(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 107077552 B
(45)授权公告日 2019.06.21

(21)申请号 201580057262.4
(22)申请日 2015.10.29
(65)同一申请的已公布的文献号
申请公布号 CN 107077552 A
(43)申请公布日 2017.08.18
(30)优先权数据
14/532,608 2014.11.04 US
(85)PCT国际申请进入国家阶段日
2017.04.21
(86)PCT国际申请的申请数据
PCT/US2015/058150 2015.10.29
(87)PCT国际申请的公布数据
WO2016/073288 EN 2016.05.12
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 菲茨杰拉德·约翰·阿希巴尔德
约翰·施耐德
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 杨林勋
(51)Int.Cl.
G06F 21/32(2013.01)
H04L 29/06(2006.01)
H04W 4/00(2009.01)
H04W 12/06(2009.01)
(56)对比文件
US 2002194003 A1,2002.12.19,
CN 103455742 A,2013.12.18,
JP 特开2008-171218 A,2008.07.24,
审查员 武晓冬

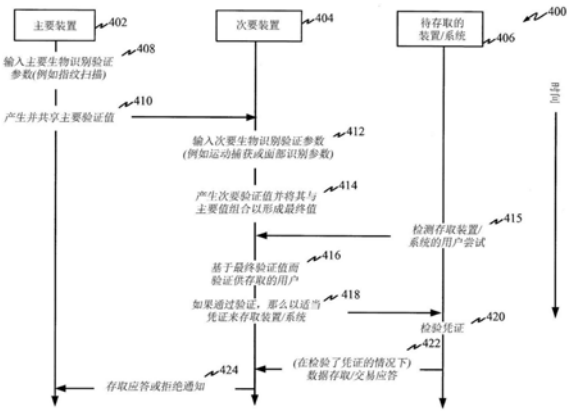
权利要求书5页 说明书18页 附图22页

(54)发明名称

在特设网络中的装置之间分布生物识别验证

(57)摘要

一个特征涉及在各装置之间对用户的生物识别验证。在一个方面中,特设个人无线网络可包含使用例如邻近策略等分组策略和其它权限的主要装置和一或多个次要装置。所述主要装置与所述一或多个次要装置共享用户的生物识别验证值。每一次要装置可接着使用相对较低可靠性生物计量传感器(例如用于面部识别的数码相机、用于语音识别的麦克风或用于手势识别的加速计)来执行对相同用户的额外验证。所述次要验证结果可与来自所述主要装置的生物识别验证得分/等级组合以形成所述次要装置的最终验证得分/等级,所述最终验证得分/等级用以针对一或多个交易(例如,消费者购买、安全内容存取或安全控制)而验证所述次要装置的所述用户。



CN 107077552 B

1.一种用于验证主要装置的用户的方法,所述方法由所述主要装置在包括所述主要装置和次要装置的特设无线网络中操作,所述方法包括:

使用所述主要装置的生物识别参数检测器获得表示所述主要装置的所述用户的至少一个生物识别参数;

基于所述至少一个生物识别参数而确定表示对所述主要装置的所述用户的验证程度的主要验证值,其中所述主要验证值指示所述主要装置的经授权用户的所述生物识别参数与对应特征之间的在数值范围内的匹配程度;

通过将所述主要验证值与阈值比较,来基于所述主要验证值而验证所述主要装置的所述用户;以及

经由所述特设无线网络将所述主要验证值发射到装备有次要生物识别参数检测器的所述次要装置,以通过使用所述次要生物识别参数检测器的所述次要装置促进对所述用户的验证。

2.根据权利要求1所述的方法,其中表示对所述用户的所述验证程度的所述主要验证值是以下各者中的至少一者:(a)验证得分或(b)信任等级。

3.根据权利要求1所述的方法,其进一步包含检测到用于取消验证所述主要装置的所述用户的触发,并作为响应而取消验证所述主要装置和所述次要装置的所述用户。

4.根据权利要求3所述的方法,其中用于取消验证所述主要装置的所述用户的所述触发包含以下各者中的至少一者:(a)用户启动的主要装置取消验证;(b)主要装置超时或(c)表示对所述主要装置的安全性危害的主要装置威胁指示。

5.根据权利要求1所述的方法,其进一步包含检测到用于取消验证所述次要装置的所述用户的触发,并作为响应而向所述次要装置发送用以取消验证所述次要装置的所述用户的信号。

6.根据权利要求5所述的方法,其中用于取消验证所述次要装置的所述用户的所述触发包含以下各者中的至少一者:(a)用户启动的次要装置取消验证;(b)次要装置超时;

(c)表示对所述次要装置的安全性危害的次要装置威胁指示;(d)与所述次要装置的通信的损失;(e)所述主要装置与所述次要装置之间的通用性的损失或(f)对预定权限策略的违反。

7.根据权利要求5所述的方法,其中用于取消验证所述次要装置的所述用户的所述触发包含位置、运动或经共享通信链路中的至少一者中的所述主要装置与所述次要装置之间的通用性的损失。

8.根据权利要求5所述的方法,其中用于取消验证所述次要装置的所述用户的所述触发包含环境噪声或环境光中的至少一者中的所述主要装置与所述次要装置之间的通用性的损失。

9.根据权利要求1所述的方法,其中所述阈值指示足够的验证程度。

10.一种用于在特设无线网络中使用的主要装置,其包括:

生物识别参数检测器,其经配置以获得表示所述主要装置的用户的至少一个生物识别参数;

发射器;以及

处理电路,其耦合到所述生物识别参数检测器和所述发射器,所述处理电路经配置以

基于所述至少一个生物识别参数而确定表示对所述主要装置的所述用户的验证程度的主要验证值，其中所述主要验证值指示所述主要装置的经授权用户的所述生物识别参数与对应特征之间的在数值范围内的匹配程度；

通过将所述主要验证值与阈值比较，来基于所述主要验证值而验证所述主要装置的所述用户；以及

经由包括所述主要装置和次要装置的所述特设无线网络，使用所述发射器来将所述主要验证值发送到装备有次要生物识别参数检测器的所述次要装置，以通过使用所述次要生物识别参数检测器的所述次要装置促进对所述用户的验证。

11.根据权利要求10所述的主要装置，其中表示对所述用户的所述验证程度的所述值为以下各者中的至少一者：(a)验证得分或(b)信任等级。

12.根据权利要求10所述的主要装置，其中所述处理电路经进一步配置以检测到用于取消验证所述主要装置的所述用户的触发，并作为响应而取消验证所述主要装置和所述次要装置的所述用户。

13.根据权利要求12所述的主要装置，其中用于取消验证所述主要装置的所述用户的所述触发包含以下各者中的至少一者：(a)用户启动的主要装置取消验证；(b)主要装置超时或(c)表示对所述主要装置的安全性危害的主要装置威胁指示。

14.根据权利要求10所述的主要装置，其中所述处理电路经进一步配置以检测到用于取消验证所述次要装置的所述用户的触发，并作为响应而使用所述发射器来向所述次要装置发送用以取消验证所述次要装置的所述用户的信号。

15.根据权利要求14所述的主要装置，其中用于取消验证所述次要装置的所述用户的所述触发包含以下各者中的至少一者：(a)用户启动的次要装置取消验证；(b)次要装置超时；(c)表示对所述次要装置的安全性危害的次要装置威胁指示；(d)与所述至少一个次要装置的通信的损失；(e)所述主要装置与所述次要装置之间的通用性的损失或(f)对预定权限策略的违反。

16.根据权利要求14所述的主要装置，其中用于取消验证所述次要装置的所述用户的所述触发包含所述主要装置与所述次要装置之间在位置、运动或经共享通信链路中的至少一者上的通用性的损失。

17.根据权利要求14所述的主要装置，其中用于取消验证所述次要装置的所述用户的所述触发包含所述主要装置与所述次要装置之间在环境噪声或环境光中的至少一者上的通用性的损失。

18.根据权利要求10所述的主要装置：

其中所述主要装置为车辆的控制计算机且所述次要装置为接近所述车辆的移动装置；

其中所述主要装置为建筑物的控制计算机且所述次要装置为接近所述建筑物的移动装置；或

其中所述主要装置为智能电话且所述次要装置为智能手表、一副智能眼镜、移动健康监视器或一件智能服装中的至少一者。

19.根据权利要求10所述的主要装置，其中所述阈值指示足够的验证程度。

20.一种用于验证次要装置的用户的方法，所述方法由所述次要装置在包括主要装置和所述次要装置的特设无线网络中操作，所述方法包括：

经由所述特设无线网络从所述主要装置接收表示对所述用户的验证程度的主要验证值，其中所述主要验证值指示所述主要装置的经授权用户的生物识别参数与对应特征之间的在数值范围内的匹配程度；以及

确定是否将执行对所述用户的次要验证，然后通过下列步骤执行次要验证：

使用所述次要装置的生物识别参数检测器使用所述次要装置来获得表示所述用户的至少一个生物识别参数；

基于使用所述次要装置所获得的所述至少一个生物识别参数而确定表示对所述用户的验证程度的次要验证值；

组合从所述主要装置接收的所述主要验证值与所述次要验证值，以得到组合式验证值；以及

通过比较所述组合式验证值与阈值使用所述组合式验证值来验证所述次要装置的所述用户。

21.根据权利要求20所述的方法，其进一步包含检测到用于取消验证所述次要装置的所述用户的触发，并作为响应而取消验证所述次要装置的所述用户且通知所述主要装置。

22.根据权利要求21所述的方法，其中用于取消验证所述次要装置的所述用户的所述触发包含以下各者中的至少一者：(a)用户启动的次要装置取消验证；(b)次要装置超时；(c)表示对所述次要装置的安全性危害的次要装置威胁指示或(d)表示对所述主要装置的安全性危害的主要装置威胁指示。

23.根据权利要求20所述的方法，其进一步包含在所述次要装置处检测主要装置威胁指示并向所述主要装置发送用以取消验证所述主要装置的所述用户的信号。

24.根据权利要求20所述的方法，其中使用所述次要装置来获得至少一个生物识别参数包含检测手势识别参数、面部识别参数和语音识别参数中的一或多者。

25.根据权利要求20所述的方法，其中所述主要装置和所述次要装置经授权以执行财务交易，且其中所述次要装置经授权以仅对于比所述主要装置经授权以执行的少的量而执行财务交易。

26.根据权利要求20所述的方法，其中所述次要装置基于用户启动的动作而确定是否需要次要验证。

27.根据权利要求26所述的方法，其中所述用户启动的动作包含以下各者中的至少一者：(a)财务交易；(b)对安全内容的存取或(c)对安全控制系统的存取。

28.根据权利要求20所述的方法，其中所述阈值指示足够的验证程度。

29.一种用于在特设无线网络中使用的次要装置，其包括：

接收器，其操作以经由包括主要装置和所述次要装置的所述特设无线网络，从所述主要装置接收表示对用户的验证程度的主要验证值，其中所述主要验证值指示所述主要装置的经授权用户的生物识别参数与对应特征之间的在数值范围内的匹配程度；

生物识别参数检测器；以及

处理电路，其耦合到所述接收器和所述生物识别参数检测器，所述处理电路操作以确定是否将执行对所述用户的次要验证，并进一步操作执行次要验证以：

使用所述生物识别参数检测器获得表示所述次要装置的所述用户的至少一个生物识别参数；

基于所述至少一个生物识别参数而确定表示对所述用户的验证程度的次要验证值；

组合从所述主要装置接收的所述主要验证值与所述次要验证值，以得到组合式验证值；以及

通过比较所述组合式验证值与阈值使用所述组合式验证值来验证所述次要装置的所述用户。

30.根据权利要求29所述的次要装置，其中所述处理电路进一步操作以检测到用于取消验证所述次要装置的所述用户的触发，并作为响应而取消验证所述次要装置的所述用户且通知所述主要装置。

31.根据权利要求30所述的次要装置，其中用于取消验证所述次要装置的所述用户的所述触发包含以下各者中的至少一者：(a)用户启动的次要装置取消验证；(b)次要装置超时；(c)表示对所述次要装置的安全性危害的次要装置威胁指示或(d)表示对所述主要装置的安全性危害的主要装置威胁指示。

32.根据权利要求29所述的次要装置，其中所述生物识别参数检测器操作以通过检测以下各者中的至少一者来使用所述次要装置获得至少一个生物识别参数：手势识别参数、面部识别参数或语音识别参数。

33.根据权利要求29所述的次要装置，其中所述主要装置与所述次要装置经由特设无线网络通信。

34.根据权利要求29所述的次要装置：

(a)其中所述主要装置车辆的控制计算机，且所述次要装置为接近所述车辆的移动装置；

(b)其中所述主要装置为建筑物的控制计算机，且所述次要装置为接近所述建筑物的移动装置；或

(c)其中所述主要装置为智能电话，且所述次要装置为智能手表、一副智能眼镜、移动健康监视器或一件智能服装中的至少一者。

35.根据权利要求29所述的次要装置：其中所述阈值指示足够的验证程度。

36.一种用于验证主要装置的用户的方法，所述方法由所述主要装置在包括所述主要装置和次要装置的特设无线网络中操作，所述方法包括：

使用所述主要装置的生物识别参数检测器获得表示所述主要装置的所述用户的至少一个生物识别参数；

基于所述至少一个生物识别参数而确定表示对所述主要装置的所述用户的验证程度的主要验证值，其中所述主要验证值指示所述主要装置的经授权用户的所述生物识别参数与对应特征之间的在数值范围内的匹配程度；

通过将所述主要验证值与阈值比较，来基于所述主要验证值而验证所述主要装置的所述用户；以及

经由所述特设无线网络将所述主要验证值发射到所述次要装置，以通过所述次要装置促进对所述用户的验证，其中所述主要装置与所述次要装置经由自组织无线网络通信。

37.一种用于在特设无线网络中使用的主要装置，其包括：

生物识别参数检测器，其经配置以获得表示所述主要装置的用户的至少一个生物识别参数；

发射器;以及

处理电路,其耦合到所述生物识别参数检测器和所述发射器,所述处理电路经配置以

基于所述至少一个生物识别参数而确定表示对所述主要装置的所述用户的验证程度的主要验证值,其中所述主要验证值指示所述主要装置的经授权用户的所述生物识别参数与对应特征之间的在数值范围内的匹配程度;

通过将所述主要验证值与阈值比较,来基于所述主要验证值而验证所述主要装置的所述用户;以及

经由包括所述主要装置和次要装置的所述特设无线网络,使用所述发射器来将所述主要验证值发送到所述次要装置,以通过所述次要装置促进对所述用户的验证,其中所述主要装置与所述次要装置经由自组织无线网络通信。

在特设网络中的装置之间分布生物识别验证

[0001] 相关申请案的交叉引用

[0002] 本申请案要求2014年11月4日在美国专利和商标局中申请的第14/532,608号非临时申请案的优先权和权益,所述非临时申请的完整内容以引用的方式并入本文中。

技术领域

[0003] 各种特征涉及例如由移动计算装置构成的网络等无线特设网络内的生物识别验证。

背景技术

[0004] 无线特设网络为不依赖于预先存在的基础结构或例如路由器等中央管理装置的分散型无线网络。确切来说,网络中的每一节点通过为其它节点转发数据来参与路由。无线特设个人网络为由例如智能电话、平板计算机、智能手表、智能眼镜等个人装置构成的无线特设网络。此些网络可具有相对精密的主要装置(例如智能电话或平板计算机)连同相对不及主要装置精密且具能力的各种次要个人装置(例如智能手表、智能眼镜、智能服装等)。

[0005] 例如智能电话或平板计算机等主要装置可具备相对可靠且精密的嵌入式生物计量传感器(例如指纹传感器)以出于各种目的(例如消费者购买或其它财务交易、安全内容存取、安全启动和控制等)而促进对主要装置的用户的验证。精密的生物计量传感器通常由于小外观尺寸、成本考虑、电池寿命考虑或其它实际原因而不在次要装置(例如智能手表、智能眼镜或智能服装)内提供。仍然,次要装置可需要用户验证用于各种应用(例如消费者购买)。举例来说,可能需要允许用户仅仅通过在零售扫描仪上方挥动智能手表来进行适度的商业购买,而不需要用户借由更繁琐的智能电话授权并验证交易。

[0006] 图1说明具有智能电话102作为主要装置并具有智能手表104和一副智能眼镜106作为次要配对装置的特设个人网络100的实例。在此实例中,智能电话102使用根据例如长期演进(LTE)等技术的无线信号来经由基站108与蜂窝式网络通信。智能电话102经由本地无线发射协议(例如无线通用串行总线(USB)或Bluetooth™)与智能手表104和智能眼镜106通信。智能电话102经装备以使用基于指纹的生物识别验证(使用指纹传感器(未展示))来验证智能电话的用户。智能手表104经装备以使用较不可靠基于运动的生物识别验证(例如通过使用经装备以检测由佩戴智能手表的用户做出的特有手势的加速计(未展示))来验证用户。智能眼镜106经装备以使用基于面部图像的生物识别验证(例如通过使用数码相机(未展示))来验证用户,基于面部图像的生物识别验证还大体上不如指纹验证可靠。图1还说明用户试图使用智能手表104从其获得资金的自动取款机(ATM)110。因为由智能手表提供的基于运动的验证不足够可靠,所以ATM将通常需要用户通过使用借记卡且将密码键入到ATM的小键盘中来验证并授权交易,此可能不便于用户,在密码难以记得的情况下尤其如此,且实际上将抵消使用智能手表以触发交易的便利性。替代地,ATM可经编程以接受智能手表的相对不可靠的基于示意动作的验证,此将更便于用户但可能允许小偷仅仅通过复制验证运动来使用被盗或假冒的智能手表获得资金。

[0007] 存在提供用以与具有主要和次要装置的特设网络内的次要装置一起使用的便利和可靠验证的需要。

发明内容

[0008] 一种供由特设网络的主要装置使用用于验证用户的方法包含:获得表示所述主要装置的所述用户的至少一个生物识别参数;基于所述至少一个生物识别参数而确定表示对所述主要装置的所述用户的验证程度的主要验证值;基于所述主要验证值而验证所述主要装置的所述用户;以及(例如,借由所述次要装置)与次要装置共享所述主要验证值以促进对所述用户的验证。所述主要装置与所述次要装置可经由特设无线网络通信。

[0009] 在另一方面中,一种装置包含:生物识别参数检测器,其经配置以获得表示特设网络的主要装置的用户的至少一个生物识别参数;发射器;以及处理电路,其经配置以:基于所述至少一个生物识别参数而确定表示对所述主要装置的所述用户的验证程度的值;基于表示所述验证程度的所述值而验证所述主要装置的所述用户;以及(例如,借由所述次要装置)使用所述发射器来与所述特设网络的次要装置共享表示所述验证程度的所述值以促进对所述用户的验证。

[0010] 在又一方面中,一种供由特设网络的次要装置使用用于验证用户的方法包含:从所述特设网络的主要装置接收表示对用户的验证程度的主要验证值;以及确定是否将执行对所述用户的次要验证,并在将执行次要验证的情况下;(a)使用所述次要装置来获得表示所述次要装置的所述用户的至少一个生物识别参数;(b)基于使用所述次要装置所获得的所述至少一个生物识别参数而确定表示对所述次要装置的所述用户的验证程度的次要验证值;(c)组合从所述主要装置接收的所述主要验证值与所述次要验证值,以得到组合式验证值;以及(d)使用所述组合式验证值来验证所述次要装置的所述用户。

[0011] 在又另一方面中,一种装置包含:接收器,其经配置以从所述特设网络的主要装置接收表示对用户的验证程度的主要验证值;生物识别参数检测器;以及处理电路,其经配置以确定是否将执行对所述用户的次要验证,且在将执行次要验证的情况下经进一步配置以:(a)使用所述生物识别参数检测器获得表示次要装置的所述用户的至少一个生物识别参数;(b)基于所述至少一个生物识别参数而确定表示对所述次要装置的所述用户的验证程度的次要验证值;(c)组合从所述主要装置接收的所述主要验证值与所述次要验证值,以得到组合式验证值;以及(d)使用所述组合式验证值来验证所述次要装置的所述用户。

附图说明

[0012] 图1说明具有智能电话作为主要装置的主要和次要装置的示范性特设个人网络。

[0013] 图2说明具有经共享验证的具有主要和次要装置的特设个人网络,其中智能电话为主要装置。

[0014] 图3说明具有经共享验证的具有主要和次要装置的特设个人网络,其中车载计算机为主要装置。

[0015] 图4为说明由具有主要和次要装置的特设个人网络的组件执行的操作的时序图,其中次要装置与待存取的装置/系统通信。

[0016] 图5为根据说明性实例的特设网络的主要装置的移动通信装置的芯片上系统

(SoC)处理电路的框图。

[0017] 图6为根据智能电话为网络的主要装置的说明性实例的特设网络的主要和次要组件的框图。

[0018] 图7说明用于使用智能电话或其它移动主要装置来形成并终止特设网络的示范性方法。

[0019] 图8说明用于使用特设网络的主要装置产生主要验证值的示范性方法。

[0020] 图9说明用于使用特设网络的次要装置产生最终组合式验证值的示范性方法。

[0021] 图10为根据家庭系统控制器为网络的主要装置的另一说明性实例的特设网络的主要和次要组件的框图。

[0022] 图11为根据车辆控制台计算机为网络的主要装置的又一说明性实例的特设网络的主要和次要组件的框图。

[0023] 图12说明用于验证特设网络的用户的示范性方法的其它细节。

[0024] 图13说明用于取消验证特设网络的用户的示范性方法的其它细节。

[0025] 图14为说明用于使用具有可利用图2到13的系统、方法和设备的主要装置的处理系统的设备的硬件实施方案的实例的框图。

[0026] 图15为说明图14的主要装置的处理电路的组件的框图。

[0027] 图16为说明图14的主要装置的机器可读媒体的指令组件的框图。

[0028] 图17概述供由特设网络的主要装置使用以验证用户的示范性方法。

[0029] 图18概述供由特设网络的主要装置使用以验证用户的示范性方法的其它方面。

[0030] 图19为说明特设网络的次要装置的处理电路的组件的框图。

[0031] 图20为说明特设网络的次要装置的机器可读媒体的指令组件的框图。

[0032] 图21概述供由特设网络的次要装置使用以验证用户的示范性方法。

[0033] 图22概述供由特设网络的次要装置使用以验证用户的示范性方法的其它方面。

具体实施方式

[0034] 在以下描述中，给出具体细节以提供对本发明的各种方面的彻底理解。然而，所属领域的技术人员将理解，可在没有这些特定细节的情况下实践所述方面。举例来说，可以框图展示电路以便避免以不必要的细节混淆所述方面。在其它情况下，可不详细展示众所周知的电路、结构和技术以便不混淆本发明的方面。

[0035] 词语“示范性”在本文中用于意指“充当实例、例子或说明”。本文中描述为“示范性”的任何实施方案或方面未必应解释为比本发明的其它方面优选或有利。同样，术语“方面”不要求本发明的所有方面包含所论述的特征、优点或操作模式。

[0036] 概述

[0037] 若干新颖特征涉及特设无线个人网络或由主要装置和一或多个次要装置构成的类似网络内的生物识别验证。在一个实例中，提供生物识别验证，其中主要装置(例如，智能电话、平板计算机等)经装备以使用一或多个相对精密且可靠的生物识别验证技术(例如指纹验证)来执行生物识别验证。借由主要装置与使用各种分组策略(例如邻近度策略)和其它权限的一或多个次要装置来产生特设个人网络。在一个实例中，特设无线网络为主要装置与次要装置之间的点对点网络，其中没有其它实体管理或帮助建立点对点连接(例如，没

有其它实体涉及建立和/或经由特设网络发射)。主要装置与特设网络中的其它装置共享验证值(例如,得分或信任等级)。网络中的每一次要装置可接着根据用户偏好或其它要求而执行额外用户验证。次要验证可使用相对低可靠性传感器(例如数码相机(例如,面部识别)、麦克风(例如,语音识别)或加速计(例如,手势识别))来予以执行。次要验证结果与来自主要装置的生物识别验证值(例如,得分或等级)组合以形成最终验证值(例如,得分或等级),最终验证值接着用以出于一或多个交易(例如消费者购买、安全内容存取、安全控制等)而验证次要装置的用户。如果对于特定次要装置不存在额外用户验证要求,那么主要装置的生物识别验证值(例如,得分或等级)映射到次要装置验证值(例如,得分或等级)。

[0038] 图2说明具有经装备以产生并共享主要验证值(例如,得分或信任等级)和其它数据(例如配对规则、装置标识符(ID)等)的智能电话202的特设个人网络200的实例。智能手表204经装备以接收主要验证值和其它数据并将基于运动捕获的验证添加到主要验证值,以得到特定针对于智能手表204的最终组合式次要验证得分(或信任等级)。一副智能眼镜206也经装备以接收主要验证得分和其它数据。智能眼镜206将基于面部图像的验证添加到主要验证值以得到特定针对于智能眼镜206的最终组合式次要验证值(例如,得分或信任等级)。在此实例中,智能电话202使用根据任何合适技术的无线信号来经由基站208与蜂窝式网络通信,但可使用WiFi或其它无线网络与外部系统通信。智能电话202经由任何合适本地无线发射协议与智能手表204和智能眼镜206通信。举例来说,智能电话可以是无线热点。

[0039] 在图2的实例中,智能电话202经装备以首先借由相对可靠的基于指纹的生物识别验证(例如通过使用指纹传感器,未展示)来验证用户并产生前述主要验证值。主要验证值可(例如)取决于用户的输入指纹与用户的所存储指纹之间的匹配的接近程度而变化。智能电话202将所得主要验证值发射到特设网络中的所有次要装置,假设次要装置满足任何所需权限且装置邻近。对于图2中所展示的类型的特设网络,邻近度范围可非常小,这是因为假设装置将全部由用户携带或穿戴。用户还可在需要时通过做出预定手臂运动来验证智能手表204,手臂运动由内部加速计(未单独地展示)检测到。智能手表204基于手臂运动匹配用户的存储运动图案的接近程度而产生次要验证值。智能手表204组合次要验证值与从智能电话202接收的主要验证值以产生并保存最终组合式验证值。可在其之后比较此值与各种预定阈值以验证特定交易。应注意,智能手表是否需要单独用户验证可取决于各种因素,例如主要验证值。如果主要验证值相对高且因此可信,那么可不需要次要验证。如果主要验证较低且因此较不可信,那么可需要次要验证。作为另一实例,如果启用智能手表以执行财务交易,那么可需要次要验证,但如果启用智能手表以仅执行其它交易,那么不需要次要验证。

[0040] 类似地,可能需要用户通过使眼睛拍摄用户的面部的数码照片来对智能眼镜206进行验证。智能眼镜接着基于照片匹配用户的预存储图像的接近程度而产生次要验证值,且组合次要验证值与从智能电话接收的主要验证值以产生并保存最终组合式验证值。可相对不频繁地需要经由网络的主要和次要装置对用户的初始验证,以免对用户造成不便。只要次要装置停止与智能电话密切邻近(或未能满足其它所需权限或参数),那么除非经再验证,否则装置被取消验证且不可用以授权交易或存取系统/装置。

[0041] 在某一点处,用户可试图通过在ATM的近场扫描仪(未单独地展示)上方挥动智能手表来从ATM 210获得现金。智能手表204基于从ATM接收的响应性信号而检测用以获得现

金的尝试，且通过(例如)比较智能手表的最终验证值与用于现金提取的预定阈值来检验最终验证值足以授权交易。阈值可取决于待提取的现金的量而变化，以便对于更大量而需要更高验证程度。如果智能手表204的最终验证值超出适当阈值，那么智能手表204的用户借此出于交易被适当地验证。智能手表接着将任何所需凭证发射到ATM机(例如与ATM帐户相关联的密码或个人身份识别码(PIN))以完成交易。假设凭证令人满意，那么ATM分配现金。

[0042] 以此方式，用户可便利地执行适度的财务交易而没有需要使用智能电话(其可收起于用户的钱包或公文包中或保持于拉住或扣紧的口袋内)的同时验证的负担，且不需要将任何PIN或密码直接键入到ATM中(此在密码难以记得的情况下可能不便于用户且将抵消使用智能手表以触发交易的便利性)。而且，此些交易是大体上安全的，这是因为使用两种类型的验证：对智能电话的基于初始指纹的验证和对智能手表的基于运动捕获的验证。此外，智能手表必须在交易期间非常接近于智能电话，否则，智能手表取消验证且无法授权交易。

[0043] 还请注意，只要组合式最终值足够地高，那么所述个别验证程序两者都不需要是完美的。举例来说，初始指纹验证可能由于略微脏的指纹而不是完美的。同样地，用户不必在验证智能手表时恰好模拟所需手臂运动。然而，组合式验证值可仍然足够高以出于特定交易可靠地验证用户。在其它实例中，没有次要验证由智能手表需要，且主要验证值仅映射到智能手表。如所提及，验证的阈值可取决于交易的类型和量，其中需要更精确的生物识别验证用于较大财务交易。还请注意，如果基于智能手表204的最终组合式值而不将用户视为出于交易被足够地验证，那么用户可仍通过将PIN键入到ATM的小键盘中或通过通过将指纹重应用到智能电话生物计量传感器使用智能电话来直接验证交易。

[0044] 作为与图2的特设网络一起使用的另一交易实例，用户可希望经由智能眼镜206从互联网网站存取机密信息。智能眼镜206将比较其最终验证值与预定阈值，以确定智能眼镜的用户是否经足够验证以准许对特定网站的存取。如果最终验证值超出阈值，那么用户借此经验证且适当存取凭证(例如，密码或PIN)经由因特网转发到网站以获得对网站的存取。接着使用因特网来下载且经由智能眼镜显示所请求信息。以此方式，用户可便利地经由智能眼镜存取机密信息，而没有需要密码或PIN的直接键入的负担。而且，存在未经授权的个人可使用另一个人的错放或被盗的智能眼镜来存取信息的极少或没有风险，这是因为眼镜一旦不再接近地邻近于用户的智能电话，那么眼镜将被取消验证。

[0045] 图3说明特设个人网络300的另一实例。在实例中，汽车302或其它车辆的仪表板控制台计算机为特设网络的主要装置。车辆的居住者的各种移动装置为次要装置。在图3的实例中，示范性次要装置包含智能电话304、一对智能眼镜306和平板计算机308。汽车302的仪表板控制台计算机展示为经由一或多个基站310与蜂窝式网络通信。在图3的实例中，仪表板控制台包含指纹传感器(或其它合适的生物计量传感器，未单独地展示)，所述指纹传感器验证车辆的操作者以允许车辆的操作并还允许各种次要移动装置存取车辆内的无线网络(例如车辆热点)。汽车302的仪表板控制台产生前述主要验证值以供发射到车辆的特设网络中的所有次要装置，假设次要装置满足任何所需权限且保持邻近。在典型状况下，家庭成员的各种装置全部经预注册到汽车，且因此自动地被授予对汽车内的无线热点的存取。对于图3的网络，邻近度范围将比图2的网络宽，这是因为一些乘客可能在前座位中而其它乘客在后座位中。而且，只要装置相对接近车辆，那么邻近度可经设定使得装置保持在特设

网络中，借此允许居住者在休息站等处从车辆携带其装置而不从特设网络即刻断开。一旦装置被充分地取走远离车辆，那么取消验证装置。在其它实例中，一旦从汽车移除装置，那么即刻取消验证装置且从特设网络移除装置。

[0046] 虽然特设网络有效(例如虽然居住者保持坐在车辆内)，但是个别居住者可能(例如)从车辆的组件的存储器下载媒体内容(经受由车辆的拥有者强加的任何内容锁定)。作为一个实例，儿童乘客可各自使用特设网络来经由其自有个人装置从车辆存取不同所存储媒体(例如音乐、电影、电视节目等)。对此些媒体内容的存取可以其它方式需要对每一个别装置的繁重验证。借由经由车辆的特设网络的共享验证，基于车辆的操作者的验证值而替代地自动地且便利地验证每一个别装置。汽车控制台计算机可经编程以准许车辆的不同操作者授权不同(或不授权)媒体内容。举例来说，当青少年驾驶员操作车辆时，可准许最少次要装置验证或不准许次要装置验证以便限制总体驾驶员分神。

[0047] 车辆特设网的其它实例包含其它类型的车辆(公共汽车、卡车、飞机、船艇、摩托车等)内的网络。又其它特设网可包含健康监视装置，例如可与智能电话或平板计算机配对的心率监视器或血压监视器。此些健康监视装置可经选择性地授权以与远程健康监视系统(例如由医生或其它医疗服务人员操作的系统)共享信息。其它特设网可包含建筑物控制网络，所述建筑物控制网络(例如)通过控制恒温器、安全监视器、遮光物等来控制房屋或其它结构内的电气设备的操作。在一个实例中，检测到陌生人入侵到房屋中至少出于所选目的而触发对家庭特设网络内的所有装置的即刻取消验证。下文更详细地描述这些特设系统中的一些的实例。

[0048] 图4概述参考时序图400说明主要装置402、次要装置404和待存取的装置或系统406(例如ATM、安全网站等)的操作的前述特设网的一些特征。在408处，主要装置输入主要生物识别验证参数(例如指纹扫描)，且在410处基于主要生物识别验证参数而产生主要验证值且与次要装置404共享所述值。在412处，次要装置404输入次要生物识别验证参数(例如运动捕获或面部识别参数)(假设启用次要验证)。在414处，次要装置404产生次要验证值，并将其与主要验证值组合以形成用于次要装置的最终验证值。系统/装置406检测用户的存取尝试，例如尝试从ATM获得现金、访问网站等(415)。作为响应，在416处，次要装置404尝试基于最终验证值而验证所请求存取的用户。如已提及，验证可取决于待存取的特定系统或装置和具有所需以存取更灵敏系统或启动具有更大值的财务交易的较高验证值的存取的目的。如果经验证，那么次要装置404接着向系统/装置406发送适当的凭证(例如密码或PIN)以供存取(418)。系统/装置406检验凭证(420)并(在检验了凭证的情况下)将所存取数据提供到次要装置或在已完成财务交易等的情况下发送交易应答(422)。取决于是否适当地验证用户并接受凭证，次要装置404将存取应答或拒绝通知424转发到主要装置402。

[0049] 尽管未在图4中展示，但可在检测到各种触发(例如从主要装置的邻近移除次要装置)之后即刻取消验证次要装置。在检测使用网络的主要装置的取消验证事件之后，还即刻取消验证特设网络中的次要装置。在检测关于次要装置的取消验证事件之后，还即刻取消验证特设网络中的所有其它次要装置。在检测次要装置的“威胁条件”之后，除了取消验证次要装置以外，还即刻将取消验证请求发布到主要装置。威胁条件的实例包含对由次要装置检测到的特设网络规则(例如，邻近度规则)的违反，其指示对主要装置的危害。其它实例包含可欺骗、侵入或以其它方式危害装置的任何指示。

[0050] 在本文中所描述的特设网的特征当中:次要装置的潜在地更好的用户体验;移除冗余验证;无缝特设安全网络产生;和主要装置的增强型安全。概括地说,本文中所描述的特设个人网络中的至少一些中的生物识别验证包含:使用用户偏好(例如,邻近度定义、装置权限)形成特设个人网络;在特设网络中从主要装置到次要装置共享生物识别验证值(例如,得分或等级);在次要装置中组合经共享生物识别值与低可靠性次要验证以形成最终验证值;和将生物识别值映射到次要装置验证。特设网络还可实现:在对主要装置取消验证之后即刻取消验证次要装置;在违反网络规则之后即刻取消验证次要装置;和在次要装置中检测威胁之后即刻将取消验证远程发布到主要装置。

[0051] 示范性特设网络系统、方法和组件

[0052] 现将描述用于与个人特设网络一起使用的各种示范性系统和方法。在许多实例中,智能电话用作主要装置。出于完整性起见,将阐述对示范性智能电话的硬件的简要说明,硬件包含用于产生并共享主要验证值的组件。其它主要装置(例如平板计算机、汽车控制台等)可包含至少一些类似组件。

[0053] 图5说明根据可利用各种新颖特征的一个实例的智能电话或其它移动通信装置的芯片上系统(SoC)处理电路500。SoC处理电路可以是由高通有限公司(Qualcomm Incorporated)制造的Snapdragon™处理电路。SoC处理电路500包含应用程序处理电路510,应用程序处理电路510多核CPU 512。应用程序处理电路510通常控制移动通信装置的所有组件的操作。在一个方面中,应用程序处理电路510包含经装备以产生主要验证值(例如,得分或等级)的主要生物识别验证控制器513,主要验证值接着与主要装置为智能电话的特设网络内的其它装置共享。应用程序处理电路510还包含用于控制具有各种次要装置的特设网络的形成和终止的特设网络控制器515。应用程序处理电路510可包含引导ROM 518,引导ROM 518存储用于SoC处理电路500的各种组件的引导顺序指令。SoC处理电路500进一步包含由应用程序处理电路510控制的一或多个外围子系统520。外围子系统520可包含但不限于存储子系统(例如,只读存储器(ROM)、随机存取存储器(RAM))、视频/图形子系统(例如,数字信号处理电路(DSP)、图形处理电路单元(GPU))、音频子系统(例如,DSP、模数转换器(ADC)、数模转换器(DAC))、电源管理子系统、安全性子系统(例如,加密、数字权限管理(DRM))、输入/输出(I/O)子系统(例如,键盘、触摸屏),以及有线和无线连接性子系统(例如,通用串行总线(USB)、全球定位系统(GPS)、WiFi、全球移动通信系统(GSM)、码分多址(CDMA)、4G长期演进(LTE)调制解调器)。示范性外围子系统520(其为调制解调器子系统)包含DSP 522、各种硬件(HW)和软件(SW)组件524,和各种射频(RF)组件526。在一个方面中,每一外围子系统520还包含存储相关联的外围子系统520的主引导映像(未展示)的引导ROM 528。

[0054] SoC处理电路500进一步包含各种内部共享硬件资源530,例如内部共享存储装置532(例如,静态RAM(SRAM)、双数据速率(DDR)同步动态(SD)RAM、DRAM、闪存存储器等),内部共享HW资源530由应用程序处理电路510和各种外围子系统520共享以存储各种运行时数据。在一个方面中,SoC处理电路500的组件510、518、520、528和530可集成到单芯片基板上。SoC处理电路500进一步包含各种外部共享HW资源540,外部共享HW资源540可位于不同芯片衬底上且经由系统总线(未展示)与SoC处理电路500通信。外部共享HW资源540可包含(例如)外部共享存储装置542(例如,DDR RAM、DRAM、闪存存储器)和/或永久数据存储装置544

(例如,安全数字(SD)卡或硬盘驱动器(HDD)等),外部共享存储装置542和永久数据存储装置544由应用程序处理电路510和各种外围子系统520共享以存储不同类型的数据,例如操作系统(OS)信息、系统文件、程序、应用程序、用户数据、音频/视频文件等。当启动并入有SoC的移动通信装置时,安全SoC处理电路500开始系统启动过程。具体地说,应用程序处理电路510存取引导ROM 518以检索用于SoC处理电路500的引导指令,包含用于各种外围子系统520的引导顺序指令。外围子系统520还可具有额外外围引导RAM 528。此外,智能电话包含生物识别输入装置550,例如指纹扫描仪或虹膜扫描仪用于输入来自用户的生物识别参数用于借由生物识别验证控制器513产生主要生物识别验证值。取决于实施方案,虹膜扫描仪可利用智能电话的数码相机(未单独地展示)。

[0055] 图6说明主要装置为智能电话602且次要装置包含智能手表604、智能眼镜606和健康监视器607(例如,心率监视器等)的示范性移动特设网络600内的装置的所选组件。仅在各种装置内展示与特设网络有关的所选内部组件。每一装置将包含用于实施装置的其它功能的其它组件。首先参考智能电话602,特设网络控制器608使用通用性评估控制器610和权限评估控制器612来控制特设网络的形成和终止。通用性评估控制器检测经由通信控制器614(其具有天线615)与智能电话602通信的任何次要装置,且评定智能电话与次要装置之间的通用性程度。在典型实例中,通信控制器614可以是无线热点控制器但可对应于用于直接地(或经由中间系统)与次要装置通信的任何合适装置。而且,通常,用户的各种次要装置经预注册用于与智能电话602一起使用,以使得智能电话可忽略未经预注册的任何和所有次要装置。

[0056] 假设特定次要装置(例如,智能手表604)与智能电话通信且经预注册,那么通用性评估控制器610检测或以其它方式获得与智能电话和次要装置相关联的各种参数,可从所述参数检测、测量、确定或以其它方式评定两个装置的通用性程度。如果发现足够的通用性程度,那么将次要装置邀请到具有主要装置的特设网络中。举例来说,智能电话的通用性评估控制器610可基于GPS信号而检测智能电话和智能手表604的位置,并确定所述两个装置在其密切邻近于彼此的情况下具有足够的通用性。所需邻近程度可经预编程,且如上文所提及,可对于由意图由用户携带或穿戴的用户装置构成的个人特设网络相对接近。在一些情况下,次要装置与主要装置通信的事实足以建立必备的邻近程度,在经由例如WiFi无线热点等相对短程通信达成通信的情况下尤其如此。

[0057] 另外地或替代性地,通用性评估控制器610可分析参数(例如运动、环境噪声、环境光等)以分析通用性。举例来说,智能电话602可使用其麦克风或相机以监视用于与经由次要装置(例如智能眼镜606)的麦克风或相机检测到的环境噪声和环境光条件比较的环境噪声和环境光条件。如果发现装置正检测相同环境光或噪声,那么装置视为在相同地点中。通用性评估控制器610接着将表示通用性的各种参数组合成单个值用于与通用性阈值比较,以确定是否应将特定次要装置邀请到特设网络中。在一些实例中,使用如果被违反那么触发对特定次要装置的取消验证或在一些情况下,触发对完整特设网络的终止的通用性规则的集合来指定通用性。假设将特定次要装置(例如智能手表604)邀请到特设网络中,那么可产生并经由通信控制器614发射合适的配对信号。

[0058] 就权限来说,权限评估控制器612可经预编程有适用于各种次要装置的各种特设网络权限规则。这些权限可包含前述注册条件,由此可仅准许已向主要装置预注册的次要

装置进入到特设网络中。然而，其它权限可指定特定经注册装置仅可在某些条件下添加到特设网络。举例来说，某些装置可取决于正被使用的通信网络添加到特设网络，其中在使用Bluetooth™但不使用WiFi的情况下添加特定装置，或反之亦然。如果用户尚未被智能电话602验证，那么指纹或虹膜扫描仪616可用以输入生物识别特征，接着经由虹膜和/或指纹验证控制器618验证生物识别特征。前述主要验证值(和其它数据，例如特设网络内的各种装置的装置ID)可接着发送到各种次要装置。

[0059] 智能手表604展示为具有通信控制器620和用于(直接地抑或经由中间通信网络)从智能电话602接收信号的天线621。智能手表还包含配对控制器622，配对控制器622对从智能电话602接收的任何配对信号作出响应并发送响应性握手信号以加入特设网络。在一些情况下，次要装置将替代地通过检测主要装置并发送请求加入特设网络的信号来启动对特设网络中的存取。此可有助于通过消除主要装置定期或连续地监视次要装置的存在的需要来减少主要装置中的功率消耗。在一个实例中，只要智能手表604启动，那么其发送宣布其存在的信号，智能电话可接着在信号在通信范围中主动的情况下对信号作出响应。如果智能手表604需要次要验证(如基于(例如)从智能电话接收的权限或规则所确定)，那么可使用用以检测独特且预编程用户运动的加速计624和运动识别授权控制器626且执行次要验证来执行此次要授权。

[0060] 智能眼镜606包含类似组件。简单来说，智能眼镜具有通信控制器628、天线630和配对控制器632(以及用于实施智能眼镜的功能的多个其它组件，未展示)。如果需要次要验证，那么可使用用以检测面部图像的相机634和面部识别授权控制器636且执行次要验证来执行次要授权。健康监视器607还具有通信控制器640、天线641和配对控制器638(以及用于实施健康监视器的功能的其它组件，未展示)。在此实例中，健康监视器不具有次要验证能力且因此其仅仅使用从智能电话602接收的主要验证值。虽然图6仅展示单个示范性智能手表，但是一对智能眼镜和健康监视器、额外或替代性次要装置可形成特设网络，包含智能服装、游戏装置和其它完全功能移动装置(例如平板计算机或其它智能电话)。

[0061] 图7为说明使用智能电话或其它主要装置来形成并终止特设网络的流程图700。主要装置检测与主要装置通信的经授权以与特设网络中的主要装置配对的一或多个次要装置，并基于邻近度、经共享周围环境(声音、光、运动等)或经共享通信网络而检测通用性(702)。主要装置评定主要装置与次要装置的通用性的程度，并确定所需用于次要装置的任何显式权限(704)。对于如基于通用性规则所确定而与主要装置具有足够通用性并匹配所有必需权限的每一次要装置，主要装置发送将次要装置邀请到特设网络中或从次要装置接收配对信号的配对信号(706)。主要装置从次要装置接收响应性信号且形成由主要装置和接受配对邀请信号且保持邻近的所有次要装置构成的特设网络(708)。

[0062] 主要装置按需求或视需要而与特设网络的各种次要装置共享信息，例如验证值、共享ID、权限、通用性规则等(710)。主要装置通过取消验证需要取消验证的任何和所有次要装置来监视次要装置取消验证条件(例如人工用户取消验证、通信缺乏、通用性规则违反和/或权限失效和响应)(712)。主要装置通过取消验证主要装置和所有次要装置来监视主要装置取消验证条件(例如人工用户取消验证和/或威胁条件(包含可疑欺骗或黑客)和响应)并终止特设网络(714)。就突然加速来说，装置可检测与正下降的装置相关联的突然加速且向次要装置发送终止特设网络的取消验证信号，期望主要装置将不受损坏且在其后可

能不能够取消验证次要装置。

[0063] 图8为说明使用智能电话或其它主要装置产生主要验证值的流程图800。主要装置在装置启动之后或在对其它验证触发的检测(例如先前取消验证)之后即刻启动主要验证(802)。主要装置使用生物识别输入装置(例如指纹扫描仪或虹膜扫描仪)来输入主要生物识别验证参数(804)。主要装置从输入参数检索生物识别特征(例如指纹细节和/或虹膜环和沟痕),并比较预存储特征以计算表示生物识别特征匹配装置的经授权用户的对应预存储特征的程度的主要验证值(806)。主要装置将主要验证值存储于装置内,并将其发射到目前在现有特设网络中的任何次要装置来用于授权由次要装置的用户请求的任何交易(808)。主要装置使用主要验证值以验证由用户经由使用主要装置来请求的任何交易(例如财务交易、安全内容存取、安全控制等)(810)。主要装置检测任何主要装置取消验证条件(例如从特设网络的次要装置中的一者发送的主要取消验证触发)并对其作出响应(812)。

[0064] 图9为说明用于使用特设网络的次要装置产生最终组合式验证值的流程图900。次要装置在装置启动之后或在对其它验证触发的检测(例如先前取消验证)之后即刻启动次要装置验证(902)。次要装置从特设网络的主要装置接收主要装置验证值并确定是否需要次要验证(904)。如果需要次要验证,那么次要装置使用生物识别输入装置(例如用于运动识别的加速计、用于面部识别的数码相机或用于语音识别的麦克风)输入次要生物识别验证参数(906)。如果需要次要验证,那么次要装置从输入参数检索生物识别特征(例如运动捕获数据、面部特征或语音图案标记),并比较预存储特征以计算表示生物识别特征匹配装置的用户的对应预存储特征的程度的次要验证值(908)。

[0065] 如果需要次要验证,那么次要装置组合次要验证值与从主要装置接收的主要验证值以得到组合式最终验证值,或在没有次要验证的情况下以其它方式将主要验证映射到组合式最终验证值(910)。次要装置使用最终组合式验证值以验证由用户经由次要装置请求的任何交易(例如财务交易、安全内容存取、安全控制等)(912)。次要装置检测任何主要或次要装置取消验证条件(包含在严重威胁条件(例如主要装置已经受欺骗或侵入的指示)的情况下产生用于发送到主要装置的主要装置取消验证触发)并对其作出响应(914)。应注意,在一些情况下,特定特设网络的次要装置可以是完全功能装置,例如具有与网络的主要装置相同或更大能力的平板计算机或智能电话。因而,次要装置可具有检测主要装置不检测的威胁条件的能力。出于至少此原因,允许网络中的次要装置将取消验证触发发送到主要装置和网络中的所有其它装置是有用的。

[0066] 图10说明主要装置为家庭系统控制器1002且次要装置包含拥有者的平板计算机1004和来宾的平板计算机1006的示范性基于家庭的特设网络1000内的装置的所选组件。仅在各种装置内展示切合到特设网络的那些内部组件。组件中的一些与图6中所展示的组件相同或类似且因此将不再次详细描述。首先参考家庭系统控制器1002,家庭特设网络控制器1008使用邻近度检测器1010和权限控制器1012来控制特设家庭网络的形成和终止。邻近度控制器(例如)通过检测房屋内、特定房间或房屋内或房屋的地面内的装置来检测经由通信控制器1014(其具有天线1016)与家庭系统控制器1002通信的任何次要装置。通信控制器1014可以是家庭无线热点控制器。而且,通常,房屋的拥有者和其它永久居住者的各种次要装置经预注册,以使得家庭系统控制器可在次要装置在一天的过程中被带到房屋且从房屋带出时自动地添加或从特设网络舍弃所述装置。

[0067] 假设特定次要装置(例如拥有者的平板计算机1004)在房屋内且经预注册,那么通过经由通信控制器1014发送合适的配对信号来将次要装置邀请到特设网络中。如果拥有者或其它居住者尚未经验证到家庭系统控制器1002,那么指纹或虹膜扫描仪1010可用以输入生物识别特征,接着经由虹膜和/或指纹验证控制器1018验证生物识别特征。前述主要验证值(和其它数据,例如特设网络内的各种装置的装置ID)可接着发送到房屋内的各种次要装置。应注意,如果家庭系统控制器如此装备,那么其可经由安全监视器跟踪居住者的进入和退出且检测入侵者的存在。

[0068] 拥有者的平板计算机1004展示为具有通信控制器1020和用于(直接地抑或经由中间通信网络)从家庭系统控制器1002接收信号的天线1021。拥有者的平板计算机还包含配对控制器1022,配对控制器1022对从家庭系统控制器1002接收的任何配对信号作出响应并发送响应性握手信号以加入特设家庭网络。在一个实例中,只要拥有者的平板计算机1004启动,那么其发送宣布其存在的信号,家庭系统控制器可接着对信号作出响应。如果拥有者的平板计算机1004需要次要验证(如基于(例如)从智能电话接收的权限或规则所确定),那么可使用相机1024和面部识别授权控制器1026且执行次要验证来执行此次要授权。一旦与家庭系统控制器配对,那么拥有者的平板计算机可接着用以便利地控制各种家庭系统,例如恒温器和/或环境控制器1028、安全系统1030和家庭媒体和娱乐系统1032。

[0069] 来宾的平板计算机1006包含类似于拥有者的智能电话的组件的组件,但将受限制于控制家庭系统。简单来说,来宾的平板计算机具有通信控制器1034、天线1036和配对控制器1038(以及用于实施健康监视器的功能的其它组件,未展示)。如果需要次要验证,那么可使用用以检测面部图像的相机1040和面部识别授权控制器1042且执行次要验证来执行次要授权。虽然图10仅展示一个拥有者的平板计算机和一个来宾平板计算机,但是额外或替代性次要装置可形成家庭特设网络,包含智能服装、健康监视器、游戏装置和各种其它完全功能移动装置,例如平板计算机或其它智能电话。

[0070] 图11说明主要装置为车辆控制台计算机1102且次要装置包含拥有者智能电话1104和来宾平板计算机1106的示范性基于车辆的特设网络1100内的装置的所选组件。仅在各种装置内展示切合到特设网络的那些内部组件。组件中的一些与图10中所展示的组件相同或类似且因此将不再次详细描述。首先参考车辆控制台计算机1102,车辆特设网络控制器1108使用邻近度检测器1110和权限控制器1112来控制特设车辆网络的形成和终止。邻近度控制器(例如)通过检测车辆内或邻近的装置来检测经由通信控制器1114(其具有天线1115)与车辆控制台计算机1102通信的任何次要装置。通信控制器1114可以是车辆无线热点控制器。而且,通常,车辆拥有者和家庭成员的各种次要装置经预注册,以使得车辆控制台计算机可在次要装置在一天的过程中被带进带出车辆时自动地添加或从特设网络舍弃所述装置,在车辆为家庭汽车的情况下尤其如此。

[0071] 假设特定次要装置(例如拥有者的智能电话1104)在车辆内且经预注册,那么通过发送合适的配对信号来将次要装置邀请到特设网络中。如果拥有者尚未经验证到车辆控制台计算机1102,那么可使用指纹扫描仪1116,接着经由指纹验证控制器1118验证指纹扫描仪1116。前述主要验证值(和其它数据,例如特设网络内的各种装置的装置ID)可接着发送到车辆内的各种次要装置。

[0072] 拥有者的智能电话1104展示为具有通信控制器1120和用于(直接地抑或经由中间

通信网络)从家庭系统控制器1102接收信号的天线1121。拥有者的智能电话还包含配对控制器1122,配对控制器1122对从车辆控制台计算机1102接收的任何配对信号作出响应并发送响应性握手信号以加入特设车辆网络。如果拥有者的智能电话1104需要次要验证(如基于(例如)从智能电话接收的权限或规则所确定),那么可使用相机1124和面部识别授权控制器1126且执行次要验证来执行此次要授权。一旦与车辆控制台计算机配对,那么拥有者的智能电话可接着用以便利地控制各种车辆系统,例如恒温器和/或环境控制器1128、安全系统1130和车辆媒体和娱乐系统1132。来宾的平板计算机1106包含类似于拥有者的智能电话1104的组件的组件,但将受限制于控制车辆系统。简单来说,来宾的平板计算机具有通信控制器1134、天线1136和配对控制器1138。虽然图11仅展示一个智能电话和一个平板计算机,但是额外或替代性次要装置可形成车辆特设网络,包含各种其它完全功能移动装置,例如其它平板计算机、游戏装置或其它智能电话。

[0073] 现转而参看图12和13,将描述说明主要和次要装置的操作的额外流程图。在这两个流程图中,借由加阴影框展示主要装置的操作,而借由无阴影框展示次要装置的操作。次要装置的功能中的至少一些可替代地由主要装置执行,且反之亦然,且因此流程图仅表示功能可分佈于主要装置与次要装置之间的方式的一个实例。

[0074] 图12说明验证程序1200。验证开始于1202处,继之以主要装置等待生物识别验证数据1204,生物识别验证数据从生物计量数据框1206接收。如已解释,用户可经由指纹扫描仪等输入生物识别参数。生物识别参数借由装置存储于例如由数据块1206展示的数据库内。主要装置执行用户验证1208以产生主要验证值或信任等级(1210)。生物识别验证值基于配对状态而映射到配对(即,次要)装置验证值(1212)。配对状态可仅指示特定次要装置是否经由先前配对程序在目前与主要装置配对(1214)。也就是说,虽然主要装置在1204处等待生物计量数据,但是主要装置还基于来自位置传感器、通信网络等的数据而检测任何配对装置(1214),如上文已描述。

[0075] 假设发现配对次要装置(1218),那么配对装置识别用于配对装置的一或多个验证方法(例如运动或面部识别方法)(1220)。配对次要装置接着识别对应次要验证传感器,例如用于运动识别的加速计、用于图像识别的相机或用于语音识别的麦克风(1222)。配对次要装置还使用上文所描述的技术(例如通过检查从主要装置接收的权限或规则)来确定是否需要次要验证(1224)。假设需要次要验证,那么配对装置基于从框1228接收的数据(例如相机、加速计或麦克风数据)而执行次要验证(1226)。配对次要装置组合(经由框1210)来自主要装置的生物识别验证与来自配对(即,本地)装置的次要验证(1230)。所得组合式值存储为最终配对装置验证值(1232)。替代地,如果不在1224处需要次要验证,那么配对装置替代地经过框1212继续进行以从框1210获得映射验证值(例如,得分或等级),验证值接着存储为最终配对值。在任一情况下,验证在1234处结束。

[0076] 图13说明取消验证程序1300。取消验证开始(1302)于主要装置等待主要取消验证触发(1304),主要取消验证触发从取消验证触发框1306接收。如已解释,此些主要取消验证触发可涉及超时、人工用户干预和来自辅助传感器的数据(例如指示特设网络的装置当中的环境噪声或光的差别的传感器)。一旦接收了主要取消验证触发,那么主要装置的取消验证状态设定为“真实”(1308),即,主要装置从特设网络取消验证(且特设网络自身借此终止)。同时,次要配对装置基于从位置传感器接收的信息、通信链路、配对信号等(1312)而更

新其配对状态(1310)。假设次要装置保持与主要装置配对(1314)，那么次要装置等待取消验证触发(1316)。由次要装置接收的取消验证触发可包含由主要装置(经由框1306)接收的相同取消验证触发和/或特定针对于次要装置(经由框1318)的取消验证触发。一旦接收到次要取消验证触发，那么次要装置的取消验证状态设定为“真”(1320)，即，从特设网络取消验证次要装置(尽管特设网络自身可与其它次要装置继续，假设主要装置也未经取消验证)。相反，如果次要装置确定其不再与主要装置1314配对，那么次要装置的取消验证状态同样地设定为“真”(1322)，即，从特设网络解除鉴认次要装置。而且，次要装置可检测对主要装置的任何威胁(1324)，例如上文所论述的黑客或假冒威胁。如果检测到此威胁，那么主要装置安全控制命令在1326处设定为“真”。此命令中继到主要装置且表示框1304的主要装置取消验证触发中的一者。最终，取消验证在取消验证次要装置抑或次要装置和主要装置两者之后在1328处结束。

[0077] 其它示范性系统和设备

[0078] 图14说明可实施图2到13的主要装置组件和方法的总体系统或设备1400。根据本发明的各种方面，元件、或元件的任何部分、或元件的任何组合可借由处理系统1414予以实施，处理系统包含一或多个处理电路1404，例如图5的SoC处理电路。举例来说，设备1400可以是移动通信系统的用户设备(UE)。设备1400可与无线网络控制器(RNC)一起使用。除了SoC之外，处理电路1404的实例还包含微处理电路、微控制器、数字信号处理电路(DSP)、现场可编程门阵列(FPGA)、可编程逻辑装置(PLD)、状态机、门控逻辑、离散硬件电路以及经配置以执行贯穿本发明所描述的各种功能性的其它合适的硬件。也就是说，处理电路1404，如在设备1400中利用，可用以实施上文所描述且在图2到13中所说明的程序(和下文论述的图17和18中所说明的程序)中的任何一或多者，例如用以基于而生物标识技术而执行用户验证的程序。

[0079] 在此实例中，处理系统1414可借由大体上由总线1402表示的总线架构予以实施。取决于处理系统1414的具体应用和总设计约束，总线1402可包含任何数目个互连总线和桥接器。总线1402将各种电路连接在一起，电路包含一或多个处理电路(大体上由处理电路1404表示)、存储装置1405和机器可读、处理电路可读或计算机可读媒体(大体上由非暂时性机器可读媒体1406表示)。总线1402还可连接各种其它电路，例如定时源、外设、电压调节器以及电源管理电路，这些各者是所属领域中众所周知的且因此将不再做任何进一步描述。总线接口1408提供总线1402和收发器1410之间的接口。收发器1410提供用于经由发射媒体与各种其它设备通信的装置。取决于设备的性质，还可提供用户接口1412(例如，小键盘、显示器、扬声器、麦克风、操纵杆)。

[0080] 处理电路1404负责管理总线1402和一般处理，包含执行存储于机器可读媒体1406上的软件。软件在由处理电路1404执行时致使处理系统1414执行在本文中针对任何特定设备所描述的各种功能。机器可读媒体1406还可用于存储由处理电路1404在执行软件时操纵的数据。

[0081] 处理系统中的一或多个处理电路1404可执行软件。软件应被广义上解释为意指指令、指令集、代码、代码段、程序代码、程序、子程序、软件模块、应用、软件应用、软件包、例程、子例程、对象、可执行文件、执行线程、程序、功能等，而不管其是被称作软件、固件、中间件、微码、硬件描述语言还是其它。处理电路可执行必需的任务。代码段可以表示程序

(procedure)、功能、子程序、程序(program)、例程、子例程、模块、软件包、类,或指令、数据结构或程序语句的任意组合。一个代码段可以通过传递和/或接收信息、数据、自变量、参数或存储器内容联接到另一代码段或硬件电路。信息、自变量、参数、数据等可经由包含存储器共享、消息传递、令牌传递、网络发射等任何合适的装置来加以传递、转发或发射。

[0082] 软件可驻留在机器可读媒体1406上。机器可读媒体1406可以是非暂时性机器可读媒体。举例来说,非暂时性处理电路可读媒体、处理器可读媒体、机器可读媒体或计算机可读媒体包含:磁性存储装置(例如,硬盘、软盘、磁条)、光盘(例如,压缩光盘(CD)或数字多功能光盘(DVD))、智能卡、闪存存储器装置(例如,卡、棒或钥匙形驱动器)、RAM、ROM、可编程ROM(PROM)、可擦除PROM(EPROM)、电可擦除PROM(EEPROM)、寄存器、可移动磁盘、硬盘、CD-ROM以及用于存储可以通过计算机存取和读取的软件和/或指令的任何其它合适的媒体。术语“机器可读媒体”、“计算机可读媒体”、“处理电路可读媒体”和/或“处理器可读媒体”可包含但不限于:非暂时性媒体,例如便携式或固定存储装置;光学存储装置;以及能够存储、包含或载送指令和/或数据的各种其它媒体。因此,本文中所描述的各种方法可完全或部分借由可存储在“机器可读媒体”、“计算机可读媒体”、“处理电路可读媒体”和/或“处理器可读媒体”中且通过一或多个处理电路、机器和/或装置执行的指令和/或数据来予以实施。举例来说,机器可读媒体还可包含载波、传输线,和用于传输可由计算机存取及读取的软件和/或指令的任何其它合适的媒体。机器可读媒体1406可驻留在处理系统1414中、在处理系统1414外部或跨越包含处理系统1414的多个实体分布。机器可读媒体1406可实施于计算机程序产品中。举例来说,计算机程序产品可包含封装材料中的处理电路可读媒体。所属领域的技术人员将认识到,如何最好地实施贯穿本发明呈现的所描述功能性取决于特定应用及强加于整个系统上的总设计约束。

[0083] 具体地说,机器可读存储媒体1406可具有在由处理电路1404执行时致使处理电路执行以下操作的一或多个指令:获得表示主要装置的用户的至少一个生物识别参数;基于至少一个生物识别参数而确定表示对主要装置的用户的验证程度的主要验证值;基于主要验证值而验证主要装置的用户;和与特设网络的次要装置共享主要验证值。

[0084] 图式中所说明的组件、步骤、特征和/或功能中的一或多者可重新布置和/或组合成单个组件、步骤、特征或功能或体现在若干组件、步骤或功能中。在不脱离所描述的特征和方面的情况下,还可添加额外元件、组件、步骤和/或功能。图式中所说明的设备、装置和/或组件可经配置以执行图式中描述的方法、特征或步骤中的一或多者。本文中所描述的算法也可高效地实施于软件中和/或嵌入于硬件中。

[0085] 可借由通用处理电路、数字信号处理电路(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑组件、离散门或晶体管逻辑、离散硬件组件或其经设计以执行本文中描述的功能的任何组合来实施或执行结合本文中揭示的实例而描述的各种说明性逻辑块、模块、电路、元件和/或组件。通用处理电路可以是微处理电路,但在替代实施例中,处理电路可以是任何常规处理电路、控制器、微控制器或状态机。处理电路还可实施为计算组件的组合,例如,DSP和微处理电路的组合、多个微处理电路的组合、结合DSP核心的一或多个微处理电路的组合或任何其它此些配置。

[0086] 因此,在本发明的一个方面中,分别在图5和14中所说明的处理电路500和/或1404可以是专用处理电路(例如,ASIC)),其专门地经设计和/或硬连线以执行在图4、7、8、12和/

或13(和/或下文论述的图17和18)中所描述的算法、方法和/或步骤。因此，此专用处理电路(例如，ASIC)可以是用于实行在图4、7、8、12和/或13(和/或下文论述的图17和18)中所描述的算法、方法和/或步骤的装置的一个实例。机器可读存储媒体可存储指令，所述指令在由专用处理电路(例如，ASIC)执行时致使专用处理电路执行本文中所描述的算法、方法和/或步骤。

[0087] 图15说明特设网络的主要装置的处理电路1404的所选和示范性组件。具体地说，图15的处理电路1404包含验证程度确定模块/电路1500，模块/电路1500经配置以基于至少一个生物识别参数而确定表示对主要装置的用户的验证程度的主要验证值。生物识别参数可由主要生物识别参数检测器1502检测，检测器1502经配置以获得表示主要装置的用户的至少一个生物识别参数。处理电路1404还包含：用户验证模块/电路1504，其经配置以基于主要验证值而验证主要装置的用户；主要验证共享模块/电路1506，其经配置以经由特设网络通信模块/电路1514与特设网络的次要装置共享主要验证值；和主要装置取消验证模块/电路1508，其经配置以检测到用于取消验证主要装置的用户的触发并作为响应而取消验证特设网络的主要装置和次要装置的用户，其中用于取消验证主要装置的用户的触发可包含以下各者中的至少一者：(a)用户启动的主要装置取消验证；(b)主要装置超时或(c)表示对主要装置的安全性危害的主要装置威胁指示。

[0088] 处理电路1404还包含次要装置取消验证模块/电路1510，模块/电路1510经配置以检测到用于取消验证次要装置的用户的触发并作为响应而向次要装置发送用以取消验证次要装置的用户的信号，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：(a)用户启动的次要装置取消验证；(b)次要装置超时；(c)表示对次要装置的安全性危害的次要装置威胁指示；(d)与次要装置的通信的损失；(e)主要装置与次要装置之间的通用性的损失或(f)对预定权限策略的违反。处理电路1404还包含：特设网络形成/终止模块/电路1512，其经配置以基于经由特设网络通信模块/电路1514发送并接收的信号而形成并随后终止特设网络；装置通用性检测模块/电路1516，其经配置以基于环境噪声、环境光、位置、运动或经共享通信链路中的至少一者上的通用性的损失而检测主要装置与次要装置之间的通用性的损失；和分组权限/策略模块/电路1518，其经配置以管理特设网络权限和策略。还可提供其它组件且图15的说明决不是穷尽的。

[0089] 图16说明机器可读或计算机可读媒体1406的所选和示范性指令组件。具体地说，图16的机器可读媒体1406包含验证程度确定指令1600，指令1600在由图15的处理电路执行时致使处理电路基于至少一个生物识别参数而确定表示对主要装置的用户的验证程度的主要验证值。可使用主要生物识别参数检测指令1602检测生物识别参数，检测指令1602经配置/操作以获得表示主要装置的用户的至少一个生物识别参数。机器可读媒体1406还包含：用户验证指令1604，其经配置/具操作性基于主要验证值而验证主要装置的用户；主要验证共享指令1606，其经配置/操作以经由特设网络通信指令1614与特设网络的次要装置共享主要验证值；和主要装置取消验证指令1608，其经配置/操作以检测到用于取消验证主要装置的用户的触发并作为响应而取消验证特设网络的主要装置和次要装置的用户，其中用于取消验证主要装置的用户的触发包含以下各者中的至少一者：(a)用户启动的主要装置取消验证；(b)主要装置超时或(c)表示对主要装置的安全性危害的主要装置威胁指示。

[0090] 机器可读媒体1406还包含次要装置取消验证指令1610，指令1610经配置/操作以

检测到用于取消验证次要装置的用户的触发并作为响应而向次要装置发送用以取消验证次要装置的用户的信号，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：(a)用户启动的次要装置取消验证；(b)次要装置超时；(c)表示对次要装置的安全性危害的次要装置威胁指示；(d)与次要装置的通信的损失；(e)主要装置与次要装置之间的通用性的损失或(f)对预定权限策略的违反。机器可读媒体1406还包含：特设网络形成/终止指令1612，其经配置/操作以基于经由特设网络通信指令1614发送并接收的信号而形成并随后终止特设网络；装置通用性检测指令1616，其经配置/操作以基于环境噪声、环境光、位置、运动或经共享通信链路中的至少一者而检测主要装置与次要装置之间的通用性的损失；和分组权限/策略指令1618，其经配置/操作以管理特设网络权限和策略。还可提供其它指令且图16的说明决不是穷尽的。

[0091] 图17大体上说明并概述可由图14和15的处理电路1404或其它经合适地装备的装置执行以供由主要装置使用来验证用户的方法或程序1700。在1702处，处理电路获得表示主要装置的用户的至少一个生物识别参数，且在1704处基于至少一个生物识别参数而确定表示对主要装置的用户的验证程度的主要验证值。在1706处，处理电路基于主要验证值而验证主要装置的用户，且在1708处(例如，经由特设网络)与次要装置共享主要验证值以促进对次要装置的用户的验证。

[0092] 图18大体上说明并概述可由图14和15的处理电路1404或其它经合适地装备的装置执行以供由特设网络的主要装置使用来验证用户的其它方法或程序1800。处理电路可基于环境噪声、环境光、位置、运动或经共享通信链路中的至少一者上的通用性(或其缺乏)而邀请次要装置到特设网络/从特设网络取消邀请次要装置(1802)。处理电路将权限和策略中的一或多者连同主要验证值转发到一或多个次要装置，主要验证值可以是验证值(例如，得分或信任等级)(1804)。处理电路可检测到用于取消验证主要装置的用户的触发并作为响应而取消验证特设网络的主要装置和所有次要装置的用户，其中用于取消验证主要装置的用户的触发包含以下各者中的至少一者：用户启动的主要装置取消验证、主要装置超时和表示对主要装置的安全性危害的主要装置威胁指示(1806)。处理电路检测到用于取消验证次要装置的用户的触发并作为响应而向次要装置发送用以取消验证次要装置的用户的信号，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：用户启动的次要装置取消验证、次要装置超时、表示对次要装置的安全性危害的次要装置威胁指示、与次要装置的通信的损失、主要装置与次要装置之间的通用性的损失或对预定权限或策略的违反(1808)。

[0093] 图19说明特设网络的次要装置的处理电路1900(其可具有类似于图14的主要装置的处理电路的架构)的所选和示范性组件。具体地说，图19的处理电路1900包含验证程度接收模块/电路1902，模块/电路1902经配置以接收并处理表示使用特设网络通信模块/电路1908来从主要装置接收的对主要装置的用户的验证程度的主要验证值。次要验证确定模块/电路1906经配置以确定是否将执行对用户的次要验证。如果是，那么次要验证由次要验证模块/电路1910执行或控制，模块/电路1910经配置以使用次要生物识别参数检测器1912获得表示次要装置的用户的至少一个生物识别参数，并基于使用次要装置所获得的至少一个生物识别参数而确定表示对次要装置的用户的验证程度的次要验证值。最终组合式验证值确定模块/电路1914经配置以组合从主要装置接收的主要验证值与次要验证值以得到组

合式验证值。次要验证模块/电路1910接着使用组合式验证值来验证次要装置的用户。

[0094] 处理电路1900还包含主要装置取消验证检测模块/电路1916，模块/电路1916经配置以检测次要装置处的主要装置威胁指示并控制(使用通信模块/电路1908)向主要装置发送取消验证主要装置的用户的信号。处理电路1900还还包含次要装置取消验证模块/电路1918，模块/电路1918经配置以检测到用于取消验证次要装置的用户的触发并作为响应而取消验证次要装置的用户且通知主要装置，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：用户启动的次要装置取消验证、次要装置超时、表示对次要装置的安全性危害的次要装置威胁指示和表示对主要装置的安全性危害的主要装置威胁指示。处理电路1900还包含分组权限/策略模块/电路1920，模块/电路1920经配置以代表次要装置管理特设网络权限和策略。还可提供其它组件且图19的说明决不是穷尽的。

[0095] 图20说明次要装置的机器可读媒体2000的所选和示范性指令组件。具体地说，图20的机器可读媒体2000包含验证程度接收指令2002，指令2002在由次要装置的处理电路执行时致使处理电路接收并处理表示使用特设网络通信指令2008来从主要装置接收的对主要装置的用户的验证程度的主要验证值。次要验证确定指令2006经配置/操作以确定是否将执行对用户的次要验证。如果是，那么次要验证由次要验证指令2010执行或控制，指令2010操作以使用次要生物识别参数检测器2012获得表示次要装置的用户的至少一个生物识别参数，并基于使用次要装置所获得的至少一个生物识别参数而确定表示对次要装置的用户的验证程度的次要验证值。最终组合式验证值确定指令2014经配置/操作以组合从主要装置接收的主要验证值与次要验证值以得到组合式验证值。次要验证指令2010接着使用组合式验证值来验证次要装置的用户。

[0096] 机器可读媒体2000还包含主要装置取消验证检测指令2016，检测指令2016经配置以检测次要装置处的主要装置威胁指示并控制向主要装置发送取消验证主要装置的用户的信号。媒体2000还还包含次要装置取消验证指令2018，验证指令2018经配置/操作以检测到用于取消验证次要装置的用户的触发并作为响应而取消验证次要装置的用户且通知主要装置，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：用户启动的次要装置取消验证、次要装置超时、表示对次要装置的安全性危害的次要装置威胁指示和表示对主要装置的安全性危害的主要装置威胁指示。媒体2000还包含分组权限/策略指令2020，指令2020经配置/操作以代表次要装置管理特设网络权限和策略。还可提供其它指令且图20的说明决不是穷尽的。

[0097] 图21大体上说明并概述可由图19的处理电路1900或其它经合适地装备的装置执行以供由次要装置使用来验证用户的方法或程序2100。处理电路(例如，经由特设无线网络)从主要装置接收表示对(次要装置的)用户的验证程度的主要验证值(2102)。处理电路确定是否将执行对用户的次要验证，如果是，那么(a)使用次要装置来获得表示用户的至少一个生物识别参数；(b)基于使用次要装置所获得的至少一个生物识别参数而确定表示对次要装置的用户的验证程度的次要验证值；(c)组合从主要装置接收的主要验证值与次要验证值以得到组合式验证值；以及(d)使用组合式验证值来验证次要装置的用户(2104)。

[0098] 图22大体上说明并概述可由图19的处理电路1900或其它经合适地装备的装置执行以供由特设网络的次要装置使用来验证用户的方法或程序2200。处理电路基于环境噪声、环境光、位置、运动或经共享通信链路中的至少一者上的通用性而从特设网络接收邀

请/取消邀请信号(2202)，且将权限和策略中的一或多者连同主要验证值接收到次要装置(2204)。处理电路基于是否基于用户启动的动作(例如财务交易、安全内容存取和安全控制系统存取中的一或多者)而需要次要验证而确定是否需要次要验证，且如果需要，那么通过检测手势识别参数、面部识别参数和语音识别参数中的一或多者来执行次要验证(2206)。处理电路检测到用于取消验证次要装置的用户的触发并作为响应而取消验证次要装置的用户且通知主要装置，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：用户启动的次要装置取消验证、次要装置超时、表示对次要装置的安全性危害的次要装置威胁指示、与主要装置的通信的-损失和对预定权限或策略或其它分组策略的违反(2208)。处理电路对于比低于特设网络的主要装置的经授权量的经授权量而执行财务交易(2210)。

[0099] 应注意，本发明的各方面可在本文中描述为某一过程，所述过程描绘为流程图表、流程图、结构图或方框图。虽然流程图可将操作描述为连续过程，但是许多操作可并行或同时执行。另外，可重新布置操作的顺序。过程在其操作完成时终止。过程可对应于方法、功能、程序、子例程、子程序等。当过程对应于功能时，过程的终止对应于功能返回到调用功能或主功能。

[0100] 所属领域的技术人员将进一步了解，结合本文所揭示的方面所描述的各种说明性逻辑块、模块、电路及算法步骤可实施为电子硬件、计算机软件或两者的组合。为了清晰地说明硬件与软件的此可互换性，已在上文中大体就其功能性来描述了各种说明性组件、块、模块、电路和步骤。此功能性是实施为硬件还是软件取决于特定应用及施加于整个系统的设计约束。

[0101] 预期本文中所描述的各种特征可在不同系统中予以实施。应注意，本发明的前述方面仅为实例，且不应解释为限制性的。本发明的各方面的描述既定是说明性的，且不限制权利要求书的范围。因此，本发明的教示可容易应用于其它类型的设备，且许多替代方案、修改及变化将对于所属领域的技术人员显而易见。

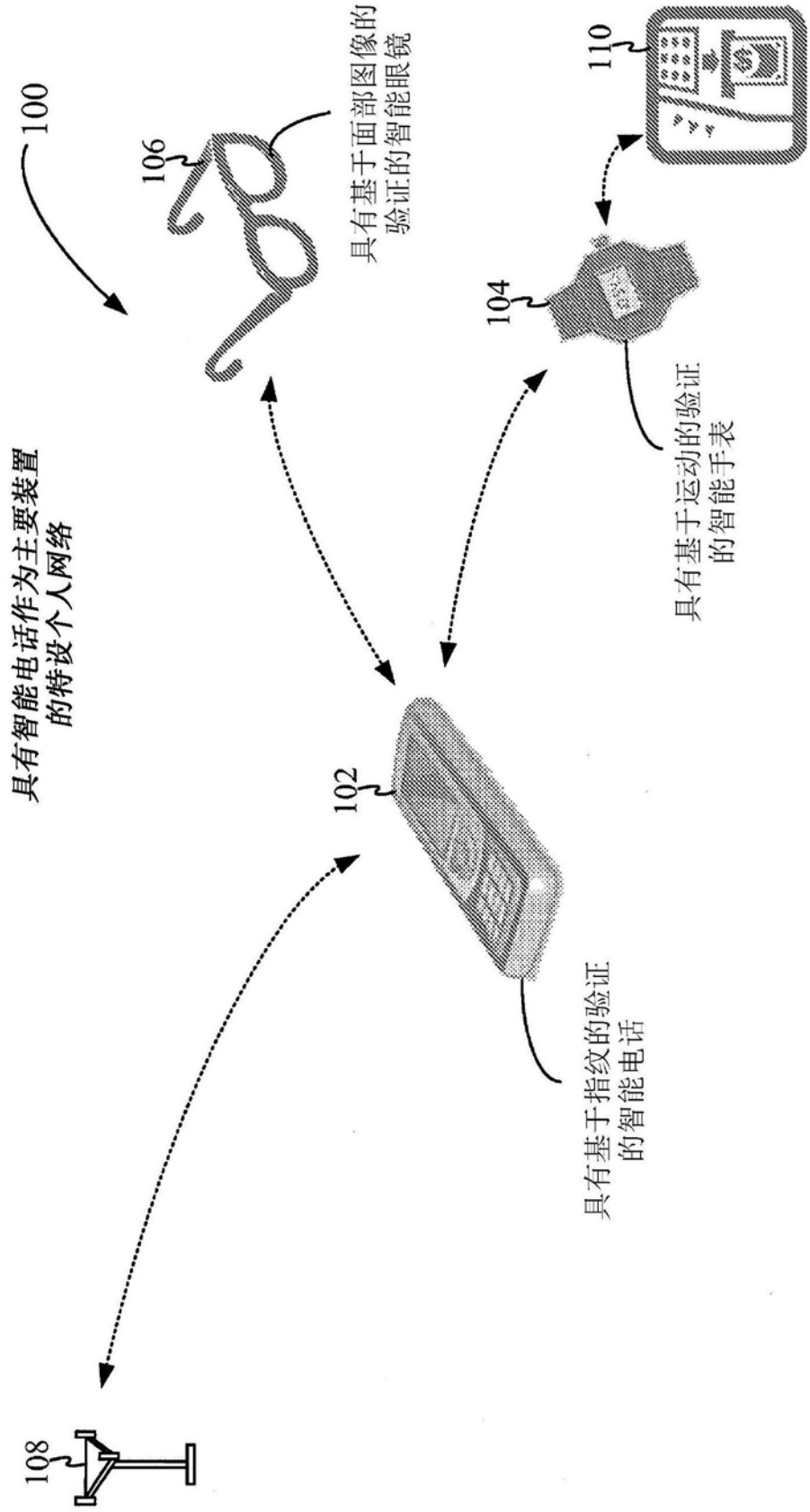

100
具有智能电话作为主要装置的特设个人网络
106
具有基于面部图像的验证的智能眼镜
110
104
具有基于运动的验证的智能手表
102
具有基于指纹的验证的智能电话
108

图1

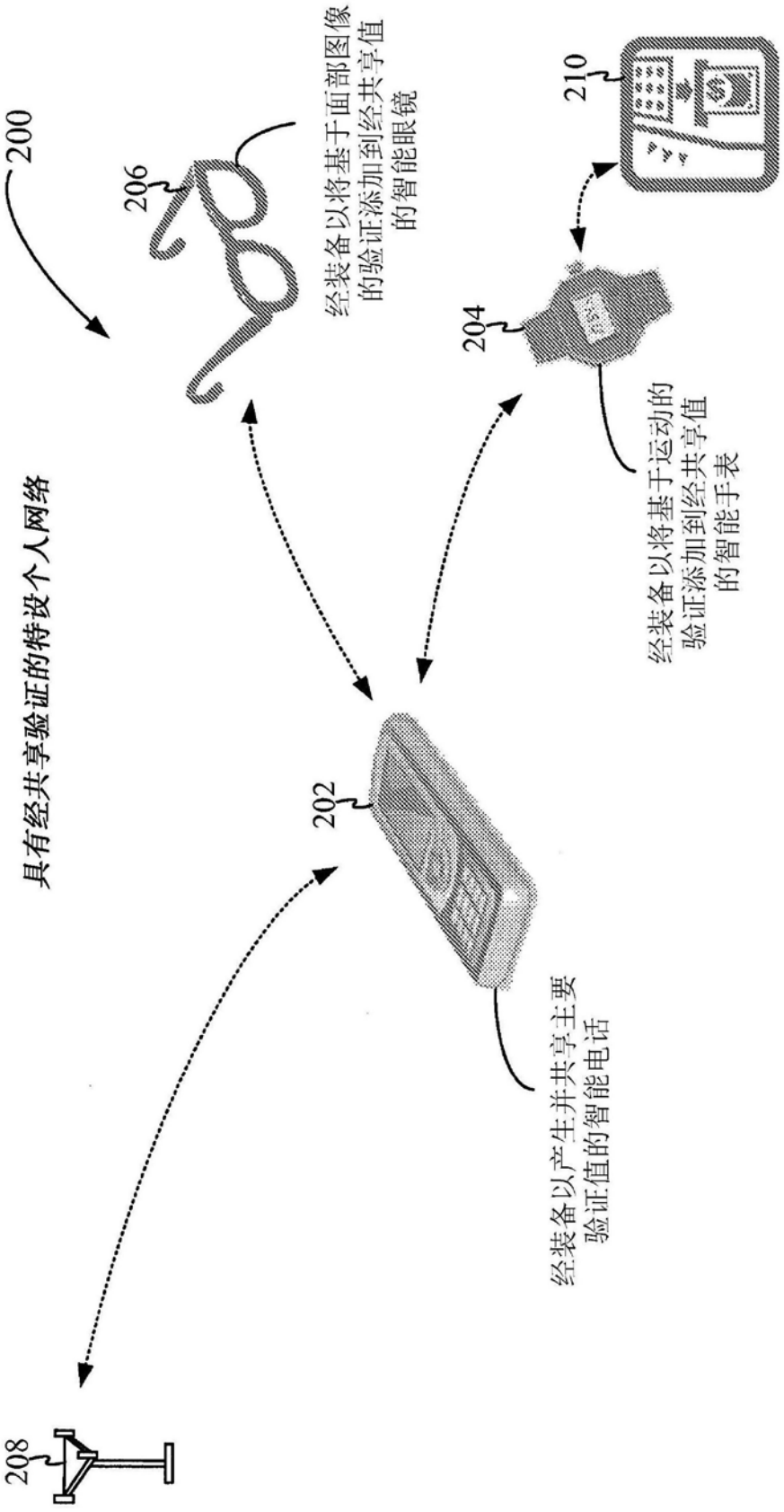

200
具有经共享验证的特设个人网络
206
经装备以将基于面部图像的验证添加到经共享值的智能眼镜
210
204
经装备以将基于运动的验证添加到经共享值的智能手表
202
经装备以产生并共享主要验证值的智能电话
208

图2

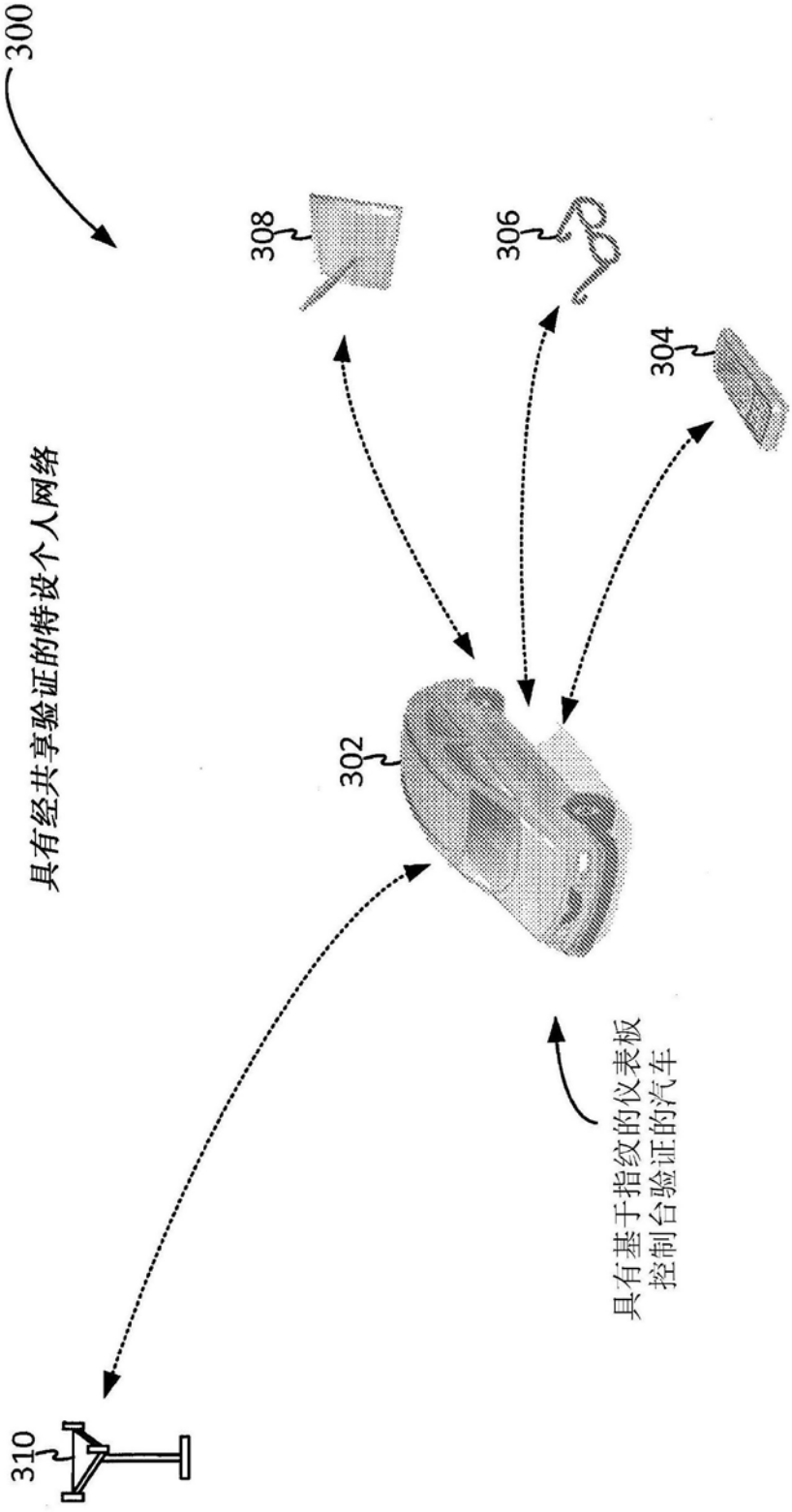

300
308
306
304
302
具有经共享验证的特设个人网络
具有基于指纹的仪表板
控制台验证的汽车
310

图3

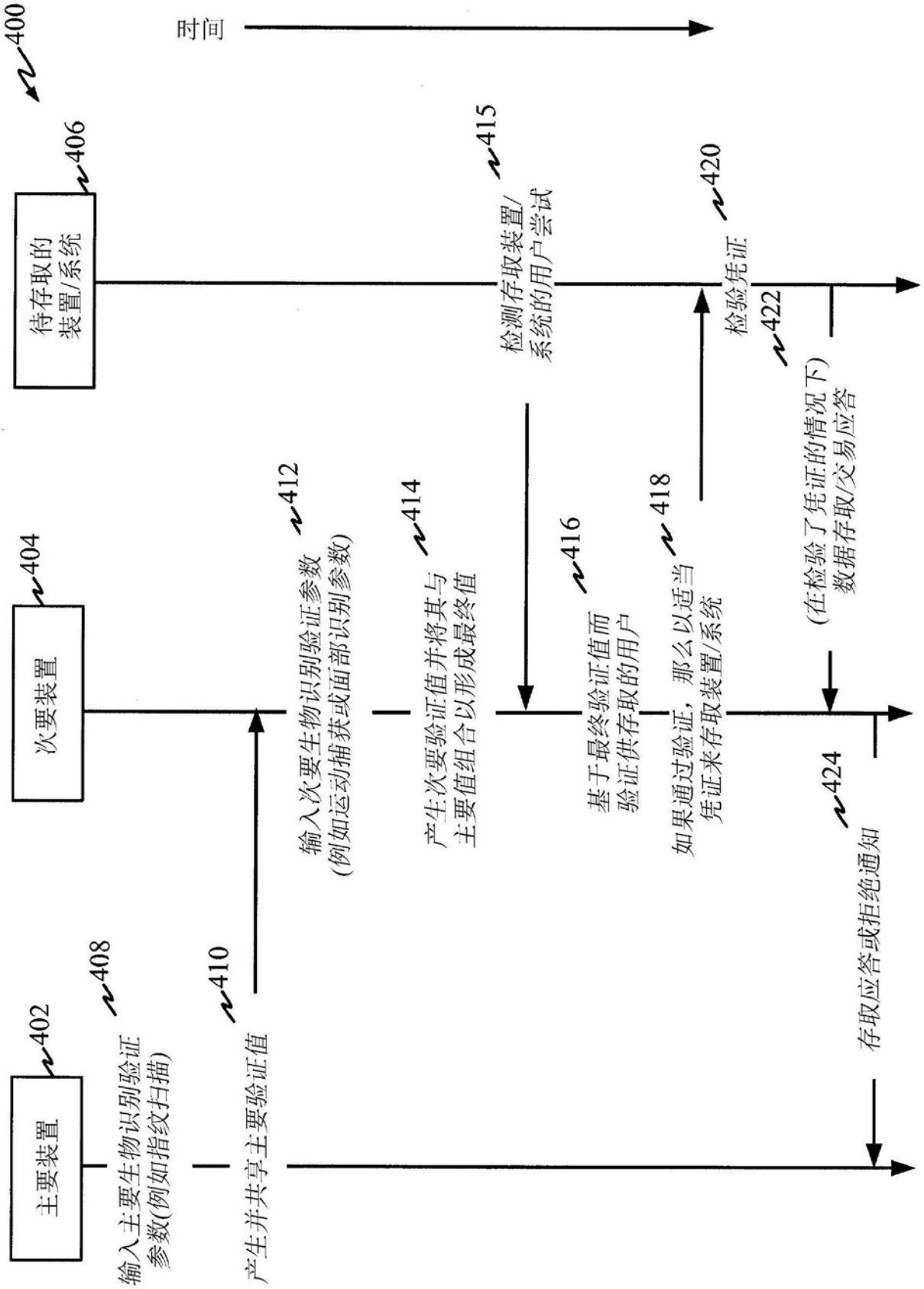

400
时间
主要装置
402
输入主要生物识别验证参数(例如指纹扫描)
408
产生并共享主要验证值
410
次要装置
404
输入次要生物识别验证参数(例如运动捕获或面部识别参数)
412
产生次要验证值并将其与主要值组合以形成最终值
414
基于最终验证值而验证供存取的用户
416
如果通过验证，那么以适当凭证来存取装置/系统
418
存取应答或拒绝通知
424
待存取的装置/系统
406
检测存取装置/系统的用户尝试
415
检验凭证
420
(在检验了凭证的情况下)数据存取/交易应答
422

图4

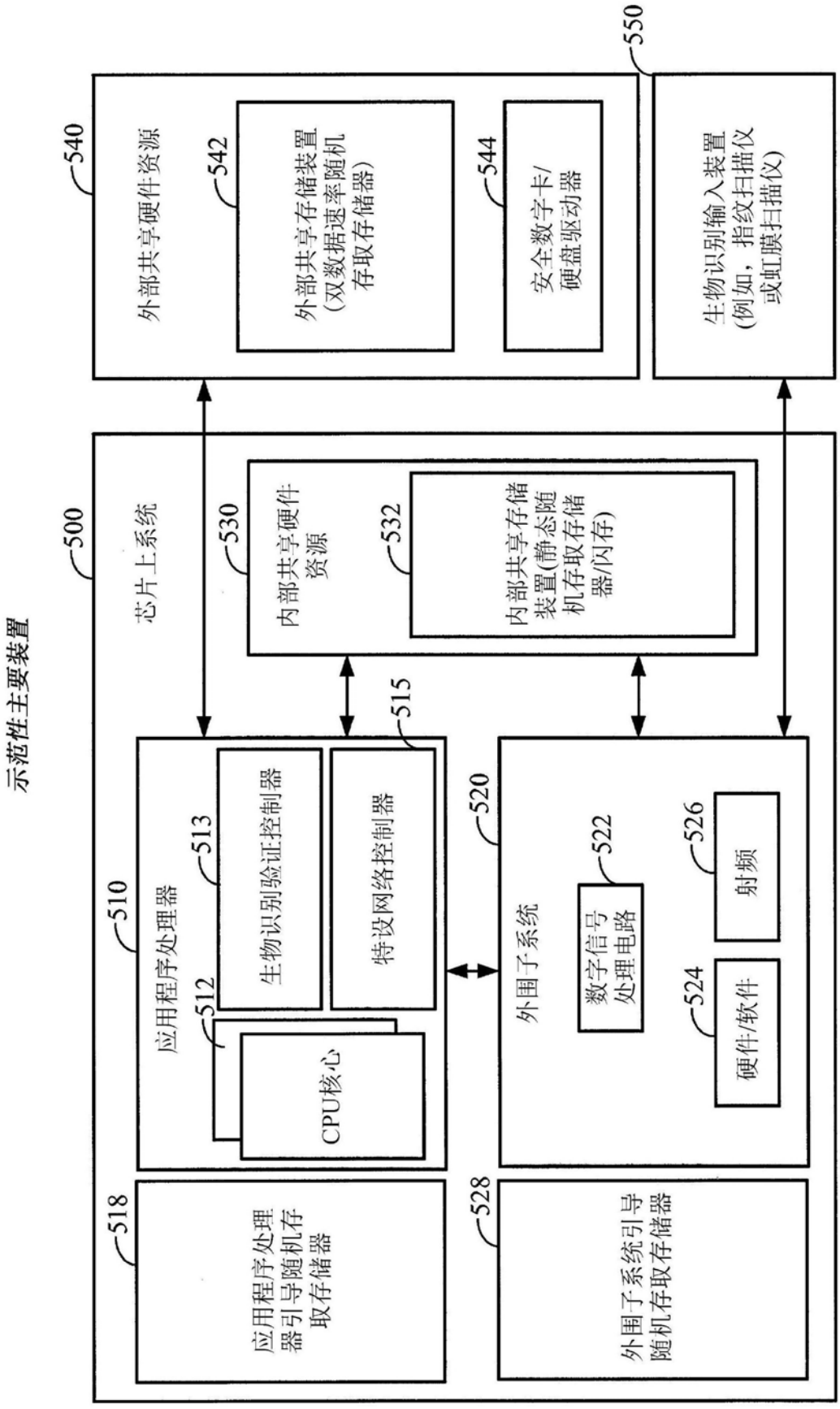

示范性主要装置
500
芯片上系统
510
应用程序处理器
512
CPU核心
513
生物识别验证控制器
515
特设网络控制器
518
应用程序处理器引导随机存取存储器
520
外围子系统
522
数字信号处理电路
524
硬件/软件
526
射频
528
外围子系统引导随机存取存储器
530
内部共享硬件资源
532
内部共享存储装置(静态随机存取存储器/闪存)
540
外部共享硬件资源
542
外部共享存储装置(双数据速率随机存取存储器)
544
安全数字卡/硬盘驱动器
550
生物识别输入装置(例如，指纹扫描仪或虹膜扫描仪)

图5

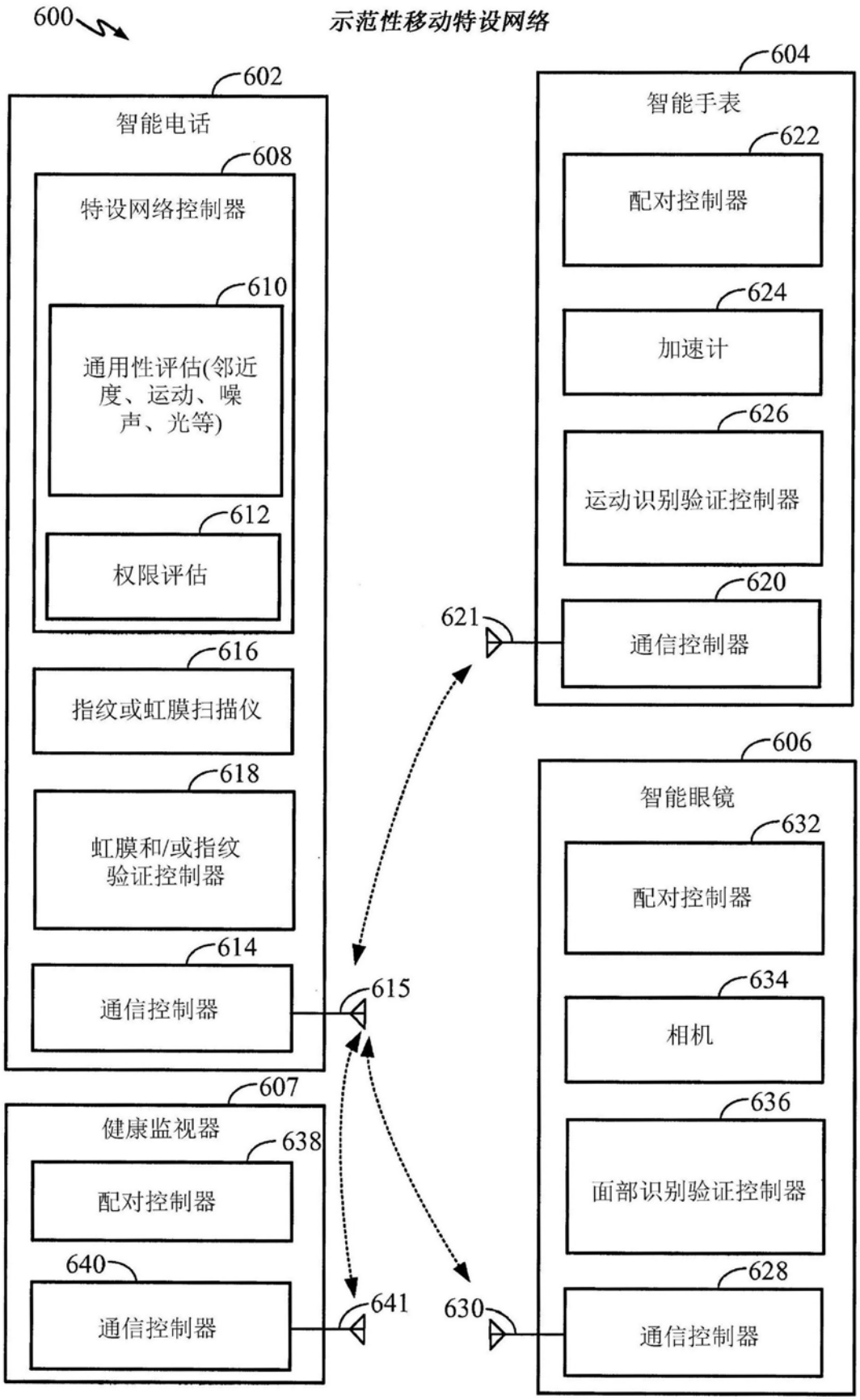

600
示范性移动特设网络
602
智能电话
608
特设网络控制器
610
通用性评估(邻近度、运动、噪声、光等)
612
权限评估
616
指纹或虹膜扫描仪
618
虹膜和/或指纹验证控制器
614
通信控制器
615
607
健康监视器
638
配对控制器
640
通信控制器
641
604
智能手表
622
配对控制器
624
加速计
626
运动识别验证控制器
620
621
通信控制器
606
智能眼镜
632
配对控制器
634
相机
636
面部识别验证控制器
628
630
通信控制器

图6

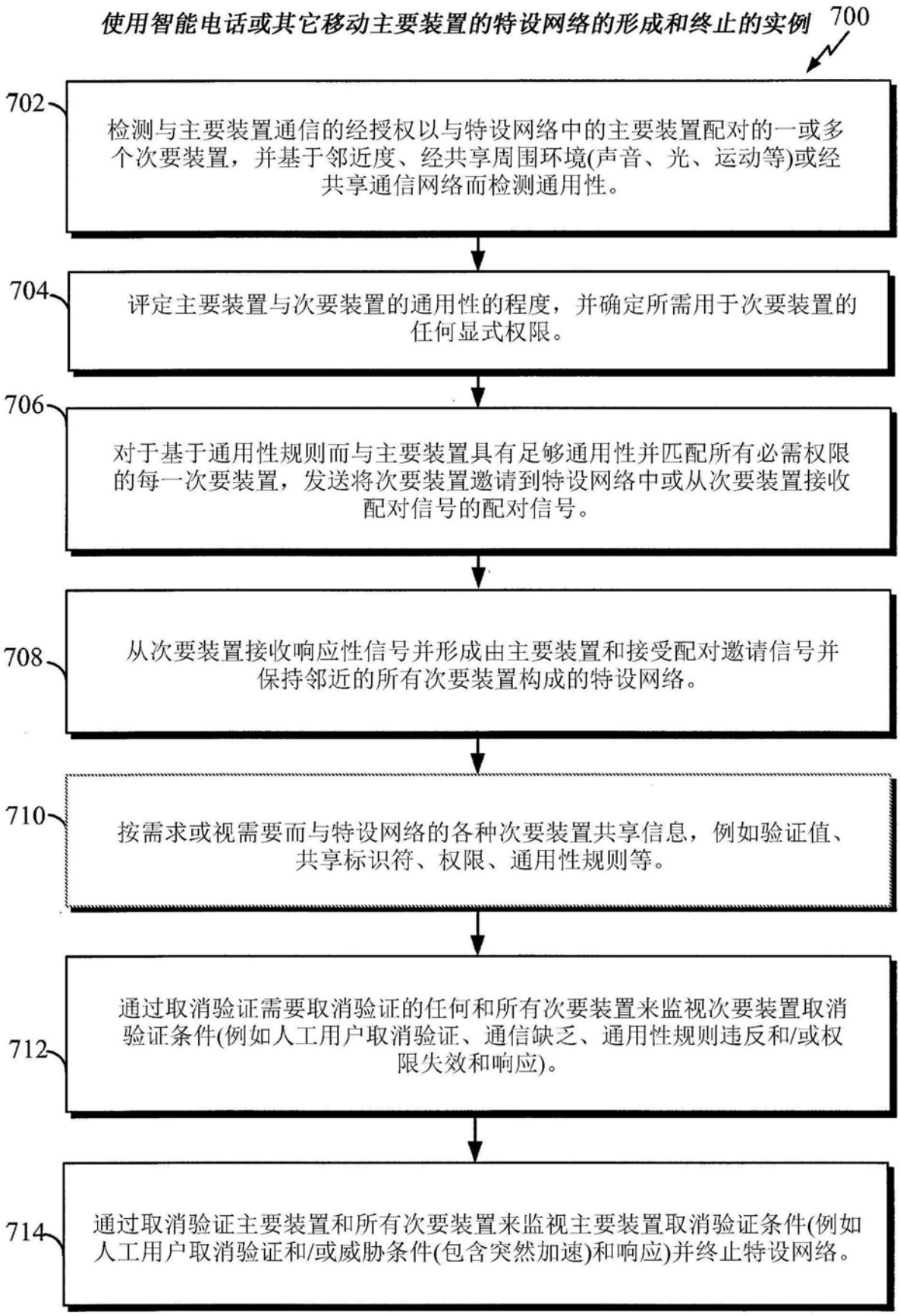

使用智能电话或其它移动主要装置的特设网络的形成和终止的实例
700
702
检测与主要装置通信的经授权以与特设网络中的主要装置配对的一或多个次要装置，并基于邻近度、经共享周围环境(声音、光、运动等)或经共享通信网络而检测通用性。
704
评定主要装置与次要装置的通用性的程度，并确定所需用于次要装置的任何显式权限。
706
对于基于通用性规则而与主要装置具有足够通用性并匹配所有必需权限的每一次要装置，发送将次要装置邀请到特设网络中或从次要装置接收配对信号的配对信号。
708
从次要装置接收响应性信号并形成由主要装置和接受配对邀请信号并保持邻近的所有次要装置构成的特设网络。
710
按需求或视需要而与特设网络的各种次要装置共享信息，例如验证值、共享标识符、权限、通用性规则等。
712
通过取消验证需要取消验证的任何和所有次要装置来监视次要装置取消验证条件(例如人工用户取消验证、通信缺乏、通用性规则违反和/或权限失效和响应)。
714
通过取消验证主要装置和所有次要装置来监视主要装置取消验证条件(例如人工用户取消验证和/或威胁条件(包含突然加速)和响应)并终止特设网络。

图7

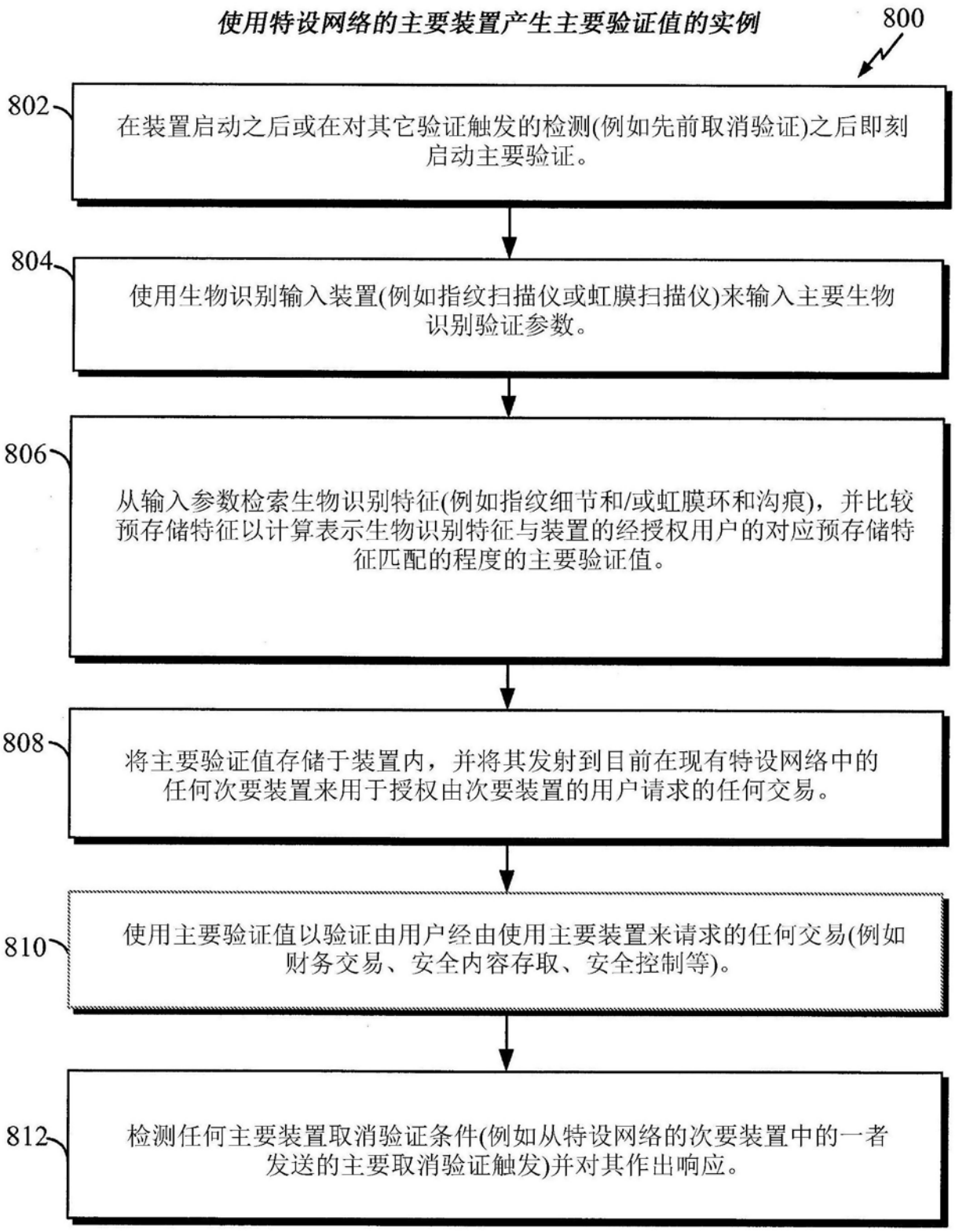

使用特设网络的主要装置产生主要验证值的实例
800
802
在装置启动之后或在对其它验证触发的检测(例如先前取消验证)之后即刻启动主要验证。
804
使用生物识别输入装置(例如指纹扫描仪或虹膜扫描仪)来输入主要生物识别验证参数。
806
从输入参数检索生物识别特征(例如指纹细节和/或虹膜环和沟痕)，并比较预存储特征以计算表示生物识别特征与装置的经授权用户的对应预存储特征匹配的程度的主要验证值。
808
将主要验证值存储于装置内，并将其发射到目前在现有特设网络中的任何次要装置来用于授权由次要装置的用户请求的任何交易。
810
使用主要验证值以验证由用户经由使用主要装置来请求的任何交易(例如财务交易、安全内容存取、安全控制等)。
812
检测任何主要装置取消验证条件(例如从特设网络的次要装置中的一者发送的主要取消验证触发)并对其作出响应。

图8

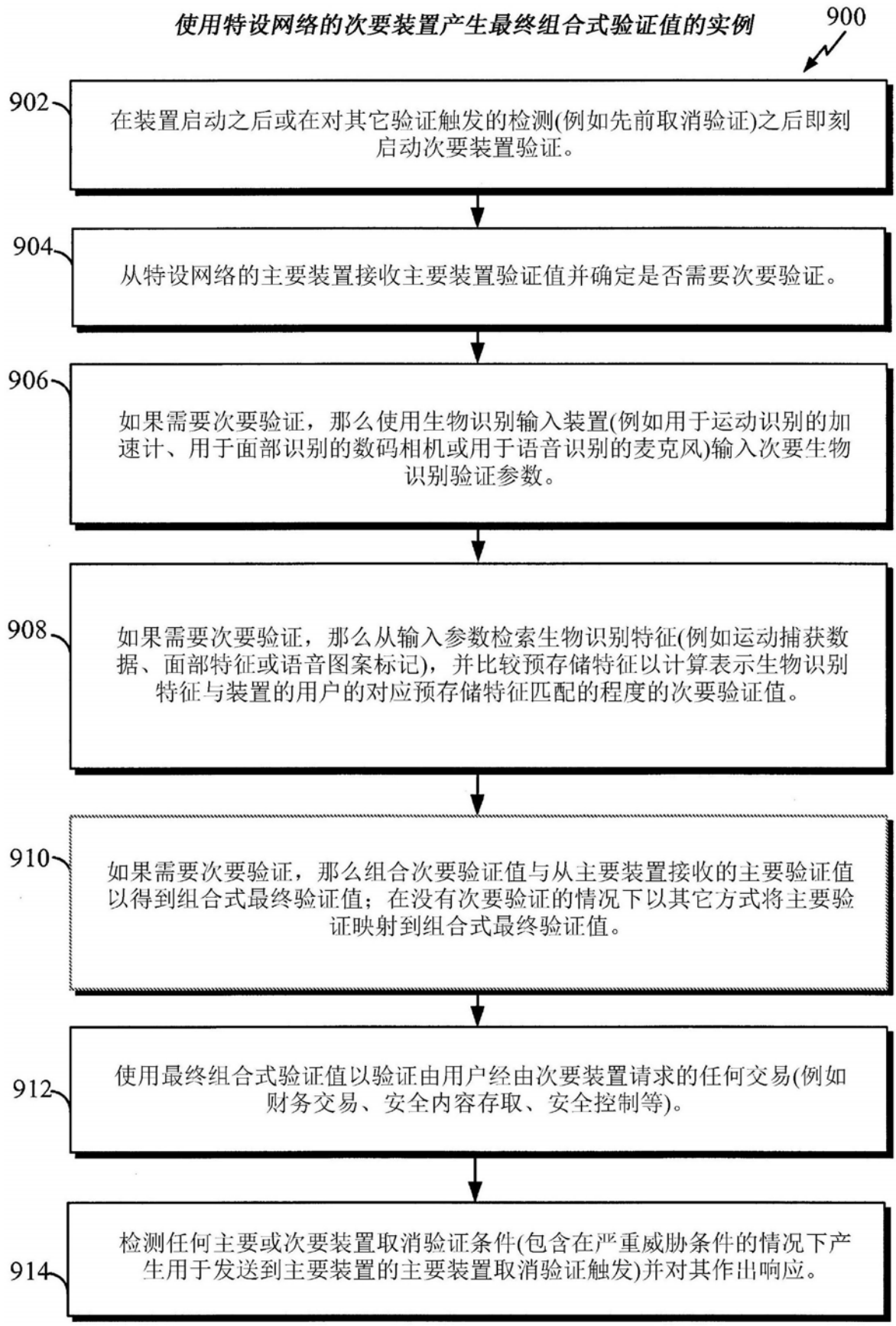

使用特设网络的次要装置产生最终组合式验证值的实例
900
902
在装置启动之后或在对其它验证触发的检测(例如先前取消验证)之后即刻启动次要装置验证。
904
从特设网络的主要装置接收主要装置验证值并确定是否需要次要验证。
906
如果需要次要验证，那么使用生物识别输入装置(例如用于运动识别的加速计、用于面部识别的数码相机或用于语音识别的麦克风)输入次要生物识别验证参数。
908
如果需要次要验证，那么从输入参数检索生物识别特征(例如运动捕获数据、面部特征或语音图案标记)，并比较预存储特征以计算表示生物识别特征与装置的用户的对应预存储特征匹配的程度的次要验证值。
910
如果需要次要验证，那么组合次要验证值与从主要装置接收的主要验证值以得到组合式最终验证值；在没有次要验证的情况下以其它方式将主要验证映射到组合式最终验证值。
912
使用最终组合式验证值以验证由用户经由次要装置请求的任何交易(例如财务交易、安全内容存取、安全控制等)。
914
检测任何主要或次要装置取消验证条件(包含在严重威胁条件的情况下产生用于发送到主要装置的主要装置取消验证触发)并对其作出响应。

图9

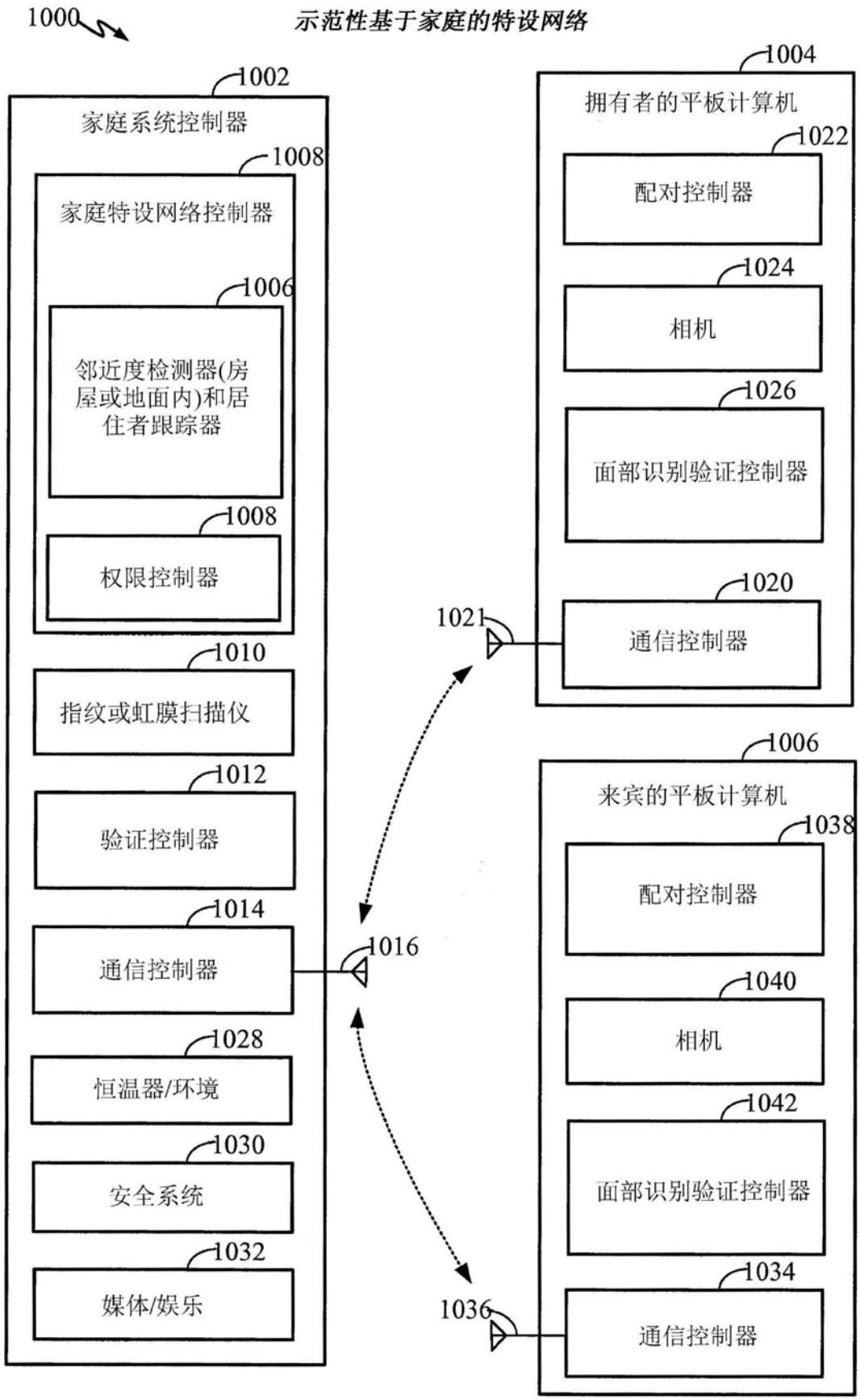

1000
示范性基于家庭的特设网络
1002
家庭系统控制器
1008
家庭特设网络控制器
1006
邻近度检测器(房屋或地面内)和居住者跟踪器
1008
权限控制器
1010
指纹或虹膜扫描仪
1012
验证控制器
1014
通信控制器
1028
恒温器/环境
1030
安全系统
1032
媒体/娱乐
1016
1004
拥有者的平板计算机
1022
配对控制器
1024
相机
1026
面部识别验证控制器
1020
通信控制器
1021
1006
来宾的平板计算机
1038
配对控制器
1040
相机
1042
面部识别验证控制器
1034
通信控制器
1036

图10

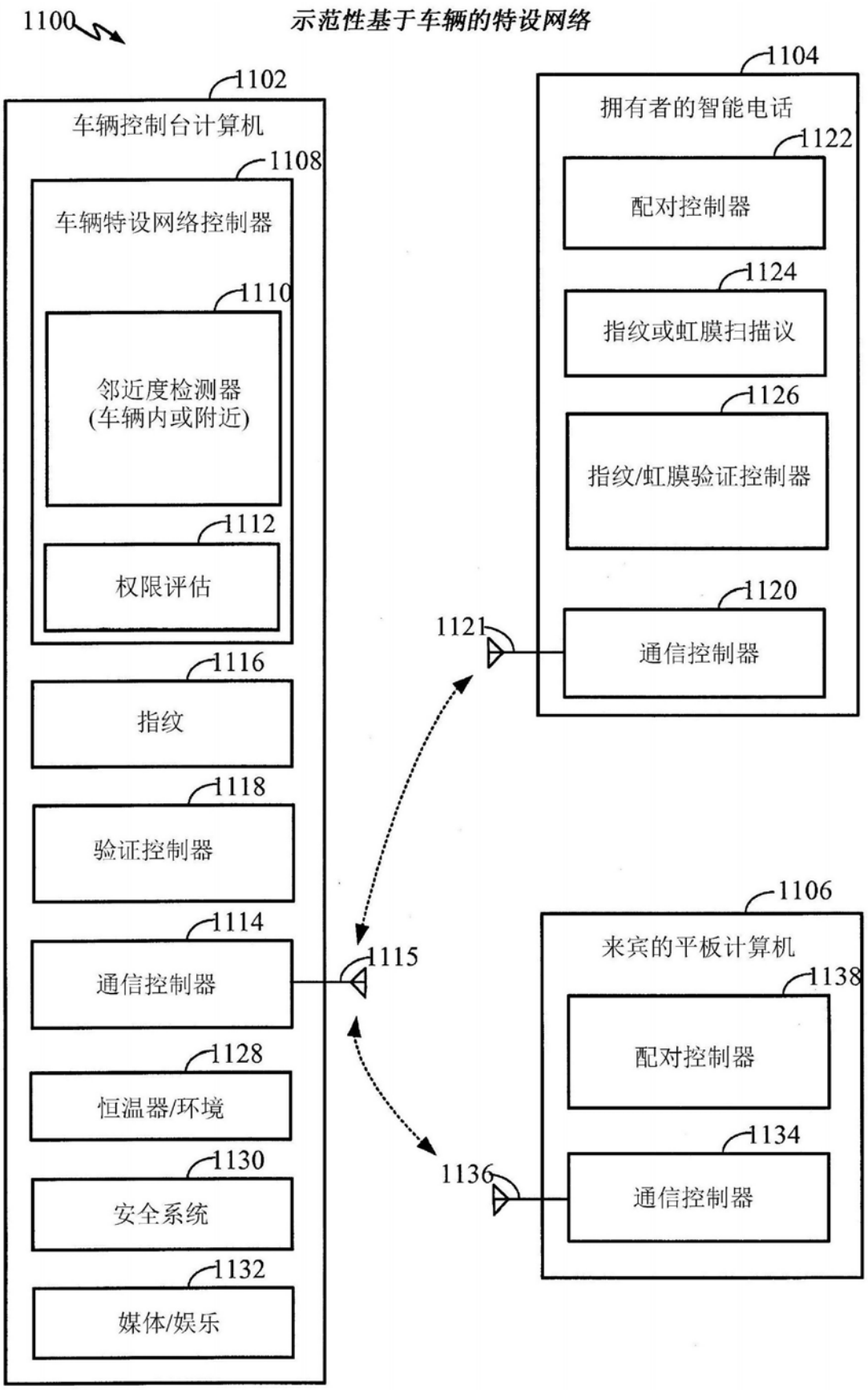

1100
示范性基于车辆的特设网络
1102
车辆控制台计算机
1108
车辆特设网络控制器
1110
邻近度检测器
(车辆内或附近)
1112
权限评估
1116
指纹
1118
验证控制器
1114
通信控制器
1128
恒温器/环境
1130
安全系统
1132
媒体/娱乐
1115
1104
拥有者的智能电话
1122
配对控制器
1124
指纹或虹膜扫描议
1126
指纹/虹膜验证控制器
1120
1121
通信控制器
1106
来宾的平板计算机
1138
配对控制器
1134
1136
通信控制器

图11

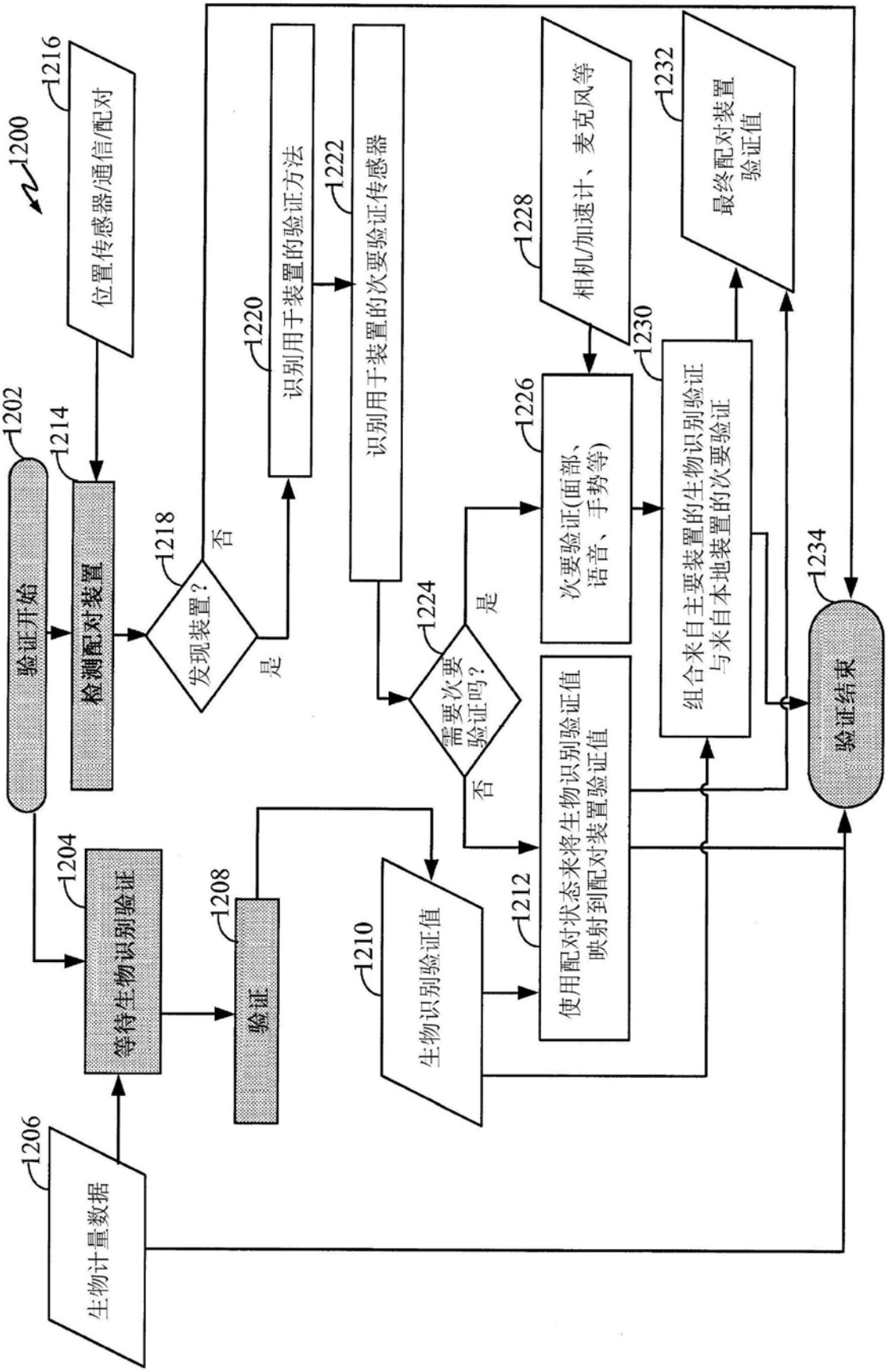

1200
1202
验证开始
1204
等待生物识别验证
1206
生物计量数据
1208
验证
1210
生物识别验证值
1212
使用配对状态来将生物识别验证值
映射到配对装置验证值
1214
检测配对装置
1216
位置传感器/通信/配对
1218
发现装置?
否
是
1220
识别用于装置的验证方法
1222
识别用于装置的次要验证传感器
1224
需要次要
验证吗?
是
否
1226
次要验证(面部、
语音、手势等)
1228
相机/加速计、麦克风等
1230
组合来自主要装置的生物识别验证
与来自本地装置的次要验证
1232
最终配对装置
验证值
1234
验证结束

图12

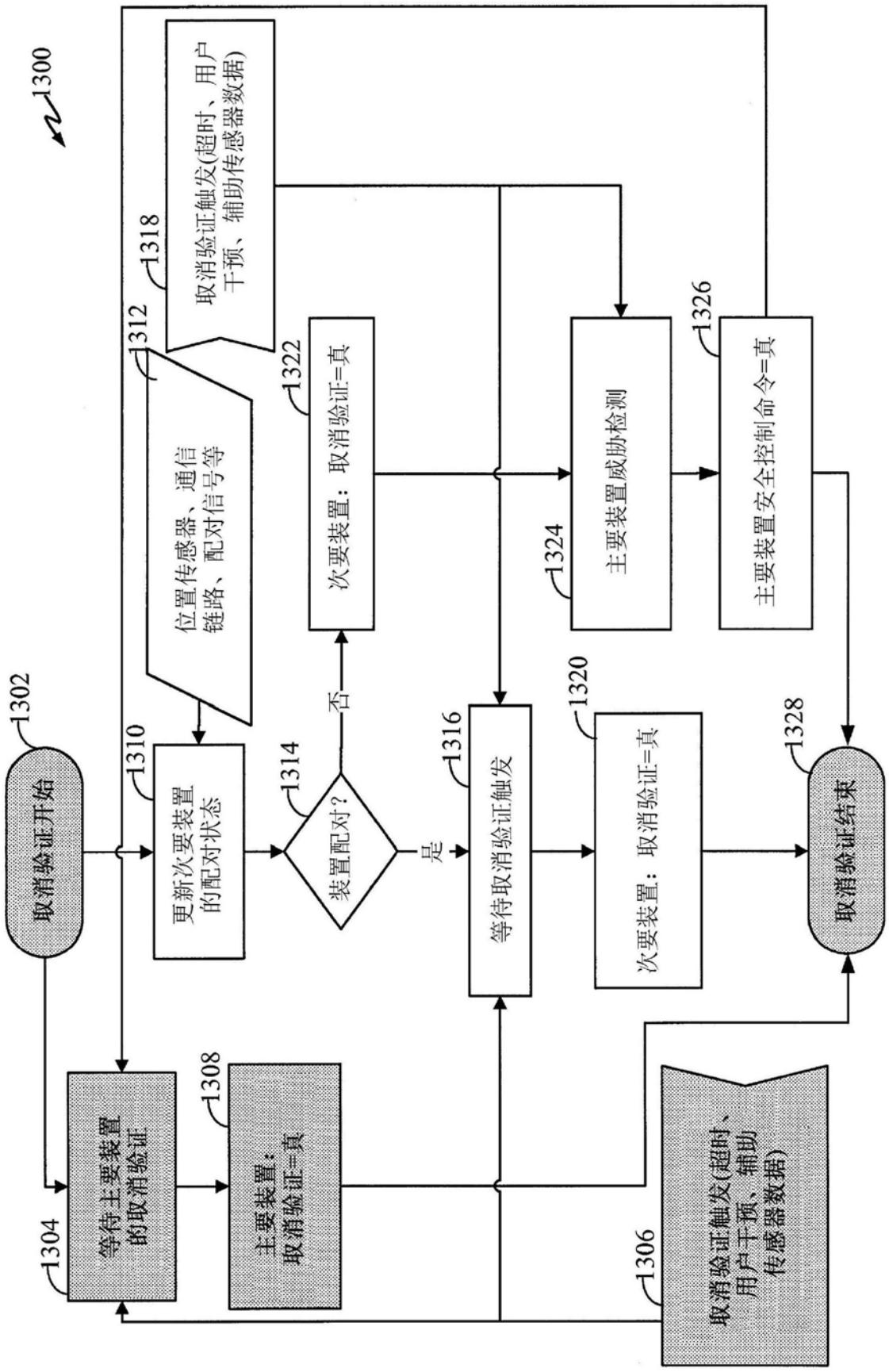

1300
取消验证开始
1302
等待主要装置的取消验证
1304
主要装置：取消验证=真
1308
取消验证触发(超时、用户干预、辅助传感器数据)
1306
更新次要装置的配对状态
1310
装置配对？
1314
否
是
次要装置：取消验证=真
1322
等待取消验证触发
1316
次要装置：取消验证=真
1320
主要装置威胁检测
1324
主要装置安全控制命令=真
1326
取消验证结束
1328
位置传感器、通信链路、配对信号等
1312
取消验证触发(超时、用户干预、辅助传感器数据)
1318

图13

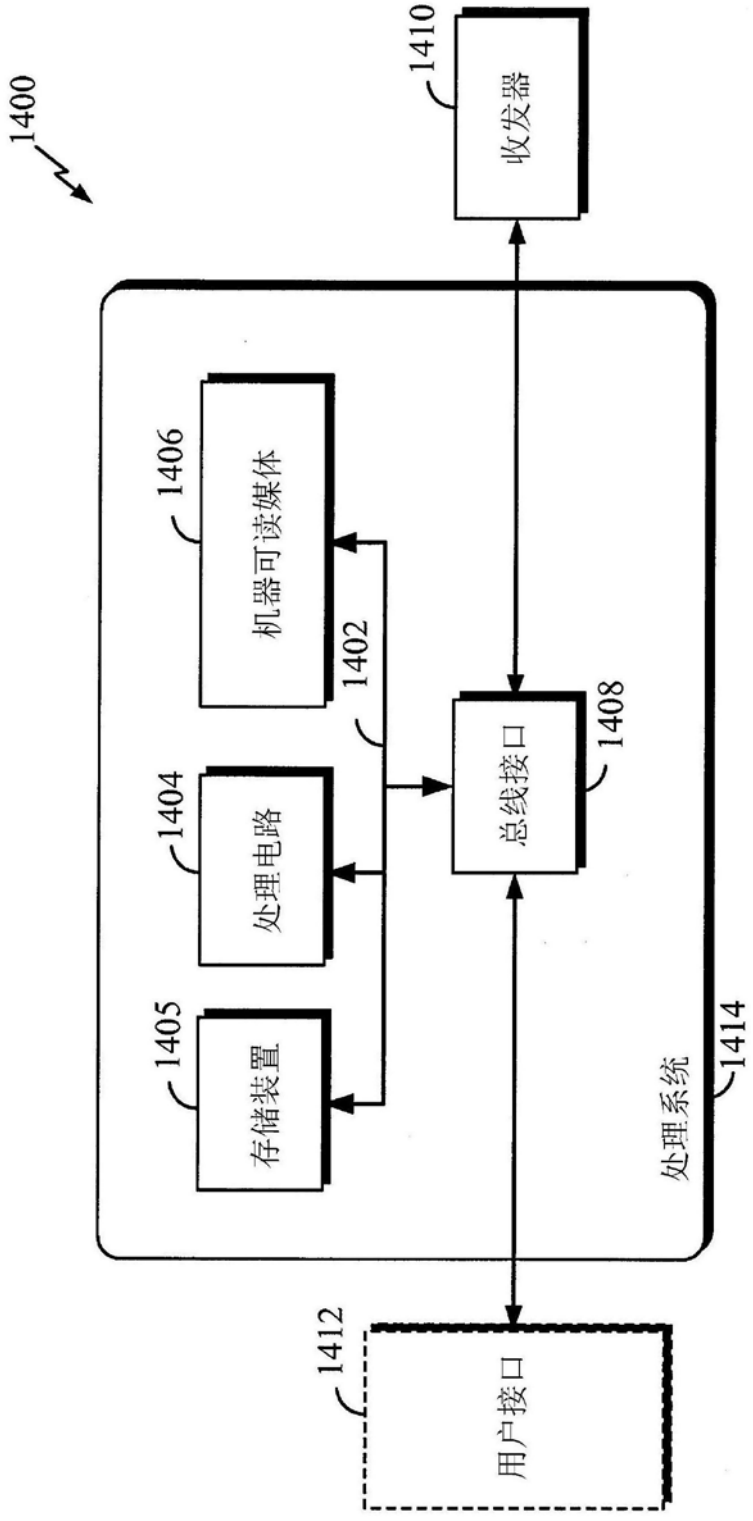

1400
1410
收发器
1406
机器可读媒体
1402
1404
处理电路
1408
总线接口
1405
存储装置
1414
处理系统
1412
用户接口

图14

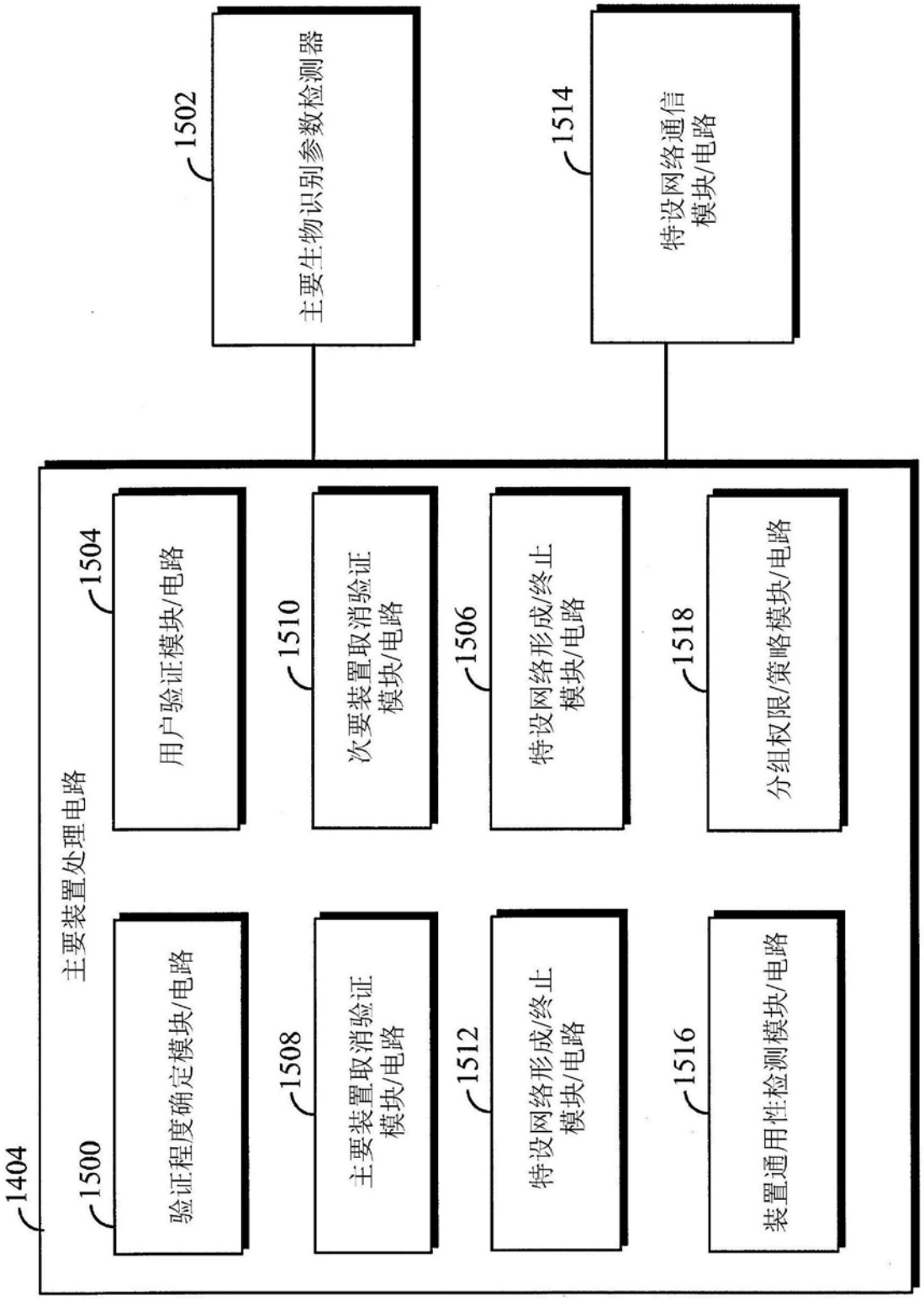

1404
主要装置处理电路
1500
验证程度确定模块/电路
1504
用户验证模块/电路
1508
主要装置取消验证模块/电路
1510
次要装置取消验证模块/电路
1512
特设网络形成/终止模块/电路
1506
特设网络形成/终止模块/电路
1516
装置通用性检测模块/电路
1518
分组权限/策略模块/电路
1502
主要生物识别参数检测器
1514
特设网络通信模块/电路

图15

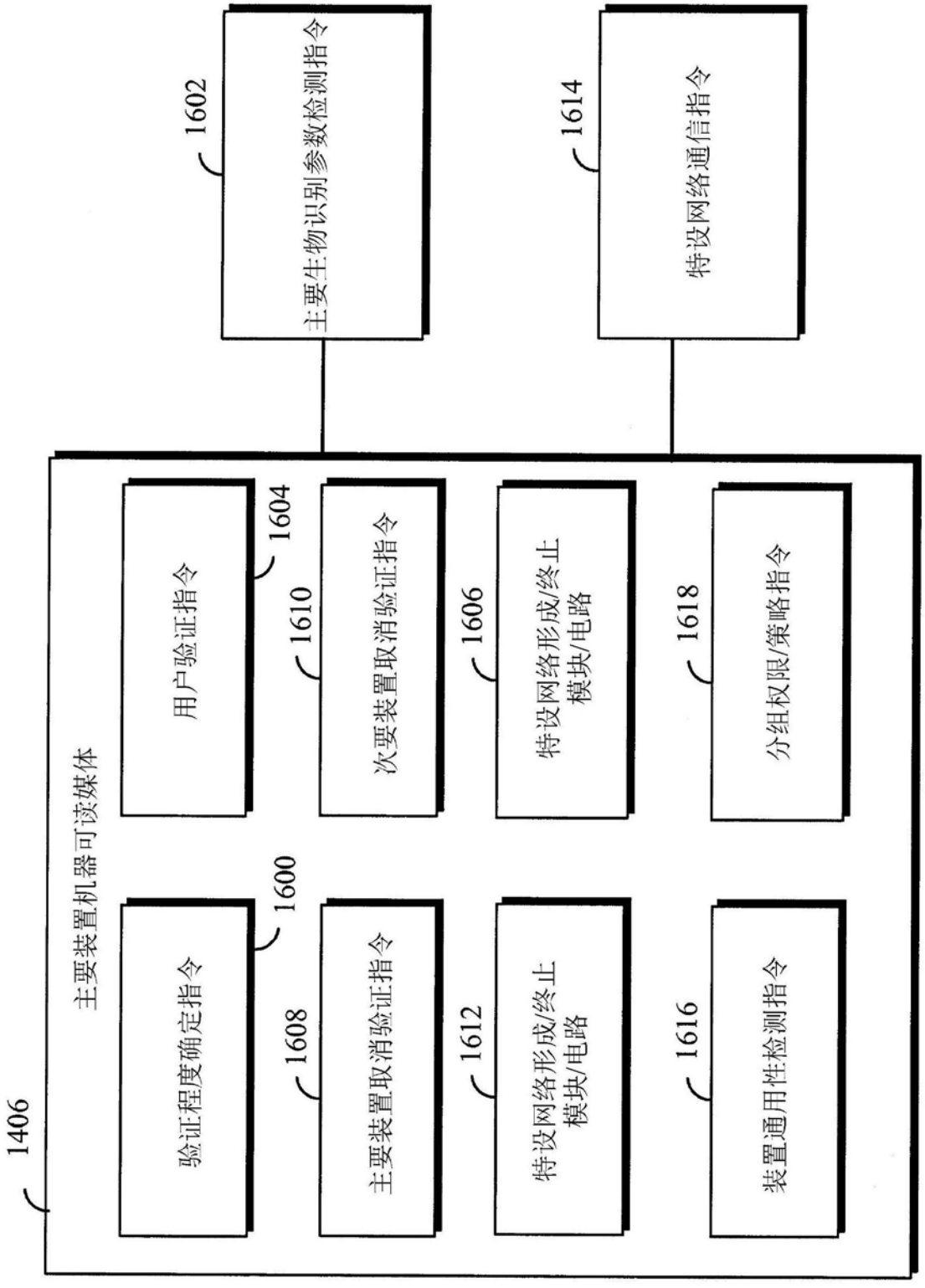

1406
主要装置机器可读媒体
1600
验证程度确定指令
1608
主要装置取消验证指令
1612
特设网络形成/终止模块/电路
1616
装置通用性检测指令
1604
用户验证指令
1610
次要装置取消验证指令
1606
特设网络形成/终止模块/电路
1618
分组权限/策略指令
1602
主要生物识别参数检测指令
1614
特设网络通信指令

图16

供由特设网络的主要装置使用以验证用户的方法的概述

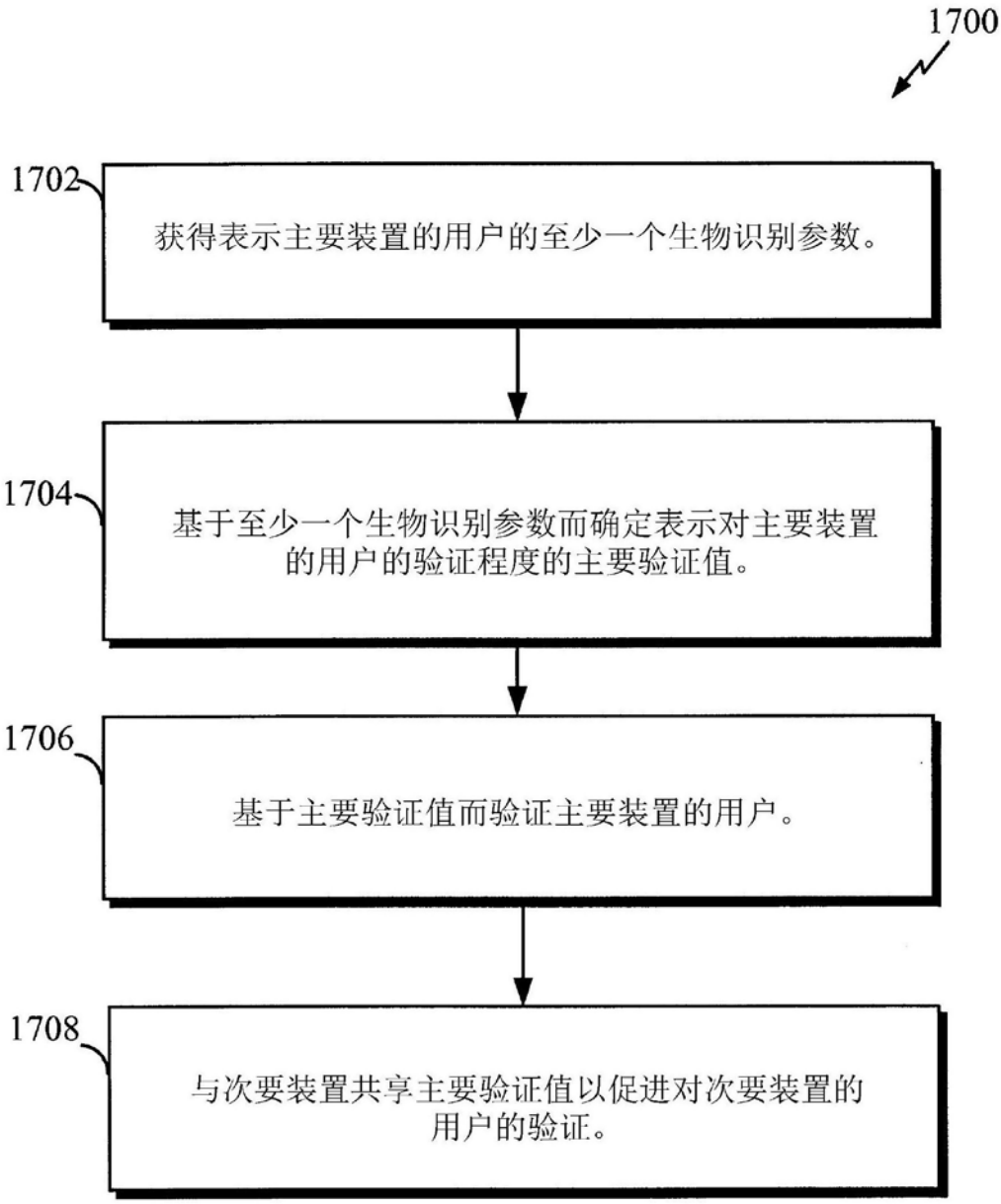


图17

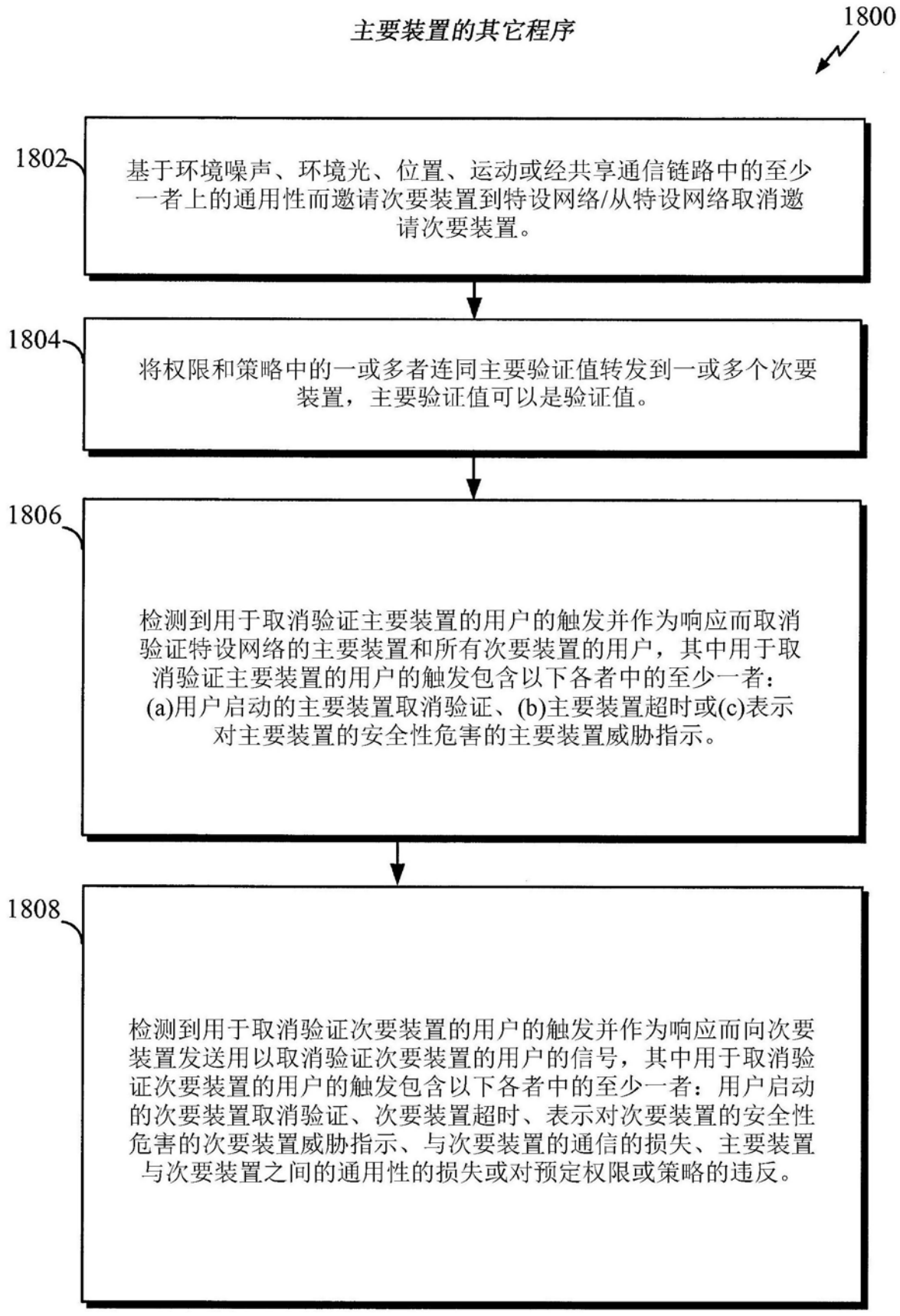

主要装置的其它程序
1800
1802
基于环境噪声、环境光、位置、运动或经共享通信链路中的至少一者上的通用性而邀请次要装置到特设网络/从特设网络取消邀请次要装置。
1804
将权限和策略中的一或多者连同主要验证值转发到一或多个次要装置，主要验证值可以是验证值。
1806
检测到用于取消验证主要装置的用户的触发并作为响应而取消验证特设网络的主要装置和所有次要装置的用户，其中用于取消验证主要装置的用户的触发包含以下各者中的至少一者：(a)用户启动的主要装置取消验证、(b)主要装置超时或(c)表示对主要装置的安全性危害的主要装置威胁指示。
1808
检测到用于取消验证次要装置的用户的触发并作为响应而向次要装置发送用以取消验证次要装置的用户的信号，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：用户启动的次要装置取消验证、次要装置超时、表示对次要装置的安全性危害的次要装置威胁指示、与次要装置的通信的损失、主要装置与次要装置之间的通用性的损失或对预定权限或策略的违反。

图18

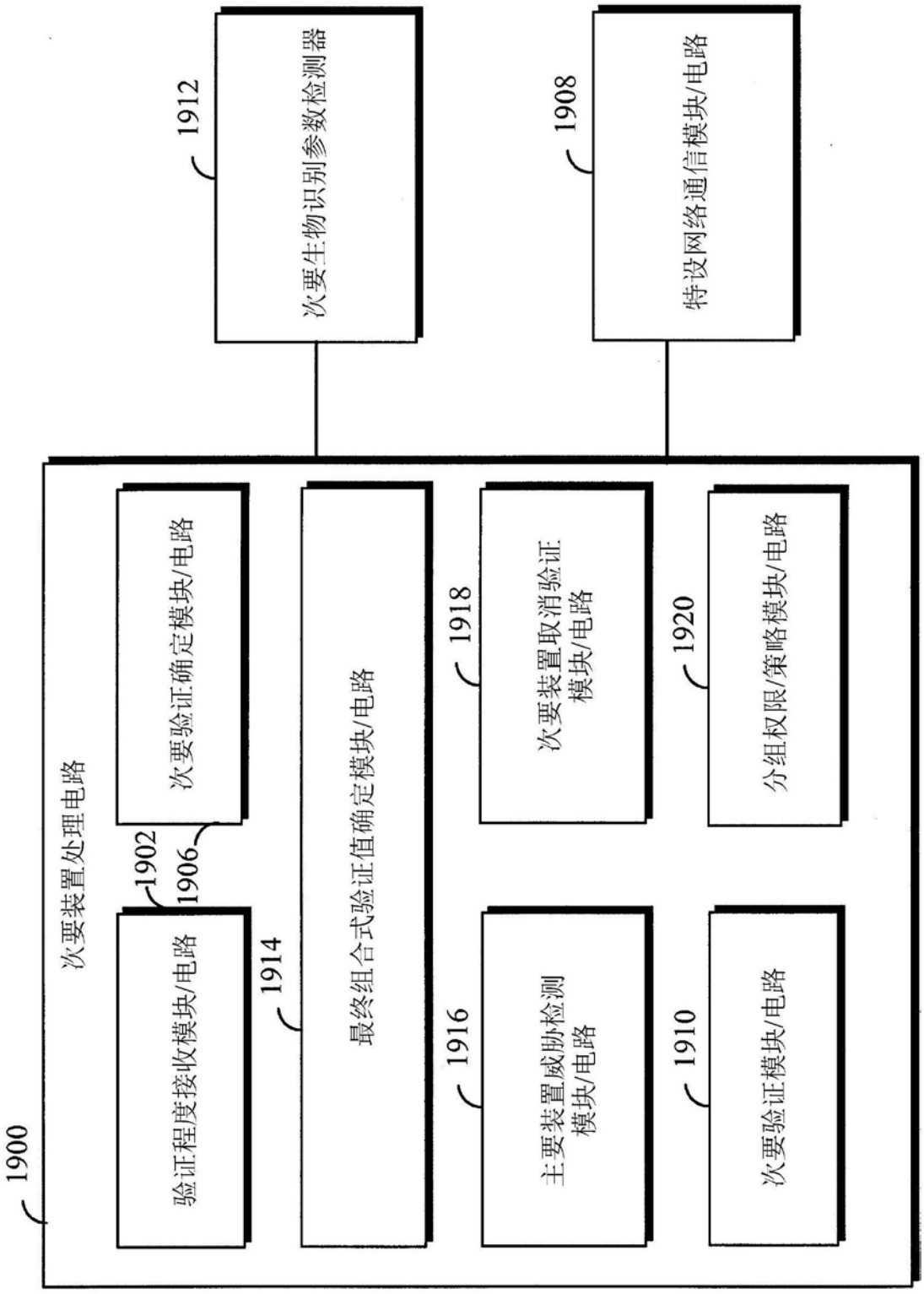

1900
次要装置处理电路
1902
1906
验证程度接收模块/电路
次要验证确定模块/电路
1914
最终组合式验证值确定模块/电路
1916
主要装置威胁检测模块/电路
1910
次要验证模块/电路
1918
次要装置取消验证模块/电路
1920
分组权限/策略模块/电路
1912
次要生物识别参数检测器
1908
特设网络通信模块/电路

图19

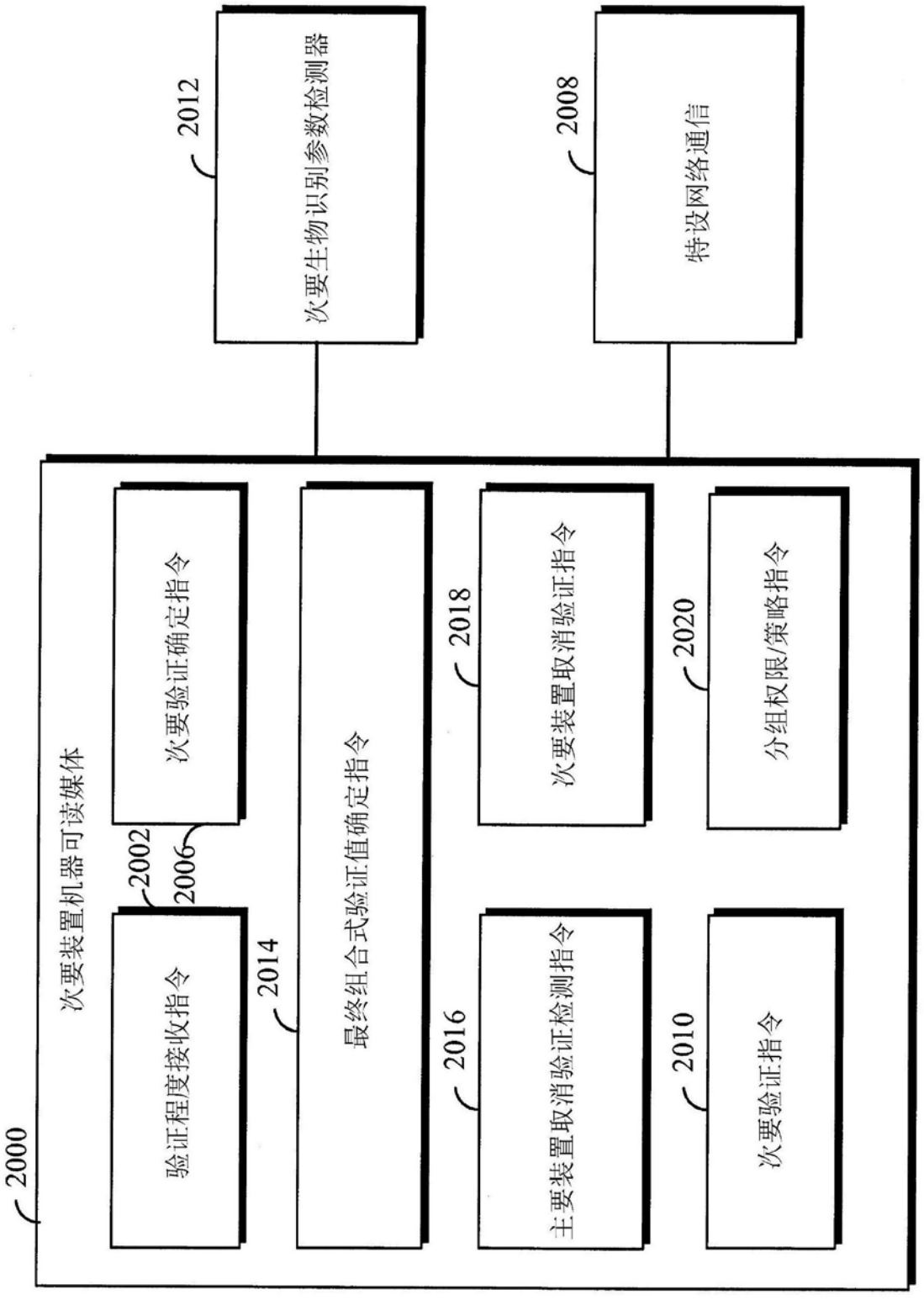

2012
次要生物识别参数检测器
2008
特设网络通信
2000
次要装置机器可读媒体
2002
验证程度接收指令
2006
次要验证确定指令
2014
最终组合式验证值确定指令
2016
主要装置取消验证检测指令
2018
次要装置取消验证指令
2010
次要验证指令
2020
分组权限/策略指令

图20

供由特设网络的次要装置使用以验证用户的方法的概述

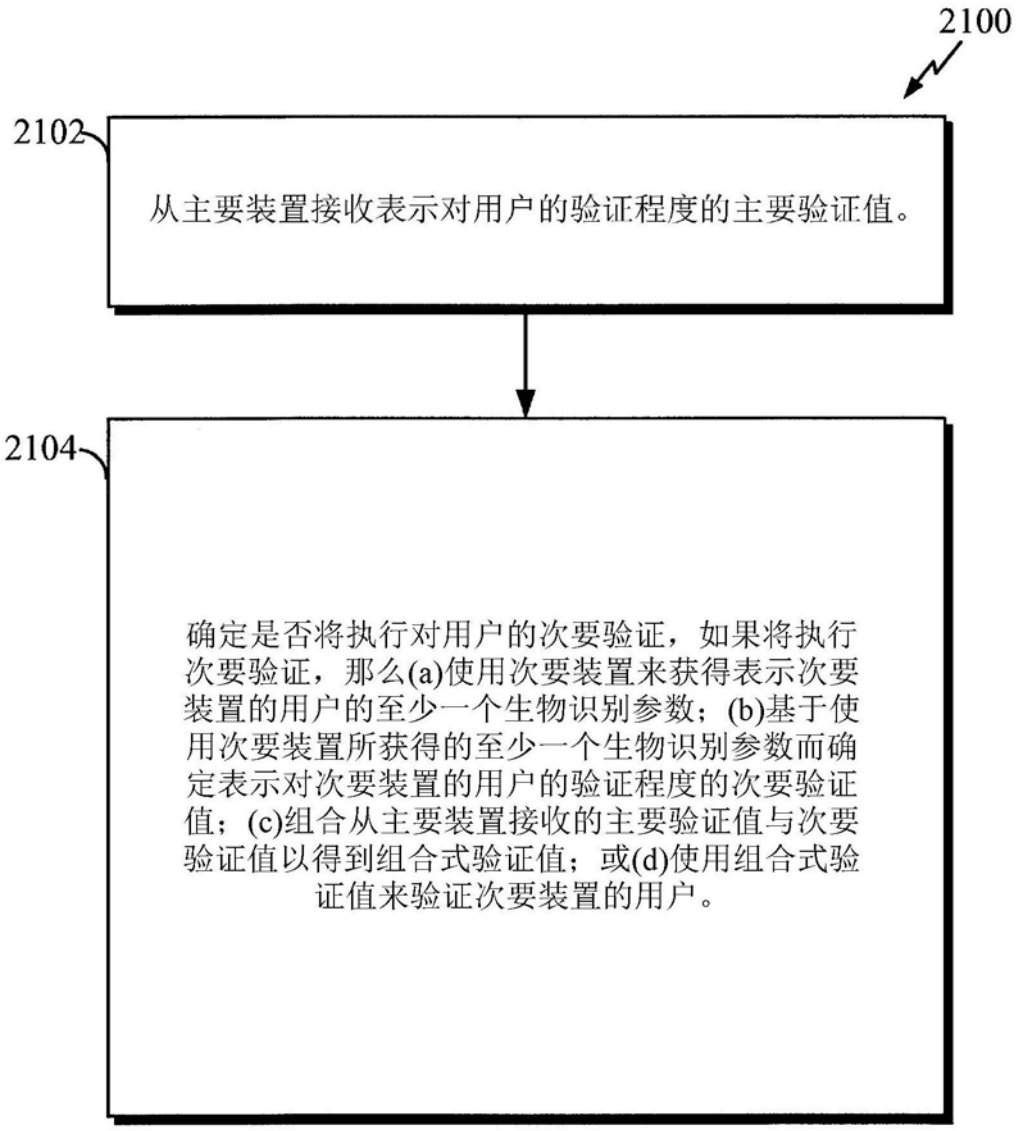


图21

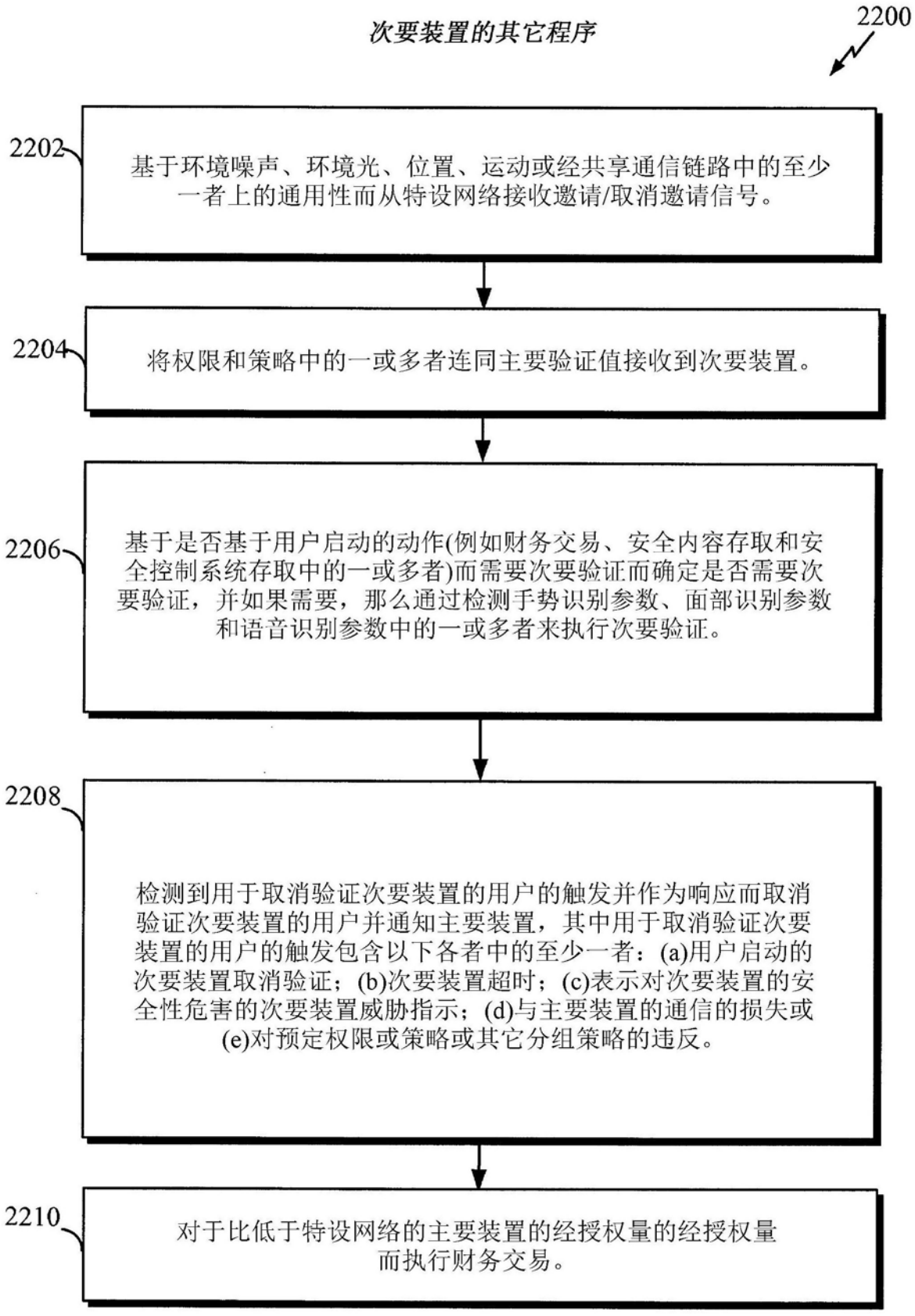

次要装置的其它程序
2200
2202
基于环境噪声、环境光、位置、运动或经共享通信链路中的至少一者上的通用性而从特设网络接收邀请/取消邀请信号。
2204
将权限和策略中的一或多者连同主要验证值接收到次要装置。
2206
基于是否基于用户启动的动作(例如财务交易、安全内容存取和安全控制系统存取中的一或多者)而需要次要验证而确定是否需要次要验证，并如果需要，那么通过检测手势识别参数、面部识别参数和语音识别参数中的一或多者来执行次要验证。
2208
检测到用于取消验证次要装置的用户的触发并作为响应而取消验证次要装置的用户并通知主要装置，其中用于取消验证次要装置的用户的触发包含以下各者中的至少一者：(a)用户启动的次要装置取消验证；(b)次要装置超时；(c)表示对次要装置的安全性危害的次要装置威胁指示；(d)与主要装置的通信的损失或(e)对预定权限或策略或其它分组策略的违反。
2210
对于比低于特设网络的主要装置的经授权量的经授权量而执行财务交易。

图22