(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 107948977 B
(45)授权公告日 2021.02.26

(21)申请号 201711272555.1
(22)申请日 2012.05.20
(65)同一申请的已公布的文献号
申请公布号 CN 107948977 A
(43)申请公布日 2018.04.20
(30)优先权数据
13/153,290 2011.06.03 US
(62)分案原申请数据
201280027078.1 2012.05.20
(73)专利权人 波音公司
地址 美国伊利诺伊州
(72)发明人 F·文
(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 徐东升 赵蓉民
(51)Int.Cl.
H04W 12/06(2021.01)
H04L 29/06(2006.01)
H04W 4/021(2018.01)
(56)对比文件
CN 101309272 A,2008.11.19
CN 101309272 A,2008.11.19
US 2010146500 A1,2010.06.10
CN 101064628 A,2007.10.31
US 2006218622 A1,2006.09.28
CN 101026466 A,2007.08.29
CN 101083530 A,2007.12.05
审查员 赵勇达

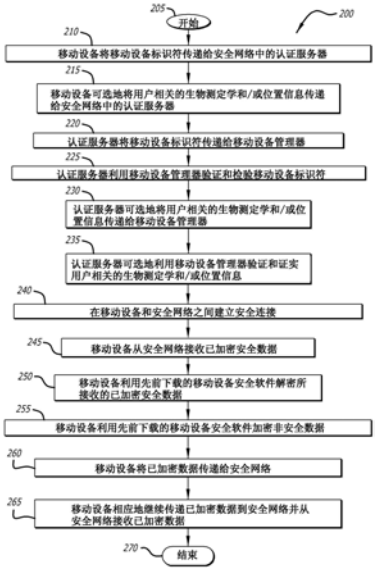
权利要求书4页 说明书8页 附图4页

(54)发明名称

用于非安全移动设备与安全网络建立通信的系统和方法

(57)摘要

本发明公开了用于利用在非安全网络中操作的非安全移动设备(105,310)与安全网络(320)建立通信的系统、方法和装置。所公开的方法涉及将移动设备标识符传送给安全网络(320)。在一个或更多实施例中,移动设备标识符是互联网协议(IP)地址和/或唯一标识(ID)代码。该方法进一步涉及利用安全网络(320)中的移动设备管理器(130,380)来验证和/或证实移动设备标识符。同样,该方法涉及在移动设备(105,310)和安全网络(320)之间建立安全连接(136,137)。另外,该方法涉及利用移动设备(105,310)从安全网络(320)接收已加密安全数据。进一步地,该方法涉及由移动设备(105,310)利用先前下载的移动设备安全软件来解密所接收的已加密安全数据。



CN 107948977 B

1.一种用于允许利用在非安全网络中操作的非安全移动设备与安全网络建立通信的方法,所述方法包括:

将请求传送到所述安全网络以下载移动设备安全软件;

由所述移动设备从所述安全网络下载并安装所述移动设备安全软件;

由所述移动设备激活所述移动设备安全软件;

利用所述移动设备将移动设备管理器登记请求传递到所述安全网络;

利用所述移动设备管理器基于所述移动设备的唯一数据项描述即UDID来证实所述移动设备;以及

由所述移动设备管理器将移动设备标识符传递到所述移动设备,

其中在认证服务器从所述移动设备接收到所述移动设备标识符之后并且在所述认证服务器将所述移动设备已经被证实传递给所述安全网络中的访问路由器之后,所述移动设备标识符允许所述移动设备经由所述访问路由器与所述安全网络建立直接通信。

2.根据权利要求1所述的方法,其中所述方法进一步包括:

利用所述移动设备管理器在载体访问列表上列入所述移动设备的电话号码,

其中来自在所述载体访问列表上具有其电话号码的移动设备的后续加密数据传送将被自动地路由到所述安全网络。

3.一种用于利用在非安全网络中操作的非安全移动设备与安全网络建立通信的系统,所述系统包括:

所述移动设备,其被配置为将移动设备标识符传送到认证服务器;

所述认证服务器,其被配置为接收所述移动设备标识符,将所述移动设备标识符传递到所述安全网络中的移动设备管理器,利用所述移动设备管理器证实所述移动设备标识符,并且将所述移动设备已经被证实传递给所述安全网络中的访问路由器;

所述移动设备管理器,其被配置为利用所述认证服务器证实所述移动设备标识符;以及

应用数据库系统,

其中当所述移动设备标识符被证实时并且在所述认证服务器将所述移动设备已经被证实传递给所述安全网络中的所述访问路由器之后,在所述移动设备和所述安全网络之间的经由所述访问路由器的直接安全连接被建立。

4.根据权利要求3所述的系统,其中所述移动设备被配置为经由蜂窝网络、Wi-Fi网络和旁波段网络中的至少一个将所述移动设备标识符传送给所述认证服务器。

5.根据权利要求3所述的系统,其中所述移动设备管理器进一步被配置为将对所述移动设备标识符的请求发送到所述移动设备。

6.根据权利要求3所述的系统,其中所述移动设备标识符是互联网协议地址即IP地址。

7.根据权利要求3所述的系统,其中所述移动设备标识符是唯一标识代码即唯一ID代码。

8.根据权利要求3所述的系统,其中移动设备管理器进一步被配置为利用所述认证服务器证实所述移动设备的用户。

9.根据权利要求8所述的系统,其中移动设备管理器进一步被配置为通过使用所述移动设备的用户的生物测定学利用所述认证服务器证实所述用户。

10.根据权利要求3所述的系统，其中所述移动设备管理器进一步被配置为通过确定所述移动设备的位置利用所述认证服务器证实所述移动设备。

11.根据权利要求3所述的系统，其中所述移动设备进一步被配置为从所述安全网络接收已加密安全数据并且使用移动设备安全软件解密所接收的已加密安全数据。

12.根据权利要求3所述的系统，其中所述移动设备进一步被配置为使用移动设备安全软件加密非安全数据并且将已加密数据传递给所述安全网络。

13.一种用于利用在非安全网络中操作的非安全移动设备与安全网络建立通信的系统，所述系统包括：

所述移动设备，其被配置为将具有移动设备标识符的请求传送给认证服务器以建立所述移动设备和所述安全网络之间的安全连接；

所述认证服务器，其被配置为接收具有所述移动设备标识符的所述请求，将所述移动设备标识符传递给在所述安全网络中的移动设备管理器，利用所述移动设备管理器证实所述移动设备标识符，并且将所述移动设备已经被证实传送给所述安全网络中的访问路由器；

所述移动设备管理器，其被配置为利用所述认证服务器证实所述移动设备标识符；以及

应用数据库系统；

其中当所述移动设备标识符被证实时并且在所述认证服务器将所述移动设备已经被证实传递给所述安全网络中的所述访问路由器之后，建立所述移动设备与所述安全网络之间的经由所述访问路由器的直接安全连接。

14.根据权利要求13所述的系统，其中所述移动设备被配置为在蜂窝网络和Wi-Fi网络中的至少一个中操作。

15.根据权利要求13所述的系统，其中所述移动设备管理器进一步被配置发送对所述移动设备标识符的请求。

16.根据权利要求13所述的系统，其中所述移动设备标识符是互联网协议地址即IP地址。

17.根据权利要求13所述的系统，其中所述移动设备标识符是唯一标识代码即唯一ID代码。

18.根据权利要求13所述的系统，其中所述移动设备管理器进一步被配置为利用所述认证服务器证实所述移动设备的用户。

19.根据权利要求18所述的系统，其中所述移动设备管理器进一步被配置为通过使用所述用户的生物测定学利用所述认证服务器证实所述用户。

20.根据权利要求13所述的系统，其中所述系统进一步包括：

发送器，其被配置为将已加密安全数据从所述安全网络传递到所述移动设备。

21.根据权利要求13所述的系统，其中所述系统进一步包括：

接收器，其被配置为从所述移动设备接收已加密数据；以及

处理器，其被配置为解密所接收的已加密数据。

22.根据权利要求13所述的系统，其中所述移动设备管理器进一步被配置为通过确定所述移动设备的位置利用所述认证服务器证实所述移动设备。

23.一种用于允许利用在非安全网络中操作的非安全移动设备与安全网络建立通信的系统,所述系统包括:

所述移动设备,其被配置为将请求传送到所述安全网络以下载移动设备安全软件,所述移动设备被配置为下载并安装从所述安全网络接收的所述移动设备安全软件,所述移动设备被配置为激活所述移动设备安全软件,并且所述移动设备被配置为经由认证服务器将移动设备管理器登记请求传递到移动设备管理器;以及

所述移动设备管理器,其被配置为基于所述移动设备的唯一数据项描述即UDID来证实所述移动设备,并且被配置为将移动设备标识符传递到所述移动设备,

其中在所述认证服务器从所述移动设备接收到所述移动设备标识符之后并且在所述认证服务器将所述移动设备已经被证实传递给所述安全网络中的访问路由器之后,所述移动设备标识符允许所述移动设备经由所述访问路由器与所述安全网络建立直接通信。

24.根据权利要求23所述的系统,其中所述移动设备管理器进一步被配置为在载体访问列表上列入所述移动设备的电话号码,

其中来自在所述载体访问列表上具有其电话号码的移动设备的后续加密数据传送将被自动地路由到所述安全网络。

25.一种用于利用在非安全网络中操作的非安全移动设备与安全网络建立通信的系统,所述系统包括:

在所述安全网络中的移动设备管理器,

其中所述移动设备管理器被配置为利用认证服务器证实与所述移动设备相关联的移动设备标识符,并且

其中当所述移动设备标识符被证实时并且在所述认证服务器将所述移动设备已经被证实传递给所述安全网络中的访问路由器之后,建立所述移动设备与所述安全网络之间的经由所述访问路由器的直接安全连接。

26.根据权利要求25所述的系统,其中所述移动设备管理器进一步被配置为将对所述移动设备标识符的请求发送到所述移动设备。

27.根据权利要求25所述的系统,其中所述移动设备标识符是互联网协议地址即IP地址。

28.根据权利要求25所述的系统,其中所述移动设备标识符是唯一标识代码即唯一ID代码。

29.根据权利要求25所述的系统,其中移动设备管理器进一步被配置为利用所述认证服务器证实所述移动设备的用户。

30.根据权利要求29所述的系统,其中移动设备管理器进一步被配置为通过使用所述移动设备的用户的生物测定学利用所述认证服务器证实所述用户。

31.根据权利要求25所述的系统,其中所述移动设备管理器进一步被配置为通过确定所述移动设备的位置利用所述认证服务器证实所述移动设备。

32.一种用于与在非安全网络中操作的非安全移动设备建立通信的安全网络,所述安全网络包括:

移动设备管理器,其被配置为利用认证服务器证实与所述移动设备相关联的移动设备标识符,

其中当所述移动设备标识符被证实时并且在所述认证服务器将所述移动设备已经被证实传递给所述安全网络中的访问路由器之后，在所述移动设备与所述安全网络之间的经由所述访问路由器的直接安全连接被建立；和

应用数据库系统。

33.根据权利要求32所述的安全网络，其中所述移动设备管理器进一步被配置为将对所述移动设备标识符的请求发送到所述移动设备。

34.根据权利要求32所述的安全网络，其中所述移动设备标识符是互联网协议地址即IP地址。

35.根据权利要求32所述的安全网络，其中所述移动设备标识符是唯一标识代码即唯一ID代码。

36.根据权利要求32所述的安全网络，其中移动设备管理器进一步被配置为利用所述认证服务器证实所述移动设备的用户。

37.根据权利要求36所述的安全网络，其中移动设备管理器进一步被配置为通过使用所述移动设备的用户的生物测定学利用所述认证服务器证实所述用户。

38.根据权利要求32所述的安全网络，其中所述移动设备管理器进一步被配置为通过确定所述移动设备的位置利用所述认证服务器证实所述移动设备。

39.根据权利要求32所述的安全网络，其中所述安全网络进一步包括安全数据存储器、远程桌面访问系统、移动网络应用系统和网站单点登录系统中的至少一个。

用于非安全移动设备与安全网络建立通信的系统和方法

[0001] 本申请是于2012年05月20日提交的名称为“移动网络”的中国专利申请201280027078.1的分案申请。

技术领域

[0002] 本公开的实施例总体涉及与安全网络建立通信。更具体地，本公开的实施例涉及利用在非安全网络控制中操作的非安全移动设备与安全网络建立通信。

背景技术

[0003] 本公开涉及与安全网络建立通信。特别地，它涉及利用在非安全网络中操作的非安全移动设备与安全网络建立通信。所公开的方法涉及将移动设备标识符传送给安全网络。在一个或更多实施例中，移动设备标识符是互联网协议(IP)地址和/或唯一标识(ID)代码。该方法进一步涉及利用安全网络中的移动设备管理器来验证和/或证实移动设备标识符。同样，该方法涉及在移动设备和安全网络之间建立安全连接。另外，该方法涉及利用移动设备从安全网络接收已加密安全数据。进一步地，该方法涉及由移动设备利用先前下载的移动设备安全软件来解密所接收的已加密安全数据。

发明内容

[0004] 本公开涉及利用在非安全网络中操作的非安全移动设备与安全网络建立通信的系统、方法和装置。特别地，所公开的方法包括将移动设备标识符传送给安全网络。该方法进一步包括利用安全网络中的移动设备管理器来验证和/或证实移动设备标识符。在一个或更多实施例中，移动设备管理器是实际用作验证设备以验证移动设备标识符的服务器。另外，该方法包括在移动设备和安全网络之间建立安全连接。

[0005] 在一个或更多实施例中，经由蜂窝网络、Wi-Fi网络和/或旁波段(out-of-band)网络将移动设备标识符传送给安全网络。在某些实施例中，该方法进一步包括利用移动设备管理器发送对移动设备标识符的请求。在一个或更多实施例中，移动设备标识符是互联网协议(IP)地址。在至少一个实施例中，移动设备标识符是唯一标识(ID)代码。

[0006] 在一个或更多实施例中，该方法进一步包括利用移动设备管理器来验证和/或证实移动设备的用户。在至少一个实施例中，通过利用用户的生物测定学来验证和/或证实移动设备的用户。在某些实施例中，通过分析和/或确定移动设备的位置来验证和/或证实移动设备的用户和/或移动设备本身。

[0007] 在至少一个实施例中，该方法进一步包括利用移动设备从安全网络接收已加密安全数据。进一步地，该方法包括由移动设备利用先前下载的移动设备安全软件来解密所接收的已加密安全数据。在至少一个实施例中，先前下载的移动设备安全软件被用于对已加密安全数据进行解密和/或对非安全数据进行加密。在一个或更多实施例中，该方法进一步包括由移动设备利用先前下载的移动设备安全软件来加密非安全数据；以及利用移动设备将已加密数据传递给安全网络。在至少一个实施例中，移动设备安全软件包括加密软件、解

密软件和/或强制固定目的地寻址软件。

[0008] 在一个或更多实施例中，一种用于与安全网络建立通信的在非安全网络中操作的非安全移动设备包括发送器、接收器和处理器。发送器被配置用于将移动设备标识符传送给安全网络，并且接收器被配置用于从安全网络接收已加密安全数据。另外，处理器被配置用于利用先前下载的移动设备安全软件来解密所接收的已加密安全数据。在至少一个实施例中，处理器进一步被配置用于利用先前下载的移动设备安全软件加密非安全数据，并且发送器进一步被配置用于将已加密数据传递给安全网络。

[0009] 在至少一个实施例中，一种利用在非安全网络中操作的非安全移动设备与安全网络建立通信的方法包括将移动设备标识符传送给安全网络，以便在移动设备和安全网络之间建立安全连接。该方法进一步包括在移动设备和安全网络之间建立安全连接。同样地，该方法包括利用移动设备从安全网络接收已加密安全数据。另外，该方法包括由移动设备利用先前下载的移动设备安全软件来解密所接收的已加密安全数据。

[0010] 在一个或更多实施例中，一种利用在非安全网络中操作的非安全移动设备与安全网络建立通信的方法包括利用接收器从移动设备接收关于移动设备标识符的请求，以便在移动设备和安全网络之间建立安全连接。该方法进一步包括利用安全网络中的移动设备管理器来验证和/或证实移动设备标识符。另外，该方法包括在移动设备和安全网络之间建立安全连接。进一步地，该方法包括利用发送器将已加密安全数据从安全网络传递给移动设备。在至少一个实施例中，该移动设备在安全或非安全蜂窝网络和/或安全或非安全Wi-Fi网络中操作。在某些实施例中，该方法进一步包括利用接收器接收从移动设备传递的加密数据；以及利用处理器解密所接收的加密数据。

[0011] 在至少一个实施例中，一种允许利用在非安全网络中操作的非安全移动设备与安全网络建立通信的方法包括将请求传送给安全网络以下载移动设备安全软件。该方法进一步包括通过由移动设备下载并安装来自安全网络的移动设备安全软件。同样地，该方法包括由移动设备激活移动设备安全软件。

[0012] 另外，该方法包括利用移动设备将移动设备管理器登记请求传递给安全网络。同样，该方法包括由移动设备管理器基于移动设备的唯一数据项描述(UDID)来验证和/或证实该移动设备。进一步地，该方法包括由移动设备管理器将移动设备标识符传递给移动设备。移动设备标识符允许移动设备与安全网络建立通信。

[0013] 在某些实施例中，该方法进一步包括利用移动设备管理器在载体访问列表上列入移动设备的电话号码，其中来自在载体访问列表上具有其电话号码的移动设备的后续加密数据传送将被自动地路由到安全网络。

[0014] 这些特征、功能和优势可以在本发明的多个实施例中独立地实现或者可以在其他实施例中被组合。

附图说明

[0015] 本公开的这些和其他特征、方面和优势将通过以下描述、随附的权利要求和附图变得更好理解，其中：

[0016] 图1示出根据本公开的至少一个实施例利用在非安全网络中操作的非安全移动设备与安全网络建立通信的系统的架构图。

[0017] 图2示出根据本公开的至少一个实施例的关于图1描述的系统的操作的流程图。

[0018] 图3A和图3B示出根据本公开的至少一个实施例由非安全移动设备获得移动设备安全软件和移动设备标识符的过程。

[0019] 图3A示出根据本公开的至少一个实施例下载、安装和激活移动设备安全软件的非安全移动设备的示意图。

[0020] 图3B示出根据本公开的至少一个实施例传递移动设备管理器登记请求和接收移动设备标识符的非安全移动设备的示意图。

[0021] 图4示出根据本公开的至少一个实施例的关于图3A和图3B所示的过程的流程图。

具体实施方式

[0022] 本文公开的方法和装置提供用于与安全网络建立通信的操作系统。具体地，该系统涉及利用在非安全网络中操作的非安全移动设备与安全网络建立通信。特别地，本公开教导了用于非安全移动设备如个人数字助理(PDA)访问安全网络的方式。目前，市售PDA(例如iPhone和iPad)不具有保护私有数据的安全架构。本公开提供一种允许在非安全网络中操作的市售现成的非安全移动设备能够访问安全网络的系统。对于本公开的至少一种应用，在野外部署的士兵利用采用所公开系统的现成的非安全移动设备，以便向安全网络传递数据并从安全网络接收数据。对于某些应用，士兵利用采用所公开系统的现成的非安全移动设备，以便彼此能够具有安全的通信。

[0023] 在以下具体实施方式中，阐述了许多具体的细节以便提供系统的更彻底描述。然而，对本领域技术人员来说显而易见的是，可以在没有这些具体细节的情况下实施所公开的系统。在其他实例中，没有详细地描述众所周知的特征，以免不必要地混淆该系统。

[0024] 图1示出根据本公开的至少一个实施例利用在非安全网络中操作的非安全移动设备105与安全网络建立通信的系统100的架构图。在该图中，移动设备安全软件被下载到移动设备105上。移动设备安全软件可用于解密已加密安全数据和/或加密非安全数据和/或将数据强制指定到专用地址，包含非武装地带(DMZ)或安全网络中的地址。在图3A、图3B和图4的讨论中介绍关于移动设备安全软件的安装程序的细节。

[0025] 在图1中，在系统100的操作期间，非安全移动设备105首先将移动设备标识符传递给安全网络。在至少一个实施例中，移动设备105利用非安全声音/数据蜂窝连接110(例如3G/4G蜂窝连接)将移动设备标识符传递给安全网络。当这样做时，移动设备105经由蜂窝塔120将移动设备标识符传递给安全网络的认证服务器115。应该注意到，针对这些实施例，移动设备105也能够经由蜂窝塔120利用声音蜂窝连接110进行非安全通话122。

[0026] 在某些实施例中，移动设备105通过非安全Wi-Fi连接123将移动设备标识符传递给安全网络。针对这些实施例，移动设备105经由Wi-Fi访问点125将移动设备标识符传递给认证服务器115。应该注意到，在其他实施例中，除了蜂窝连接或Wi-Fi连接之外，移动设备105可以利用多种通信手段将旁波段移动设备标识符传送给安全网络的认证服务器115和/或移动设备管理器130。这样的一个示例是，其中移动设备用户利用不同的电话呼叫求助台操作员，向求助台操作员证实他自己或她自己，告诉求助台操作员移动设备标识符，以及使求助台操作者将移动设备标识符输入移动设备管理器130和/或认证服务器115中。可替换地，移动设备用户可以通过不同的远程系统访问安全网络，对那个系统证实他自己或她自

己，然后将移动设备标识符输入移动设备管理器130和/或认证服务器115中。

[0027] 移动设备标识符提供用于安全网络识别和验证移动设备105的手段。在一个或更多实施例中，移动设备标识符是互联网协议(IP)地址、唯一标识(ID)代码或者IP地址和唯一ID代码的组合，如安全设备标识符或电话号码。在其他实施例中，移动设备标识符是随机数或包含随机数，该随机数由包含在先前下载的移动设备安全软件中的随机数发生器算法产生。在某些实施例中，该随机数周期性地改变，例如当移动设备105移动时改变，以特定的时间间隔改变，和/或在电话通话之间改变。在至少一个实施例中，该随机数从真实随机数变成假随机数，以便混淆任何可能的偷听者。

[0028] 在认证服务器115接收移动设备标识符之后，认证服务器115将移动设备标识符传递给安全网络中的移动设备管理器130。移动设备管理器130连同认证服务器115一起利用移动设备标识符来识别和验证移动设备105。应该注意，在某些实施例中，移动设备管理器130连同认证服务器115一起也证实移动设备105的用户。对于这些实施例，移动设备管理器130通过利用用户的生物测定学和/或通过利用地理定位信号如全球定位系统(GPS)信号确定移动设备105是否位于合法位置处来证实移动设备105。

[0029] 在移动设备管理器130和认证服务器115识别、验证和/或证实移动设备105并且可选地证实移动设备105的用户之后，认证服务器115将该信息传递给访问路由器135。一旦访问路由器135接收该信息，安全网络就在移动设备105和访问路由器135之间建立直接的安全连接136、137(即该连接不通过认证服务器115进行路由)，其中移动设备105可以直接传递数据给安全网络并从安全网络接收数据。

[0030] 一旦建立数据连接136、137，安全网络就能够经由数据连接136、137将已加密安全数据传递给移动设备105。在移动设备105接收已加密安全数据之后，移动设备105中的处理器运行移动设备安全软件以解密已加密安全数据。另外，如果移动设备105的用户希望将数据传递给安全网络，移动设备105中的处理器将运行移动设备安全软件以加密该数据。在加密该数据之后，移动设备105将经由数据连接136、137将已加密数据传递给安全网络。应该注意，在某些实施例中，在移动设备105将移动设备标识符传递给安全网络之前，移动设备管理器130向移动设备105发送对移动设备标识符的请求。

[0031] 在该图中，安全网络被显示为也包括安全数据存储器140、远程桌面访问系统145、移动网络应用系统150、网站单点登录系统155和/或应用数据库系统172。安全数据存储器140在该图中被显示为包括远程桌面访问网关系统160、移动网络应用网关系统165和移动应用数据库访问网关系统170。

[0032] 当安全网络在移动设备105和访问路由器135之间建立直接的非安全连接136、137之后，移动设备105仍然能够访问公用互联网175。如果移动设备105的用户期望访问互联网175，则访问路由器135将经由网络地址翻译器(NAT)系统180和网络代理系统185将该连接路由到公用互联网175。域名系统(DNS)服务器190被用于将由用户输入的域名翻译成其相应的数字IP地址。

[0033] 在本公开的一个或更多实施例中，在非安全网络中操作的非安全移动设备105的用户能够通过经由安全网络的通信与在非安全网络中操作的另一个非安全移动设备105的另一个用户往来传送安全数据。该数据可以是多种类型的数据，其包含但不限于声音数据、视频数据和文本数据。在这些实施例中，第一移动设备105的第一用户和第二移动设备的第

二用户(未显示)已经具有建立到安全网络的直接连接136、137,从而两个移动设备105都可以直接地传递数据给安全网络并从安全网络接收数据。

[0034] 对于这些实施例,如果第一移动设备105的第一用户期望将安全数据传递给第二移动设备的第二用户,则第一移动设备105中的处理器将运行移动设备安全软件以便加密该数据。一旦该数据被加密,第一移动设备105将经由数据连接136、137将已加密数据传递给安全网络中的访问路由器135。然后,访问路由器135将经由直接数据连接将已加密数据传递给第二移动设备。在第二移动设备接收到已加密数据之后,第二移动设备中的处理器将运行移动安全软件以便解密已加密数据,从而第二用户能够理解该数据。

[0035] 应该注意,如果第一移动设备105一开始就具有建立到安全网络的直接连接136、137,但是第二移动设备没有,则第一移动设备105仍然能够经由安全网络将安全数据传送给第二移动设备。针对这些情况,如果第一移动设备105的第一用户期望将安全数据传递给第二移动设备的第二用户,则第一移动设备105中的处理器将运行移动设备安全软件以便加密该数据。一旦该数据被加密,第一移动设备105将经由数据连接136、137将已加密数据传递给安全网络中的访问路由器135。

[0036] 在访问路由器135接收到已加密数据之后,访问路由器135确定第二移动设备是否已经具有建立到该网络的直接连接。在访问路由器135确定第二移动设备尚不具有建立到该网络的直接连接之后,访问路由器135将传递请求给第二移动设备以要求将其移动设备标识符发送给安全网络进行验证。在第二移动设备接收到该请求之后,第二移动设备将其移动设备标识符发送给认证服务器115。然后,安全网络执行先前描述的程序以建立从第二移动设备到安全网络的直接安全连接。一旦建立了从第二移动设备到安全网络的直接安全连接,访问路由器135将已加密数据传递给第二移动设备。在第二移动设备接收到已加密安全数据之后,第二移动设备中的处理器将运行移动设备安全软件以便解密已加密安全数据。

[0037] 图2示出根据本公开的至少一个实施例的关于图1描述的系统的操作的流程图200。在该过程开始205时,移动设备将其移动设备标识符传递给安全网络中的认证服务器210。可选地,移动设备将用户相关的生物测定学和/或定位信息传递给安全网络中的认证服务器215。然后,认证服务器将移动设备标识符传递给移动设备管理器220。然后,认证服务器利用移动设备管理器来验证和证实移动设备标识符225。

[0038] 认证服务器可选地将用户相关的生物测定学和/或定位信息传递给移动设备管理器230。然后,认证服务器可选地利用移动设备管理器来验证和证实用户相关的生物测定学和/或定位信息235。

[0039] 然后,在移动设备和安全网络之间建立安全连接240。然后,移动设备经由所建立的连接从安全网络接收已加密安全数据245。在移动设备接收已加密安全数据之后,移动设备利用先前下载的移动设备安全软件解密所接收的已加密安全数据250。然后,移动设备利用先前下载的移动设备安全软件加密将要传递给安全网络的非安全数据255。在移动设备加密非安全数据之后,移动设备将已加密数据传递给安全网络260。因此,移动设备将继续传递加密数据给安全网络并从安全网络接收加密数据。然后,该过程结束270。

[0040] 图3A和图3B示出根据本公开的至少一个实施例由非安全移动设备获得移动设备安全软件和移动设备标识符的过程。特别地,图3A示出根据本公开的至少一个实施例非安

全移动设备310下载并安装移动设备安全软件以及激活移动设备310的移动设备安全软件的示意图300。在该图中，移动设备310首先可选地经由用户桌面计算机330发送请求给安全网络320以下载和安装移动设备安全软件。应该注意，可替换地，可以按照旁波段方式对安全网络320做出该请求，例如通过安全网络操作者，其已经获得用于授权和使能移动设备310的必要信息。在安全网络320接收该请求之后，安全网络320允许移动设备310下载并安装移动设备安全软件。在移动设备310可选地经由用户桌面计算机330下载并安装移动设备安全软件之后，移动设备310激活移动设备310上的移动设备安全软件。

[0041] 图3B示出根据本公开的至少一个实施例非安全移动设备310传递移动设备管理器登记请求和接收移动设备标识符的示意图360。在该图中，移动设备310首先将移动设备登记请求传递给安全网络。网络服务网关370可选地被用于翻译关于安全网络中的移动设备管理器380的移动设备管理器登记请求。在移动设备管理器380接收该请求之后，移动设备管理器380基于移动设备310的唯一数据项描述(UDID)来证实移动设备310。在移动设备管理器380证实了移动设备310之后，移动设备管理器380可选地经由网络服务网关370将移动设备标识符传递给移动设备310。

[0042] 在某些实施例中，一旦移动设备管理器380证实了移动设备310，移动设备管理器380就将移动设备的电话号码列入载体访问列表上。在载体访问列表上具有其电话号码的移动设备310将经由直接安全连接与安全网络进行通信。

[0043] 图4示出根据本公开的至少一个实施例针对图3A和图3B所示的过程的流程图400。在该过程开始405时，与安全网络进行通信以下载移动设备安全软件410。可选地，如果存在蜂窝网络连接，则在载体访问列表上列入移动设备电话号码415。然后，移动设备下载并安装来自安全网络的移动设备安全软件420。在移动设备下载并安装移动设备安全软件之后，移动设备激活安全软件425。

[0044] 然后，在移动设备和移动设备管理器之间建立安全连接430。然后，移动设备将移动设备登记请求传递给安全网络435。移动设备管理器基于移动设备的UDID来证实移动设备440。移动设备可选地基于用户相关的生物测定学和/或定位信息来证实移动设备445。在移动设备管理器证实移动设备之后，移动设备管理器将移动设备标识符传递给移动设备450。在移动设备管理器传递移动设备标识符之后，该过程结束455。

[0045] 本公开的一个方面涉及利用在非安全网络中操作的非安全移动设备105,310与安全网络320建立通信的方法。在一个示例中，该方法包括：将移动设备标识符传送给安全网络320；利用安全网络320中的移动设备管理器130,380证实移动设备标识符；以及在移动设备105,310和安全网络320之间建立安全连接136、137。在一个变体中，经由蜂窝网络、Wi-Fi网络和/或旁波段网络中的至少一个将移动设备标识符传送给安全网络320。在另一个示例中，该方法也包括利用移动设备管理器130,380发送对移动设备标识符的请求。在另一个可替换示例中，移动设备标识符是互联网协议(IP)地址。在另一个示例中，移动设备标识符是唯一标识(ID)代码。在另一变体中，该方法也包括利用移动设备管理器130,380证实移动设备105、310的用户。在另一个可替换示例中，通过利用用户的生物测定学来证实移动设备105,310的用户。在另一个示例中，通过确定移动设备105,310的位置来证实移动设备105,310。在另一个变体中，该方法也包括：利用移动设备105,310从安全网络320接收已加密安全数据；以及由移动设备105,310利用移动设备安全软件来解密所接收的加密安全数据。在

另一个示例中，该方法也包括：由移动设备105，310利用移动设备安全软件来加密非安全数据；以及利用移动设备105，310将已加密数据传递给安全网络320。

[0046] 本公开的另一个方面涉及用于与安全网络320建立通信的在非安全网络中操作的非安全移动设备105，310。在一个变体中，移动设备105，310包括：发送器，其被配置用于将移动设备标识符传送给安全网络320；接收器，其被配置用于从安全网络320接收已加密安全数据；以及处理器，其被配置用于利用移动设备安全软件解密所接收的加密安全数据。在一个示例中，移动设备安全软件包括加密软件、解密软件和/或强制固定目的地寻址软件中的至少一个。在另一个变体中，发送器经由蜂窝网络、Wi-Fi网络和/或旁波段网络中的至少一个将移动设备标识符传送给安全网络320。在另一个示例中，移动设备标识符是互联网协议(IP)地址。在另一个可替换示例中，移动设备标识符是唯一标识(ID)代码。在另一个变体中，处理器也被配置用于利用先前下载的移动设备安全软件对非安全数据进行加密，并且发送器也被配置用于将已加密数据传递给安全网络320。本公开的另一个方面涉及利用在非安全网络中操作的非安全移动设备105，310与安全网络320建立通信的方法。在一个变体中，该方法包括：将移动设备标识符传送给安全网络320，以便在移动设备105，310和安全网络320之间建立安全连接136，137；以及在移动设备105，310和安全网络320之间建立安全连接136，137。

[0047] 本公开的另一个方面涉及利用在非安全网络中操作的非安全移动设备105，310与安全网络320建立通信的方法。在一个示例中，该方法包括接收关于移动设备标识符的请求，以便在移动设备105，310和安全网络320之间建立安全连接136，137；利用安全网络320中的移动设备管理器130，380证实移动设备标识符；以及在移动设备105，310和安全网络320之间建立安全连接136，137。在另一个变体中，移动设备105，310在蜂窝网络和Wi-Fi网络的至少一个中操作。在一个可替换示例中，该方法也包括利用移动设备管理器130，380发送对移动设备标识符的请求。在另一个示例中，移动设备标识符是互联网协议(IP)地址。在另一个变体中，移动设备标识符是唯一标识(ID)代码。在另一个可替换示例中，该方法也包括利用移动设备管理器130，380证实移动设备105、310的用户。在另一个示例中，该方法也包括利用发送器将已加密安全数据从安全网络320传递给移动设备105，310。在另一个变体中，该方法也包括：利用接收器接收从移动设备105，310传递的已加密数据；以及利用处理器解密所接收的已加密数据。在一个示例中，通过利用用户的生物测定学来证实移动设备105，310的用户。在另一个可替换示例中，通过确定移动设备105，310的位置来证实移动设备105，310。

[0048] 本公开的另一方面涉及用于允许利用在非安全网络中操作的非安全移动设备105，310与安全网络320建立通信的方法。在一个变体中，该方法包括：传送请求给安全网络320以下载移动设备安全软件；由移动设备105，310下载并安装来自安全网络320的移动设备安全软件；由移动设备105，310激活移动设备安全软件；由移动设备105，310将移动设备管理器登记请求传递给安全网络320；由移动设备管理器130，380基于移动设备105，310的唯一数据项目描述(UDID)来证实移动设备105，310；以及由移动设备管理器130，380将移动设备标识符传递给移动设备105，310，其中移动设备标识符允许移动设备105，310与安全网络320建立通信。在另一个示例中，该方法也包含利用移动设备管理器130，380将移动设备105，310的电话号码列入载体访问列表上，其中来自在载体访问列表上具有其电话号码的

移动设备105,310的后续加密数据传送将被自动地路由到安全网络320。

[0049] 尽管此处已经公开了某些说明性的实施例和方法,但本领域技术人员可以从前述公开内容中显然可见,可以在未脱离所公开技术的实际精神和范围的情况下做出这些实施例和方法的变化和修改。存在所公开技术的很多其他示例,每一个只在细节的方面与其他的不同。因此,希望所公开的技术应该只限于随附的权利要求和适用法律的规则和原理要求的范围。

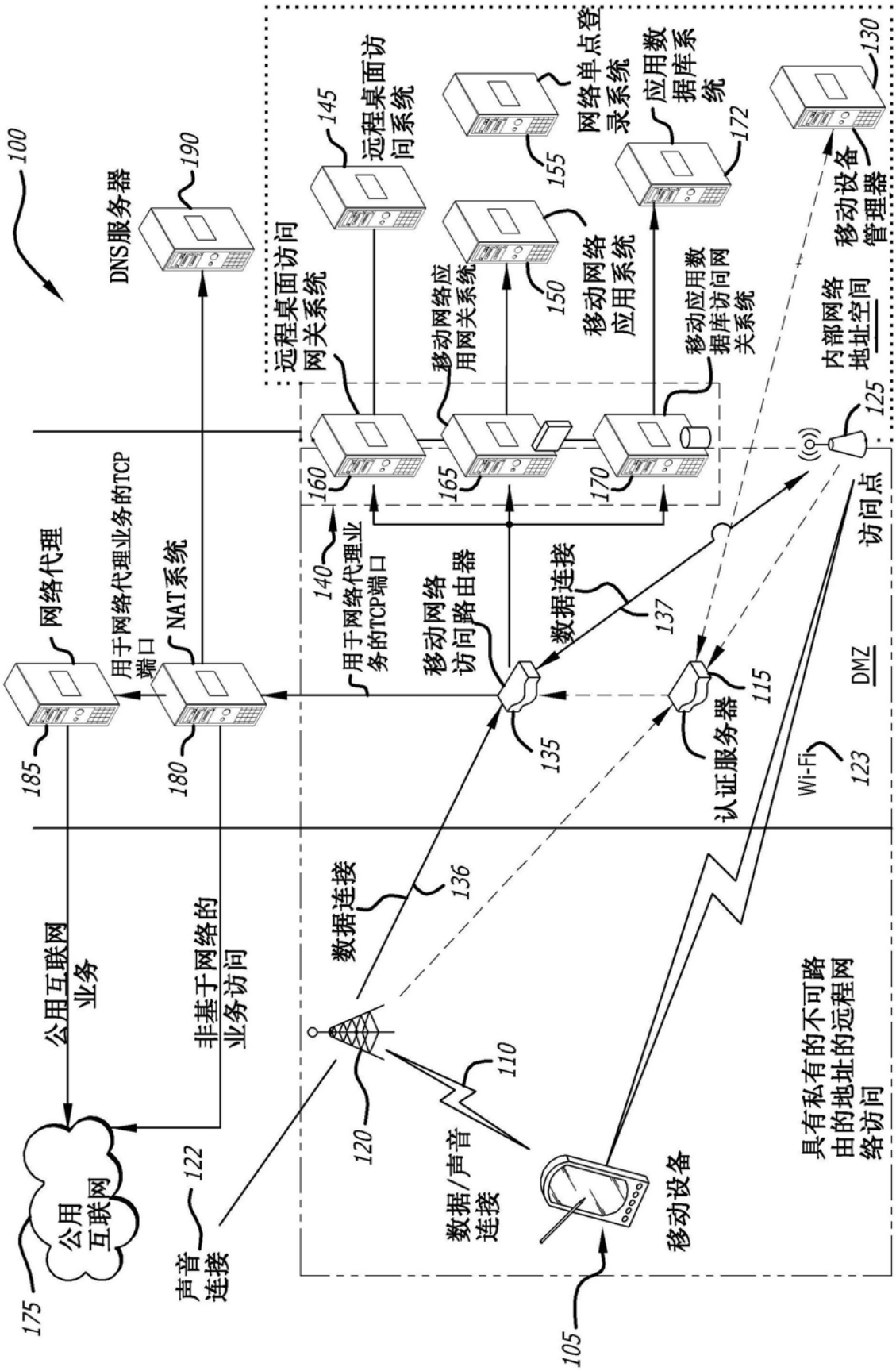

100
DNS服务器
190
远程桌面访问网关系统
145
远程桌面访问系统
网络单点登录系统
155
应用数据库系统
172
130
移动网络应用网关系统
150
移动网络应用系统
移动应用数据库访问网关系统
移动设备管理器
内部网络地址空间
125
160
165
170
网络代理
用于网络代理业务的TCP端口
NAT系统
140
用于网络代理业务的TCP端口
移动网络访问路由器
数据连接
137
访问点
185
180
135
115
DMZ
Wi-Fi
123
认证服务器
公用互联网业务
非基于网络的业务访问
数据连接
136
120
110
数据/声音连接
移动设备
具有私有的不可路由的地址的远程网络访问
公用互联网
175
122
声音连接
105

图1

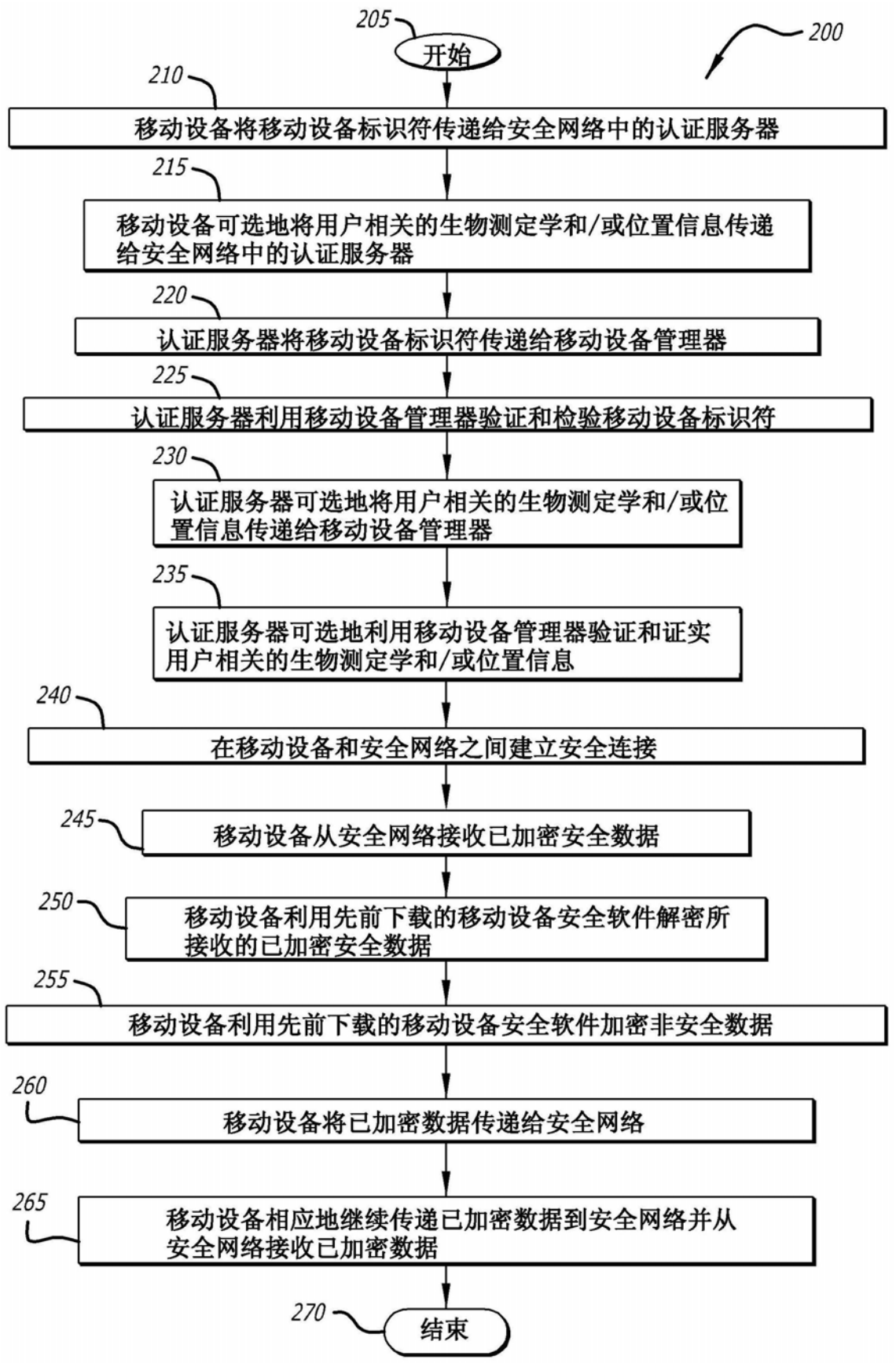

205
开始
200
210
移动设备将移动设备标识符传递给安全网络中的认证服务器
215
移动设备可选地将用户相关的生物测定学和/或位置信息传递给安全网络中的认证服务器
220
认证服务器将移动设备标识符传递给移动设备管理器
225
认证服务器利用移动设备管理器验证和检验移动设备标识符
230
认证服务器可选地将用户相关的生物测定学和/或位置信息传递给移动设备管理器
235
认证服务器可选地利用移动设备管理器验证和证实用户相关的生物测定学和/或位置信息
240
在移动设备和安全网络之间建立安全连接
245
移动设备从安全网络接收已加密安全数据
250
移动设备利用先前下载的移动设备安全软件解密所接收的已加密安全数据
255
移动设备利用先前下载的移动设备安全软件加密非安全数据
260
移动设备将已加密数据传递给安全网络
265
移动设备相应地继续传递已加密数据到安全网络并从安全网络接收已加密数据
270
结束

图2

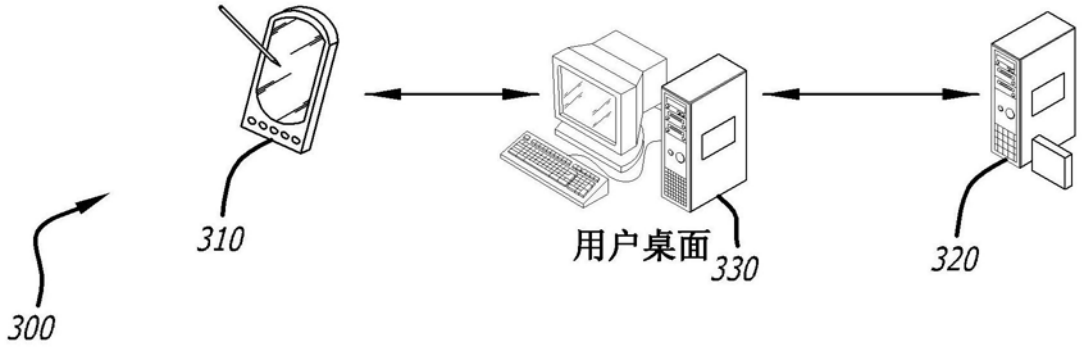


图3A

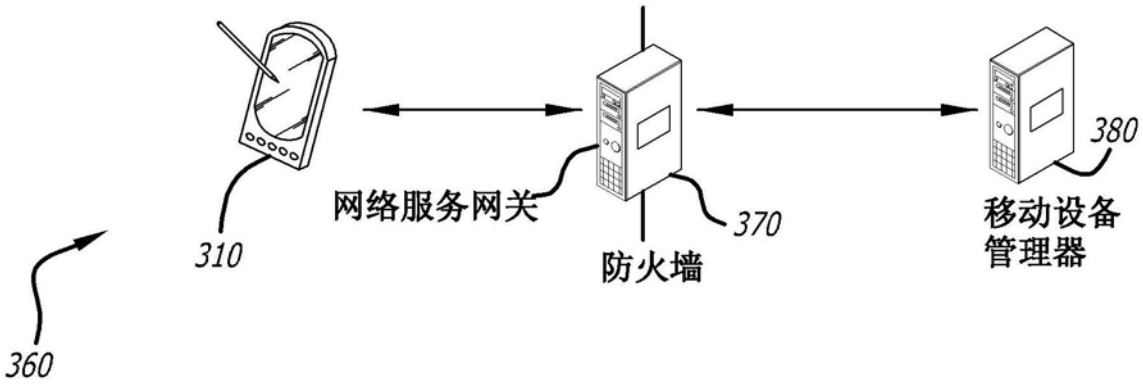


图3B

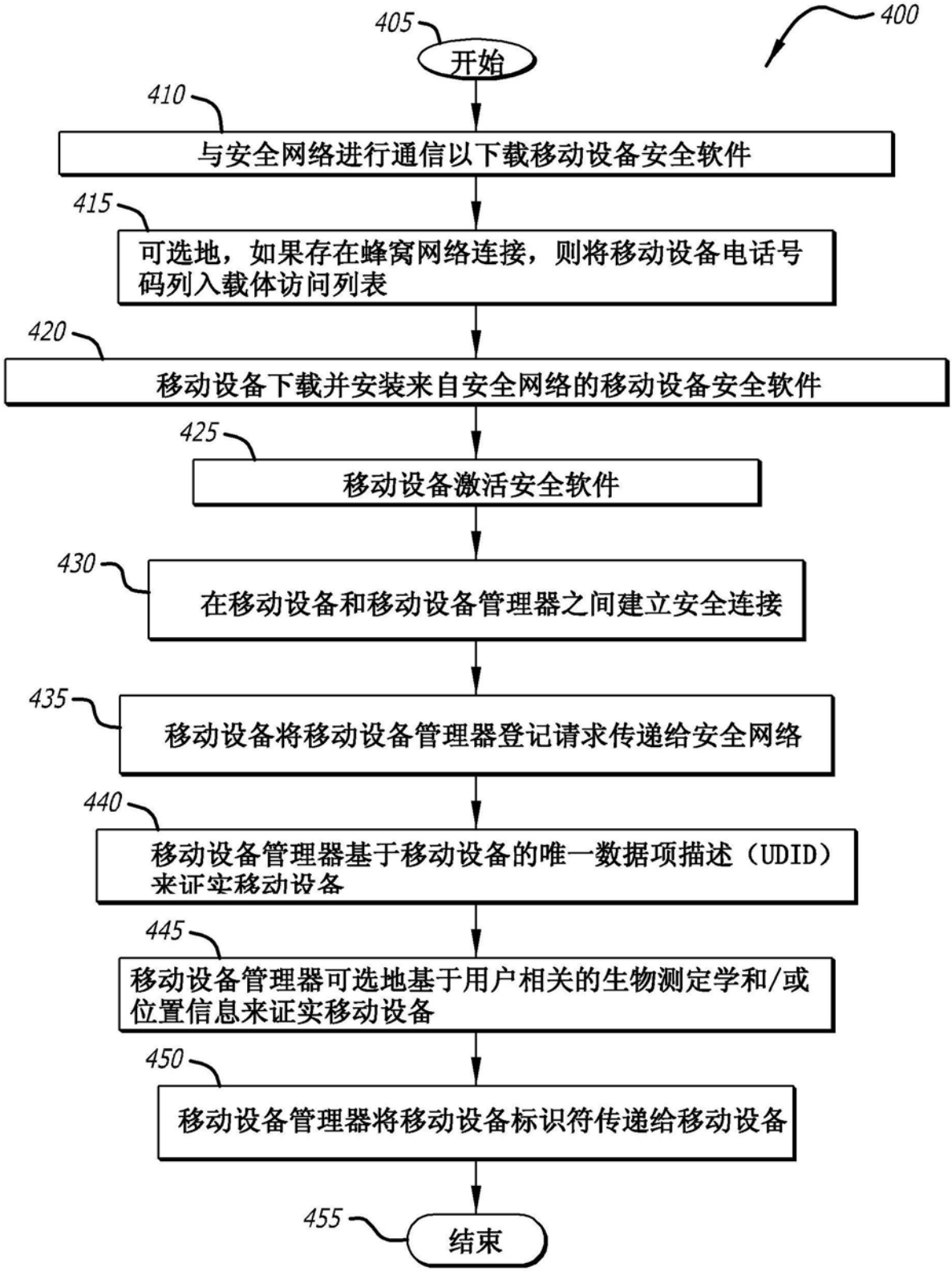

400
405
开始
410
与安全网络进行通信以下载移动设备安全软件
415
可选地，如果存在蜂窝网络连接，则将移动设备电话号码列入载体访问列表
420
移动设备下载并安装来自安全网络的移动设备安全软件
425
移动设备激活安全软件
430
在移动设备和移动设备管理器之间建立安全连接
435
移动设备将移动设备管理器登记请求传递给安全网络
440
移动设备管理器基于移动设备的唯一数据项描述（UDID）来证实移动设备
445
移动设备管理器可选地基于用户相关的生物测定学和/或位置信息来证实移动设备
450
移动设备管理器将移动设备标识符传递给移动设备
455
结束

图4