(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112368713 B
(45)授权公告日 2024.10.29

(21)申请号 201980042139.3
(22)申请日 2019.06.28
(65)同一申请的已公布的文献号
申请公布号 CN 112368713 A
(43)申请公布日 2021.02.12
(30)优先权数据
1810658.3 2018.06.28 GB
(85)PCT国际申请进入国家阶段日
2020.12.22
(86)PCT国际申请的申请数据
PCT/EP2019/067473 2019.06.28
(87)PCT国际申请的公布数据
WO2020/002678 EN 2020.01.02
(73)专利权人 维普公司
地址 挪威奥斯陆
(72)发明人 基姆·克里斯蒂安·亨伯斯塔
克里斯蒂安·特伦讷雷德
(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 张润
(51)Int.Cl.
*G06K 19/07*(2006.01)
*G06K 19/077*(2006.01)
*G06F 21/32*(2006.01)
*G06Q 20/34*(2006.01)
(56)对比文件
CN 101019138 A,2007.08.15
CN 107924517 A,2018.04.17
审查员 石海霞

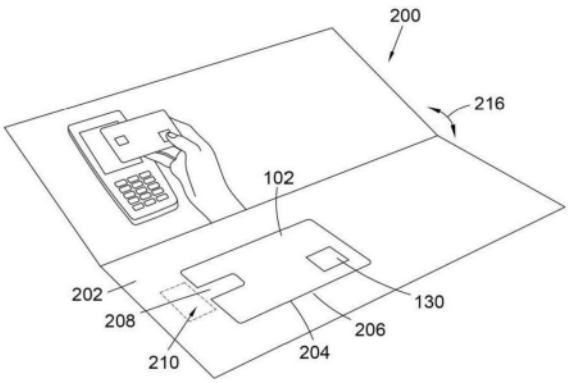
权利要求书3页 说明书14页 附图4页

(54)发明名称

# 生物特征注册

(57)摘要

本发明揭露一种用于生物特征验证装置(102)的生物特征注册的方法,该生物特征验证装置包括:生物特征传感器(130),用于识别授权的用户;及处理器,其能够基于经由该生物特征传感器(130)对用户身份的验证以允许访问该生物特征验证装置(102)的一个或多个安全特征。该注册方法包括将该生物特征验证装置(102)安装到固持件(202),以形成注册系统(200),其中该注册系统(200)配置成藉由邮件传递服务交付给终端用户。该固持件(202)具有能够供电给该生物特征验证装置(102)的电源(210),其中该固持件(202)配置成使得在交付该注册系统期间,停止从该电源(210)到该生物特征验证装置(102)的电力供应,而且该固持件(202)包括开关配置,该开关配置构造成响应在交付该注册系统之后用户操作该固持件而启动从该电源到该生物特征验证装置的电力供应。该注册系统(200)交付给用户,而且响应用户操作该固持件而启动电力供应。在注册处理期间,使用来自该电源(210)的电力给该生物特征验证装置(102)供电,以启用该生物特征验证装置(102)的注册模式。




CN 112368713 B

1.一种用于生物特征验证装置的生物特征注册的方法,其中所述生物特征验证装置包括:生物特征传感器,用于识别经授权用户;及处理器,能够基于经由所述生物特征传感器对用户身份的验证以允许访问所述生物特征验证装置的一个或多个安全特征,并且其中所述方法包括:

将所述生物特征验证装置安装到固持件以形成注册系统,其中含有所述生物特征验证装置和所述固持件的所述注册系统被配置以通过邮件传递服务交付给终端用户;

将能够供电给所述生物特征验证装置的电源提供给所述固持件,其中所述固持件配置成使得在交付所述注册系统期间,停止从所述电源到所述生物特征验证装置的电力供应,以及所述固持件包括开关配置,所述开关配置构造成响应在交付所述注册系统后用户对所述固持件的操作而启动从所述电源到所述生物特征验证装置的电力供应;

将所述注册系统交付给所述终端用户;

响应用户对所述固持件的操作而启动从所述固持件中的所述电源到所述生物特征验证装置的电力供应;

启用所述生物特征验证装置的注册模式,在所述注册模式中,使用所述生物特征验证装置的所述生物特征传感器,经由注册处理能够将所述用户的生物特征数据注册到所述生物特征验证装置;以及

在所述注册处理期间使用来自所述电源的电力以供电给所述生物特征验证装置。

2.如权利要求1所述的方法,其中所述生物特征验证装置没有内部电源,而是配置成依赖于来自外部电源的电力,所述来自外部电源的电力包括来自所述固持件的电力及经由所述装置的天线从电场收集的电力。

3.如权利要求1所述的方法,其中在所述交付期间,所述固持件和所述生物特征验证装置以信封的形式收容在外包装内。

4.如权利要求1所述的方法,其中所述开关配置包括用于使电路完整且因此启动所述电力供应的实体开关。

5.如权利要求1所述的方法,其中由所述用户对所述固持件的操作包括于交付的接收之后进行的动作。

6.如权利要求5所述的方法,其中所述固持件是折叠卡,以及对所述固持件的操作包括打开所述折叠卡。

7.如权利要求1所述的方法,其中所述生物特征验证装置是智能卡,所述智能卡的宽度在85.47㎜和85.72㎜之间、高度在53.92㎜和54.03㎜之间,且厚度小于0.84㎜。

8.如权利要求1所述的方法,其中在启用所述注册模式之前,所述注册系统需要附加验证以确认用户的身份,其中经由所述固持件上的接口和/或所述生物特征验证装置上的接口而获得所述附加验证。

9.如权利要求8所述的方法,其中经由所述生物特征验证装置上的所述接口而获得所述附加验证,以及所述生物特征验证装置上的所述接口是所述生物特征传感器。

10.如权利要求1所述的方法,其中无需所述用户的附加验证,在启动所述电力供应时执行启用所述生物特征验证装置的注册模式的步骤。

11.如权利要求1所述的方法,其中在生物特征注册之后及在所述装置的至少一个安全特征启动之前,所述生物特征验证装置需要经由外部系统的后续验证步骤。

12.如权利要求11所述的方法,其中所述至少一个安全特征包括支付智能卡的支付功能。

13.如权利要求11所述的方法,其中在启动所述生物特征验证装置的至少一个安全特征之前,经由外部系统的后续验证步骤包括使用下列中的一个或多个:支付卡的在线银行;由所述生物特征验证装置的发行者提供的智能电话或计算机应用;电话来电;或利用验证码而使用所述生物特征验证装置。

14.如权利要求1所述的方法,其中将所述生物特征验证装置安装到所述固持件包括将所述生物特征验证装置实体安装到形成在所述固持件中的适当凹部内的固持件。

15.如权利要求1所述的方法,其中将所述生物特征验证装置安装到所述固持件包括用于与用于生物特征验证装置与所述固持件的电源形成电路的电连接,使得在用户操作所述固持件的期间,所述生物特征验证装置不需要相对于所述固持件移动或重新构建以启动电力供应。

16.如权利要求1所述的方法,其中所述生物特征验证装置是智能卡,所述智能卡以在所述智能卡上延伸的凸片而保持在所述固持件上的凹部中,其中所述凸片提供与所述智能卡上的“芯片密码”接触片的电连接。

17.如权利要求1所述的方法,其中除了电力传输之外,所述固持件和所述生物特征验证装置之间还存在数据通信,其中数据经由有线和/或无线通信协议在所述固持件与所述生物特征验证装置之间传输。

18.如权利要求17所述的方法,其中所述数据通信包括数据的有线通信,并且所述有线通信使用与从所述固持件到所述生物特征验证装置的电力供应相同的电连接。

19.如权利要求17所述的方法,其中所述固持件包括处理器,所述处理器用于控制数据通信和/或用于随着数据传输而控制所述固持件的操作。

20.如权利要求17所述的方法,其中在所述固持件上经由PIN输入的附加验证的情况下,所述固持件为所述生物特征验证装置提供解锁信号,和/或其中所述固持件与所述生物特征验证装置使用公钥交换用于附加安全性。

21.如权利要求17所述的方法,其中所述固持件与所述注册模式结合以提示所述生物特征验证装置的部分操作模式。

22.如权利要求21所述的方法,其中通过使LED亮起或使所述生物特征验证装置上的显示器对用户显示信息,所述固持件与所述注册模式结合以提示所述生物特征验证装置的部分操作模式。

23.一种用于生物特征验证装置的生物特征注册的注册系统,所述注册系统包括所述生物特征验证装置和用于所述生物特征验证装置的固持件,其中所述生物特征验证装置安装到所述固持件,以及其中所述注册系统包括所述生物特征验证装置,所述固持件配置成通过邮件传递服务交付给终端用户;

其中所述生物特征验证装置包括:生物特征传感器,用于识别经授权的用户;及处理器,能够基于经由所述生物特征传感器对用户身份的验证而允许访问所述生物特征验证装置的一个或多个安全特征;

其中所述固持件包括:电源,能够供电给所述生物特征验证装置;及开关配置,构造成响应在交付所述注册系统之后用户对所述固持件的操作,启动从所述电源到所述生物特征

验证装置的电力供应,其中所述固持件配置成使得在交付所述注册系统期间,停止从所述电源到所述生物特征验证装置的电力供应;

其中所述注册系统配置成响应用户对所述固持件的操作而启动从所述固持件中的所述电源到所述生物特征验证装置的电力供应之后,启用所述生物特征验证装置的注册模式,其中所述生物特征验证装置的所述注册模式包括注册处理,在所述注册处理中使用所述生物特征验证装置的所述生物特征传感器能够将所述用户的生物特征数据注册到所述生物特征验证装置;以及

其中所述注册系统被构造成在所述注册处理期间使用来自该电源的电力以供电给该生物特征验证装置。

24.如权利要求23所述的注册系统,其中所述注册系统被构造成执行如权利要求1至22中任一项所述的方法。

# 生物特征注册

## 技术领域

[0001] 本发明有关具有一或多个安全特征之生物特征验证装置的生物特征注册之方法、以及有关一对应的生物特征注册系统。

## 背景技术

[0002] 生物特征验证装置(诸如智能卡)正变得越来越广泛使用,而且包括例如门禁卡、信用卡、签帐金融卡、预付卡、会员卡、身份识别卡等。智能卡是具有储存数据及能例如经由诸如RFID的非接触技术而与用户及/或外部装置相互作用的能力之电子卡。这些卡片可与卡片阅读机相互作用来沟通信息,以能存取、授权交易等。其他生物特征验证装置包括诸如智能手表、安全通证(Security token)、加密保护锁(Dongle)等的随身携带装置。

[0003] 诸如指纹验证的生物特征验证正变得越来越广泛使用。具有生物特征验证的智能卡可经由传感器来与用户相互作用,以能访问智能卡的安全特征,例如,以授权金融交易。其他生物特征验证装置包括。

[0004] 有关生物特征验证装置(诸如智能卡),在装置尺寸、可用电力资源、和所需功能限制面临挑战。对智能卡而言,如果智能卡当作支付卡使用的情况,装置的尺寸可能受限于信用卡的ISO标准。因此,所有组件必须调适成紧缩封装的形式,以及理想下必须是柔性且轻巧。

[0005] 可用的电力受限于装置的尺寸和所选定的电源。可包括与外部电源的有线连接,诸如经由与「芯片密码」型智能卡的触点的连接而吸取电力。然而,存在来自外部电源的技术上限制,在于经由此方法所吸取的电流以及智能卡本身处理大电力的困难度。可使用无线连接,其中利用在该装置上的天线及与一外部天线(诸如,智能卡读卡器的天线)的一非接触式耦接而收集电力。在专利案第WO 2016/055663号和第WO 2017/025481号中描述有关实施此的先前技术建议。将了解到,使用所收集的电力具有明显的优点,但是鉴于以此方式可获得电力量的限制,可能得有所妥协。

[0006] 众所周知,生物特征数据的注册针对诸如智能卡之类的较小装置带来特殊的挑战,特别是在使用收集电力的情况,即是,在不可能有经由电池等储存在智能卡上的任何大电量的情况。在如申请案第WO 2016/055661号公开的较早申请案中,申请人特别描述利用在RFID终端机(例如,银行卡的ATM)处使用的智能卡来启用注册模式的方法,其中注册模式受到从智能卡分开发送的授权码保护。随着在申请案第WO 2016/055661号中的示例中,当智能卡从RFID终端机接收电力时,用户则可经由整合到智能卡的生物特征传感器来注册其生物特征(例如指纹)。。

[0007] 想要在注册期间使用整合在智能卡中的该生物特征传感器。此避免对于在网络上潜在不安全传输生物特征数据的需要,而是该智能卡可安全保存生物特征数据,而无需外部储存或传输。由于用于注册的传感器与用于稍后藉由针对储存的生物特征而检查用户的生物特征进行验证时的传感器完全相同,使得也可提高生物特征身份验证处理的准确性。然而,虽然申请案第WO 2016/055661号中的提议在本技艺中提供明显的进步,但是仍然需

要能用于诸如智能卡的生物特征验证装置的替代注册系统。

## 发明内容

[0008] 从一第一态样来看,本发明提供一种用于生物特征验证装置的生物特征注册之方法,其中该生物特征验证装置包括:一用于识别授权用户的生物特征传感器;及一处理器,其能够基于经由该生物特征传感器对用户身份的验证来允许访问该生物特征验证装置的一个或多个安全特征,而且其中该方法包括:

[0009] 将该生物特征验证装置安装到固持件上以形成一注册系统,其中含有该生物特征验证装置和该固持件的所述注册系统配置成藉由邮件传递服务来交付给终端用户;

[0010] 提供给该固持件具有能够供电给该生物特征验证装置的电源,其中该固持件配置成使得在该注册系统交付期间,停止从电源供电给该生物特征验证装置,而且该固持件包括一开关配置,该开关装置构造成响应在交付注册系统之后用户操作该固持件而启动从电源到该生物特征验证装置的电力供应;

[0011] 将该注册系统交付给终端用户;

[0012] 回应用户操作该固持件,以启动从该固持件中的电源到该生物特征验证装置的电力供应;

[0013] 启用该生物特征验证装置的注册模式,其中可使用该生物特征验证装置的生物特征传感器,经由注册处理将用户的生物特征数据注册到该生物特征验证装置;及

[0014] 在注册处理期间使用来自该电源的电力供电给该生物特征验证装置。

[0015] 藉由在可采单次递送来交付给用户的注册系统中提供该生物特征验证装置以及一固持件,则可明显简化该注册处理。该注册系统可为完备系统,因为其使得可注册生物特征数据而无需与任何外部系统或网络进行相互作用。该生物特征验证装置可接入来自该固持件的电源,因此即使在没有内部电源的生物特征验证装置情况下,用户亦可在交付时执行注册处理,而无需将该生物特征验证装置转移到分离的读卡器或注册系统,或将该装置与其他地方可供用户使用的电源配对。优选是,该生物特征验证装置可没有内部电源,因此可依赖于来自外部源的电力,包括收集的电力,诸如在专利案第WO 2016/055663号或第WO 2017/025481号中的描述经由天线获得的电力。

[0016] 在将智能卡(例如支付卡)当作该生物特征验证装置的情况,用户经历的注册处理恰好适当习知卡片启动程序,因为当交付该智能卡时,用户具有包装中所有必要的特征,以在用户家中或工作场所能经由该固持件的电力进行注册。如果提供用于启动该智能卡的安全特征的适当系统,则用户可能够立即使用该受生物特征保护的智能卡,诸如用于支付卡的生物特征安全非接触式支付。该注册系统和该固持件可配置成用于直觉启动从该固持件中的电源供电给该生物特征验证装置。例如,如下述,用户操作该固持件可包括通常在收到交付后进行的动作,诸如打开包装或打开「礼品卡」类型固持件。因此,用于注册处理的电源可类似于已知的可交付电源,诸如用于「唱歌礼品卡」等的电池。因此,该注册系统可选择性使用已证明可在邮件传递服务中安全使用的电池技术,其避免否则可能发生的法规问题。

[0017] 提及邮件传递应了解为包括用于交付实体物品的任何适当系统,诸如邮政服务、快递服务等。该固持件和该生物特征验证装置可收容在适当外包装内,以在交付给用户期间受到保护。在具有扁平形状的生物特征验证装置(诸如智能卡)的情况,该包装可为一信

封,因此将藉由可递送信件和类似物品的所有邮件传递系统轻易交付给用户。

[0018] 该固持件可为一折叠卡,而且该折叠卡可构造成由用户展开以露出智能卡和注册系统(即是,一生物特征传感器)。或者,该固持件可包括含有类似药丸盒等的滑件之匣盒。如果该固持件包括一匣盒,则其可更包括一凸片,当用户拉动该凸片时,从匣盒内部露出智能卡及/或注册系统。该智能卡及/或该注册系统可附接到滑件,而且该滑件可构造成当拉动凸片时从匣盒的内部出现(例如,藉由从匣盒开口滑出)。虽然该固持件可采用任何前述配置,但是熟习该项技艺者应明白,该固持件可包括适于邮件递送且构造成在运送期间保持所述智能卡和注册系统的任何系统。用户操作该固持件的步骤导致经由开关配置启动电源。此可包括一用于完成电路的实体开关。如前述,该固持件可类似于所谓「唱歌礼品卡」,而且可使用从此装置已知的开关配置,在这情况,该固持件的操作可包括打开一折叠卡。可使用其他操作,诸如拉动凸片或按下按钮。在某些情况,应明白,该操作可为用户将进行的自然动作,诸如打开一折叠卡。在该固持件包括一具有滑件的匣盒之情况,则用户操作该固持件的步骤可包括将卡片滑出匣盒及/或拉动凸片。该固持件可包括用户的印刷说明,以提示用户进行所需操作。例如,该固持件上可包括书写或图解说明。该固持件亦可对用户提供有关在启动来自电源的供电之后如何进行该生物特征注册的说明。例如,这些说明可为印刷在该固持件上的书写或图解说明,及/或该固持件可包括一用于提供说明的有源接口,诸如用于提供可听说明的喇叭或用于提供可见说明的图形用户界面。

[0019] 正如从前面讨论明白,该注册方法的优选实施将其用于智能卡(诸如支付卡或门禁卡),尤其是没有内部蓄电的智能卡(诸如使用收集电力的智能卡)的生物特征注册。该智能卡可为下列之任一者:门禁卡、信用卡、签帐金融卡、预付费卡、会员卡、身份识别卡、交通卡等。该智能卡选择性具有介于85.47mm和85.72mm之间的宽度、及介于53.92mm和54.03mm之间的高度。该智能卡可具有小于0.84mm厚度,而选择性约0.76mm(例如,±0.08mm)。更普遍是,该智能卡可符合智能卡规范ISO 7816。

[0020] 其他生物特征验证装置亦可使用该注册方法,诸如使用在经由物联网进行相互作用环境的穿戴器件和装置,尤其是小型便携设备。可穿戴生物特征验证装置的实例是智能手表。在本发明的实施例中,此可能是生物特征验证装置,其中在首次将手表交付给用户时,诸如在线购买之后,该固持件在注册处理期间供电给手表。在一实例中,该固持件是一手表匣盒,并且打开匣盒启动电源。

[0021] 该生物特征验证装置可能够进行无线通信,诸如使用RFID或NFC通信。或者或更甚者,该生物特征验证装置可包括触点连接,例如经由诸如用于「芯片密码」卡之类的接触片等。在各种实施例中,该生物特征验证装置可允许无线通信和接触通信两者。应明白,该生物特征验证装置可具有用于从该固持件上的电源接收电力的电触点,而且在这情况,用于接收电力的电触点亦可作为通信目的之触点连接。

[0022] 该生物特征传感器可为一指纹传感器,其最好是嵌入该生物特征验证装置中。使用此特征,授权的用户可首先将其指纹注册到该生物特征验证装置,然后可能需要将其手指或拇指置放在指纹传感器上,以授权该生物特征验证装置的部分或全部使用。该处理器上的指纹比对算法可用于识别已注册用户和该指纹传感器感测到指纹之间的指纹比对。

[0023] 启用该生物特征验证装置的注册模式之步骤可无需任何附加步骤便可启动电源时执行。因此,可在简单实体操作该固持件之后且无需用户的额外认证,便可自动允许生物

特征注册。在这情况，该生物特征验证装置在生物特征注册之后及在启动该装置的某些或全部安全特征(诸如用于支付智能卡的支付功能)之前，可需要经由一外部系统进行后续授权步骤。下面讨论经由一外部系统进行可能的后续授权步骤。此方法的优势在于简化该注册系统及使该注册方法符合现有启动处理(诸如，启动经由邮件收到的支付卡)。或者，在启用注册模式之前，该注册系统可需要添加身份验证以确认用户的身份。该方法可包括使用该注册系统进行附加身份验证以及经由外部系统进行后续授权步骤两者。

[0024] 在该注册系统需要附加身份验证以在启用注册模式之前确认用户身份的情况，则此可利用在该固持件上的一接口及/或在该生物特征验证装置上的一接口。

[0025] 该生物特征验证装置上的接口可为生物特征传感器。如申请人在专利案第WO 2017/149015号和第WO 2018/087336号中的描述，存有各种可能性与当作辅助识别系统的生物特征传感器相互作用，特别是当存在指纹传感器并且可用于侦测与该生物特征验证装置的非指纹相互作用。在这情况，可向用户提供定义该指纹传感器(或其他生物特征传感器)可侦测到的动作模式或序列的适当说明，以确认用户授权。此的进一步详细信息阐述如下。此说明可个别交付给该注册系统的用户，诸如采取从支付卡分开寄送PIN的相同方式的个别邮件递送。

[0026] 另一可能性是固持件上包括一接口，诸如一PIN键盘或允许输入密码的其他接口。再者，可为分开交付密码的详细信息，诸如经由个别的邮件递送。用户可输入密码以启动该生物特征验证装置的注册模式。或者，此亦可启动对该装置的某些或全部安全特征的访问，诸如用于支付智能卡的支付功能。

[0027] 如果该方法包括在启动该生物特征验证装置的某些或全部安全特征之前，经由一外部系统的后续授权步骤，则此可藉由各种方法来完成，包括已知用于启动习知支付卡的方法。使用此方法是优选的，由于其效益在于藉由允许在该固持件简单实体操作之后自动允许生物特征注册而无需增加用户的身份验证，从而简化特征注册及用户的注册步骤。在这情况，可使用下列一或多者方法，经由后续授权步骤来启动该生物特征验证装置的安全特征：

[0028] • 一在线系统，诸如用于支付卡的在线银行业务，在这情况，启动可能需要用户进行下列动作：

[0029] • 登录到在线银行

[0030] • 选择要启动卡片的帐户

[0031] • 点击「启动新卡」，然后按照说明进行操作。

[0032] • 可由该生物特征验证装置的发行者提供的APP，诸如智能型手机或PC应用程序：

[0033] • 用户打开安全APP以确认注册和使用安全特征的意图，这些特征将在根据APP的安全特征进行身份验证后启动。

[0034] • 打电话，诸如经由呼叫该生物特征验证装置的发行单位(例如，支付卡的银行)而且藉由提供适当的个人详细信息来确认用户的身份。

[0035] • 针对支付智能卡，在ATM或销售点使用该卡：

[0036] • 用户使用PIN码进行交易(诸如提现款、余额查询或手机储值)，而且该智能卡按用户及/或发卡单位的需要将自动启动进一步使用链接PIN的智能卡及/或生物特征验证。

[0037] 该固持件和该生物特征验证装置之间的相互作用可有关将该生物特征验证装置

实体安装到该固持件,诸如安装在适当凹部内。将该生物特征验证装置安装到该固持件可包括一用于与该生物特征验证装置和该固持件的电源形成电路的电连接。因此,该生物特征验证装置将不需要相对于该固持件动作或重新配置以启动电力供应。而是,当将该注册系统交付给用户时,所需的电连接应该已就位,而电源的启动将依赖于该固持件的操作,而无需该固持件和该生物特征验证装置的相对动作。在一示例中,该生物特征验证装置保持在该固持件的凹部中,其中一凸片在该生物特征验证装置上延伸以提供对该生物特征验证装置上的接触点之电连接。在该生物特征验证装置是一智能卡的情况,则该接触点可为一「芯片密码」接触片。

[0038] 该固持件和该生物特征验证装置之间的相互作用可能受限于电力供应,使得该固持件可包括一简单的电源电路,该简单的电源电路具有经由开关配置的开关功能而没有其他功能。或者,该固持件本身可为一「智能」装置,而且除了电力之外,该固持件和该生物特征验证装置之间可进行数据通信。数据可经由有线或无线通信协议在该固持件和该生物特征验证装置之间传输。在有线数据通信的情况,此可使用相同于电源的电气连接。如前述,该生物特征验证装置可包括触点连接,例如经由诸如用于「芯片密码」智能卡之类的接触片等,而且此接触片可用于从该固持件供电给该生物特征验证装置及用于数据通信两者。在无线数据通信的情况,此可使用在该生物特征验证装置上提供的无线通信系统供其他目的使用,诸如在该生物特征验证装置的正常使用期间针对RFID通信提供RFID通信接口。在该生物特征验证装置是一智能卡的情况,通常包括一RFID天线,诸如用于支付智能卡或交通系统智能卡的非接触式通信。

[0039] 在该生物特征验证装置与该固持件彼此通信以传输数据的情况,该固持件可包括一处理器,以控制数据传输及/或随着数据传输以控制该固持件的操作。在经由该固持件上的PIN输入等进行附加验证的情况,该固持件可对该生物特征验证装置提供解锁信号。该固持件和该生物特征验证装置可使用公钥交换来增添安全性。该固持件可结合注册模式来提示该生物特征验证装置的某些操作模式,诸如使LED亮起或使该生物特征验证装置上的显示器对用户显示某些信息。在后者情况,该生物特征验证装置可包括GUI,诸如一LED或LCD显示器等。

[0040] 从一第二态样来看,本发明提供一种用于该生物特征验证装置的生物特征注册之注册系统,该注册系统包括该生物特征验证装置及一用于该生物特征验证装置的固持件,其中该生物特征验证装置安装到该固持件,而且其中含有该生物特征验证装置和该固持件的注册系统配置成藉由邮件传递服务交付给终端用户;

[0041] 其中该生物特征验证装置包括:一用于识别授权用户的生物特征传感器;及一处理器,其能够基于经由该生物特征传感器对用户身份的认证来允许访问该生物特征验证装置的一或多个安全特征。

[0042] 其中该固持件包括一能够供电给该生物特征验证装置的电源及一开关配置,该开关配置构造成响应在交付该注册系统之后用户操作该固持件而启动从电源到该生物特征验证装置的电力供应,其中该固持件配置成使得在交付该注册系统期间,停止从该电源到该生物特征验证装置的电力供应;

[0043] 其中该注册系统配置成响应用户操作该固持件而启动从该固持件的电源到该生物特征验证装置的电力供电之后,启用该生物特征验证装置的注册模式,该生物特征验证

装置的注册模式包括使用该生物特征验证装置的生物特征传感器,将用户的生物特征数据注册到该生物特征验证装置的注册处理;及

[0044] 其中该注册系统构造成在注册处理期间使用来自电源的电力以供电该生物特征验证装置。

[0045] 该注册系统可构造成执行第一态样的方法,而且可选择性包括前面所讨论进一步特征以及该方法之任一者。因此,例如,该固持件为一折叠卡或一具有滑件的匣盒,如前述。

[0046] 提及邮件传递将了解为包括用于交付实物的任何适当系统,诸如邮政服务、快递服务等,因此,该注册系统将适于此类系统的交付,例如就其实体尺寸而言。该注册系统可为完备系统,因为其无需与任何外部系统或网络相互作用便可注册生物特征数据。该注册系统可包括一适当外包装,以在交付给用户期间保护该固持件和该生物特征验证装置。在一具有扁平形状的生物特征验证装置(诸如一智能卡)的情况,则该包装可为一信封,因此将可藉由可传递信件和类似物品的所有邮件传递系统轻易交付给用户。

[0047] 该开关配置可包括一用于完成电路的实体开关。如前述,该固持件可类似于所谓的「唱歌礼品卡」,而且可使用从此装置已知的开关配置,在这情况,该固持件的操作可包括打开一折叠卡。可使用其他操作,诸如拉动凸片或按下按钮。在某些情况,应明白,该操作可为用户将进行的自然动作,诸如打开折叠卡。该固持件可包括用户的印刷说明,以提示用户进行所需操作。例如,该固持件上可包括书写或图解说明。该固持件亦可对用户提供有关在启动电源的电力供应之后如何进行生物特征注册的说明。例如,这些说明可为印刷在该固持件上的书写或图解说明,及/或该固持件可包括一用于提供说明的有源接口,诸如用于提供可听说明的喇叭或用于提供可见说明的图形用户界面。

[0048] 该生物特征验证装置可为一智能卡。该智能卡可为下列之任一者:门禁卡、信用卡、签帐金融卡、预支付卡、会员卡、身份识别卡等。该智能卡可选择性具有介于85.47mm和85.72mm之间的宽度、及介于53.92mm与54.03mm之间的高度。该智能卡可具有小于0.84mm厚度,而且选择性约0.76mm(例如,±0.08mm)。更普遍是,该智能卡可符合智能卡规范ISO7816。

[0049] 其他生物特征验证装置亦可使用该注册方法,诸如经由物联网使用在相互作用环境下的穿戴器件和装置,尤其是小型便携设备。因此,该注册系统可包括这些装置之一。

[0050] 该生物特征验证装置可能够无线通信,诸如使用RFID或NFC通信。或者或更甚者,该生物特征验证装置可包括触点连接,例如经由诸如用于「芯片密码」卡之类的接触片等。在各种实施例中,该生物特征验证装置可允许无线通信和接触通信两者。应明白,该生物特征验证装置可具有用于从该固持件上的电源接收电力的电触点,而且在这情况,用于接收电力的电触点亦可当作用于通信目的之触点连接。

[0051] 该生物特征传感器可为一指纹传感器,其最好是嵌入该生物特征验证装置。授权的用户可使用此特征开始将其指纹注册到该生物特征验证装置,然后可需要将其手指或拇指置放在指纹传感器上,以授权该生物特征验证装置的部分或全部使用。该处理器可包括一指纹比对算法,以在注册的用户与该指纹传感器所感测到的指纹之间识别指纹比对。

[0052] 该注册系统可构造成使得可在没有任何附加步骤下启动电源来启用该生物特征验证装置的注册模式。因此,在简单实体操作该固持件之后且无需用户的额外认证,可自动允许该生物特征注册。在这情况,该生物特征验证装置可配置成在启动该装置的某些或全

部安全特征(诸如用于支付智能卡的支付功能)之前,需要经由一外部系统的后续授权步骤。因此,该处理器可需要此添加步骤以及有关访问安全特征的生物特征识别。经由一外部系统的可能后续授权步骤可如前的讨论。

[0053] 或者,该注册系统可配置成在启用该注册模式之前需要添加身份验证以确认用户的身份。该注册系统可配置成需要使用注册系统进行添加的身份验证以及经由一外部系统进行后续授权步骤两者。

[0054] 在该注册系统需要附加身份验证以在启用该注册模式之前确认用户身份的情况,则此可利用该固持件上的一接口及/或该生物特征验证装置上的一接口。如前述,该生物特征验证装置上的接口可为该生物特征传感器。另一可能性是一接口包括在该固持件上,诸如PIN键盘或允许输入密码的其他接口。该固持件可配置成在用户输入正确密码时启动该生物特征验证装置的注册模式。该生物特征验证装置亦可选择性使用经由此密码的授权以启动访问该装置的某些或全部安全特征。

[0055] 该固持件和该生物特征验证装置之间的相互作用可关于将该生物特征验证装置实体安装到该固持件,诸如安装在适当凹部内。因此,该固持件可包括一用于接受该生物特征验证装置的凹部。该凹部可诸如经由摩擦力固持(Friction fit))及/或使用弹性可变形组件来弹性握持该生物特征验证装置。此可允许该生物特征验证装置在交付和注册期间由该固持件稳固保持,但是一旦完成注册处理,则可由用户轻易用手移开。该生物特征验证装置到该固持件的安装可包括用于与该生物特征验证装置和该固持件的电源形成电路的电连接。因此,该生物特征验证装置应不需要相对于该固持件来移动或重新配置以启动电力供应。而是,当该注册系统交付给用户时,所需的电连接应该已就位,而电源的启动依赖于该固持件的操作,而无需该固持件和该生物特征验证装置的相对移动。

[0056] 该固持件和该生物特征验证装置之间的相互作用可能受限于电力供应,使得该固持件包括一简单的电源电路,该简单的电源电路具有经由开关配置的开关功能而没有其他功能。或者,该固持件本身可为一「智能」装置,且除了电力之外,该固持件和该生物特征验证装置之间还可存在数据通信。数据可经由有线或无线通信协议而在该固持件和该生物特征验证装置之间传输。在有线数据通信的情况,此可使用相同于电源的电气连接。如前述,该生物特征验证装置可包括触点连接,例如经由诸如用于「芯片密码」智能卡这之类的接触片等,而且此接触片可用于从该固持件到该生物特征验证装置的电源及用于数据通信两者。在无线数据通信的情况,此可使用在该生物特征验证装置上提供的无线通信系统供其他目的使用,诸如在该生物特征验证装置的正常使用期间针对RFID通信提供的RFID通信接口。在该生物特征验证装置是一智能卡的情况,则通常包括一RFID天线,诸如用于支付智能卡或交通系统智能卡的非接触式通信。

[0057] 在该生物特征验证装置与该固持件彼此通信以传输数据的情况,则该固持件可包括一处理器,以控制数据传输及/或随着数据传输来控制该固持件的操作。在经由该固持件上的PIN输入等进行附加身份验证的情况,该固持件可对该生物特征验证装置提供解锁信号。该固持件和该生物特征验证装置可使用公钥交换来增添安全性。该固持件可配置成结合注册模式来提示该生物特征验证装置操作的某些模式,诸如使LED亮起或使该生物特征验证装置上的显示器对用户显示某些信息。在后者情况,该生物特征验证装置可包括GUI,诸如LED或LCD显示器等。

[0058] 关于前面引用的方法或系统,该注册系统可包括如下描述的进一步特征。

[0059] 如前述,经由该生物特征验证装置上的一接口使用附加身份验证可包括以不同于标准指纹输入的方式来与该指纹传感器的相互作用。

[0060] 因此,使用此态样的指纹验证装置,可让用户无法对经由非指纹验证仍然使用该装置的某些或全部特征的指纹验证注册。可向用户提供采取指纹传感器可侦测到的动作模式或序列之形式来定义非指纹验证的适当说明,以确认用户授权。该指纹传感器用于部分或全部非指纹验证处理,此意味不需要对该装置添加其他传感器即可实现建议的非指纹验证,尽管如果存在其他传感器(诸如(例如)一加速度计),则亦可使用这些传感器。

[0061] 经由该指纹传感器侦测到的该(等)动作可包括下列一或多者:固定接触传感器、移动接触传感器、接触传感器的时段、接触传感器的移动方向、接触传感器次数、没有接触传感器的时段(即是接触间的时段)。最好是,所述非指纹验证需要不同动作的组合,其可包括在该指纹传感器上的一系列动作及/或在该指纹传感器上的至少一动作结合经由另一输入或传感器的至少一动作。

[0062] 该触点可为经由该装置的指纹传感器可侦测到的任何触点。指纹传感器的本质意味其配置成识别与皮肤接触,因此该触点可为皮肤的触点,例如接触指尖或姆指尖。由于指纹传感器没有用于收集有关接触以启用指纹验证的足够信息程度,使得可区别在非指纹验证期间所使用指纹传感器的相互作用与在指纹验证期间的相互作用。

[0063] 指纹传感器侦测到的固定接触形式的动作可包括侦测接触的存在,此有别于没有接触。

[0064] 该指纹传感器侦测到的移动接触形式的动作可包括移动方向及/或移动速度的侦测。该方向可相对于该装置的一或多个轴来识别。例如,在智能卡的情况,该处理器可配置成区分平行于卡片长边移动的触点和平行于卡片短边移动的触点。该(等)动作可包括具有平行及/或垂直移动、或由用户定义的更复杂移动的序列,诸如旋转接触或圆形移动。

[0065] 无论该指纹传感器是否用来简单侦测存在接触或侦测更复杂的特征,该指纹传感器侦测到的动作可包括一或多个接触的时段、多个接触及/或接触间的间隔,例如类似于诸如摩尔斯电码(Morse code)的密码。因此,非指纹验证所需装置的相互作用可包括或由一系列固定或移动接触该传感器的密码输入所组成。

[0066] 非指纹验证可替代性或另外包括下列之一或多者:

[0067] • 使用或没有施加于传感器的指纹来遮盖传感器的一部分,例如遮盖该传感器的某个角落;

[0068] • 在传感器上置放两手指,使得传感器看到并排的指纹,其间有缝隙或接合。

[0069] • 按默认顺序来触贴或刷一下传感器或该传感器的某些部分;

[0070] • 使用手指或其他方式来遮盖该传感器一段时间;及/或

[0071] • 相对于该指纹传感器的其他相互作用。

[0072] 该生物特征验证装置的安全特征可例如包括银行卡交易的授权、卡片储存数据存取、经由门禁卡进入安全区域等。

[0073] 该生物特征验证装置可包括一用于感测该生物特征验证装置的移动之加速度计,而且该处理器可使用该加速度计所感测到当作添加验证步骤之部分或全部的移动。因此,可让用户经由该生物特征验证装置的移动来输入密码,以确认其身份或启动该生物特征验

证装置的安全特征。此可需要用户以某种方式来与智能卡实体相互作用,诸如藉由在硬表面上轻触智能卡。

[0074] 该加速度计亦可基于由所述加速度计感测到的移动来控制该生物特征验证装置。例如,该加速度计感测到的移动可用于启动该生物特征验证装置的各种操作模式。优选是,该智能卡是一非接触式智能卡,因此用户可在用户仅握卡接触的不同模式之间切换。此可允许增加特征及增添如何使用智能卡而不会伤害卡片易操作性的复杂性。

[0075] 该处理器可配置成基于该加速度计的输出以识别该生物特征验证装置的移动,而且随着预设的移动来改变该生物特征验证装置的操作模式或决定用户授权。预设移动可包括平移、旋转、加速度、加加速度(Jerk)/冲量(Impolse)等之任一者或全部。另外,该处理器可决定没有移动的时段长度,即是指示没有有效使用该生物特征验证装置的时段,而且此亦可用于改变该生物特征验证装置的操作模式及/或停止目前启动的特征(诸如安全特征)。该处理器亦可配置成识别重复的移动或移动序列,诸如双触贴(Double tap)、或平移随后旋转(诸如滑动和扭转运动)。

[0076] 虽然使用单感测轴的加速度计可侦测移动,但是最好能够侦测全方位的加速度。此可经由多个加速度计来完成,但是最好是,使用可侦测全方位加速度的一单个加速度计,诸如3轴加速度计。

[0077] 该加速度计可为一微机械加速度计,诸如一MEMS加速度计。或者,一压电传感器可使用,诸如可感测加速度的一专属压电加速度计或另一压电传感器(例如,一压电发声器或麦克风)。使用这些类型装置允许其安装在智能卡上,而不会增加智能卡的尺寸。这些类型装置还具有低功率消耗,此可可能是如前述智能卡的设计限制。压电传感器可优选采用「压电传感器侦测到输入之前是零功率消耗」的方式并入该装置中。该加速度计可使用诸如微机械悬臂(Cantilever)或测震质量(Seismic mass)的感测组件。在一示例实施中,加速度感测是基于从感测组件的加速度引起动作所导致差动电容(Differential capacitance)的原理。可使用的可能加速度计诸如由位于美国纽约伊萨卡(Ithaca)的美商嘉速力微机电股份有限公司(Kionix,Inc.)提供的3轴数字加速度计(Tri-axis Digital Accelerometer)。一示例实施例使用Kionix KXCJB-1041加速度计。该生物特征验证装置的处理器可配置成经由该生物特征传感器来控制生物特征数据的注册。

[0078] 在本说明书中引用的处理器,应了解,此可包括多个同时工作的处理器。例如,该生物特征传感器及/或该加速度计(如果有的话)之每一者可具有一专属处理器,其能与具有控制智能卡其他特征的主处理器进行相互作用。此外,尽管在较佳实施例中,虽然说有一处理器以控制与该生物特征验证装置以及指纹处理器(作为该指纹验证引擎之一部分)的通信,但应明白,这两处理器之每一者可由多个处理器所组成、或可为单一组合的处理器之分离软件模块。

[0079] 在注册处理之后,该生物特征验证装置通常可需要用户经由该生物特征传感器来识别用户本身,以授权该装置的某些或全部使用。在指纹传感器的情况,该处理器可使用指纹比对算法来识别已注册用户和该指纹传感器感测到指纹之间的指纹比对。

[0080] 最好是,该装置配置成使得其不可能撷取用于识别用户的数据。此类型数据在该装置外部的传输认为对该装置的安全性构成很大风险。因此,注册可为仅需要访问该注册系统的注册处理的完备处理,而且所注册的生物特征数据不会与该生物特征验证装置外部

进行通信。

[0081] 根据提出的装置,可使用相同的生物特征传感器来执行比对扫描和注册扫描两者。因此,可平衡扫描错误,因为例如如果用户在注册期间倾向于将其手指侧偏向指纹传感器,则用户很可能在使用相同传感器比对时亦同样做。

[0082] 该生物特征验证装置的第一注册用户可具有稍后提示添加后续用户注册模式的能力。或者或更甚者,其可经由外部构件来提示控制系统的注册模式,诸如经由该生物特征验证装置与一安全系统之间的相互作用,所述安全系统可为业者或另一授权实体单位控制的安全系统。

[0083] 该生物特征验证装置可为一便携设备,其意指设计成可由人携带的装置,最好是,体积小且轻巧便于携带的装置。例如,该生物特征验证装置可配置成在口袋、手提包或钱包内携带。如前述,该生物特征验证装置可为一智能卡,诸如一指纹可认证RFID卡。该装置可为一用于控制对该控制通证的外部系统存取的控制通证(Control token),诸如用于存取计算机系统的一次性密码装置或用于车辆无钥匙进入系统的密钥卡(Fob)。在不依赖于有线电源而言,该生物特征验证装置最好是亦是可移植性。该生物特征验证装置可由一内部电池、及/或由从读卡器等(例如从RFID读卡器)非接触式所收集电力进行供电。

[0084] 该生物特征验证装置可为一单用途装置,即是一用于与单外部系统或网络相互作用或用于与单类型外部系统或网络相互作用的装置,其中该装置没有任何其他目的。因此,该装置将有别于诸如智能型手机等的复杂和多功能装置。

## 附图说明

[0085] 现将仅藉由实例及参考附图更详细描述本发明的某些较佳实施例,在附图中:

[0086] 图1为针对结合一加速度计及一使用指纹区域传感器形式的生物特征传感器之智能卡的电路图;

[0087] 图2示意说明具有一外壳体的智能卡;

[0088] 图3显示一示例压合型智能卡;

[0089] 图4为具有智能卡和相关固持件之注册系统的示例;及

[0090] 图5为使用图4所示注册系统进行注册之一系列步骤的示意图。

## 具体实施方式

[0091] 举例来说,使用非接触技术及使用从读卡器所收集电力之指纹验证智能卡的特性下描述本发明。这些特征认为是使用所提出注册系统的生物特征验证装置的有利特征,但是未视为必要特征,因此该生物特征验证装置可针对从事「物联网」的生物特征安全相互作用而采用不同形式,诸如可穿戴器件、硬件保护锁(Dongle)及/或装置。在下面的讨论中,首先参考图1至3描述指纹验证智能卡的实施例,然后参考图4和5描述注册方法和相关的注册系统。

[0092] 图1显示一智能卡102的架构。一有源读卡器104经由一天线106传送信号。该信号对于NXP Semiconductors公司制造的MIFARE®和DESFire®系统通常是13.56MHz,但对于由HID Global Corp制造的较低频率PROX®产品可为125kHz。此信号由该智能卡102的天线108接收,其中该天线包括一调谐线圈和一电容器,然后传递给一通信芯片110。该接收到

的信号是由一桥式整流器112进行整流,该桥式整流器112的DC输出提供给该处理器114,以控制从该通信芯片110的发讯。

[0093] 从该处理器114输出的一控制信号控制连接天线108的一场效晶体管116。藉由导通及关闭该场效晶体管116,信号可藉由该智能卡102传送及藉由该读卡器104中的适当控制电路118译码。此类型发信称为反向散射调变(Backscatter modulation),其特征在于使用读卡器104来驱动其的返回讯息。

[0094] 一加速度计16(在提供的情况)是采取适当方式连接到该处理器114。该加速度计16可为位于美国纽约伊萨卡(Ithaca)的美商嘉速力微机电股份有限公司(Kionix,Inc.)提供的3轴数字加速度计(Tri-axis Digital Accelerometer),而且在此示例中,其是Kionix KXCJB-1041加速度计。该加速度计16感测卡片的移动并且对该处理器114提供输出信号,该处理器配置成侦测及识别有关卡片所需操作模式的移动,如下述。该加速度计16亦可用于有关生物特征(指纹)数据注册的验证处理,如下述。

[0095] 一指纹验证引擎120连接到该处理器114,以允许基于手指或拇指指纹对用户进行生物特征验证。该指纹验证引擎120可由天线108供电,使得卡片是一完全无源式智能卡102。在这情况,只有当从读卡器104收集电力或从使用有线连接该智能卡102的外部电源电力时,才可对授权用户进行指纹识别。

[0096] 如本说明书的使用,术语“无源式智能卡”应了解成意指一内含通信芯片110仅藉由收集自激励场(例如由读卡器118产生)的电能供电之智能卡102。即是,一无源式智能卡102依靠读取器118来供其电力以进行广播。虽然可包括电池以供电给电路的辅助组件(但不广播),但是一无源式智能卡102通常不包括一电池。此装置通常称为「半无源式装置(Semi-passive device)」。

[0097] 同样地,术语“无源式指纹/生物特征验证引擎”应了解成意指仅由收集自激励场(例如由读卡器118产生的RF激励场)的电能进行供电的一指纹/生物特征验证引擎。

[0098] 应注意,在替代实施例中,可提供供电的电池且因此是非无源式智能卡,而且相对于该加速度计、指纹传感器、注册处理等可具有相同特征。利用这些替代方案,该智能卡除了使用收集的电力取代成来自卡体内含电池的电力以外,可具有相同特征。

[0099] 该卡体可为如图2所示的一卡片壳体134或如图3所示的一压合卡体140。应明白,该智能卡102有明显的尺寸限制。

[0100] 该天线108包括一调谐电路,该调谐电路包括一感应线圈和一电容器,其调谐成从读卡器104接收RF信号。当暴露于由读卡器104产生的激励场时,在天线108感应电压。

[0101] 该天线108具有第一端输出线122和第二端输出线124,天线108的每一端有一输出线。该天线108的输出线连接到该指纹验证引擎120,以提供电力给该指纹验证引擎120。在此配置中,一整流器126提供成整流由天线108接收的AC电压。整流后的DC电压是使用一滤波电容器进行滤波,并将其提供给该指纹验证引擎120。

[0102] 该指纹验证引擎120包括一指纹处理器128和一指纹读取器130,该指纹读取器可为一区域指纹读取器130,如图2所示安装在卡片壳体134上,或者装配成如图3所示从一压合卡体140露出。该卡片壳体134或该压合体140收容图1所示的全部组件,而且其尺寸类似于传统的智能卡。该指纹验证引擎120可为被动式(Passive),因此仅由从天线108输出的电压来供电,或其可如前述的电池供电。该指纹处理器128包括一微处理器,该微处理器系经

选择具有非常低的电力和非常高的速度,以能够在合理时间内执行生物特征比对。

[0103] 该指纹验证引擎120配置成扫描提供给指纹读取器130的手指或拇指,而且使用该指纹处理器128来比较手指或拇指的扫描指纹与预先储存的指纹数据。然后决定是否扫描的指纹符合预先储存的指纹数据。捕获的指纹影像及验证该智能卡102的持有人所需的时间可小于1秒钟。

[0104] 如果决定生物特征比对,则该处理器114根据其编程采取适当动作。在此示例中,完全存取该智能卡的安全特征(例如,支付功能)需要生物特征验证(在此示例中藉由指纹验证体现)。如果符合注册的生物特征数据,则该处理器114允许使用该智能卡102与非接触式读卡器104。因此,当满足多因素验证时,才授权通信芯片110发送信号给读卡器104。该通信芯片110藉由反向散射调变(Backscatter modulation)来传送信号。

[0105] 在使用该加速度计16的情况,该处理器114接收来自该加速度计16的输出,此允许该处理器114决定该智能卡102已进行哪些移动。该处理器114可识别有关该智能卡102的操作模式所需改变的默认移动。如前述,所述移动可包括该加速度计16可侦测到的旋转、平移、加速、加加速度、冲量及其他移动的任何类型或组合。

[0106] 该处理器114随着有关操作模式需要改变的所识别移动来启动或切换成的操作模式可包括如前述的任何操作模式,包括打开或关闭卡、启动智能卡102的安全态样,诸如非接触式支付及/或沟通读卡器104,或者例如藉由用作门禁卡、支付卡、交通智能卡之间的切换、在相同类型的不同账户(例如两银行账户)之间的切换、在通信协议(诸如蓝牙、Wifi、NFC)之间的切换及/或启动一通信协议、启动显示器(诸如LCD或LED显示器)、从智能卡102获得输出(诸如一次性密码等、或提示智能卡102以自动执行智能卡102的标准操作,以改变智能卡102的基本功能。应明白,从随着该加速度计16侦测到事件所采取动作的观点,可使用任何需要的特征而轻易对该智能卡102进行编程。

[0107] 该处理器114具有学习模式以允许用户指定哪些动作(包括动作的组合)应启动特定操作模式。在学习模式下,该处理器114提示用户进行想要的移动序列,并重复移动预定时间。然后这些移动分配给所需要的操作模式。该处理器114可如前述实施一丢弃的卡模式及/或一生物特征故障备份模式。

[0108] 在某些情况,该生物特征智能卡102的拥有者可能受伤,导致已注册在智能卡102的手指损坏。例如,此损坏可能是所要辨识手指部分的疤痕。此损坏可能意味无法进行指纹配对,无法由智能卡102授权拥有者。在这情况,该处理器114可经由一系列移动来提示用户进行备份识别/授权检查。因此,用户可具有使用在生物特征验证失败情况下所使用卡片的动作所输入的「密码」。

[0109] 在此备份授权之后,智能卡102可配置成正常使用,或可能具有启用智能卡102的较少操作模式或较少特征之降级模式。例如,如果该智能卡102可作用为一银行卡,则备份授权可允许最大消费限额低于该卡片的通常最大限额的交易。

[0110] 请即参考图4和图5的揭示,将了解,这些显示可用于图2或图3所示智能卡102的生物特征注册的注册系统200、以及进一步其他生物特征验证装置。

[0111] 该注册系统200是针对智能卡的生物特征注册,因此,在此示例中,其使用于经由该智能卡102的指纹传感器130的指纹资料注册期间。该注册系统200包括安装到一固持件202的智能卡102。在此示例中,该固持件202是一折叠卡形状,类似于一礼物卡,具有一用于

保持该智能卡102的凹部204。该凹部204包括切口206,使得能够更容易移开主要藉由密封件(Friction fit)保持在凹部的智能卡102。一凸片208在该凹部204中的智能卡102的顶部上向内延伸,以允许在该固持件上的一电源系统210和在该智能卡102上的接触片212之间进行电接触。该等接触片212由于位于凸片208的下方,因此无法在图4看见,但是相对于图3所示的一压合智能卡102则可看见。所述含有该生物特征验证装置和该固持件的注册系统200配置成藉由邮件传递服务交付给终端用户,而且在这情况,可清楚看见其可藉由邮政服务或快递服务进行交付,因为其形状和尺寸相同于普通信件。为了交付目的,该固持件202和安装其内的该智能卡102将置于信封214内,如图5所示。

[0112] 该固持件202包括电源系统210,该电源系统具有一能够在注册处理期间供电给该智能卡的电源。该电源可例如是具有适当薄外形轮廓的钮扣型电池(手表电池)。该电源系统210更包括一开关配置,该开关配置构造成响应在交付该注册系统之后用户操作该固持件而启动从该电源到该智能卡102的电力供应。在这情况,该固持件202的操作采用打开折叠卡的形式,如箭头216所示。打开卡片可例如移动内滑件及完成电路启动供电给该智能卡102。当该固持件在邮件内时,则该固持件处于关闭状态,因此停止从该电源供电给该智能卡。

[0113] 在针对固持件202的替代配置中,其采用具有保持该智能卡102的内滑件的匣盒形式。在这情况,该固持件202可包括一凸片,当用户拉动时,可从匣盒内部露出该智能卡102。该智能卡102及/或该注册系统可附接到该滑件,而且该滑件可构造成当拉动凸片时从匣盒内部出现(例如,藉由从匣盒开口滑出)。该电源可收容在匣盒内,或者可安装在该滑件上。该滑件的移动用于完成电路以启动供电给该智能卡102。

[0114] 在启动来自该固持件202中电源的供电之后,该注册系统200启用该智能卡102的注册模式,其中该注册模式使用来自该电源的电力,以在注册处理期间供电该智能卡102。经由电源210供电给该智能卡102可简单启用该注册模式。在这情况,最好是藉由启用对所有安全特征的存取之前,需进一步授权步骤,以进一步保护该智能卡102的安全特征(例如,支付功能)。此可类似于对现有银行卡片的卡片启用,因此可能涉及使用在线银行、APP、发卡单位的电话及/或在读卡器(诸如ATM或销售装置点)处使用PIN码。

[0115] 或者或更甚者,该注册系统200可配置成需要附加验证以在启用注册模式之前来确认用户的身份。此选择性特征可利用该固持件202上的一接口及/或该智能卡102上的一界面。该智能卡102上的所述接口可为指纹传感器130,而且此可用于侦测用户与该传感器130的相互作用下的「模式」,如前述。另一可能性是一接口包括在该固持件上,诸如PIN键盘(Pin pad)或允许输入密码的其他接口。

[0116] 该固持件202和该智能卡102之间的相互作用可能受限于电力供应,使得该固持件202包括一简单的电源电路210,该电源电路具有经由开关配置的开关功能且没有其他功能。或者,该固持件202本身可为一「智能型」装置,而且可经由有线或无线通信协议而在该固持件202和该智能卡之间进行数据通信。

[0117] 如图5所示,一支付卡的典型注册处理将因此包括接收密封在信封214内的注册系统200,打开信封214并取出附加有智能卡102的固持件202。举例来说,固持件202在图5中显示为如同图4所示的折叠式卡固持件202。如箭头216所示打开该固持件202,然后启动该智能卡102的注册模式,用户经由在该智能卡102上的传感器130进行注册,然后经由PIN输入

或使用计算机、智能型手机APP或语音呼叫与发卡单位联系来后续启动该智能卡102的支付功能。

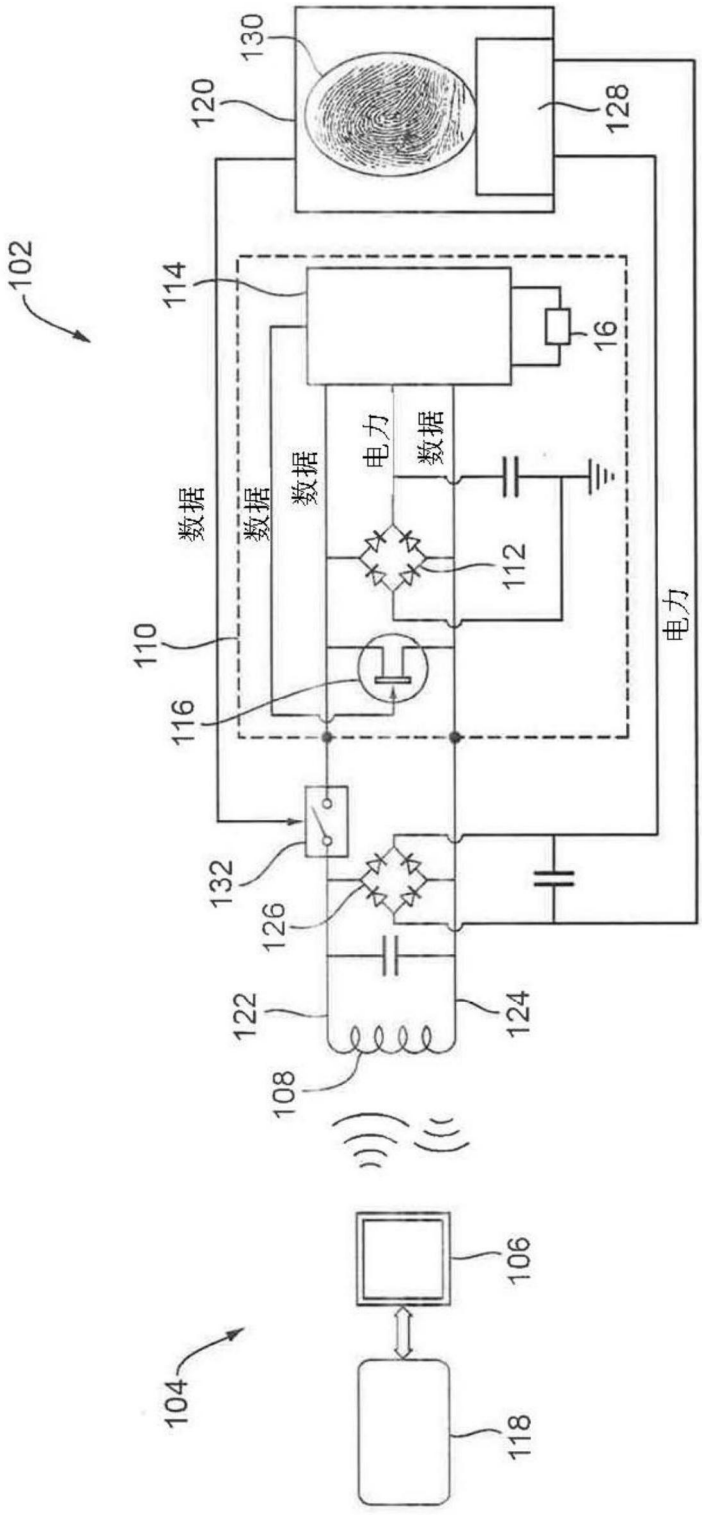

102
104
106
108
110
112
114
116
118
120
122
124
126
128
130
132
16
数据
数据
数据
电力
电力

图1

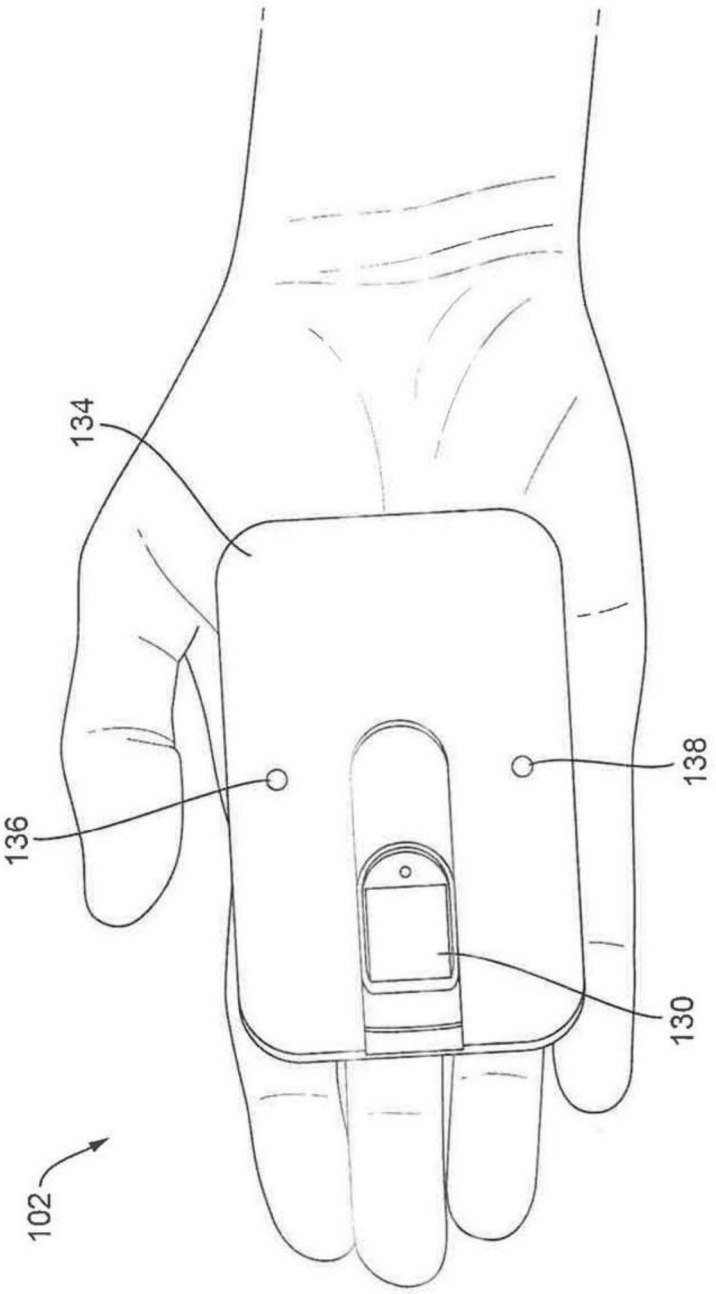



图2

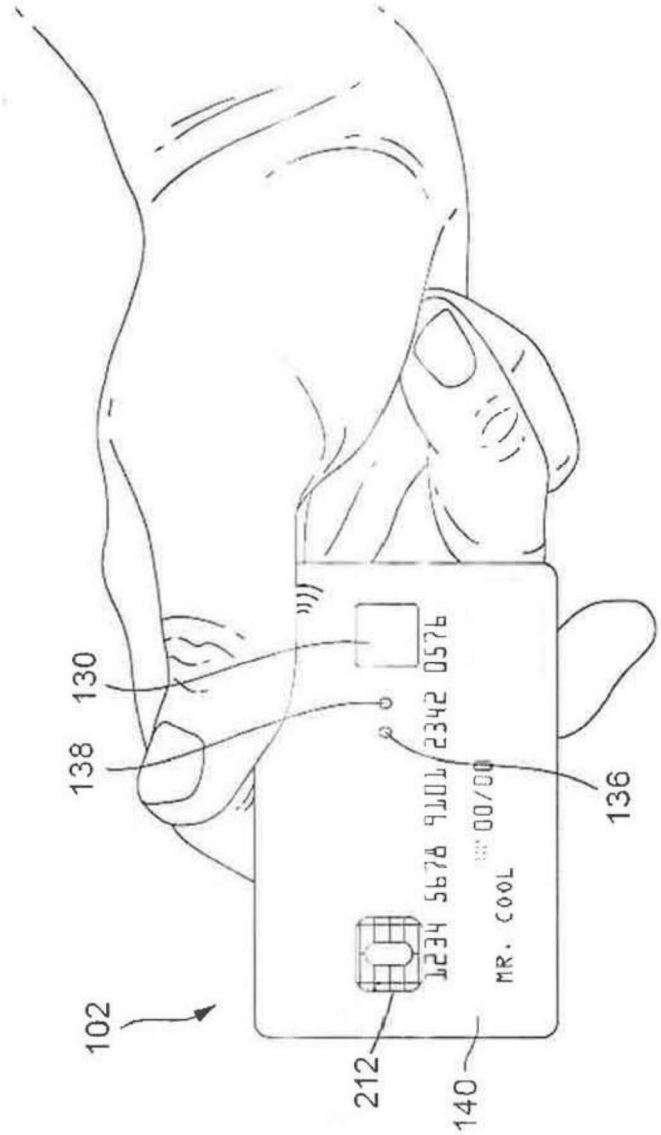



图3

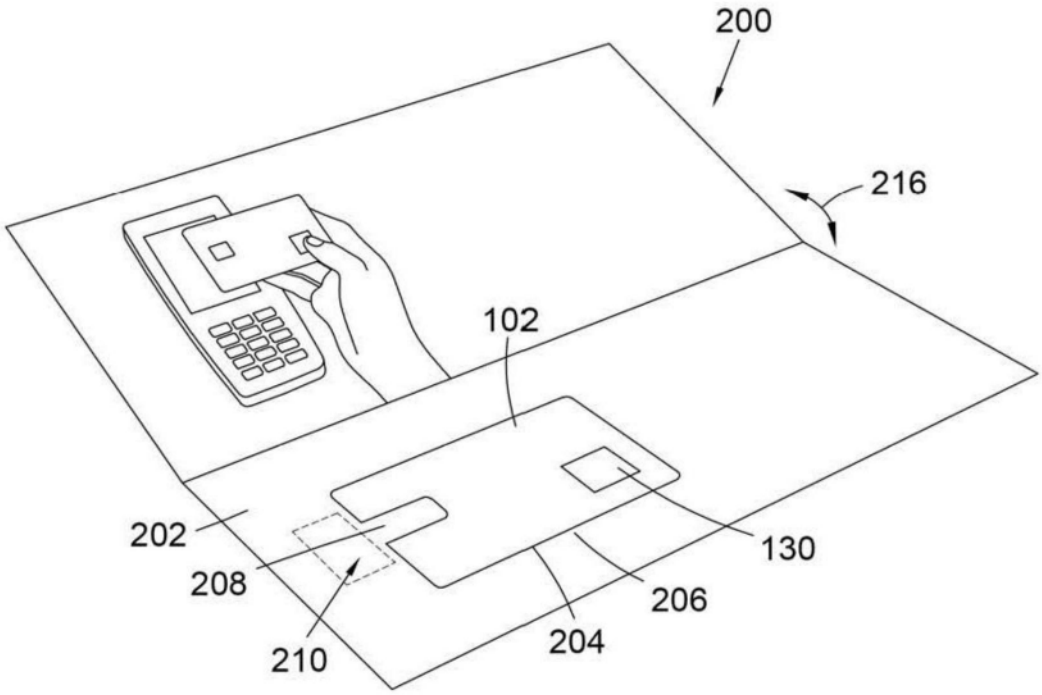

200
216
102
202
208
210
204
206
130

图4

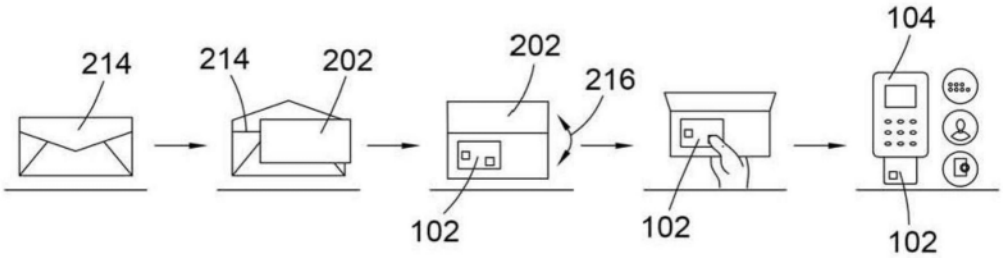

214
214
202
202
216
104
102
102
102

图5