(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 103930899 B
(45)授权公告日 2017.03.08

(21)申请号 201280055916.6
(22)申请日 2012.10.26
(65)同一申请的已公布的文献号
申请公布号 CN 103930899 A
(43)申请公布日 2014.07.16
(30)优先权数据
11290523.7 2011.11.14 EP
61/568,187 2011.12.08 US
(85)PCT国际申请进入国家阶段日
2014.05.14
(86)PCT国际申请的申请数据
PCT/EP2012/071227 2012.10.26
(87)PCT国际申请的公布数据
WO2013/072177 EN 2013.05.23
(73)专利权人 意法爱立信有限公司
地址 瑞士普朗莱乌特尚德菲耶路39号
(72)发明人 赫尔维·西贝尔
尼可拉斯·安奎特
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 杨黎峰 李欣
(51)Int.Cl.
G06F 21/83(2013.01)
G06F 21/74(2013.01)
G06F 21/60(2013.01)
(56)对比文件
US 2009/0282261 A1,2009.11.12,全文.
US 2002/0111920 A1,2002.08.15,全文.
审查员 陈玲

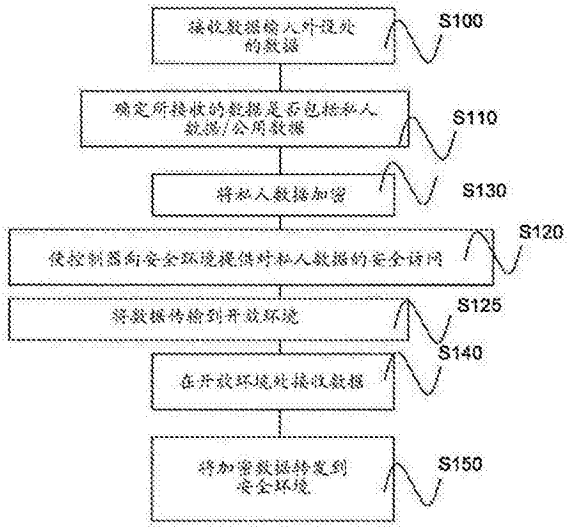
权利要求书2页 说明书11页 附图9页

(54)发明名称

用于管理在设备处输入的公用数据和私人数据的方法

(57)摘要

本发明提出了一种用于管理在设备处输入的公用数据和私人数据的方法，所述设备包括：-数据输入外设；-开放环境，-安全环境，-控制器，所述控制器连接到所述数据输入外设，且所述方法包括下列步骤：-在所述控制器处接收所述数据输入外设处所输入的数据，-在所述控制器处确定所接收的数据是否包括私人数据，-如果所接收的数据包括私人数据，则使所述控制器将对所述私人数据的安全访问提供给所述安全环境，所述控制器通过将操作数据经由所述开放环境发送到所述安全环境来使所述安全环境访问所述私人数据。从安全角度，该方法能够将操作数据和公用数据两者以最小的风险发送到开放环境。



CN 103930899 B

1.一种用于管理在设备(10)处输入的公用数据和私人数据的方法,所述设备(10)包括:

-数据输入外设(12);

-开放环境(24),

-安全环境(26),

-控制器(44),所述控制器(44)连接到所述数据输入外设(12),

且所述方法包括下列步骤:

-在所述控制器(44)处接收所述数据输入外设(12)处所提供的数据,

-在所述控制器(44)处确定所接收的数据是否包括私人数据,

-如果所接收的数据包括私人数据,则所述控制器(44)将对所述私人数据的安全访问提供给所述安全环境(26),所述控制器(44)通过将操作数据经由所述开放环境(24)发送到所述安全环境(26)来使所述安全环境(26)访问所述私人数据,

其中,所述开放环境(24)不能够访问所述私人数据,以及,仅在所述控制器(44)借助所述开放环境(24)请求时,所述安全环境(26)才访问所述私人数据。

2.根据权利要求1所述的方法,其中,所述方法包括下列步骤:

-在所述控制器(44)处确定所接收的数据是否包括公用数据,

-如果所接收的数据包括公用数据,则使所述控制器(44)将所述公用数据传输到所述开放环境(24)。

3.根据权利要求1或2所述的方法,其中,基于通过所述安全环境(26)提供到所述控制器(44)的识别公用数据和私人数据的指令,执行在所述控制器处的确定步骤。

4.根据权利要求1或2所述的方法,其中,所述控制器(44)具有加密能力,且所述方法还包括在所述控制器(44)处将所述私人数据加密成加密数据的步骤,所述操作数据是所述加密数据。

5.根据权利要求4所述的方法,其中,所述方法还包括下列步骤:

-在所述开放环境(24)处接收所述操作数据和未加密的所述公用数据,且将所述加密数据从所述开放环境(24)转发到所述安全环境(26)。

6.根据权利要求5所述的方法,其中,通过在所述控制器(44)中的加密部件或者通过所述控制器(44)的适应软件,提供所述加密能力。

7.根据权利要求5所述的方法,其中,通过高级加密标准AES技术执行所述加密的步骤。

8.根据权利要求1或2所述的方法,其中,所述设备包括仅能够通过所述控制器(44)和所述安全环境(26)访问的缓冲存储器(90)且所述方法还包括下列步骤:

-将所述私人数据从所述控制器(44)传输到所述缓冲存储器(90)。

9.根据权利要求8所述的方法,其中,所述方法包括:

-通过所述控制器(44)检测所述私人数据的长度,

-在所述控制器(44)处生成具有与所述私人数据相同长度的操作数据。

10.根据权利要求9所述的方法,其中,所述方法还包括下列步骤:

-通过所述安全环境(26)读取所述缓冲存储器的内容,

-在所述安全环境(26)处处理通过所述安全环境(26)读取的数据,

-根据在所述安全环境(26)处所获得的处理的数据,在所述开放环境(24)处处理从所

述控制器传输到所述开放环境(24)的所述操作数据。

11.根据权利要求10所述的方法,其中,在所述开放环境(24)处处理的所述步骤在于:通过在所述安全环境(26)处所获得的所述处理的数据替换所述操作数据。

12.一种用于管理输入的公用数据和私人数据的设备(10),包括:

-数据输入外设(12);

-开放环境(24),

-安全环境(26),

-控制器(44),所述控制器(44)连接到所述数据输入外设(12),

其中,所述控制器(44)用于实现根据权利要求1至11中至少一项所述的方法。

13.根据权利要求12所述的设备,其中,所述设备(10)选自移动手持终端、个人数字助理、个人计算机和平板电脑。

用于管理在设备处输入的公用数据和私人数据的方法

技术领域

[0001] 本发明涉及一种用于管理在设备处输入的公用数据和私人数据的方法。本发明还涉及一种适于执行该方法的设备、一种包括用于执行该方法的指令的计算机程序和一种记录有该计算机程序的数据存储介质。

背景技术

[0002] 移动手持终端、以及PC或者平板电脑，通常使用相同的输入装置来用于所有目的。例如，这样的输入装置可以是键盘、鼠标、触敏屏幕。这涉及：运行在该设备上的所有环境共享相同的输入装置。在这些环境之一处理敏感数据的情况下，期望对用户显示的内容和从用户输入的内容仅对于用户和敏感环境而言是已知的。在包括通信系统的数据处理和信息系统上的安全性有助于责任、公平性、精确性、机密性、可操作性以及种类繁多的其他所需标准。

[0003] 控制显示器有多种技术。显示器就像是存储缓冲器(帧缓冲器)，其内容恰好是屏幕显示。使用专用硬件来控制对帧缓冲器的读访问和写访问是可行的。通常，使用专用硬件容易控制对任何输出或者无源外设的访问。例如，控制寄存器可以用于规定哪一个主机可以访问帧缓冲器，该控制寄存器反过来通过平台上的最安全的环境来控制，该最安全的环境决定在该设备上的访问策略。当使用虚拟化方案时，另一可能性是让超级监督者决定哪一个虚拟机可以看见帧缓冲器-且将帧缓冲存储器仅映射到该虚拟机。

[0004] 共享诸如小键盘或触摸屏的输入外设的控制是相当更加复杂的。事实上，当通过外设检测到用户行为时，通过已经正确配置的通用输入/输出(也采用首字母缩略词GPIO来命名)，使用中断和信令来触发中央处理单元(也采用首字母缩略词CPU来命名)。为了能够采用隔离在该中央处理单元上同时运行的环境之间共享该输入外设，可以使用多种技术。

[0005] 已知使用虚拟化方案运行虚拟机和将来自输入外设的通用输入/输出编程和中断限制到超级监督者。每个虚拟机对应于一种环境。超级监督者也称为虚拟机管理器。该超级监督者随后负责决定哪一个虚拟机可以得到输入，且将该输入调度到该虚拟机。该方案的主要缺点是其需要虚拟化方案。在该情况下，由于超级监督者可以被给予该访问，然后应用其本身的策略用于与虚拟机进行交互，故访问控制是静态的。

[0006] 还已知一种技术，其包括：将来自输入外设的GPIO编程和中断限制到可以需要这些输入的最安全的环境。安全环境然后负责决定平台上的哪些环境可以得到输入，且将该输入调度到该环境。因此，每个输入会触发该安全环境中的第一执行。由于运行时间期间的大多数输入专用于另一环境(例如，Linux-注册商标-)，安全环境通常触发开放环境中的执行，提供信息到开放环境。一旦开放环境已完成，则其切换到安全环境以清除最初的输入触发，且再次返回到开放环境中的正常执行。这样的操作不是最有效的。

[0007] 可以考虑另一方案。可以添加专用硬件以使用例如限定哪一个主机具有使用权的控制寄存器，控制输入外设信息(中断，GPIO)的调度以及对GPIO编程接口的访问。反过来，控制寄存器通过最安全的环境来控制。对于不同的环境不需要在超级监督者之上虚拟化。

例如，安全环境和开放环境可以运行在同一CPU上，该CPU使用诸如Trustzone(信任区)(注册商标)的硬件虚拟化。该方案的缺点是，动态保护对GPIO的访问是非常复杂的。因此，该方案的实施几乎是不切实际的。

发明内容

[0008] 本发明的目的是至少部分地减少上述提到的缺点。

[0009] 在第一方面中，本发明提供了一种用于管理在设备处输入的公用数据和私人数据的方法，所述设备包括数据输入外设、开放环境、安全环境、控制器，所述控制器连接到所述数据输入外设。该方法包括下列步骤：在所述控制器处接收所述数据输入外设处所提供的数据；在所述控制器处确定所接收的数据是否包括私人数据；以及如果所接收的数据包括私人数据，则所述控制器将对所述私人数据的安全访问提供给所述安全环境，所述控制器通过将操作数据经由所述开放环境发送到所述安全环境，使所述安全环境访问所述私人数据。

[0010] 本发明的第二方面提供了一种设备，其包括：数据输入外设；开放环境；安全环境；控制器，所述控制器连接到所述数据输入外设，其中，所述控制器适于实现根据本发明的第一方面的方法。

[0011] 本发明的第三方面提供了一种计算机程序，包括用于执行根据本发明的第一方面的方法的指令。

[0012] 本发明的第四方面涉及一种数据存储介质，其上记录有根据本发明的第三方面的计算机程序。

[0013] 从属权利要求限定本发明的各个实施方式。

[0014] 参考下文列举的附图，从作为非限制性示例给出的本发明的实施方式的下列描述，本发明的另外的特征和优点将明显。

[0015] 术语“私人数据”和“公用数据”应该从广义上理解。通常，私人数据是在某个时刻出于防止未授权的人访问数据的目的而隐藏的数据。然而，权利要求书不限于该解释。术语私人数据可替选地认为是第一类数据而公用数据认为是第二类数据。这两类如在权利要求书中的描述分别被处理为私人数据和公用数据。

附图说明

[0016] 图1、图2、图3和图4示出该设备的不同的示意图，

[0017] 图5和图6示出银行用户界面，

[0018] 图7和图8是所提出的方法的两个实施方式的两个流程图，

[0019] 图9和图10是根据现有技术的设备的两个示意图；

[0020] 图11和图12、图14和图15是根据说明性实施方式的设备的示意图；

[0021] 图13是所提出的方法的实施方式的流程图。

具体实施方式

[0022] 提出来一种用于管理在设备处输入的公用数据和私人数据的方法。举例而言，将针对两种使用案例阐明该方法：电话通信和浏览网上银行网站，网上银行网站通过远程服

务器来提供。在以下描述中，电话通信将被称为“案例1”，且浏览网上银行网站将被称为“案例2”。

[0023] 私人数据是特别敏感的且应该以安全方式传输，然而，公用数据不需要特殊保护。在案例1中，私人数据可以是GSM移动电话的pin(个人识别号)码，以及公用数据可以是用于电话通信的电话号码。为了说明，pin码是“1000”以及电话号码是“000000”。在案例2中，当用户输入其银行代码(例如，“0123456789”)时，这应该被视为私人数据，然而点击网上银行网站的标签通常被视为公用数据。可以注意到，在案例1中，私人数据在该设备的内部，而在案例2中，私人数据通过通信网络被发送到外部服务器。

[0024] 所考虑的设备可以是不同的种类。例如，该设备可以是移动手持终端、个人数字助理、个人计算机或者平板电脑。在图1、图2、图3和图4的示意图中阐明了这样的设备10的示例。

[0025] 设备10可包括数据输入外设12。参考图1、图2和图3，这样的外设12能够使由手14象征的用户在设备10中输入数据输入。举例而言，外设12可以是小键盘、键盘、鼠标或触摸屏。

[0026] 根据图1、图2和图3的示例，外设12是触敏屏幕，因此在触摸外设12时，执行用户与用户的交互。如位于屏幕表面上的圆圈16所示，手14的手指与触敏屏幕接触。外设的相应部分是激活的。在图4的示例中，数据输入外设是具有十二个键的数字键盘，十个键18表示从0至9的数字，键20表示符号“*”且键22表示符号“#”。

[0027] 如图2、图3和图4所示，设备10包括开放环境24。开放环境24通常是丰富操作系统(也称为“丰富OS”)。丰富OS是具有丰富容量集且允许用户下载和运行应用程序的高级操作系统环境。Android(注册商标)、Linux(注册商标)、Symbian OS(注册商标)和Microsoft(注册商标)Windows(注册商标)Phone7是该开放环境24的示例。开放环境24专用于公用数据。

[0028] 对比来说，设备10还包括专用于私人数据的安全环境26。安全环境26不可以由用户访问以下载和运行应用程序，也不可以通过开放环境24访问以下载和运行应用程序。因此，安全环境26是安全的而免受任何外部攻击。更一般地，与安全环境26相比，开放环境24应该理解为在安全性方面有较少要求的执行环境。

[0029] 例如，在设备10中安全环境26和开放环境24的这样的组合适于案例1和案例2。在案例1中，安全环境26检查所输入的PIN码是否是正确的码，而开放环境24确保基于通过用户在设备10中所输入的电话号码建立通信。

[0030] 案例2可以通过图5来阐明，图5是从互联网可以访问的银行界面28的示意图。该银行界面包括通过银行服务器提供的同时显示的两个区域29、42。根据图5的示例，第一区域29是银行界面28的所有用户共用的公用区域。第一区域29可包括图像，这里诸如为银行名称30和分别标有“你的银行”32、“计数、卡和服务”34、“证券交易”36、“储蓄”38或者“财产”40的选择标签。在选择一个标签32、34、36、38或40时，通过服务器可以提供另外的信息，其可以包括显示新的信息。由于待提供到服务器的公用数据是不敏感的，故第一区域29通过运行在开放环境24上的应用程序来控制。

[0031] 第二区域42可以是私人区域，其可以通过特定用户来访问。在该私人区域中输入用户的银行代码。由于用户的银行代码是敏感数据，故第二区域通过运行在安全环境26上的应用程序来控制。

[0032] 在两种案例中，安全环境26和开放环境24的组合确保私人数据不可由任何外部攻击来访问。如下文中的说明，图6对应于图5，图6是根据本发明获得的银行界面28，而图5示出根据现有技术获得的银行界面28。

[0033] 设备10还包括控制器44，该控制器44连接到数据输入外设12。控制器44适于执行用于管理在设备10上输入的公用数据和私人数据的方法。

[0034] 图7是在控制器44中可以实施的用于管理公用数据和私人数据的方法的示例性流程图。该方法包括步骤S100：在所述控制器44处接收数据输入外设12处所输入的数据。该数据可以包括公用数据和私人数据两者。

[0035] 在案例1中，在用于输入PIN码的区域中输入的数据是“1000”以及在用于输入电话号码的区域中输入的数据是“000000”。在案例2中，数据在于在用户输入用户的银行代码的区域中输入“01234”，然后点击标签。

[0036] 在步骤S110处，确定所接收的数据是否包括私人数据。同时，该方法还可包括确定所接收的数据是否包括公用数据的步骤。至于仅存在两个替选例，即数据要么是公用的，要么是私人的，则同时执行确定步骤确保了更快的确定。

[0037] 在案例1中，数据“1000”被确定为私人数据而数据“000000”被确定为公用数据。在案例2中，数据“01234”被确定为私人的，而在标签上的点击被确定为公用数据。

[0038] 基于通过安全环境26提供到控制器44的指令，可以执行该确定步骤S110。这些指令能够在私人数据和公用数据之间做出区分。私人数据用于安全环境26而公用数据用于开放环境24。

[0039] 举例而言，识别公用数据和私人数据的指令可包括对用户输入私人数据的地点的指示。参考图4和图5，在私人区域42中所输入的数据应该被视为私人数据，而在公用区域29中所输入的数据应该被视为公用数据。这些示例可以被实施用于案例1和案例2两者。

[0040] 根据图4的具体示例，数据输入外设12是键盘。可以认为，十个数字键18是第一组键以及两个其他的键20、22是第二组键。在该实施方式中，识别公用数据和私人数据的指令可包括将采用第一组键所输入的数据视为私人数据以及将采用第二组键所输入的数据视为公用数据的指令。因此，公用数据和私人数据的识别对于控制器更容易。事实上，包含数字的数据是私人数据，而公用数据不包含数字。这也可以被应用到案例2，其中，私人数据是代码且公用数据仅是在标签上的点击。

[0041] 根据图7的流程图的方法还包括条件步骤S120：使控制器44向安全环境26提供对私人数据的安全访问，控制器44通过将操作数据借助开放环境24发送到安全环境26，使安全环境26访问所述私人数据。如果所接收的数据包括私人数据，则执行该步骤。

[0042] 这意味着，在案例1中，安全环境26可以访问通过用户输入的数据“1000”，以及在案例2中，安全环境26可以访问数据“01234”。基于控制器44的请求进行该访问。

[0043] 因此，开放环境24不可以访问私人数据，以及，仅在控制器44借助开放环境24请求时，安全环境26才访问私人数据。

[0044] 根据图7的流程图的方法还包括另一个条件步骤S125：使所述控制器44将所述公用数据传输到所述开放环境24。如果所接收的数据包括公用数据，则执行该步骤。

[0045] 在案例1和案例2中，因为如上文的解释，所输入的数据包含公用数据，故执行步骤S125。更具体地，在案例1中，电话号码“000000”被传输到开放环境24以及，在案例2中，用户

已点击标签的信息被传输到开放环境24。

[0046] 因此，该方法能够将操作数据和公用数据两者发送到开放环境24，而从安全性观点来看风险最小，尤其是窃取的风险受到限制。由于公用数据被直接发送到开放环境24而没有经过安全环境26，在设备10和开放环境24之间的交互变得更快，这导致通过用户对设备10上的开放环境24的应用程序的激活的要求和设备10上的所需的应用程序的激活之间的延迟最小化。

[0047] 此外，所提出的方法可以以相对容易的方式实施。具体而言，从图3和图4的描述可以推断，设备10的不同元件的架构不需要可动态地配置，以属于安全环境26或者不属于安全环境26。这也适用于GPIO。

[0048] 根据具体实施方式，用于管理在设备处输入的公用数据和私人数据的方法可以是图8的流程图。在该情况中，控制器44具有加密能力。加密能力是对数据加密的能力。加密术或者密码学的通用领域用在电子商务、无线通信、广播中且具有无限制的应用范围。在电子商务中，加密术用来防止诈骗和确认金融交易。在数据处理系统中，加密术用来核实参与者的身份。加密术还用来防止黑客行为、保护网页和防止对保密文献的访问。

[0049] 基于通过外部服务器所提供的密钥，可以执行该加密。通过将部件添加到控制器，可以对控制器提供加密能力。这是图2和图4的情况，其中，硬件部件48对控制器44提供其加密能力。

[0050] 通过对控制器44的软件重新编程，也可以对控制器44提供加密能力。只要重新编程能够使传统控制器适于用于管理数据的方法，则重新编程是特别有利的。图3示出该情况的示例。

[0051] 根据图8的流程图，该方法包括如参考图7的流程图的方法所描述的接收数据的步骤S100和确定步骤S110。该方法还包括在控制器44处将私人数据加密的步骤S130。一旦已经执行步骤S130，则用于安全环境26的数据被加密而用于开放环境24的数据是不加密的。

[0052] 数据的该加密不应该与标准通信设备中所用的用于借助外部网络通信的加密方法混淆。事实上，传统地，安全服务器提供密钥给安全环境26，其中，私人数据在通过网络发送之前被加密。在标准通信设备中所用的这样的加密方法可以充当外部加密，而根据图8的流程图的实施方式的加密可以被理解为内部加密，这是由于该密钥仅在设备10的内部部件或者软件之间共享。

[0053] 为了执行该加密，在步骤S110处将指令提供到控制器44的情况下，提供到控制器44的指令还可以包括待用来加密私人数据的加密参数。

[0054] 例如，用于像CCM的AES加密认证模式的密钥和初始化向量可以被提供在指令中。高级加密标准或AES(也称为密钥生成算法Rijndael)是采用对称加密的算法，其在2000年10月通过NIST被选为用于美国政府组织的加密标准。通过对称，这意味着相同的密钥(也称为秘密钥匙)被用来加密数据和解密数据。在该情况中，所加密的数据被称为密码数据(cypherdata)。CCM模式是用于用密码写的分组密码的操作模式。加密认证算法被设计成提供认证和机密性。当用于像CCM的AES加密认证模式的密钥和初始化向量被提供在指令中时，加密步骤130可以通过AES技术来执行。

[0055] 对于图3的示例，设备10设置有传感子系统46，该传感子系统46包括传感处理器45和加密软件54。通过传感处理器45的加密软件54所用的用来加密第一数据的加密参数通过

安全环境26来选择并且在受保护的消息中发送。例如，加密参数可以被存储在通过安全环境和传感子系统46所共享的存储器中。

[0056] 根据图2和图4的实施方式，指令被提供到部件44且包括识别待加密的数据和公用数据的指示和用来加密私人数据的加密参数。

[0057] 作为基本示例，在说明书的其余部分中将认为：将数据编码在于在控制器处将一连串1加到数据的各位以及从加密数据的各位减去一连串1以解密该数据。因此，对于案例1，加密数据是“2111”，然而，对于案例2，加密数据是“12345”。

[0058] 根据图8的流程图，该方法还包括步骤S120：使控制器44将对私人数据的安全访问提供给安全环境26，控制器44通过将操作数据借助开放环境24发送到安全环境26，使安全环境26访问私人数据。在该具体实施方式中，操作数据是加密数据。如果所接收的数据包括私人数据，则执行该步骤。

[0059] 根据图8的流程图的方法还包括条件步骤S125：使所述控制器44将公用数据传输到所述开放环境24。如果所接收的数据包括公用数据，则执行该步骤。

[0060] 对于案例1，这意味着，数据“2111000000”被传输到开放环境。在案例2中，所传输的数据是“12345”以及随后的用户已输入的对标签的点击的信息。

[0061] 因此，该方法确保公用数据和操作数据二者被传输到开放环境24，而从安全性角度看有最小的风险，尤其是窃取风险受到限制。由于公用数据被直接发送到开放环境24而没有经过安全环境26，因此在设备10和开放环境24之间的交互变快，这导致在通过用户在其设备10处的对开放环境24的应用程序的激活的要求和其设备10处的所需的应用程序的激活之间的延迟最小化。

[0062] 此外，仅需要安全传输的数据被加密。这意味着，加密步骤S130比其用来加密每个数据更有效。事实上，用于开放环境24的数据然后将被加密，这是无用的。

[0063] 此外，所提出的方法可以以相对容易的方式实施。具体而言，从图3和图4的描述可以推断，设备10的不同元件的架构不需要可动态地配置，以属于安全环境26或者不属于安全环境26。这也适用于GPIO。

[0064] 根据图8的方法还包括步骤S140：在开放环境24处接收加密的数据和未加密的公用数据。如上文的解释，对于案例1，这意味着，通过开放环境24接收数据“2111000000”。在案例2中，所接收的数据是“12345”和随后的由用户已输入的对标签的点击的信息。

[0065] 该方法还包括步骤S150：将加密数据从开放环境24转发到安全环境26。这意味着，开放环境24能够在公用数据和操作数据之间进行确定。例如，如果公用数据不包含任何数字，操作数据包含数字，则确定是容易的。包括数字的所有的数据被转发到安全环境。

[0066] 在案例1中，数据“2111”被发送到安全环境26，以及在案例2中，数据“2345”被发送到安全环境26。

[0067] 根据另一实施方式，该方法可包括另外的步骤：在安全环境26处处理数据。该步骤可包括加密数据的解密。按照本发明的基本示例，解密过程在于从各位减去1。因此，对于案例1，当解密时，数据“2111”变为“1000”。对于案例2，获得数据“01234”。

[0068] 此外，在案例1中，处理的步骤可包括认证过程。事实上，所输入的数据可以与PIN码比较。在案例1中，所输入的数据和PIN码是相同的，该结果为设备的用户是正确的用户。

[0069] 在案例2中，处理的步骤可包括标准加密过程，使得私人数据可以通过非安全的网

络(诸如,互联网)来传输。

[0070] 与示出不同的使用时刻的相同的现有技术的图9和图10的示意图相比,对于案例2的根据图8的方法所提供的优点还可以通过图11的示意图来说明。图9示出在设备10中的控制器44、开放环境24和安全环境26之间的交互。图9是其中数据输入外设12是触敏屏幕的示例。图9的控制器44包括在现有技术已知的微控制器56(在图9上标记为"传感MCU")的传感器上运行的传感固件50(在图9上标记为"传感FW")。开放环境24包括主中央处理单元(CPU)58、丰富操作系统60和用于允许较高级应用程序与触敏屏幕交互的触敏屏幕驱动62。开放环境24包括多个应用程序,一个应用程序能够借助互联网67访问外部服务器64。根据图9,外部服务器64包括加密部件,例如,用于加密在服务器和与服务器连接的客户端之间的通信的加密部件。还可以说,服务器64是安全服务器。外部服务器64通过网络浏览器66和Javascript68的组合与开放环境24交互。在网络浏览器中所需的功能可以通过信任插件来提供。对插件的信任是指,浏览器的操作对于目前的目标来说是可以信任的。此外,插件可以在信任环境中执行。插件提供了在javascript68和信任输入信任应用程序("TA")74之间的连接。例如,触敏屏幕驱动62能够检测,特定的标签已经通过用户在网络浏览器66中激活,且该所检测的信息可以被发送到服务器64。安全环境26也包括主CPU70和信任执行环境(也以首字母缩略词"TEE"命名)72。TEE72是与丰富操作系统60同时运行的独立执行环境。TEE72对丰富环境60提供安全服务且将对其硬件和软件安全资源的访问与丰富操作系统60及其应用程序隔离。安全环境26还包括信任输入信任应用程序(在图9上称为"信任输入TA")74。信任输入TA74能够借助在开放环境24的javascript功能和信任输入TA74之间的交互82将私人数据从安全环境26传送到服务器64。

[0071] 公用数据流借助控制器44被传输到开放环境24。公用数据流通过图9上的线78来表示。更具体地,公用数据通过数据输入外设12输入,然后经过传感微控制器56和在微控制器56上运行的传感固件50。公用数据然后依次被发送到开放环境24的主CPU58、丰富操作系统60和触敏屏幕驱动62。在该期间,公用数据可以被处理和/或修改。例如,用户按压屏幕的特定区域以在选择相应的标签32、34、36、38或40时,激活显示。在触敏屏幕驱动62侧,该数据被转换成激活链接到通过用户所选择的标签32、34、36、38或40的应用程序。

[0072] 私人数据流被传输到安全环境26而不经过控制器44。私人数据流通过图9上的线80来表示。更具体地,私人数据通过数据输入外设12输入,然后经过安全环境26的主CPU70、TEE72和信任输入TA74。在该传输期间,私人数据可以被处理和/或修改。例如,用户输入PIN码,且该PIN码通过信任输入TA74认证,信任输入TA74发送关于在所输入的PIN码和在安全环境26中所存储的PIN码之间的比较的信息。

[0073] 在根据图9和图10的示例中,数据的管理是有顺序的。这通过以下事实来说明:说明公用数据流的线78在图9上是连续的,而说明私人数据流的线80在图9上是断开的。与此相反,说明私人数据流的线80在图10上是连续的,而说明公用数据流的线78在图10上是断开的。连续的线对应于数据流实际上被传输的事实,而断开的线对应于数据流没有被传输的事实。更详细地,这意味着,在图9上,仅公用数据被传输到开放环境24,而在图10上,仅私人数据被传输到安全环境26。换句话说,在根据现有技术的示例中,公用数据被传输或者私人数据被传输,但这两种数据不能同时都被传输。

[0074] 对于想要与互联网银行网页交互的用户,这导致图5的使用案例的情形。当用户开

始输入私人数据时，标准用户界面冻结。这意味着，用户不能与该标准用户界面交互，其中，公用数据输入在标准用户界面中。这通过窗口中的阴影线33示意性地示出。例如，在开放环境24是Windows® OS的情况下，灰色是阿尔法混合的。事实上，仅一部分屏幕通过安全环境26来管理，其作为输入和输出。这导致以下事实：当用户试图输入私人数据时，仅基本用户体验被支持。用于设备10的相应的情形是图10中的情形。因此，用户交互的结果被加密，然后被发送到安全服务器64用于处理。但是，通过安全银行服务器64管理一个密钥76。

[0075] 为了便于比较，只要有关，在图11中保留与图9和图10中相同的附图标记。图11的控制器44还包括流控制器84和AES加密软件86。该软件86能够基于通过信任输入TA74提供的信任输入密钥88来加密数据。

[0076] 与图9和10中表示的流相比，图11的公用数据流和私人数据流不同。这标志着根据图11的在设备10中进行用于管理公用数据和私人数据的不同方法。

[0077] 事实上，在图11中，公用数据流通过数据输入外设12输入，然后经过传感微控制器56和传感固件50。数据然后被发送到流控制器84。然后，公用数据被发送到开放环境24的主CPU58，然后经过丰富操作系统60，最后被发送到触敏屏幕驱动62。

[0078] 私人数据流通过数据输入外设12输入，然后经过传感微控制器56和传感固件50。该数据然后被发送到流控制器84，然后到AES加密软件86。在该软件中，使用AES技术加密私人数据。然后，加密数据被发送到开放环境24的主CPU58，然后经过丰富操作系统60，最后被发送到触敏屏幕驱动62。此后，所加密的私人数据被发送到TEE72，然后到信任输入TA74。私人数据在具有密钥88的信任输入TA74中被解密，该密钥先前被提供到软件86用于实现AES技术。

[0079] 表示私人数据流的线80和表示公用数据流的线78都是连续的线，其指示相应的数据流实际上被传输。换句话说，这意味着，根据图11的方法并不是像图9和图10中所示的现有技术中那样是有顺序的。

[0080] 如在案例2中，对于想要与互联网银行网页交互的用户，这导致图6的使用案例的情形。当用户开始输入私人数据时，银行界面28的标准用户界面不再被冻结。这意味着，用户可以与该标准用户界面交互，标准用户界面中，输入公用数据。HTML页面通过开放环境24的标准网络浏览器66来呈现。当触摸专用于私人数据的区域42时，网络浏览器javascript68接收表示以下事实的加密数据：数据已经输入在专用于私人数据的区域42中。浏览器调用安全环境26以处理该输入事件。该安全环境26解密该加密数据。通过用户所输入的数据然后被推断且通过信任输入TA74利用通过安全服务器76所提供的密钥76加密。应该理解，通过安全服务器76所提供的密钥76不同于通过信任输入TA74提供到加密软件86的密钥88。密钥88仅通过安全环境26和控制器44共享。换句话说，在该实施方式中，存在两个密钥：一个密钥通过TEE72来管理，另一个密钥通过安全银行服务器76来管理。通过来自安全银行服务器64的密钥76所加密的数据以HTML的形式被发送到安全服务器64用于进一步处理。在所有该操作期间，所有的公用区域对于用户是可进入的。这导致以下事实：当用户试图输入私人数据时，最佳用户体验通过设备10来支持。

[0081] 此外，在图10、图8和图9之间的比较表明：该方法可以在标准设备中容易地实施。仅需要控制器的重新程序设计。

[0082] 这导致以下事实：关于案例2，优选执行根据图11的用于管理私人数据和公用数据

的方法。

[0083] 图12等效于图11，但用于案例1。因此，安全服务器64被网络96替换，该网络96与在开放环境24中所包含的通信应用程序98交互。通信应用程序98替换图11的网络浏览器66和javascript66。如上文所解释的，在该情况下，私人数据是PIN码“1000”以及公用数据是电话号码“000000”。在该情况中，仅存在一个加密密钥86，该加密密钥86是通过安全环境26和控制器44所共享的密钥86。

[0084] 从前文描述的图11可以推断，图3的实施方式尤其适于触敏屏幕。在该实施方式中，通过输入外设12所发出的数据在嵌入有传感处理器45(运行通过安全环境26认证的信任软件的微控制器单元)的子系统46中处理。处理器45从硬件输入外设12获得通过元件16所获取的纯数据，并且执行所接收的数据的处理/转化的多个步骤，以便产生通过包含在开放环境24中的开放环境驱动27可以利用的数据。安全环境26通过安全信道与软件54通信以在所处理的数据被发送到开放环境24之前打开和关闭所处理的数据的加密。在特定的实施方式中，安全环境26可以告知传感处理器45，在触摸屏中的哪个输入区域要被保护。菜单选择因此可以保持不加密。

[0085] 图3的实施方式尤其适于触敏屏幕，在此程度上，该实施方式需要一些智能以从来自触敏屏幕的信号提取可利用的数据。软件的传感处理器45被信任，在这种程度上，其被认证且因此是合法的。没有特定需求其是机密的，故其源代码可以完全开放。

[0086] 对比之下，在根据图4的实施方式中，外设12是小键盘或者键盘。在开放环境24中的驱动将加密数据转发到安全环境26，安全环境在解密层之上实现其本身的外设驱动。该实施方式尤其适于硬件小键盘，硬件小键盘发出可以直接解译的数据。在该实施方式中，硬件部件44还可以对安全环境26提供控制以选择哪些输入条目必须被加密(例如，仅小键盘，但不是功能键)。与图3的实施方式类似，菜单选择可以保持不加密。

[0087] 根据另一特定实施方式，用于管理在设备处所输入的公用数据和私人数据的方法可以是图13的流程图的方法，图14的示意图中示出案例2的使用的示例。在该情况中，设备10包括仅通过安全环境26和控制器44可以访问的缓冲存储器90(在图14上标记为用于信任区保护的缓冲器的TZ保护缓冲器)。因此，缓冲存储器90应该理解为安全存储器，开放环境24不能访问该存储器90。

[0088] 根据图13的流程图的方法包括参照图8的流程图的方法所描述的在数据输入外设21处接收数据的步骤S100和确定步骤S110。根据图13的流程图的方法还包括从控制器将数据传输到开放环境的步骤S120。在图13的流程图的示例中，该方法还包括将私人数据从控制器传输到缓冲存储器90的步骤S200。

[0089] 除了上文提到的优点之外，在该实施方式中，私人数据和公用数据被管理而不使用加密，其可以更容易实施。

[0090] 在图13的具体实施方式中，该方法还包括通过控制器44检测私人数据的长度的步骤S160。该方法还包括在控制器44处生成与私人数据相同长度的数据的步骤S170。所生成的数据是虚拟数据。虚拟数据是仅符合规定条件(此处是长度)的在计算机中所输入的字符或其他条信息。例如，如果代码“0123456789”是用户的银行代码，则虚拟数据可以是“0xDEADBEEF”。在该示例中，所生成的数据“0xDEADBEEF”因此表示存在私人数据“0123456789”。在将数据从控制器44传输到开放环境24的步骤S120处，公用数据和如

“0xDEADBEEF”的虚拟数据被传输到开放环境24。

[0091] 如所示出的，传输步骤S200的执行与检测步骤S160、生成步骤S170和将数据从控制器传输到开放环境的步骤S120同时进行，但是其可以在另一时刻执行。

[0092] 根据图13的流程图，该方法还包括读取缓冲存储器90的内容的步骤S210。读取步骤在安全环境26处实现。在处理所读取的数据的步骤S220处，数据还在安全环境26中被处理。例如，处理数据可在于将它们与在安全环境26中已经存储的其他数据比较。该方法还包括另一步骤S230：根据在安全环境26处所获得的处理的数据，在开放环境24处处理从控制器44传输到开放环境24的数据。举例来说，对于案例1，仅在所输入的PIN码是正确的PIN码的情况下，该设备将拨打电话号码。

[0093] 当与图8和图9的示意图比较时，通过根据图13的方法所提供的优点还可以通过图14的示意图来说明。

[0094] 在相关的情况下，在图14中保持与图9和图10和图11中相同的附图标记。图14的控制器还包括流控制器84。

[0095] 与图9和图10中所示出的流相比，图14中的公用数据流和私人数据流是不同的。这标志着用于管理公用数据和私人数据的不同方法在根据图14的设备中执行。

[0096] 事实上，在图14中，公用数据流通过数据输入外设12输入，然后经过传感微控制器56和在传感微控制器56上运行的传感固件50。数据然后被发送到流控制器84。然后，公用数据被发送到开放环境24的主CPU58，然后经过丰富操作系统60，最后被发送到触敏屏幕驱动62。

[0097] 私人数据流通过数据输入外设12输入，然后经过传感微控制器56和在传感微控制器56上运行的传感固件50。该私人数据然后被发送到流控制器86。流控制器86检测私人数据的长度且生成虚拟数据。然后，虚拟数据被发送到开放环境24的主CPU58，然后经过丰富操作系统60，最后被发送到触敏屏幕驱动62。开放环境24然后要求信任输入TA74应该如何处理该虚拟数据。虚拟数据是用于开放环境24的指示，其指示安全环境26期待该输入。

[0098] 私人数据被发送到信任输入TA74可以访问的信任区所保护的缓冲器(称为TZ保护缓冲器)90。该访问由断线73表示。信任输入TA74基于开放环境24的请求访问TZ保护缓冲器90。

[0099] 因此，表示私人数据流和公用数据流的线78和线80都是连续的，其指示相应的数据流事实上被传输。换句话说，这意味着，根据图14的方法不是像图9和图10中所示的现有技术中那样是顺序的。从图11和图9、图10之间以前做出的比较推断出的相同优势也通过该实施方式提供给设备10的用户。

[0100] 此外，与图11的实施方式比较，图14的实施方式能够使实际触敏屏幕信息被存储在TZ保护缓冲器中，而无需内部加密。

[0101] 图15与图14等同，但用于案例1。因此，安全服务器64用网络96替换，该网络96与开放环境24中含有的通信应用程序98交互。通信应用程序98替换图14的网络浏览器66和javascript66。如上文的解释，在该情况中，私人数据是PIN码“1000”，公用数据是电话号码“000000”。在该情况中，仅存在一个加密密钥86，该加密密钥86是安全环境26和控制器44所共享的密钥86。

[0102] 在每个实施方式中，基于包括用于执行该方法的指令的计算机程序，可以执行该

方法。程序可在可编程设备上执行。如果需要，则应用程序可以在高阶程序的或者面向对象的编程语言上或者以汇编语言或机器语言实施。在任一情况下，语言可以是编译语言或解译语言。程序可以是全安装程序或者更新程序。在后一情况下，程序是这样的更新程序，该更新程序将预先编程为执行该方法的一部分的可编程设备更新到适于执行整个方法的设备的状态。

[0103] 程序可以记录在数据存储介质上。数据存储介质可以是适于记录计算机指令的任一存储器。因此，数据存储介质可以是任一形式的非易失性存储器，例如，包括：半导体存储装置，诸如，EPROM、EEPROM，和闪存装置；磁盘，诸如，内置硬盘和移动硬盘；磁光盘；和CD-ROM盘。

[0104] 参考优选的实施方式已经描述了本发明。然而，在本发明的范围内可以有多个变型。

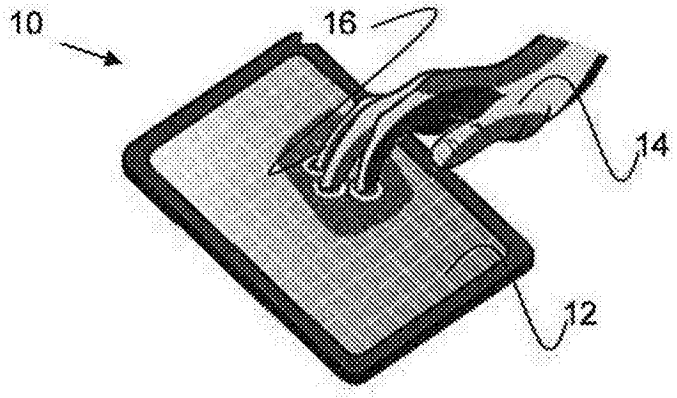


图1

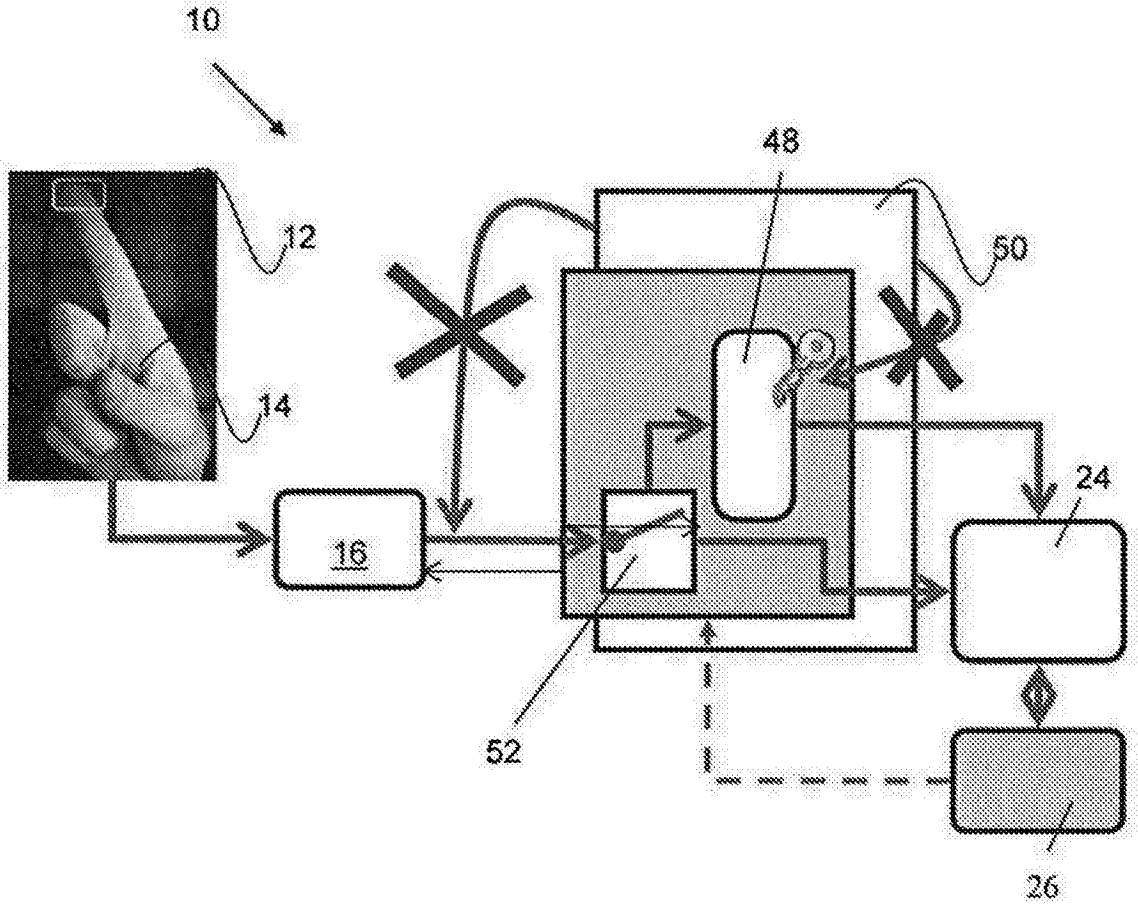


图2

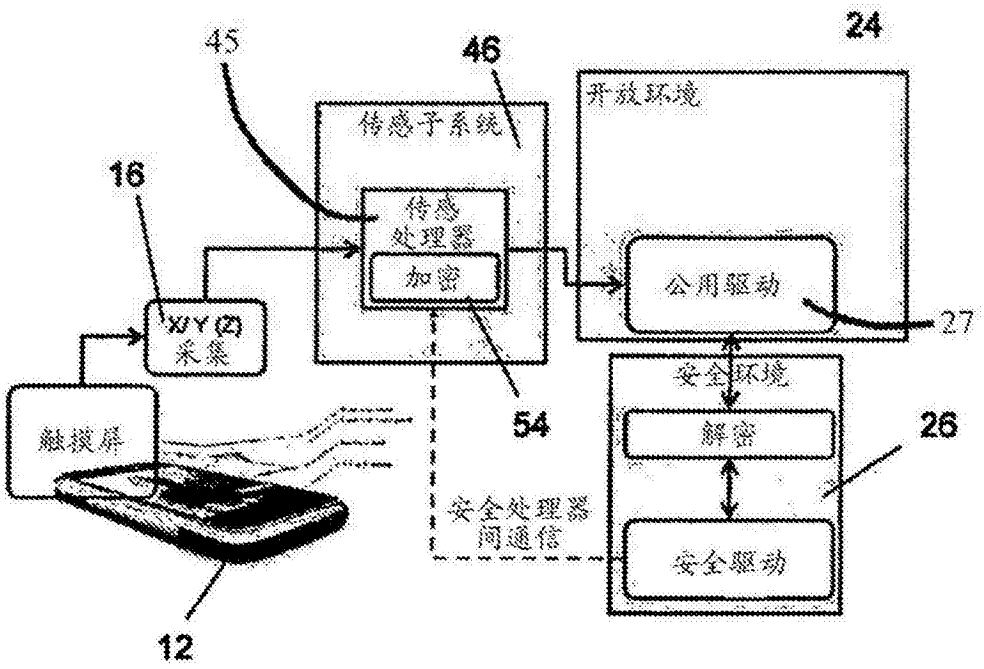

45
46
24
传感子系统
开放环境
16
传感处理器
加密
公用驱动
27
X/Y (Z) 采集
触摸屏
54
安全环境
解密
26
安全处理器间通信
安全驱动
12

图3

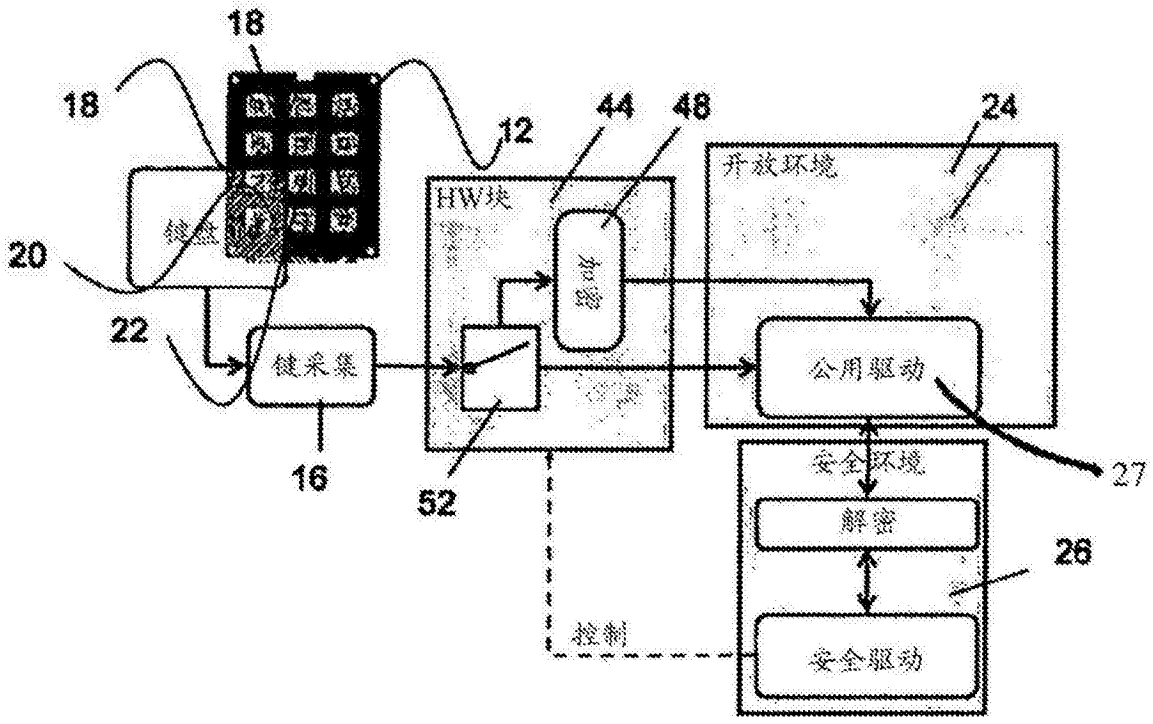

18
18
12
44
48
24
开放环境
HW块
20
键盘
密钥
22
键采集
公用驱动
27
安全环境
16
52
解密
26
控制
安全驱动

图4

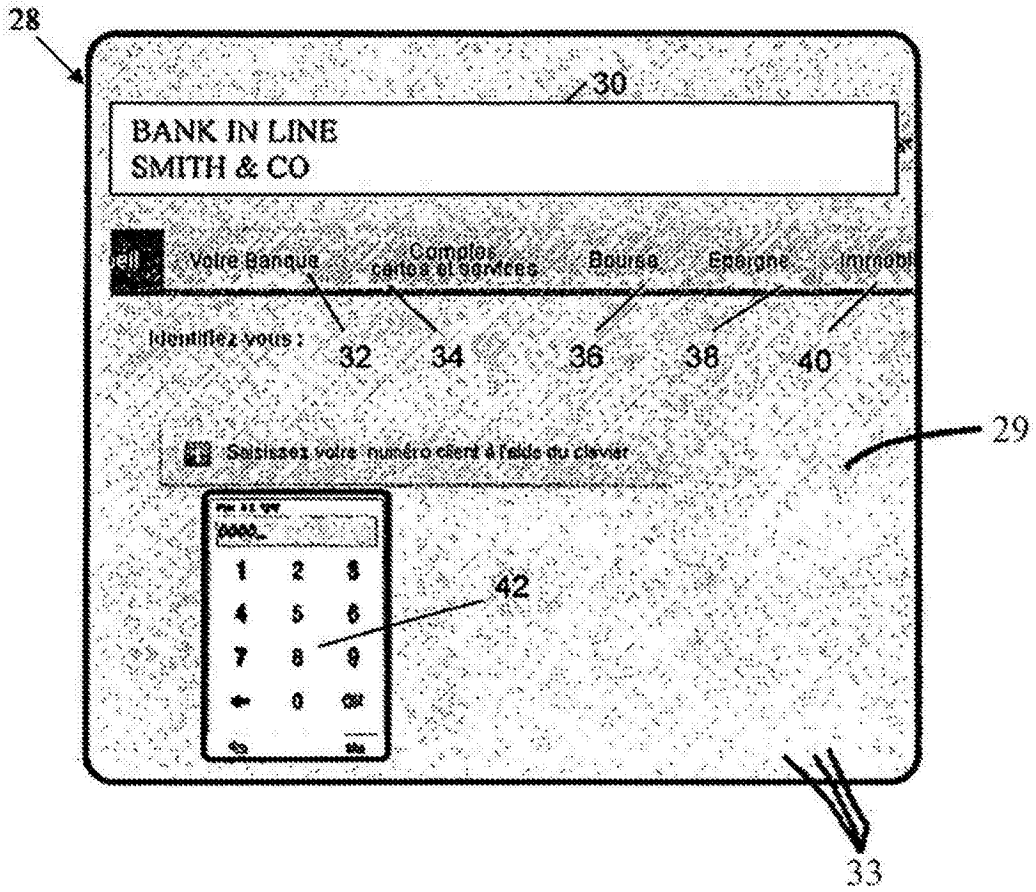

28
30
BANK IN LINE
SMITH & CO
Votre Banque
Comptes cartes et services
Bourse
Epargne
Identifiez vous :
32
34
36
38
40
29
42
33

图5

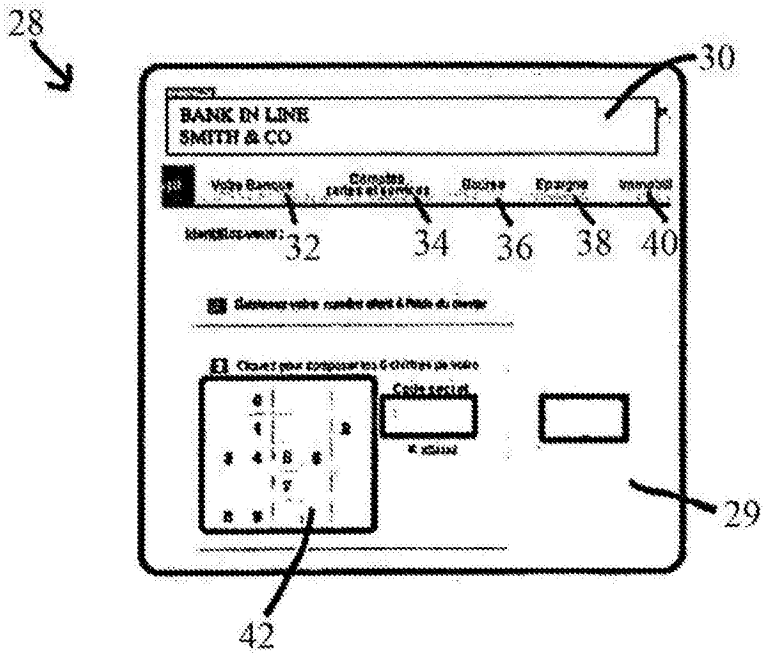

28
30
BANK IN LINE
SMITH & CO
32
34
36
38
40
29
42

图6

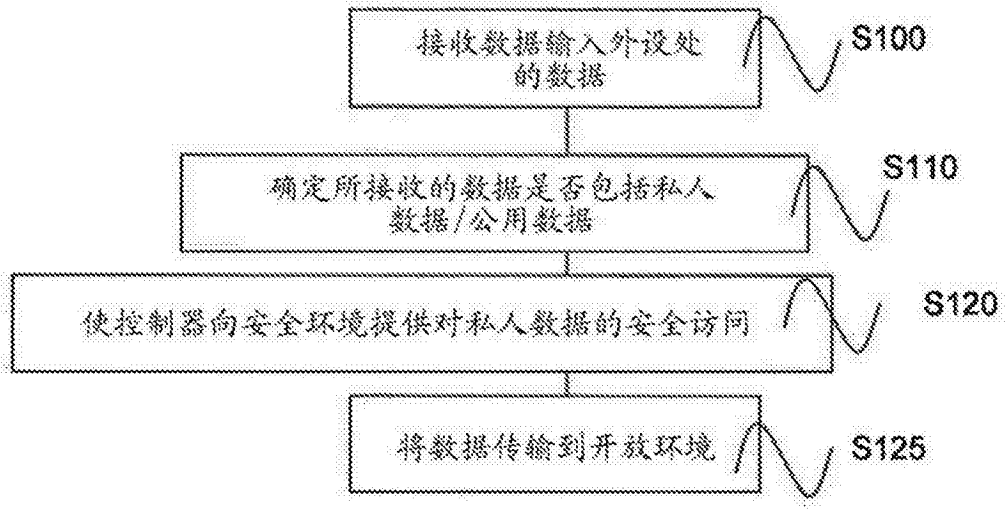

接收数据输入外设处的数据
S100
确定所接收的数据是否包括私人数据/公用数据
S110
使控制器向安全环境提供对私人数据的安全访问
S120
将数据传输到开放环境
S125

图7

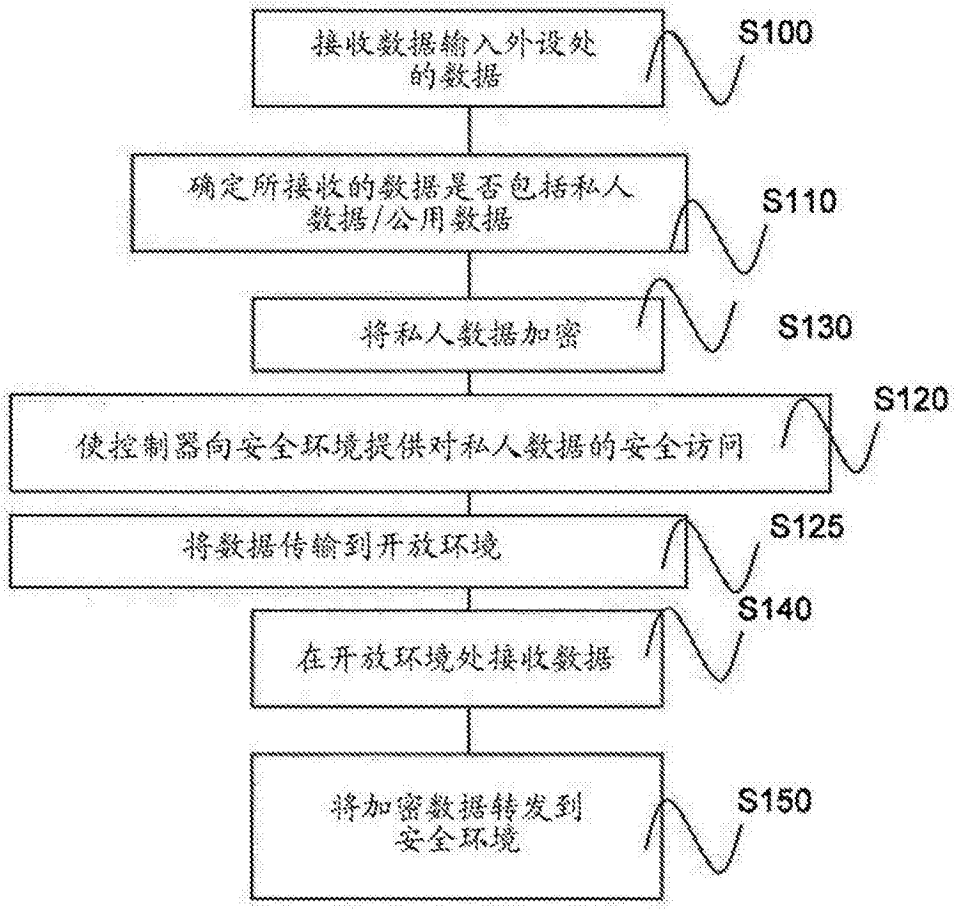

接收数据输入外设处的数据
S100
确定所接收的数据是否包括私人数据/公用数据
S110
将私人数据加密
S130
使控制器向安全环境提供对私人数据的安全访问
S120
将数据传输到开放环境
S125
在开放环境处接收数据
S140
将加密数据转发到安全环境
S150

图8

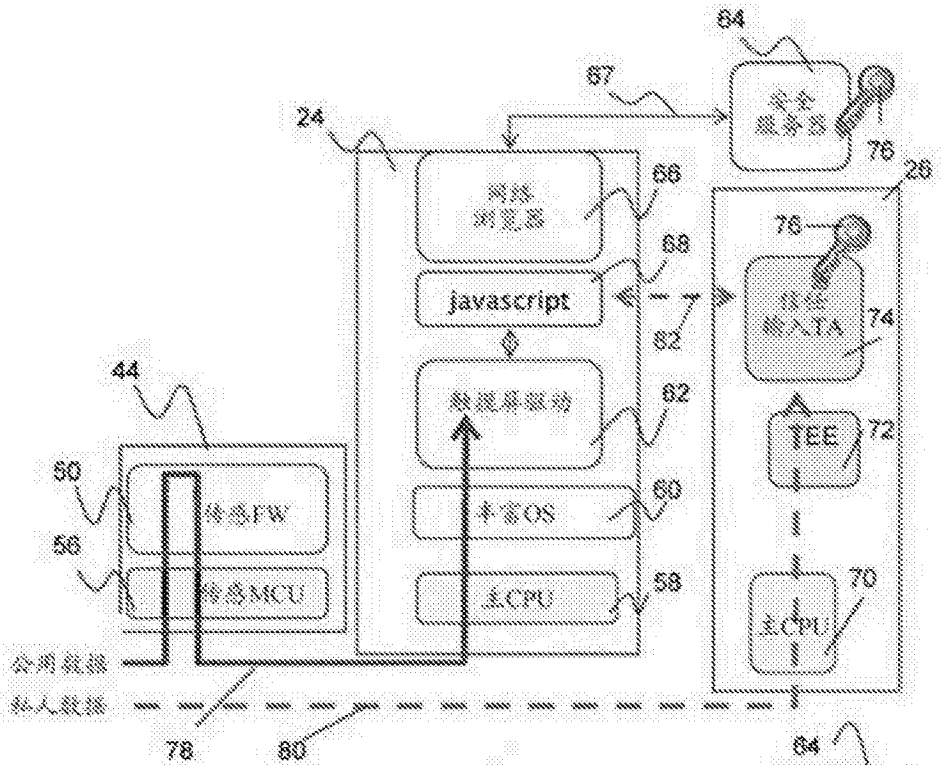

84
67
24
66
68
javascript
82
76
26
78
74
TEE
72
44
62
60
58
70
50
56
78
80
84

图9

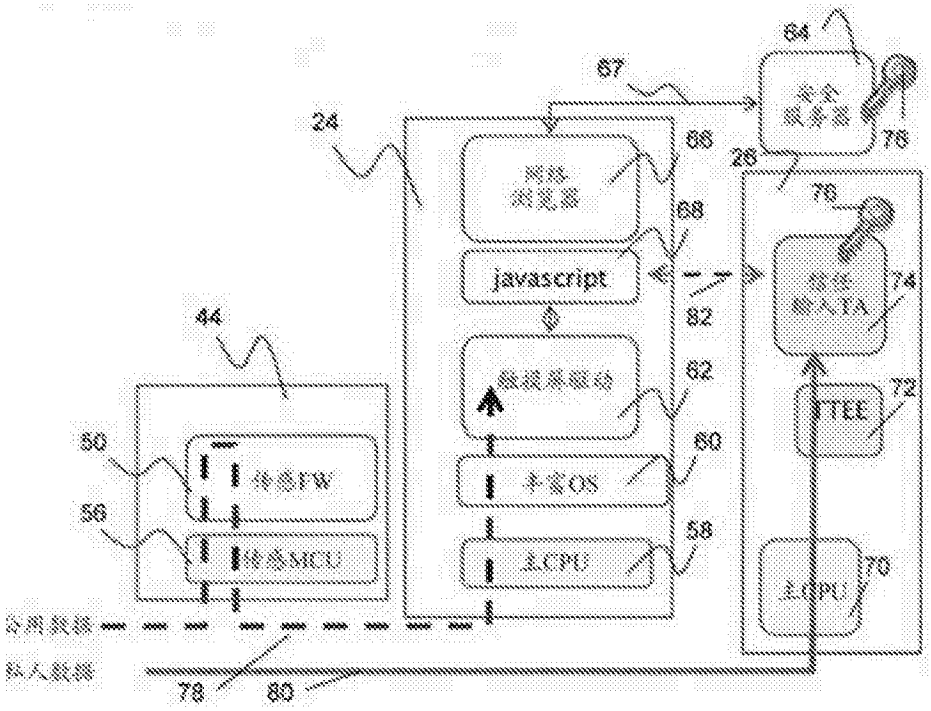

84
67
24
66
68
javascript
82
76
26
78
74
TEE
72
44
62
60
58
70
50
56
78
80

图10

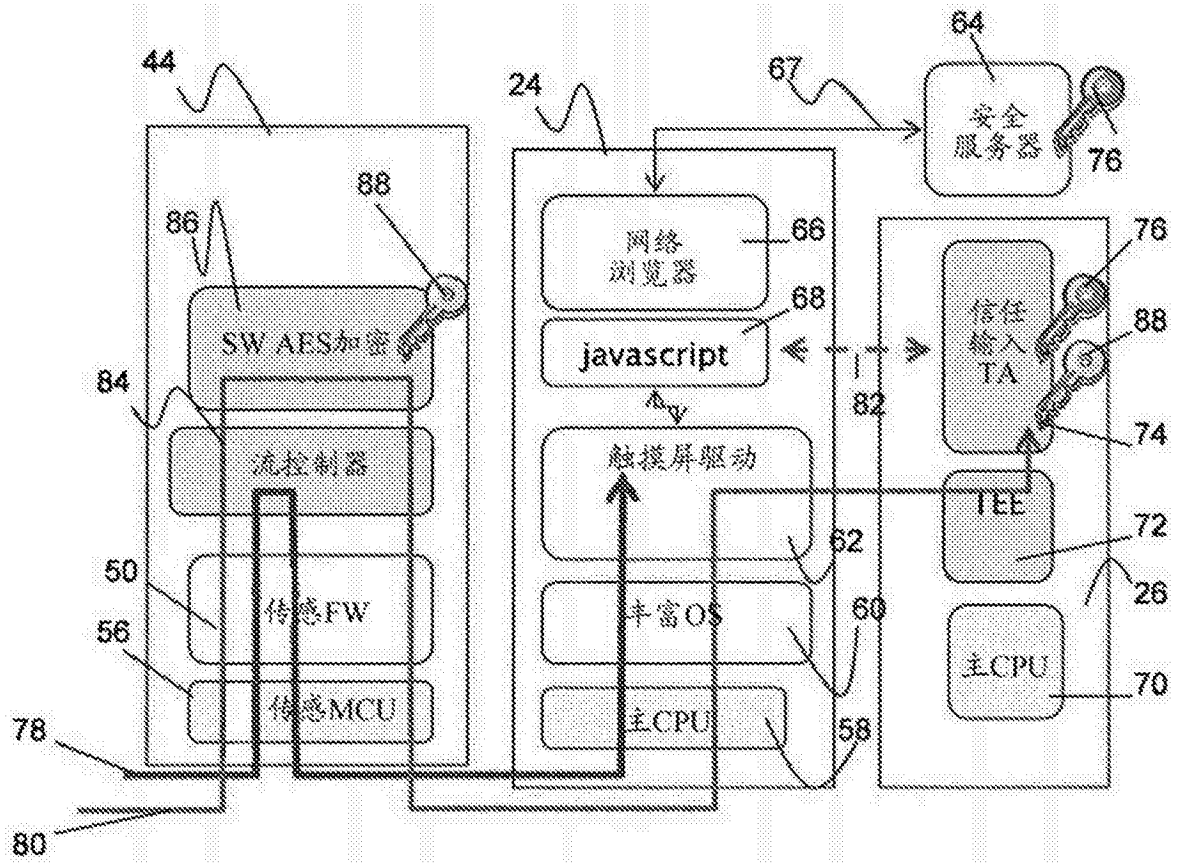

44
24
67
64
安全
服务器
76
88
86
网络
浏览器
66
76
SW AES加密
68
javascript
信任
输入
TA
88
84
流控制器
82
74
触摸屏驱动
TEE
62
72
50
传感FW
丰富OS
60
26
56
传感MCU
主CPU
70
78
主CPU
58
80

图11

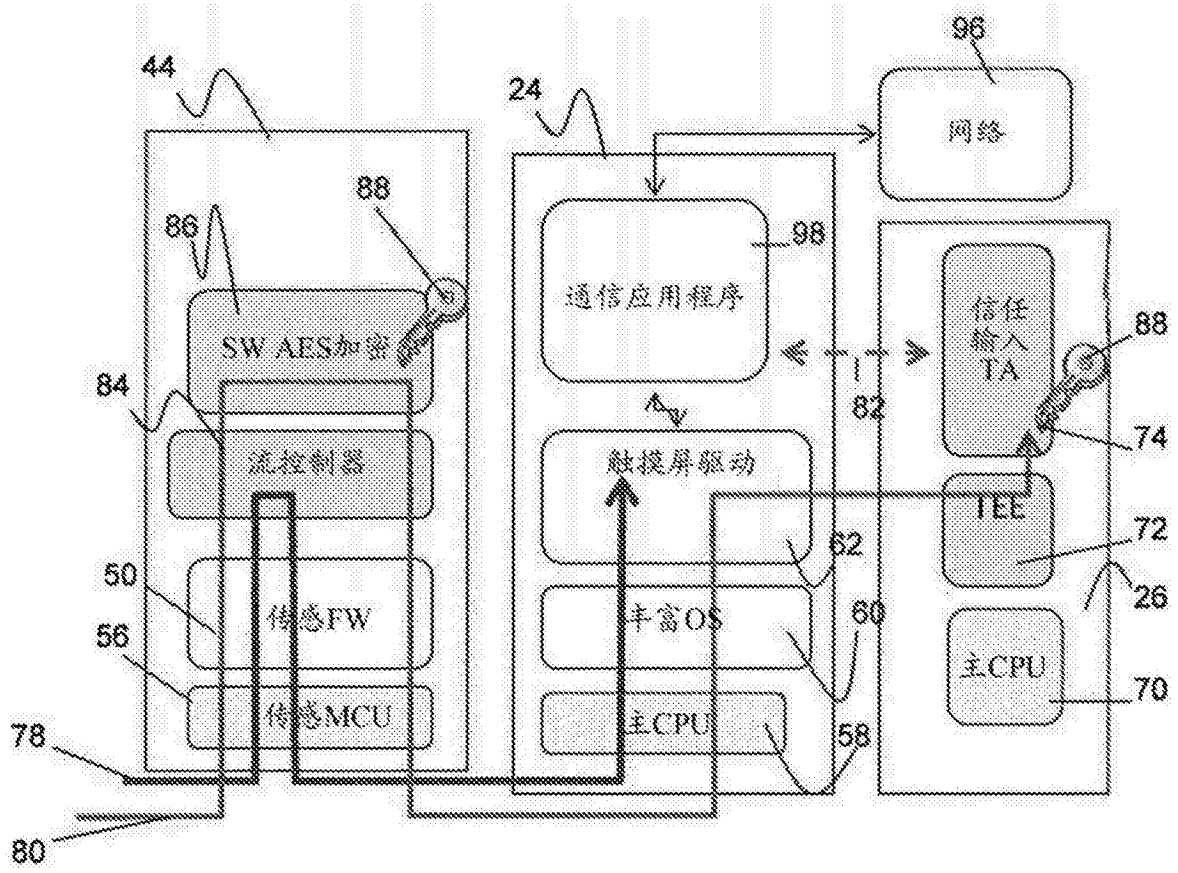

44
24
96
网络
88
86
98
通信应用程序
信任输入TA
88
SW AES加密
84
流控制器
82
74
触摸屏驱动
TEE
72
62
50
传感FW
丰富OS
60
26
56
传感MCU
主CPU
70
78
主CPU
58
80

图12

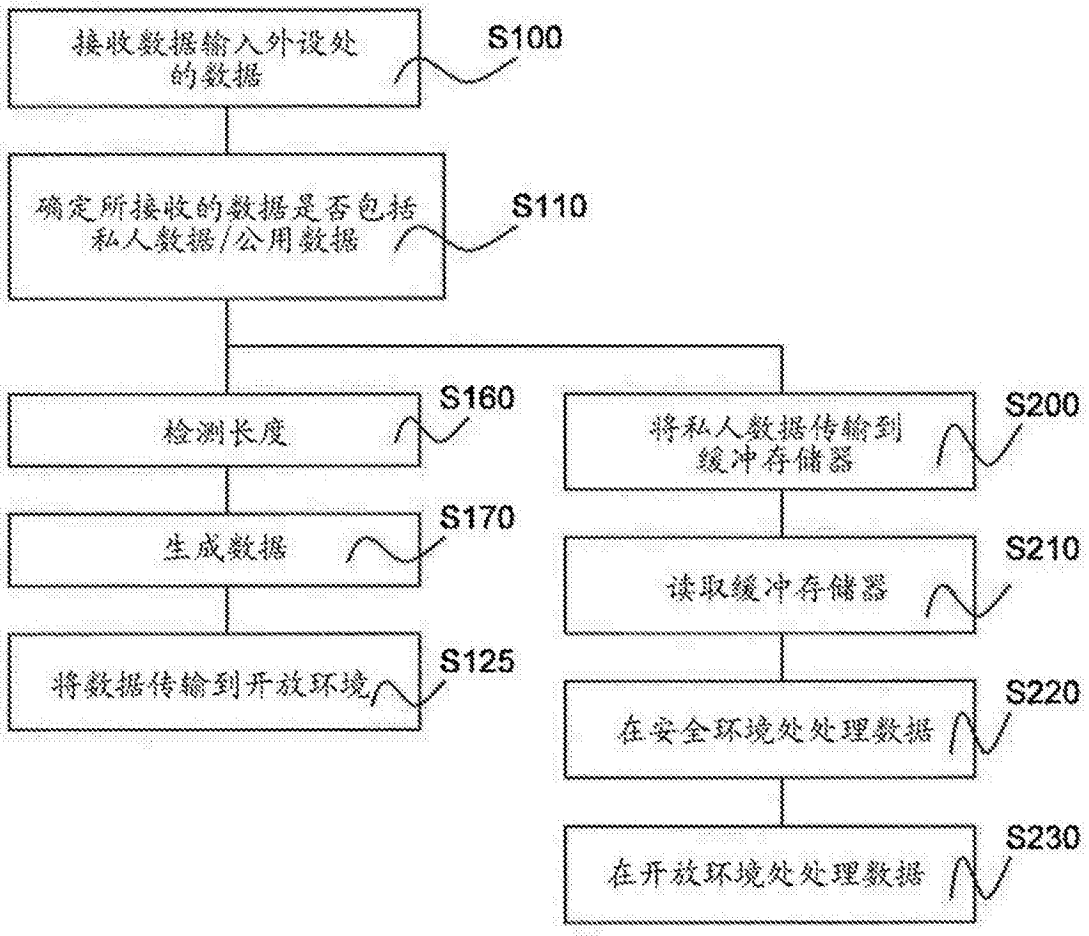

接收数据输入外设处的数据
S100
确定所接收的数据是否包括私人数据/公用数据
S110
检测长度
S160
生成数据
S170
将数据传输到开放环境
S125
将私人数据传输到缓冲存储器
S200
读取缓冲存储器
S210
在安全环境处处理数据
S220
在开放环境处处理数据
S230

图13

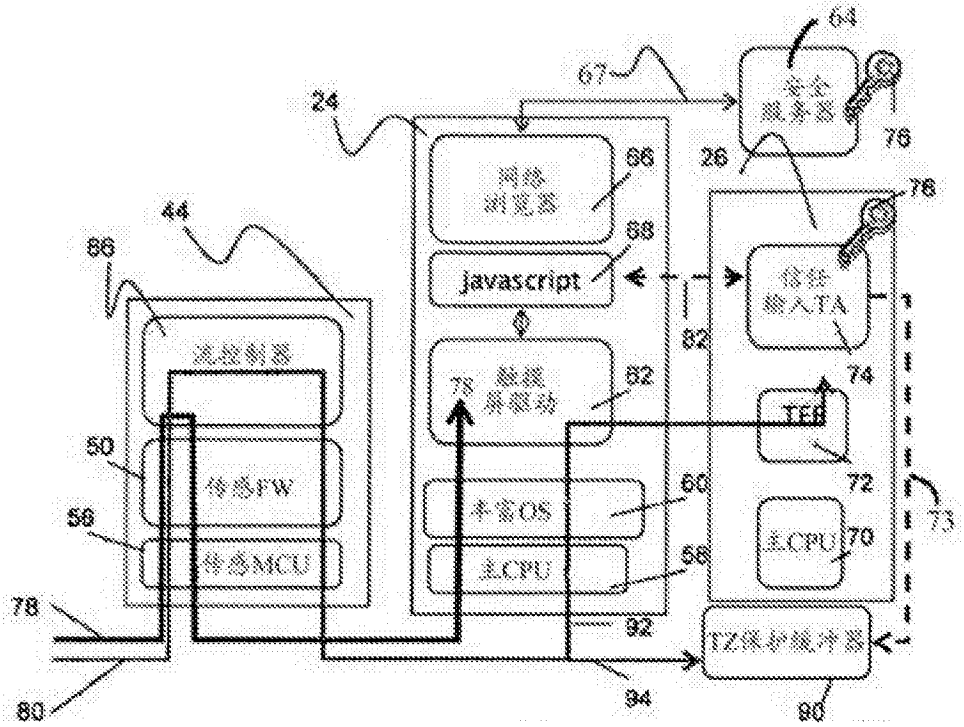

64
67
24
26
76
66
68
44
86
javascript
82
78
82
74
TEE
50
72
60
73
56
70
58
78
92
94
80
90

图14

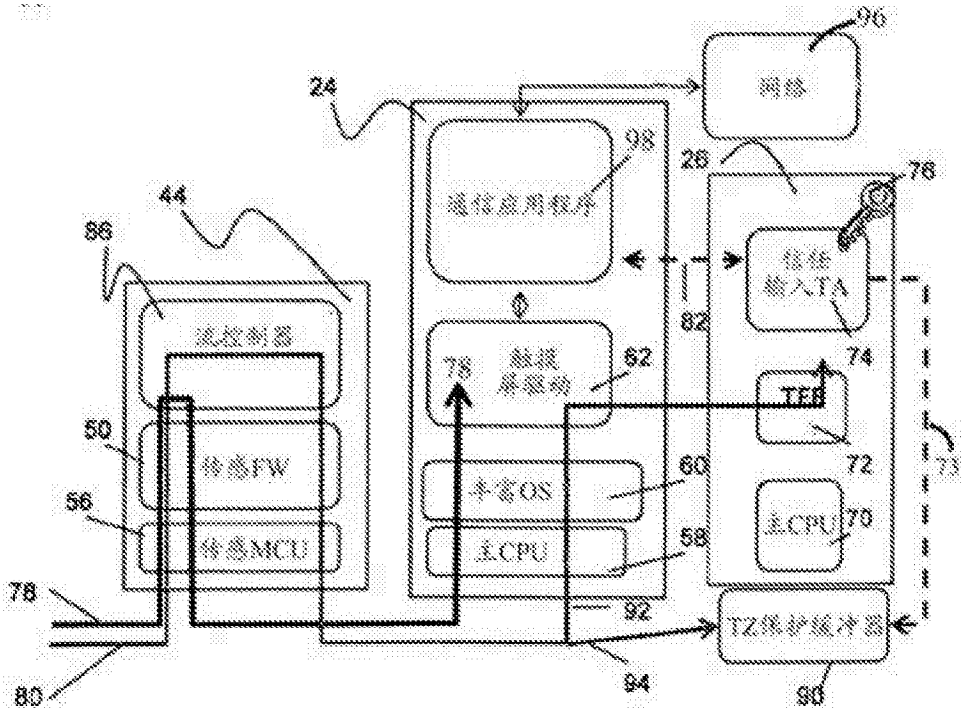

96
24
98
26
76
44
86
82
78
62
74
TEE
50
72
60
73
56
70
58
78
92
94
80
90

图15