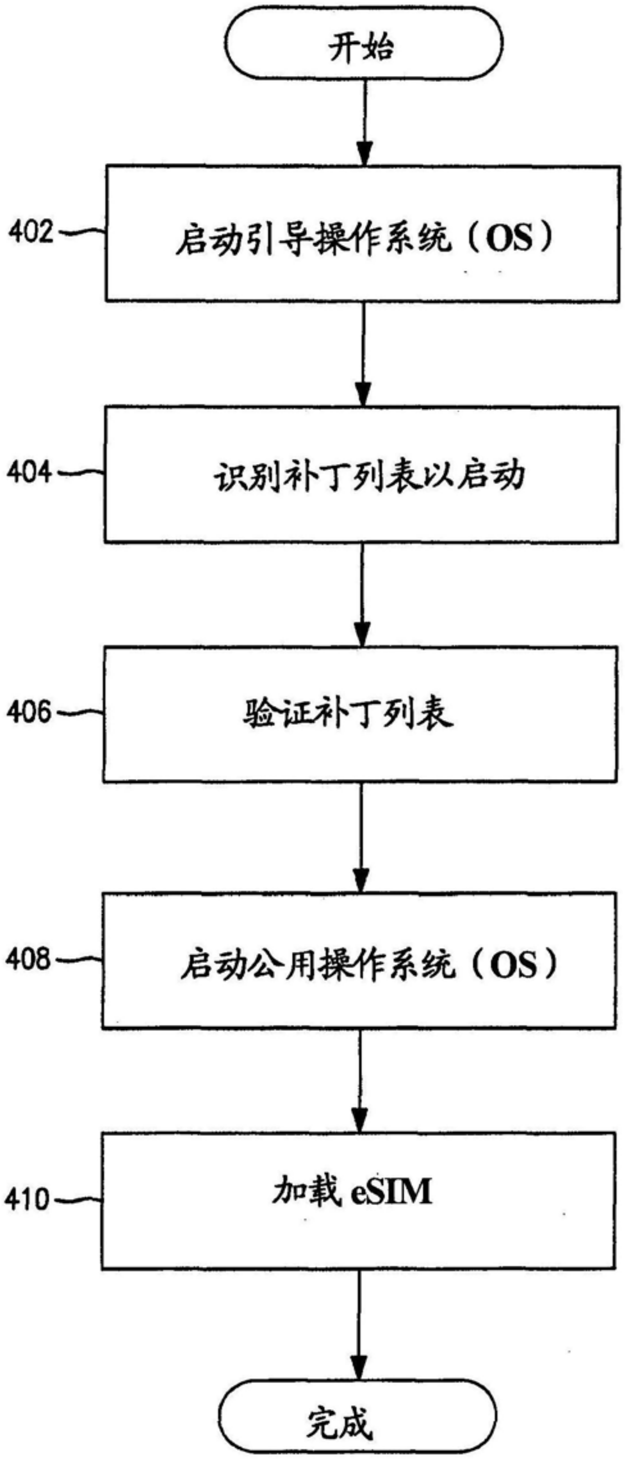
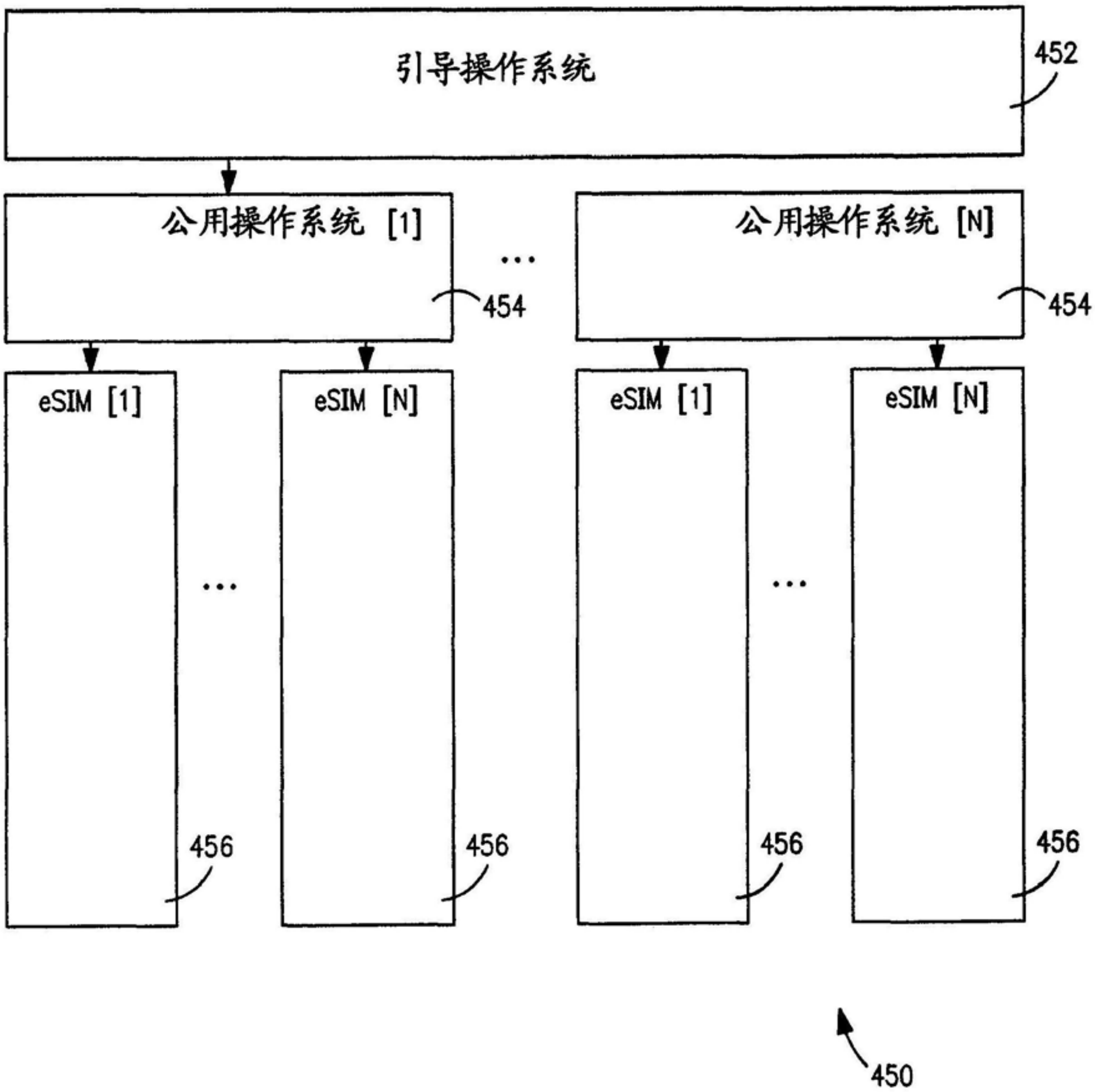

开始
402
启动引导操作系统（OS）
404
识别补丁列表以启动
406
验证补丁列表
408
启动公用操作系统（OS）
410
加载 eSIM
完成

图4



引导操作系统
452
公用操作系统 [1]
454
公用操作系统 [N]
454
eSIM [1]
eSIM [N]
eSIM [1]
eSIM [N]
456
456
456
456
450

图4A

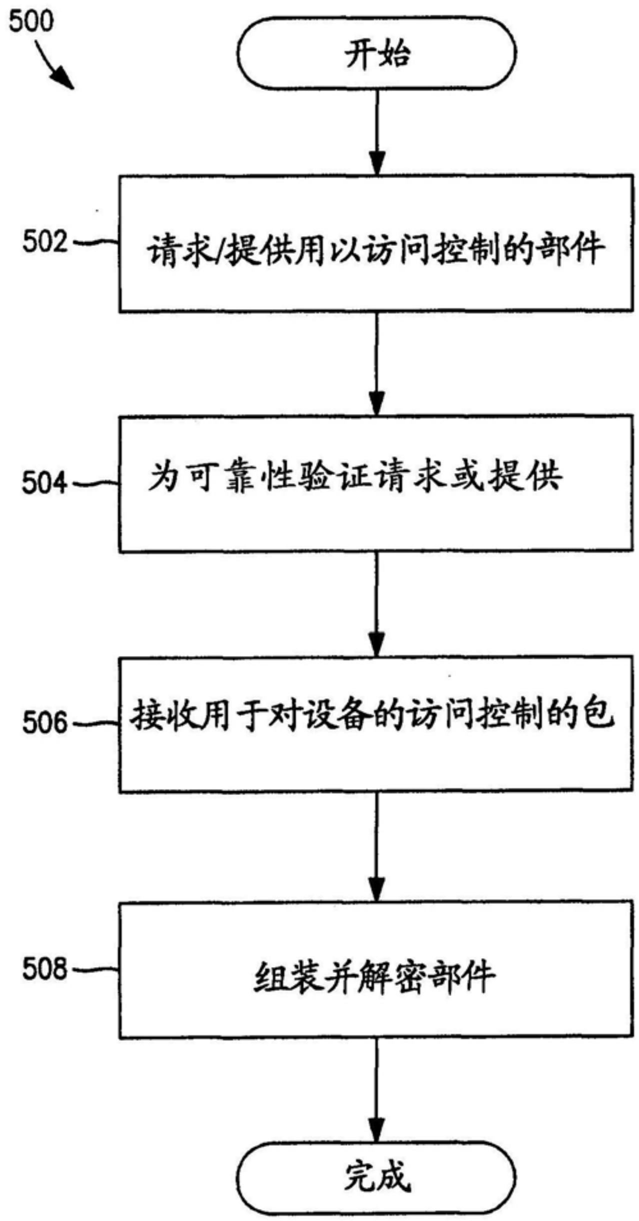

500
开始
502
请求/提供用以访问控制的部件
504
为可靠性验证请求或提供
506
接收用于对设备的访问控制的包
508
组装并解密部件
完成

图5

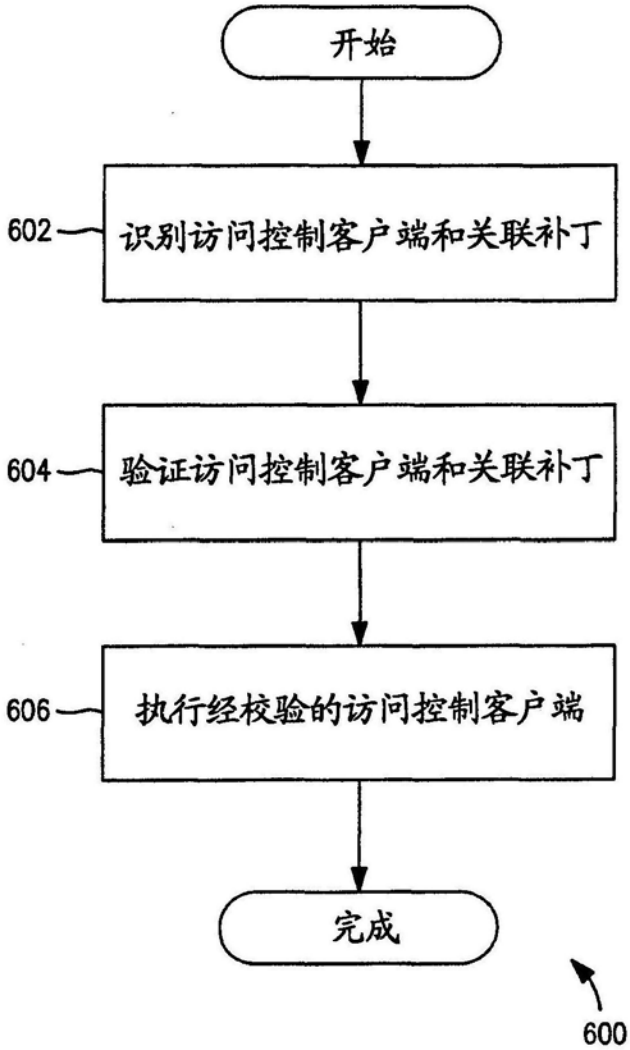

开始
602
识别访问控制客户端和关联补丁
604
验证访问控制客户端和关联补丁
606
执行经校验的访问控制客户端
完成
600

图6

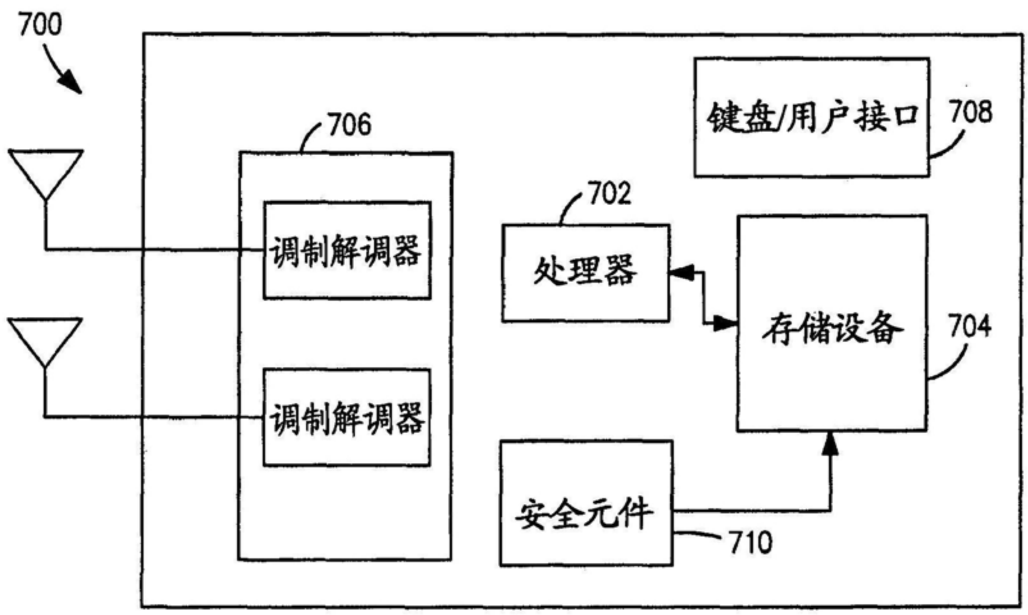


图7

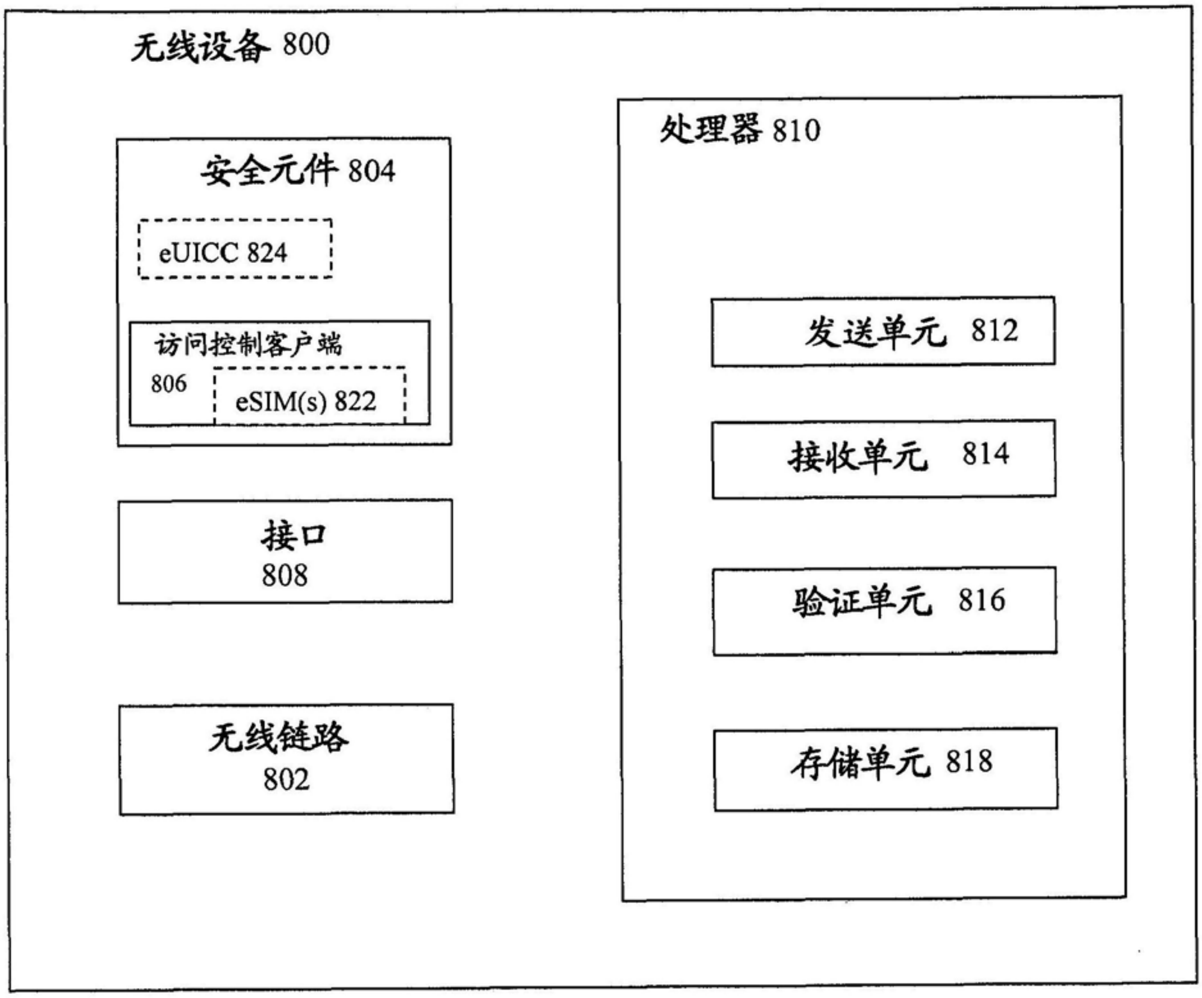

无线设备 800
安全元件 804
eUICC 824
访问控制客户端
806
eSIM(s) 822
接口
808
无线链路
802
处理器 810
发送单元 812
接收单元 814
验证单元 816
存储单元 818

图8