(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105144182 A
(43)申请公布日 2015.12.09

(21)申请号 201380075932.6

(22)申请日 2013.04.24

(85)PCT国际申请进入国家阶段日
2015.10.23

(86)PCT国际申请的申请数据
PCT/US2013/038023 2013.04.24

(87)PCT国际申请的公布数据
WO2014/175879 EN 2014.10.30

(71)申请人 惠普发展公司,有限责任合伙企业
地址 美国德克萨斯州

(72)发明人 阿利斯泰尔·科莱斯
阿莱德·爱德华兹
克里斯托弗·牛顿

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 康泉 宋志强

(51)Int.Cl.
G06F 21/30(2006.01)

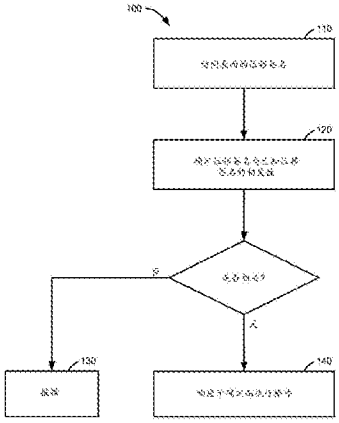
权利要求书2页 说明书10页 附图5页

(54)发明名称

位移签名

(57)摘要

在一个实施方式中,安全管理系统访问关于与表面的物理接触而定义的位移签名,并且确定位移签名与已知位移签名相关。然后,安全管理系统响应于确定位移签名与已知位移签名相关而执行操作。



CN 105144182 A

1. 一种处理器可读介质，包括表示指令的代码，当在处理器上执行时所述指令引起所述处理器：

访问位移签名，所述位移签名是关于与表面的物理接触而定义的；

确定所述位移签名与已知位移签名相关；

响应于确定所述位移签名与所述已知位移签名相关而执行操作。

2. 如权利要求 1 所述的处理器可读介质，其中，所述操作包括建立实体的可信状态，所述处理器可读介质还包括表示当在所述处理器上执行时引起所述处理器执行下述步骤的指令的代码：

监测定义有所述位移签名的装置的移动。

3. 如权利要求 1 所述的处理器可读介质，其中，所述位移签名是使用装置处的加速计定义的，并且所述操作包括建立实体的可信状态，所述处理器可读介质还包括表示当在所述处理器上执行时引起所述处理器执行下述步骤的指令的代码：

使用所述加速计监测所述装置的移动。

4. 如权利要求 1 所述的处理器可读介质，其中，所述操作包括建立实体的可信状态，所述处理器可读介质还包括表示当在所述处理器上执行时引起所述处理器执行下述步骤的指令的代码：

确定定义有所述位移签名的装置已移动超出阈值距离；并且

响应于确定所述装置已移动超出所述阈值距离而取消所述实体的所述可信状态。

5. 如权利要求 1 所述的处理器可读介质，其中，所述操作是特权操作，并且确定所述位移签名与所述已知位移签名相关包括：向位移签名服务提供所述位移签名，所述处理器可读介质还包括表示当在所述处理器上执行时引起所述处理器执行下述步骤的指令的代码：

接收安全凭据以执行所述特权操作。

6. 如权利要求 1 所述的处理器可读介质，其中，所述操作是特权操作，并且确定所述位移签名与所述已知位移签名相关包括：向位移签名服务提供所述位移签名，所述处理器可读介质还包括表示当在所述处理器上执行时引起所述处理器执行下述步骤的指令的代码：

接收安全凭据以执行所述特权操作；

确定定义有所述位移签名的装置已移动超出阈值距离；并且

响应于确定所述装置已移动超出所述阈值距离而取消所述安全凭据。

7. 如权利要求 1 所述的处理器可读介质，其中，所述已知位移签名与包括所述表面的触觉标签相关联。

8. 如权利要求 1 所述的处理器可读介质，还包括表示当在所述处理器上执行时引起所述处理器执行下述步骤的指令的代码：

在装置的加速计处探测所述装置在沿着所述表面的第一方向上的位移，所述第一方向上的位移基本垂直于所述装置在沿着所述表面的第二方向上的移动，所述位移签名是基于所述位移而定义的。

9. 如权利要求 1 所述的处理器可读介质，还包括表示当在所述处理器上执行时引起所述处理器执行下述步骤的指令的代码：

在装置的加速计处探测所述装置在沿着所述表面的第一方向上的位移以生成波形，所述第一方向上的位移基本垂直于所述装置在沿着所述表面的第二方向上的移动，并且

由所述波形获取数值以定义所述位移签名。

10. 一种安全管理系统，包括：

位移模块，针对表面定义位移签名并且监测装置的移动；

相关模块，确定所述位移签名是否与已知位移签名相关；以及

安全模块，与所述相关模块和所述位移模块通信，如果所述位移签名与所述已知位移签名相关，则建立实体的可信状态，并且如果所述位移模块确定所述装置已移动超出阈值距离，则取消所述实体的所述可信状态。

11. 如权利要求 10 所述的系统，其中，

所述位移模块包括加速计，在所述加速计处探测所述装置在沿着所述表面的第一方向上的位移以生成波形，并且由所述波形获取离散数值以定义所述位移模块，所述第一方向上的位移基本垂直于所述装置在沿着所述表面的第二方向上的移动。

12. 如权利要求 10 所述的系统，其中，

所述相关模块经由通信链路与位移签名服务通信，以确定所述位移签名是否与所述已知位移签名相关。

13. 如权利要求 10 所述的系统，其中，

如果所述位移签名与所述已知位移签名相关，则所述相关模块向所述安全模块提供安全凭据；并且

如果所述位移模块确定所述装置已移动超出阈值距离，则所述安全模块取消所述安全凭据。

14. 一种安全管理方法，包括：

在装置的加速计处探测所述装置在沿着表面的第一方向上的位移，所述第一方向上的位移基本垂直于所述装置在沿着所述表面的第二方向上的移动；

基于所述检测定义位移签名；

确定所述位移签名与已知位移签名相关；以及

如果所述位移签名与所述已知位移签名相关，则建立实体的可信状态。

15. 如权利要求 14 所述的安全管理方法，还包括：

在所述探测之后，在所述加速计处监测所述装置的移动；以及

如果所述装置已移动超出阈值距离，则取消所述实体的所述可信状态。

位移签名

背景技术

[0001] 在许多系统中，实体的可信状态的建立取决于该实体持有的凭据或密钥。例如，实体可通过向基于网络的服务或资源提供诸如密码的凭据来建立实体在服务内的可信状态，从而可登入基于网络的服务或资源。实体通常可在登入该服务之后执行特权操作，直至可信状态被取消。当实体要求登出服务时，或者当实体响应于诸如禁用操作或无效操作（或请求操作）的一些情况时，可信状态可被取消。

[0002] 类似地，在一些系统中，实体的可信状态取决于由该实体与另一系统的关系所证实的凭据。例如，只要实体与基于网络的服务或资源经由建立在该服务与另一系统之间的通信链路（例如，企业内部网）而通信，则可在基于网络的服务或资源内建立该实体的可信状态。作为另一示例，只要另一系统向基于网络的服务或资源证实实体在其它系统内具有可信状态，则可在基于网络的服务或资源内建立实体的可信状态。

附图说明

[0003] 图 1 是根据一种实施方式的安全管理过程的流程图；

[0004] 图 2 例示了根据一种实施方式的触觉标签的位移签名的定义；

[0005] 图 3 例示了根据另一种实施方式的触觉标签；

[0006] 图 4 是根据一种实施方式的包括安全管理系统的环境的示意性框图；

[0007] 图 5 是根据另一种实施方式的安全管理过程的流程图；以及

[0008] 图 6 是根据一种实施方式的托管安全管理系统的计算系统的示意性框图。

具体实施方式

[0009] 通常，在实体证实其对一些凭据或一组凭据具有访问权之后，针对服务（或资源）或者在该服务（或资源）内建立该实体的可信状态。如上所讨论的，这样的凭据可以是诸如密码的密钥、记号（token）或者与另一系统的关系（例如，可信的或者安全的通信会话）。作为另一示例，实体可提供关于其身份的带签名的声明（例如，数据集合），并且该声明经验证是来自于或属于可信为可做出此类声明的主体，其中，使用凭据来验证该声明来自该主体。可使用诸如个人密钥或公共 / 个人加密密钥对、对称加密密钥或者一些其它密钥或个人数据的凭据来进行这种验证。

[0010] 作为替换方案，如果实体或与实体相关联的一些装置位于特定地理位置，则可针对服务建立实体的可信状态。例如，通过使用诸如全球定位系统（GPS）的定位系统，装置可确定其位置，并且将该位置提供给服务。如果该位置位于由服务认可或授权的区域内，则可针对服务建立实体的可信状态。在一些实施方式中，这种 GPS 定位器（或接收器）可以是可信的 GPS 定位器，其包括一个或多个安全模块，该安全模块可用于证实或验证由该可信的 GPS 定位器输出的数据是真实可信的（例如，未经篡改的）。

[0011] 在一些应用中，当与实体相关联的装置位于或靠近特定位置时，建立并维持（例如，不取消）该实体的可信状态。在一些这种应用中，当传统的定位系统不可用时（例如，

当无法接收或检测到GPS卫星或其它信标时），要求应仅在与实体相关联的装置位于或靠近特定位置时建立并且维持该实体的可信状态。

[0012] 在此讨论的实施方式基于与实体相关联的装置与一表面的物理接触来确定该装置是否位于或靠近特定位置。作为一个示例，在此讨论的实施方式关于与一表面的物理接触来定义位移签名，并且在确定该位移签名与已知位移签名相关时执行操作。作为一个具体的示例，位移模块可针对具有已知（例如，先前确定的或先前定义的）位移签名的触觉标签（或者触觉标签的表面）定义位移签名。如果由位移模块定义的位移签名与触觉标签的已知位移签名相关（例如，与其匹配或大致匹配），则建立实体的可信状态。

[0013] 而且，在此处讨论的一些实施方式中，在定义位移签名之后，位移模块监测位移模块（或包括位移模块的装置）的移动。如果位移模块确定该位移模块已移动超出阈值距离，则可取消实体的可信状态。由此，可通过与一表面的物理接触来建立实体的可信状态，并且可在位移模块从该表面移动（或被移动）超出阈值距离后取消可信状态。

[0014] 图1是根据一种实施方式的安全管理过程的流程图。可在例如托管在计算系统的安全管理系统处实施过程100。在框110中，访问一表面的位移签名。例如，可在安全管理系统的存储器处访问位移签名。在一些实施方式中，可在位移模块生成位移签名之后在安全管理系统的存储器处访问位移签名，从诸如数据库的数据存储中检索出位移签名，或者从装置接收位移签名。

[0015] 位移签名表示在一表面处的位移或者沿着该表面的位移，并且可具有任意各种表示方式。换言之，位移签名是关于与一表面的物理接触而定义的。换句话说，位移签名表示物体在与表面的物理接触过程中的位移。例如，位移签名可表示：在与物体沿表面移动的方向垂直的一个或多个方向上的物体的位移。

[0016] 与表面（或触觉标签）的物理接触可以是直接的或间接的。直接物理接触意味着装置触碰了表面。例如，如果智能手机的一部分触碰或接触了触觉标签，那么智能手机与触觉标签直接物理接触。间接物理接触意味着装置没有触碰表面，但碰触了直接或间接触碰该表面的其它物体。例如，位移模块可嵌在戒指内并且与安全管理系统的其它组件通信。佩带有戒指的人手可沿着触觉标签的表面移动，而不是使戒指沿着触觉标签的表面移动。相应地，可通过戒指（通过手）与表面的间接物理接触来定义位移签名。作为另一示例，可由人手握持智能电话并且用这只手接触触觉标签，而不是使智能电话触碰智能标签。

[0017] 作为一个具体的示例，图2例示了根据一种实施方式的触觉标签的位移签名的定义。触觉标签是一种使物体在其表面上移位的设备。例如，触觉标签200是一种包括一系列凸起和凹陷的设备。凸起是触觉标签的相对于凹陷突出的部分。凹陷是触觉标签的相对于凸起凹入的部分。通常，触觉标签的这一系列凸起和凹陷限定了足够独一无二的图案，从而唯一地区分该触觉标签与触觉标签组中的其它触觉标签。

[0018] 在一些实施方式中，触觉标签是难以复制或重制的。例如，可围绕触觉标签放置物理屏障或安全装置从而限制访问，和/或，可从包括触觉标签的房间移除窗户。在其它实施方式中，触觉标签可由单一颜色的材料制成，或者可为透明的并且被照射大致均匀的光从而防止对该触觉标签的特征进行拍照。在一些实施方式中，触觉标签可由基本不具反射性或具有低反射性的材料制成，从而防止对触觉标签进行光学或激光扫描。在其它实施方式中，可采取其它措施来使触觉标签的复制或重制复杂化。

[0019] 如上所示，位移签名表示表面处的位移或沿该表面的位移，并且可以具有任意各种表示方式。例如，位移签名可以是诸如波形 220 的波形。如在此更详细讨论的，波形 220 表示在位移模块 211 处检测到的、当装置 210 在方向 291 上移动时、装置 210 在方向 292 和 293 上的位移。波形 220 可在计算系统内的存储器的存储位置处存储为一系列数值。

[0020] 作为另一示例，位移签名可以是数值串、数值序列或数值集合，比如位串 230。如在此更详细讨论的，位串 230 用数值 1 表示正位移（例如，在选定方向上的位移，比如凸起）并且用数值 0 表示负位移（例如，在不同于正位移所选定方向的选定方向上的位移，比如凹陷）。在其它实施方式中，位移签名可以是例如在 -10.0 和 10.0 之间变化的数值的集合，其识别位移的方向（例如，正位移还是负位移）以及位移的程度或大小（例如，位移的相对或绝对测量值或位移率）。

[0021] 位移签名可以由包括位移模块 211 的装置 210 定义。位移模块 211 探测或检测位移（或由位移造成的移动或力）。例如，位移模块 211 可包括加速计、陀螺仪或其它用于检测位移的机构。作为一个具体的示例，位移模块 211 可包括 MEMS（微机电系统）加速计 211。装置 210 可以是包括位移模块 211 的任意装置。例如，装置 210 可以是计算系统，比如笔记本电脑、平板装置、智能手机或其它包括位移模块的计算系统。作为另一示例，装置 210 可以是媒体播放器、录音针、激光指示棒或包括位移模块的笔。在一些实施方式中，装置 210 通过有线连接（例如，USB（通用串行总线）连接）或无线连接（例如，蓝牙®连接）与计算系统通信，从而将来自位移模块 211 的数值提供给计算系统。

[0022] 在图 2 所示的示例中，当装置 210 沿着表面 201 移动（例如，当人沿表面 201 横跨触觉标签 200 拖动或移动装置 210）时，位移模块 211（在本示例中为加速计）探测或检测位移并且输出或记录表示该位移的数值，从而生成波形 220。换言之，当装置 210 在方向 291 上沿表面 201 移动（或被移动）时，装置 210 因触觉标签 200 的凸起和凹陷而经历在方向 292 和 293 上的位移。触觉标签 200 是触觉标签的一个示例。在其它实施方式中，触觉标签可以更为复杂。例如，在其它实施方式中，触觉标签可包括具有多种高度的凸起和 / 或具有多种深度的凹陷和 / 或除图 2 所示之外的凸起和 / 或凹陷。

[0023] 该位移在位移模块 211 处被检测为是具有加速度的变化，并且记录为波形 220。波形 220 可通过由诸如（或包括）加速计的位移模块输出的数值定义。在一些实施方式中，由位移模块输出的数值被过滤，并且波形 220 由过滤后的数值定义。例如，可以使用由加速计输出的数值的滑动平均值来定义波形 220，从而平滑波形 220。参照图 2 中的曲线 280，当装置 210 在方向 292 或 293 上不移动时，位移模块 211 检测到近似为 -1g 的加速度（其中，“g”代表因地球重量而产生的加速度）。然而，当装置 210 朝着凸起的顶部升起或者从凹陷升起（即，在方向 292 上移动）时，位移模块 211 检测到在方向 293 上的加速度的增加（或曲线 280 中负加速度的增加），然后检测到在方向 292 上的加速度的增加（或曲线 280 中正加速度的增加），直至结束升起动作。换句话说，方向 292 上的位移的特征在于：在方向 293 上的加速度的短暂上升之后，紧接着的是在方向 292 上的加速度的短暂上升。

[0024] 类似地，当装置 210 从凸起降下或者朝着凹陷的底部降下（即，在方向 293 上移动）时，位移模块 211 检测到曲线 280 中正加速度的增加，然后检测到曲线 280 中负加速度的增加，直至结束降下动作。换言之，方向 293 上位移的特征在于：在方向 292 上的加速度的短暂上升之后，紧接着的是在方向 293 上的加速度的短暂上升。即，加速度上的加速度上

升对指示位移。在本示例中，负加速度的上升之后紧随着正加速度的上升，这指示向上（在方向 292 上）的位移，而正加速度的上升之后紧随着负加速度的上升，这指示向下（在方向 293 上）的位移。

[0025] 由于在位移模块 211 处探测的加速度与装置 210 的位移相关，可对波形 220 进行分析以识别触觉标签 200（或触觉标签 200 的表面 201）的位移签名。如图 2 所示，可从波形 220 提取或确定位串 230 作为位移签名。例如，波形 220 的跟随在负加速度的增加之后的部分可分配数值“1”，其代表凸起；而波形 220 的跟随在正加速度的增加之后的部分可分配数值“0”，其代表凹陷。

[0026] 在一些实施方式中，可通过以周期性的间隙采样波形 220 来对波形 220 进行分析，如图 2 所示。在一些实施方式中，在分析过程中，可对波形 220 进行拉伸和 / 或挤压来校正装置 210 在方向 291 上沿表面 201 移动的速率的变化。例如，应用于条形码扫描的拉伸技术可用于校正装置 210 在方向 291 上沿表面 201 移动的速率（比如，速度）的变化。作为又一示例，在一些实施方式中，除方向 292 和 293 之外，位移模块 211 可探测或检测方向 291 上的位移。方向 291 上的位移信息可用于确定应在波形 220 上在哪些点或什么时候采样方向 292 和 293 上的位移。换言之，方向 291 上的位移信息可用于确定应在波形 220 的哪些部分上采样以针对触觉标签 200 的表面 201 定义位移签名。

[0027] 在一些实施方式中，可将条形码或其它标记加入到触觉标签内。可将这种标记印刷到触觉标签上、雕刻到触觉标签内或与触觉标签模制在一起。在一些实施方式中，这种标记可用于确定或校准装置 210 沿表面 201 移动的速率。例如，装置 210 可包括成像模块（未示出），比如照相机、条形码扫描器或其它成像模块，以识别这种标记并确定装置 210 沿表面 201 移动的速率。作为一个具体示例，这种标记可以彼此均匀地间隔开或者以预定或限定距离彼此间隔开，并且当装置 210 在各标记之间移动时，成像模块可基于经过时间 (elapsed time) 获得移动的速度。

[0028] 而且，在一些实施方式中，触觉标签处的这种标记可包括或表示信息或数据。作为一个具体示例，这种标记可以是由成像模块读取的快速响应 (QR) 码。这种标记可增加存储在触觉标签处的信息内容。在一些实施方式中，这种由触觉标签处的标记表示的信息或数据可以被加密。触觉标签的（或由触觉标签确定的）位移签名可以是加密密钥或者可以用于访问加密密钥以解密存储在这种标记处或由这种标记表示的加密信息。

[0029] 作为生成位移签名的另一示例，图 3 例示了根据另一种实施方式的触觉标签。触觉标签 300 包括表面 301 和致动器 350。致动器 350 是比如螺线管、扬声器、电机（例如，带有平衡轴的电机）、压电装置或其它当被致动时引起表面 301 处位移的装置的装置。致动器 350 因此可被致动以引起装置 210 的位移。在一些实施方式中，位移较小（例如，毫米或微米量级），但仍可在位移模块 211 处被探测到。

[0030] 如上所讨论的，装置 210 包括探测或检测位移的位移模块 211。相应地，装置 210 可通过检测由致动器 350 产生的、表面 301 处的位移图案来针对触觉标签 300 定义位移签名。作为具体的示例，致动器 350 可以是带有平衡轴的电机，并且触觉标签 300 可包括与致动器 350 通信的处理器（未示出）。处理器引起致动器 350 根据图案旋转平衡轴，这在表面 301 处诱发根据该图案的位移。然后，在位移模块 211 处检测到该位移，以针对触觉标签 300 定义位移签名，该签名与该图案一致。换言之，处理器促使致动器 350 致动所依据的图案（或

者，由致动器的该图案引起的位移）可被探测到或检测到，并作为用于触觉标签 300（或触觉标签 300 的表面 301）的位移签名或者作为触觉标签 300（或触觉标签 300 的表面 301）的位移签名。

[0031] 再次参照图 1，在框 110 中定义位移签名之后，在框 120 处确定该位移签名与已知位移签名的相关性。例如，安全管理系统可包括已知位移签名（即，触觉标签的已知位移签名）的资料库或数据库，并且可将在框 110 中定义的位移签名与那些已知位移签名进行比较，以确定该位移签名是否与已知位移签名相关。在一些实施方式中，安全管理系统可接收与位移签名有关的已知位移签名的标识符，并且确定该位移签名是否与该已知位移签名相关。

[0032] 如果位移签名符合或超出与已知位移签名的相似性阈值，则可认为位移签名与已知位移签名相关。换言之，如果位移签名满足与已知位移签名的相似性阈值，则可认为位移签名与已知位移签名相关。即，如果位移签名与已知位移签名的一部分或多个部分的相似性达到预定百分比，则可认为位移签名与已知位移签名相关。作为具体示例，如果位移签名（或其相关部分）与已知位移签名（或其相关部分）的相似性大于或等于 95％，则可认为位移签名与已知位移签名相关。

[0033] 在一些实施方式中，安全管理系统可将在框 110 中生成的位移签名提供给位移签名服务，以确定位移签名是否与已知位移签名相关。例如，位移签名服务可以是一资源，该资源包括或访问已知位移签名的资料库或数据库，并且可将从安全管理系统实施过程 100 接收到的位移签名与那些已知位移签名进行比较，以确定该位移签名是否与已知位移签名相关。

[0034] 然后，位移签名服务可向安全管理系统实施过程 100 提供信息以指示位移签名是否与已知位移签名相关。例如，位移签名服务可提供一指示，其表明：位移签名与已知位移签名相关，或者，位移签名与已知位移签名不相关。在其它实施方式中，位移签名服务可提供额外的信息，比如与位移签名相关的已知位移签名的标识符；与位移签名相关的已知位移签名的关联凭据或授权；与位移签名相关的已知位移签名的关联说明或操作；与已知位移签名相关联的阈值距离，和 / 或其它信息。作为替换方案，这种信息可在安全管理系统实施过程 100 处（例如，在数据库内）获得并且与已知位移签名相关联。

[0035] 如果位移签名与已知位移签名不相关，则可在框 130 报错。在一些实施方式中，报错可提示：在框 110 中定义另一位移签名，然后可重复过程 100。如果位移签名与已知位移签名相关，则可在框 140 中响应于位移签名与已知位移签名相关的确定而执行操作。例如，如果位移签名与已知位移签名相关，则安全管理系统实施过程 100 可执行一个或多个特权操作。

[0036] 作为另一示例，在框 140 中，可响应于位移签名与已知位移签名相关的确定而建立实体的可信状态。实体是服务或资源的客户端、诸如用户代理的软件应用、用户账号或可处于可信状态（或任意各种可信状态）或非可信状态的网络应用的环境。可信状态是这样一种状态，其中实体被授权以执行诸如特权操作的操作，当实体不处于可信状态时，这些操作是不被允许的。例如，这种特权操作可包括访问（例如，读取、写入或修改）诸如机密信息或受限信息的数据、经由通信链路与其它实体通信、与其它实体通信或关联、访问企业的内联网或内网、执行指令或应用，和 / 或其它特权操作。在一些实施方式中，实体使用诸如

密码或数字证书的凭据来向资源或服务证实实体处于可信状态。

[0037] 响应于确定位移签名与已知位移签名相关，安全管理系统实施过程 100 可通过修改实体的一个或多个状态变量、通过向实体提供凭据（直接地或经由定义有位移签名的装置）或者通过另外指示实体处于可信状态来建立实体的可信状态。例如，在框 110 中生成了位移签名的触觉标签可以位于物理上安全的位置。由于在框 110 中生成的位移签名与该触觉标签的已知位移签名匹配，可确定安全管理系统物理地位于靠近触觉标签处并且是可信或安全的。相应地，安全管理系统可建立诸如托管在安全管理系统（或与安全管理系统共同托管）的实体这样的实体的可信状态。

[0038] 图 1 所示的过程 100 是安全管理过程的一个示例。其它安全管理过程可包括不同的和 / 或额外的框或步骤。例如，在一些实施方式中，安全管理过程包括接收与在框 110 中定义的位移签名相关的已知位移签名相关联的凭据。

[0039] 图 4 是根据一种实施方式的包括安全管理系统的环境的示意性框图。安全管理系统 410 包括位移模块 411、相关模块 412 和安全模块 413。尽管关于图 4 和其它示例性实施方式示出并讨论了诸如引擎的具体模块（即，硬件和软件的组合），但在其它实施方式中可包括各模块的其它组合或子组合。换句话说，尽管在图 4 中例示并且在其它示例性实施方式中讨论的各模块执行在此讨论的示例中的具体功能，但这些和其它功能可在不同的模块或模块的组合中完成、实施或实现。例如，所例示和 / 或讨论的、分离的两个或更多模块可组合为一个模块，该模块可执行关于两个模块讨论的功能。作为另一示例，关于这些示例讨论的、在一个模块处执行的功能可在不同的一个或多个模块处执行。而且，在一些实施方式中，关于一个示例实施方式讨论的一些模块在其它实施方式中可被排除。

[0040] 位移模块 411 是确定（或探测或检测）位移以定义位移签名的硬件和软件的组合。例如，位移模块 411 可包括加速计或陀螺仪以及可执行指令，这些可执行指令被存储在存储器中并且可在处理器中执行以解读和 / 或分析加速计或陀螺仪处输出的数值。

[0041] 在一些实施方式中，位移模块 411 还确定移动的距离。例如，通过使用航位推算法，包括加速计的位移模块 411 的实施方式可确定位移模块 411 的移动量。作为一个具体示例，在一些实施方式中，位移模块 411 对在位移模块 411 处探测或检测到的加速度数值求积分，以确定安全管理系统 410 是已移动超出阈值距离还是尚未达到阈值距离（例如，与定义有触觉标签的位移签名的位置之间的阈值距离）。

[0042] 在一些实施方式中，位移模块 411 可物理地与安全管理系统 410 分离、但逻辑地位于安全管理系统 410 内。例如，位移模块 411 可以是探针或与诸如托管相关模块 412 和安全模块 413 的计算系统这样的装置（例如，经由诸如无线通信链路的通信链路）通信的其它装置，或者可在该探针或其它装置处实施。即，位移模块 411 可将位移签名传送给相关模块 412 和 / 或安全模块 413。在其它实施方式中，位移模块 411、相关模块 412 和安全模块 413 可托管在或实施在单个装置。

[0043] 关联模块 412 是确定位移签名是否与已知位移签名相关的硬件和软件的组合。例如，相关模块 412 可将位移签名提供给位移签名服务 420 以确定位移签名是否与已知位移签名相关。作为另一示例，相关模块 412 可访问安全管理系统 410 处的已知位移签名的资料库或数据库（未示出），并且将位移签名与那些已知位移签名进行比较，以确定位移签名是否与已知位移签名相关。

[0044] 安全模块 413 与相关模块 412 通信，从而当位移签名与已知位移签名相关时建立实体的可信状态。作为一个具体示例，安全模块 413 可通过修改实体的一个或多个状态变量、通过提供凭据给实体或者通过另外指示实体处于可信状态来建立实体的可信状态。此外，在一些实施方式中，安全模块 413 与位移模块 411 通信，从而当位移模块 411 确定其已移动超出阈值距离时取消实体的可信状态。在此例如结合图 1、2、3 和 5 讨论了关于位移模块 411、相关模块 412 和安全模块 413 的功能的额外的细节。换句话说，位移模块 411、相关模块 412 和安全模块 413 可执行在此描述的其它示例中讨论过的那些功能。

[0045] 在图 4 例示的示例中，安全管理系统 410 使用位移签名来建立实体的可信状态以访问资源 430。位移模块 411（或包括位移模块 411 的装置，或其一部分）基于与一表面的物理接触来生成该表面的位移签名，例如，如结合图 2 和 3 所讨论的。通过相关模块 412 经由通信链路 490 向位移签名服务 420 提供位移签名的表示形式，如通信 451 所示。

[0046] 通信链路 490 包括定义安全管理系统 410 与位移签名服务 420、资源 430 和 / 或其它装置或服务之间的通信路径的装置、服务或其组合。例如，通信链路 490 可包括缆线（例如，双绞电缆、同轴电缆或光缆）、无线链路（例如，射频链路、指示链路、光链路或声链路）或其它任何传输信号或支持信号传输的连接器或系统中的一个或多个。而且，通信链路 490 可包括通信网络，比如交换结构 (switch fabric)、内部网、因特网、电信网络或其组合。此外，通信链路 490 可包括代理器、路由器、交换机、网关、桥接器、负载平衡器以及类似的通信装置。而且，图 4 中例示并且在此讨论的各连接器或通信路径可以是逻辑的或物理的。

[0047] 位移签名服务 420 将位移签名与已知位移签名进行比较，以确定位移签名是否与已知位移签名相关。例如，位移签名服务 420 可包括或访问与触觉标签相关联的已知位移签名的资料库或数据库。此外，位移签名服务 420 可访问诸如与已知位移签名相关联的凭据（例如，许可、密码或数字证书）的信息，当从安全管理系统 410 接收到与那些已知位移签名相关的位移签名时，将该凭据提供给安全管理系统 410。

[0048] 在本示例中，位移签名服务 420 确定由相关模块 412 提供的该位移签名与已知位移签名相关，并且将与该已知位移签名相关联的凭据提供给相关模块 412，如由通信 452 所示。安全模块 413 从相关模块 412 接收凭据，并且建立托管在安全管理系统 410 的实体（未示出）的可信状态。

[0049] 例如，安全模块 413 可向诸如用户代理（例如，软件应用）的配置以访问资源 430 处受限数据的实体提供凭据。然后，实体向资源 430 发送针对受限数据的、包括凭据的请求，如由通信 461 所示。资源 430 验证凭据，并且提供受限数据，如由通信 462 所示。由此，作为由位移模块 411 定义的位移签名的结果，实体得以访问受限数据。

[0050] 图 5 是根据另一实施方式的安全管理过程的流程图。尽管关于图 5 讨论了具体实施方式，但图 5 所例示的并且在此讨论的过程可应用于其它实施方式。在本示例中，过程 500 在包括加速计的智能手机处实施。换言之，智能手机是包括作为位移模块的加速计的安全管理系统。智能手机的用户进入包括触觉标签的房间。例如，房间里的桌子可包括具有已知位移签名的触觉标签。

[0051] 在框 510 中，当用户使智能手机横跨触觉标签的表面而移动时，智能手机（或托管在智能手机的应用）通过采样加速计的输出来针对触觉标签的表面定义位移签名。然后，在框 520 中，智能手机确定位移签名与触觉标签的已知位移签名相关。在本示例中，智能手

机与位移签名服务通信，以确定位移签名是否与触觉标签的已知位移签名相关。更具体地，智能手机向位移签名服务提供位移签名的表示方式，并且位移签名服务向智能手机提供表明位移签名与已知位移签名相关的指示。在其它实施方式中，例如如上讨论的，智能手机可包括已知位移签名的资料库或数据库，并且可将在框 510 中定义的位移签名与那些已知位移签名进行比较，以确定位移签名是否与已知位移签名相关。

[0052] 在确定位移签名与触觉标签的已知位移签名相关之后，在框 530 中，智能手机建立托管在智能手机（或与其通信）的实体的可信状态。在图 5 例示的示例中，在框 531 中，智能手机响应于由位移签名服务做出的位移签名与触觉标签的已知位移签名相关的确定、从位移签名服务接收凭据（或安全凭据）。然后，在框 532 中，凭据被提供给实体，以建立实体的可信状态。

[0053] 在一些实施方式中，可直接将凭据提供给实体。例如，实体可托管在与智能手机分离的计算系统，并且可基于智能手机和实体之间的关系将凭据提供给实体。作为具体示例，智能手机可向位移签名服务或一些其它服务指示：位移签名是代表实体而提供的。作为此类指示的示例，智能手机可向具有位移签名的位移签名服务提供实体的标识符或与实体相关联的记号。然后，位移签名服务可使用标识符或记号来向指定的实体提供凭据。作为另一示例，智能手机可在与实体相关联的通信会话（或会话）内向位移签名服务提供位移签名。

[0054] 然后，在框 540 中，实体基于可信状态执行特权操作。例如，特权操作可包括访问受限数据或者与受限服务或受限资源通信。在实体执行特权操作的同时，智能手机（或其位移模块）监测移动以确定其是否移动超出阈值距离。例如，智能手机可对加速计输出的数值求积分和 / 或对那些数值应用航位推算法，以确定智能手机是否已从定义有位移签名的位置处移动超出阈值距离。阈值距离可以是例如与已知位移签名相关联的并且针对于触觉标签的距离。例如，阈值距离可以小于从触觉标签到房间的门的距离。由此，如果将智能手机从房间中拿走，则将超出阈值距离。

[0055] 作为另一示例，智能手机（或另一装置）离开触觉标签的移动可受限于任意三维 (3D) 空间（由一组坐标定义）。例如，3D 空间可以是从触觉标签（例如，其前方）向特定方向投射的圆锥形空间。在这种实施方式中，方向特性可参照触觉标签的凸起和 / 或凹陷。例如，通过使用陀螺仪和加速计，位移模块可识别智能手机（或其它装置）横跨或沿着触觉标签的移动方向以及在生成位移签名之后智能手机的移动方向。换言之，可在陀螺仪的辅助下追踪智能手机在 3D 空间内的移动，以提供与智能手机的方位相关的信息，其中沿着触觉标签的移动方向被定义为初始或参考方向。

[0056] 当智能手机还未移动超出阈值距离时，维持所建立的可信状态。然而，如果智能手机移动超出阈值距离，则在框 550 中取消可信状态。例如，智能手机可删除凭据以防止实体进一步使用凭据。作为另一示例，智能手机（例如，托管在智能手机的安全模块）可通过向实体提供取消通知或可通过修改实体的状态变量以引起实体的可信状态被取消来取消可信状态。在一些实施方式中，智能手机可通知资源或安全验证服务（资源和 / 或服务通过其验证可信状态或凭据）：应取消可信状态。换言之，在智能手机从触觉标签移动超出阈值距离之后，取消实体的可信状态。作为一个具体示例，当智能手机离开房间之后，实体无法执行特权操作。

[0057] 在一些实施方式中，如果智能手机（或其它装置）停止与和实体相关联的服务或计算系统通信，也可取消可信状态。例如，如果智能手机在指定期限（例如，周期性的指定期限）之前无法向计算系统的此类服务提供信号，则可取消可信状态。此外，如果智能手机停止与实体相关联，则也可取消可信状态。例如，如果与实体相关联的通信会话被切断或过期，或者如果智能手机的用户使与实体相关联的用户代理登出服务，则可取消实体的可信状态。

[0058] 图5所示的过程500是一种示例安全管理过程。其它安全管理过程可包括不同的和/或额外的框或步骤，和/或，可与不同装置一起实施。例如，过程500可在包括或联接至位移模块的计算系统处而不是智能手机处实施。在一些实施方式中，位移模块可以物理地联接至计算系统以限制（物理地或者逻辑地）位移模块与计算系统的分离。作为一个具体示例，如果位移模块移动超出阈值距离或与计算系统分离，则可取消可信状态。

[0059] 图6是根据一种实施方式的托管安全管理系统的计算系统的示意性框图。在图6所示的示例中，计算系统600包括处理器610、通信接口620和存储器630。计算系统600可以为，例如，诸如台式电脑和笔记本电脑的个人电脑、平板装置、智能手机或一些其它计算系统。在一些实施方式中，托管安全管理系统的计算系统本身被称为安全管理系统。

[0060] 处理器610是执行或解读指令、代码或信号的硬件和软件的组合。例如，处理器610可以是微处理器、专用集成电路(ASIC)、诸如通用图形处理单元(GPGPU)的图形处理单元(GPU)、诸如处理器或计算系统的集群或网络的分布式处理器、多核或多处理器处理器、或者虚拟机的虚拟或逻辑处理器。

[0061] 通信接口620是一种模块，处理器610可通过通信接口经由通信链路与其它处理器或计算系统通信。作为一个具体示例，通信接口620可包括网络接口卡和托管在处理器610的通信协议栈（例如，存储在存储器630处的指令或代码，其可在处理器610处执行或解读以实施网络协议）以接收和发送数据。作为具体示例，通信接口620可以是有线接口、无线接口、以太网接口、IEEE 802.11接口或其它可供处理器610交换表示与其它处理器或计算系统通信的数据的信号或符号的通信接口。

[0062] 存储器630是存储指令、代码、数据或其它信息的处理器可读介质。如在此使用的，处理器可读介质是非临时地存储指令、代码、数据或其它信息的任意介质，并且可由处理器直接或间接访问。换句话说，处理器可读介质是一种非临时性介质，处理器可在该非临时性介质处访问指令、代码、数据或其它信息。例如，存储器630可以是易失性随机存取存储器(RAM)、诸如硬盘驱动或固态驱动的永久性数据存储、光盘(CD)、数字化通用磁盘(DVD)、安全数码™(Secure Digital™,SD)卡、多媒体卡(MMC)、压缩闪存™(CompactFlash™,CF)卡或者其或其它存储器的组合。换言之，存储器630可表示多处理器可读介质。在一些实施方式中，存储器630可与处理器610集成、与处理器610分离或在计算系统600外部。

[0063] 存储器630包括指令或代码，当在处理器610上执行时，该指令或代码实施操作系统631和安全管理系统，安全管理系统包括位移模块634的组件634B、相关模块635和安全模块636。换言之，包括位移模块634B、相关模块635和安全模块636的安全管理系统被托管在计算系统600。

[0064] 如图6所示，位移模块可包括多组件或组件。特别是在图6所示的示例中，位移模块634包括组件634B和组件634A。组件634A可以是，例如，诸如加速计、陀螺仪或其它探

测或检测位移和 / 或移动的装置这样的装置。组件 634B 可以是例如指令，当在处理器 610 上执行时，该指令访问、解读和 / 或分析由组件 634A 输出的数值。

[0065] 在一些实施方式中，位移模块 634 的组件 634A 可在计算系统 600 的外部。例如，位移模块 634 的组件 634A 可经由 USB 接口（未示出）联接至计算系统 600。

[0066] 虽然已示出并在上文中描述了一些实施方式，但可对其形式和细节做出各种修改。例如，已关于一种实施方式和 / 或过程描述过的一些特征可与其它实施方式相关。换言之，关于一种实施方式描述的过程、特征、组件和 / 或特性可用于其它实施方式。又例如，上面关于特定模块或元件讨论的功能可包含在其它实施方式中的不同模块、引擎或元件中。此外，应理解的是，在此描述的系统、设备和方法可包括在此描述的不同实施方式中的组件和 / 或特征的各种不同组合和 / 或子组合。由此，参照一种或多种实施方式描述的特征可与在此描述的其它实施方式相结合。

[0067] 如在此使用的，术语“模块”指的是硬件（例如，诸如集成电路或其它线路的处理器）和软件（例如，机器或处理器可执行的指令、命令或代码，比如固件、程序或目标代码）的结合。硬件和软件的结合可仅包括硬件（即，不带有软件元件的硬件元件），可包括托管在硬件的软件（例如，存储在存储器中并且可在处理器上执行或解读的软件，或者存储或编码于非临时性的处理器可读存储器中的软件）或者托管在硬件的硬件和软件。

[0068] 此外如在此使用的，单数形式的“一”和“该”包括复数形式，除非上下文另外明确指示。由此，例如，术语“模块”意指一个或多个模块或模块的组合。而且，在此使用的术语“提供”包括推送机制（例如，经由通信路径或通道向计算系统或代理发送数据）、拉取机制（例如，响应于来自计算系统或代理的请求而向计算系统或代理递送数据）和存储机制（例如，在数据存储处或者在供计算系统或代理访问数据的服务处存储数据）。此外，如在此使用的，术语“基于”意指“至少部分在其基础上”。由此，描述为基于一些原因的特征可仅基于该原因，或者基于该原因并且还基于一个或多个其它原因。

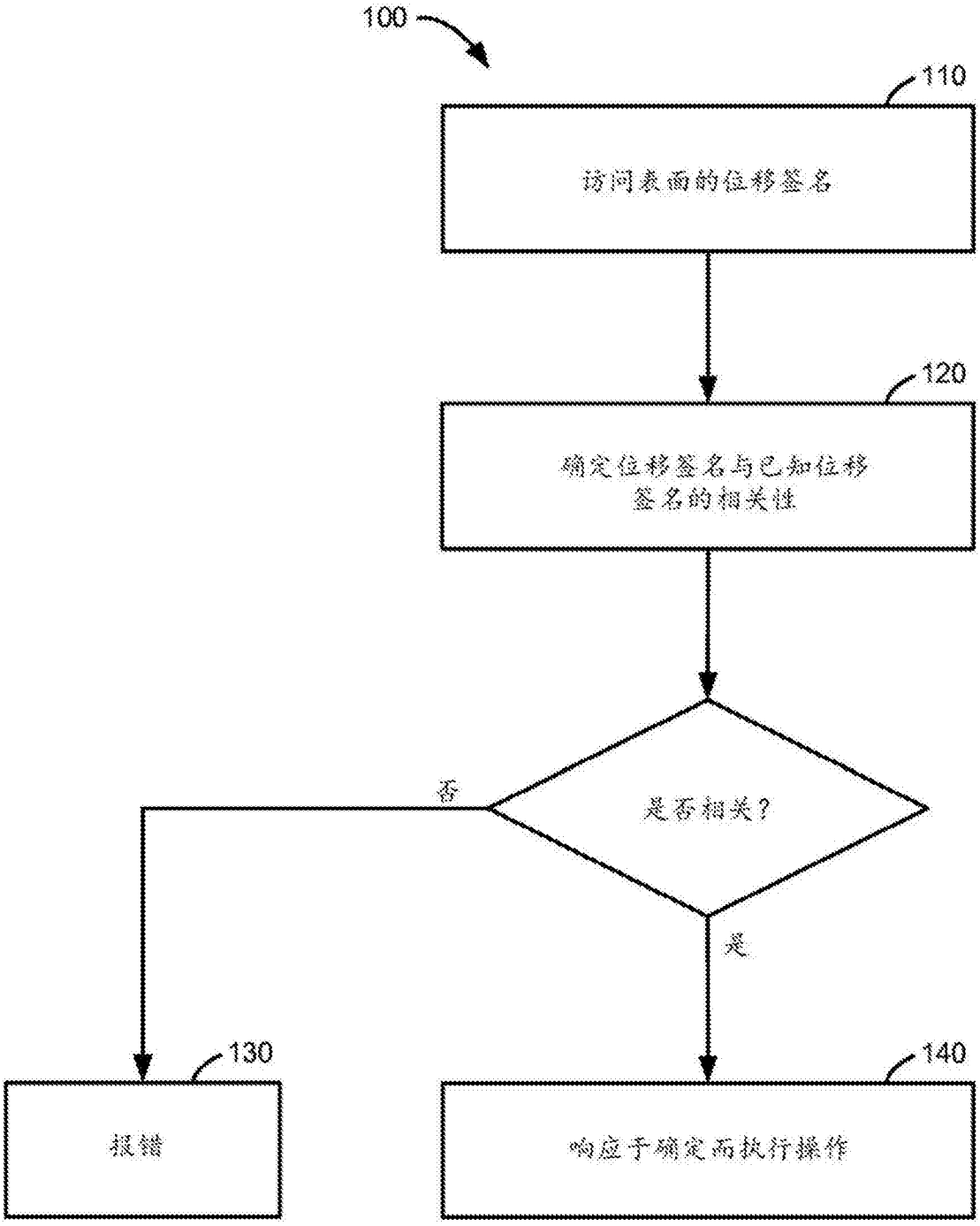

100
110
访问表面的位移签名
120
确定位移签名与已知位移签名的相关性
是否相关？
否
是
130
报错
140
响应于确定而执行操作

图 1

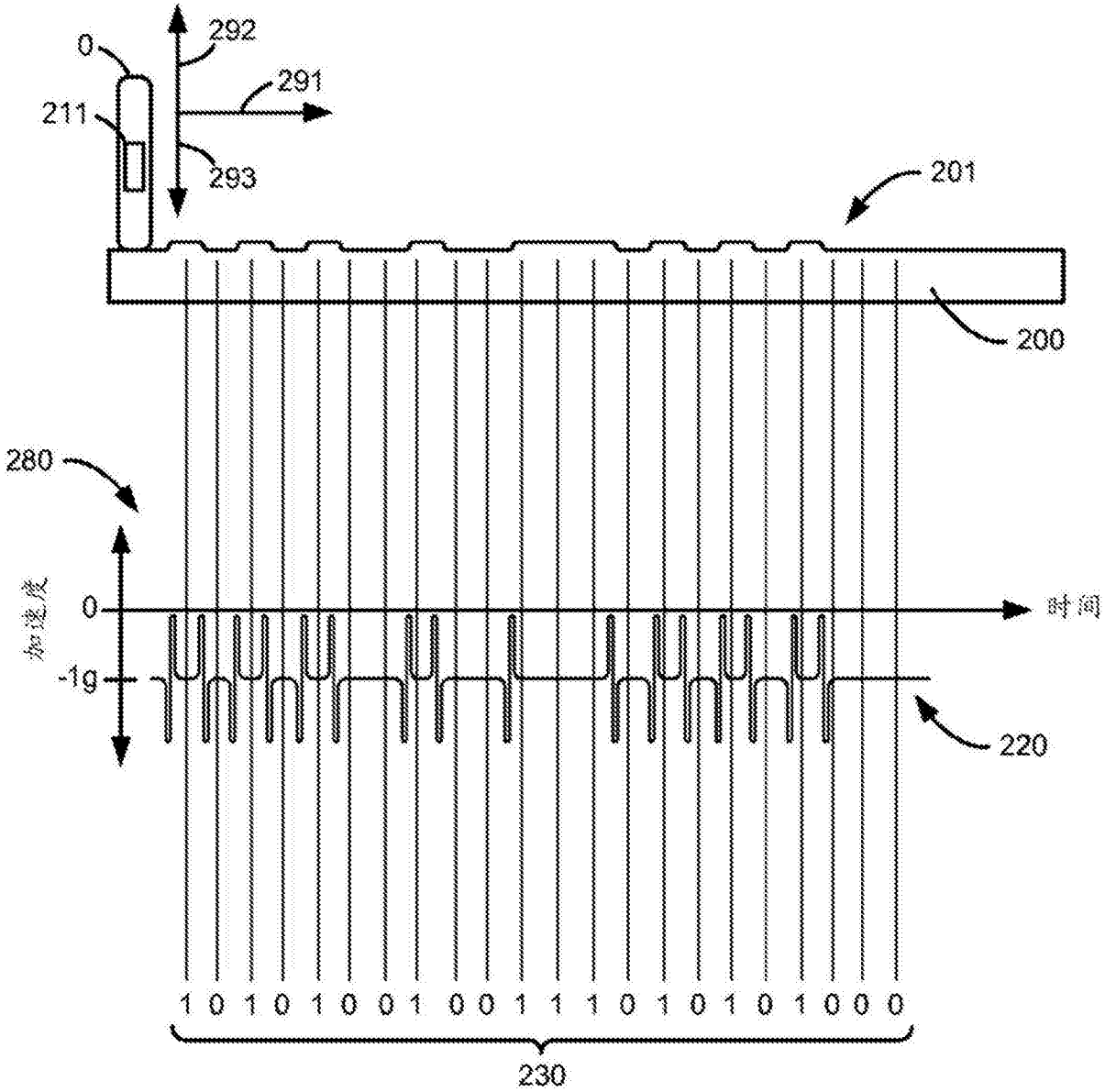

0
292
291
211
293
201
200
280
加速度
0
-1g
时间
220
1 0 1 0 1 0 0 1 0 0 1 1 1 0 1 0 1 0 1 0 0 0
230

图 2

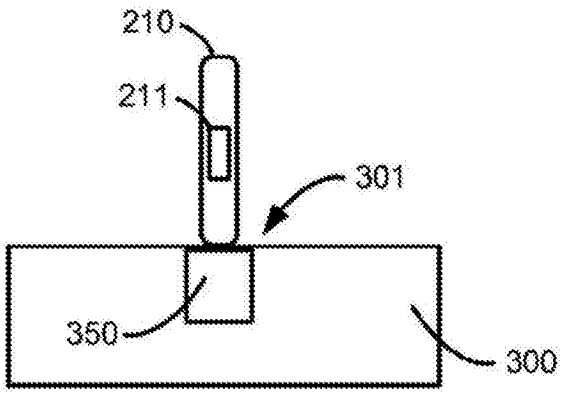

210
211
301
350
300

图 3

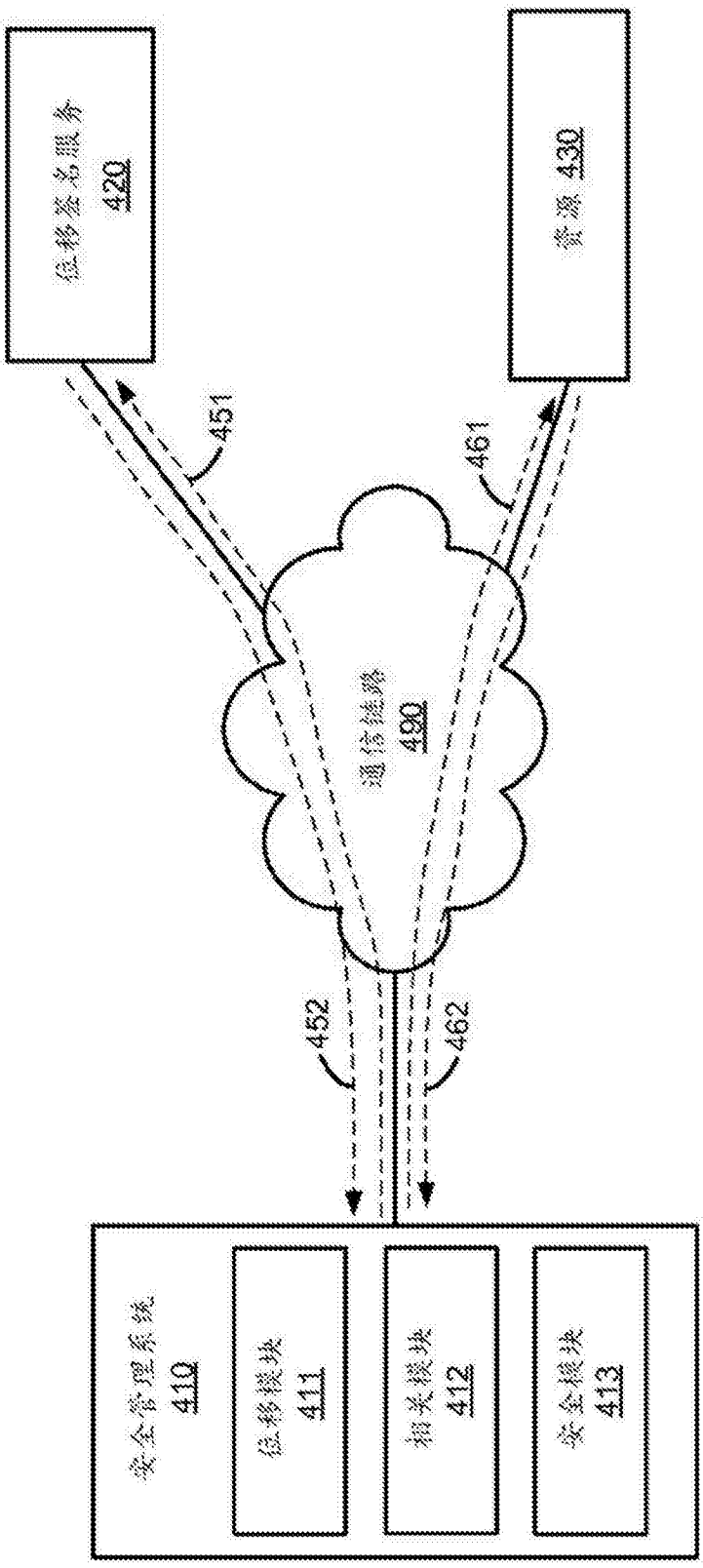

位移签名服务
420
资源 430
451
461
通信链路
490
452
462
安全管理系统
410
位移模块
411
相关模块
412
安全模块
413

图 4

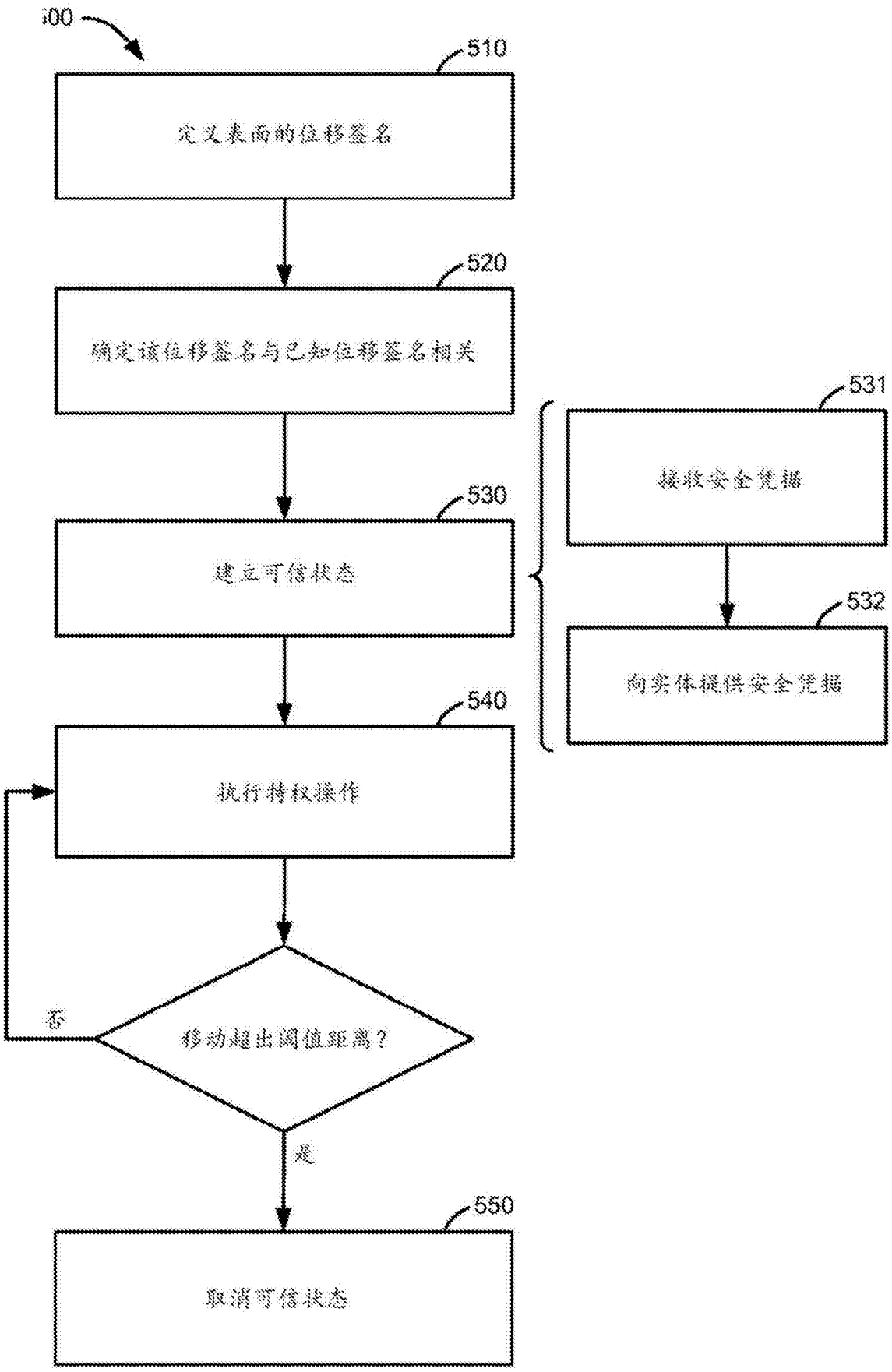

500
510
定义表面的位移签名
520
确定该位移签名与已知位移签名相关
530
建立可信状态
531
接收安全凭据
532
向实体提供安全凭据
540
执行特权操作
否
移动超出阈值距离？
是
550
取消可信状态

图 5

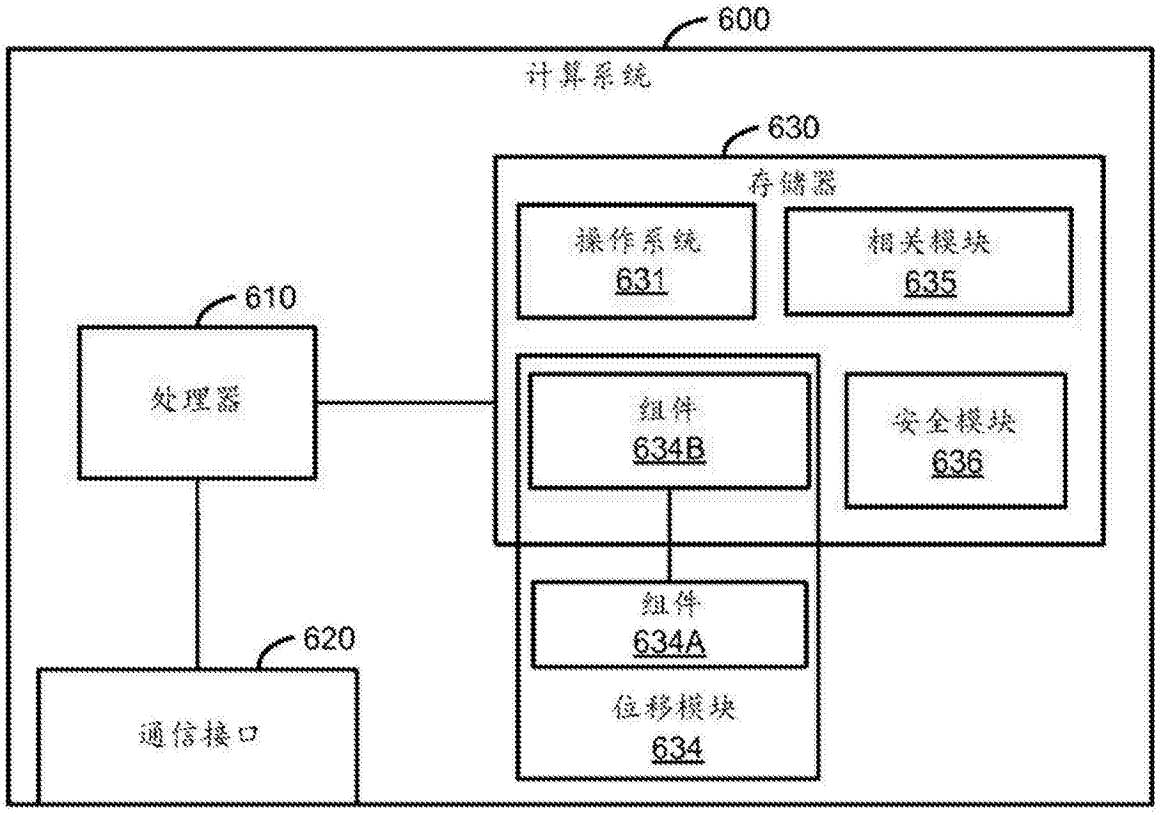

600
计算系统
630
存储器
操作系统
631
相关模块
635
610
处理器
组件
634B
安全模块
636
组件
634A
620
通信接口
位移模块
634

图 6