



(12) 发明专利申请

(10) 申请公布号 CN 105160254 A

(43) 申请公布日 2015. 12. 16

(21) 申请号 201510423882. 7

(22) 申请日 2015. 06. 05

(30) 优先权数据

1455186 2014. 06. 06 FR

(71) 申请人 欧贝特科技公司

地址 法国科隆贝

(72) 发明人 O·查雷 N·布斯凯

(74) 专利代理机构 北京市中咨律师事务所

11247

代理人 雷明 马江立

(51) Int. Cl.

G06F 21/57(2013. 01)

G06F 21/74(2013. 01)

G06F 21/31(2013. 01)

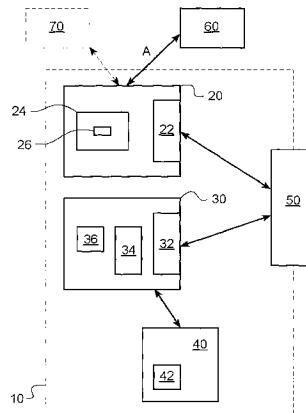
权利要求书1页 说明书8页 附图3页

(54) 发明名称

包括安全电子单元的电子设备和用这种电子设备实施的方法

(57) 摘要

本发明涉及一种电子设备 (10)，它包括第一处理器和配备有第二处理器的安全电子单元 (40)，该电子设备 (10) 设计成通过可信操作系统 (30) 的第一处理器的执行来运转。位于安全电子单元 (40) 之外并且不同于该可信操作系统 (30) 的构件 (20) 设计成触发第二处理器对应用程序 (42) 的执行，由该第二处理器执行的应用程序 (42) 设计成请求实施可信操作系统 (30) 的服务。本发明还涉及在该电子设备中实施的方法。



1. 一种电子设备 (10 ;80), 包括第一处理器和配备有第二处理器的安全电子单元 (40 ;86), 该电子设备 (10 ;80) 设计成借助于可信操作系统 (30) 的第一处理器的执行来运转, 其特征在于, 设有位于安全电子单元 (40 ;86) 外部且不同于该可信操作系统 (30) 的构件 (20 ;88), 以便触发第二处理器对应用程序 (42) 的执行, 以及, 由第二处理器执行的应用程序 (42) 设计成请求实施可信操作系统 (30) 的服务。
2. 根据权利要求 1 所述的电子设备, 其中, 该不同的构件为在电子设备中实施的多功能操作系统 (20)。
3. 根据权利要求 2 所述的电子设备, 其中, 所述多功能操作系统 (20) 设计成由第一处理器来执行。
4. 根据权利要求 3 所述的电子设备, 包括基于多功能操作系统 (20) 的功能和基于可信操作系统 (30) 的功能之间的功能切换的切换装置。
5. 根据权利要求 2 所述的电子设备, 其中, 所述电子设备包括第三处理器, 并且该多功能操作系统 (20) 设计成由该第三处理器来执行。
6. 根据权利要求 1 所述的电子设备, 其中, 该不同的构件为该电子设备 (80) 的通信模块 (88)。
7. 根据权利要求 1-6 之一所述的电子设备, 其中, 该不同的构件 (20 ;88) 设计成直接控制第二处理器以触发对应用程序 (42) 的执行。
8. 根据权利要求 1-6 之一所述的电子设备, 其中, 该不同的构件 (20) 设计成将触发应用程序的执行的命令发送到可信操作系统 (30), 该可信操作系统 (30) 设计成控制由第二处理器进行的应用程序 (42) 的执行。
9. 根据权利要求 8 且从属于权利要求 4 所述的电子设备, 其中, 该切换装置设计成将基于多功能操作系统 (20) 的功能切换到基于可信操作系统 (30) 的功能, 以发送触发命令。
10. 根据权利要求 1-6 之一所述的电子设备, 其中, 所述服务包括实施电子设备 (10 ;80) 的外围设备 (50 ;84) 的功能性。
11. 根据权利要求 10 所述的电子设备, 其中, 所述外围设备为电子设备 (10 ;80) 的人 - 机界面 (50 ;84)。
12. 根据权利要求 1-6 之一所述的电子设备, 其中, 所述服务包括在该电子设备 (10 ;80) 的人 - 机界面 (50 ;84) 上返回信息。
13. 根据权利要求 1-6 之一所述的电子设备, 其中, 所述服务包括接收用户识别信息。
14. 一种电子设备 (10 ;80) 的实施方法, 该电子设备包括第一处理器和配备有第二处理器的安全电子单元 (40 ;86), 该电子设备 (10 ;80) 设计成借助于可信操作系统 (30) 的第一处理器的执行来运转, 该方法包括如下步骤:
 - 通过位于该安全电子单元 (40 ;86) 外部并且不同于该可信操作系统 (30) 的构件触发由该第二处理器执行的应用程序 (42) 的执行;
 - 通过由该第二处理器执行的应用程序 (42) 来请求该可信操作系统 (30) 实施服务。

包括安全电子单元的电子设备和用这种电子设备实施的方法

技术领域

- [0001] 本发明涉及电子设备的安全性。
- [0002] 更具体地,本发明涉及包括第一处理器和装配有第二处理器的安全电子单元(实体)的电子设备,该电子设备设计成利用可信操作系统的第一处理器的执行(运行,实施,execution)来运转(运行,起作用)。本发明还涉及用这种电子设备的实施方法。
- [0003] 本发明特别有利地应用于在电子设备上执行多功能操作系统的情况。

背景技术

- [0004] 已知如前所定义的电子设备,一方面通过使用可信操作系统(英文为“Trusted OS”)保证其安全性,其能够提供可信执行环境(或TEE,“Trusted Execution Environment”),其中的一些应用程序仅可被安装和执行,另一方面通过使用安全电子单元保证其安全性,该安全电子单元实施要求高安全级别的处理,如数据的加密处理。
- [0005] 这种电子设备通过还包括非安全构件,例如在电子设备上执行的多功能操作系统(英文为“Rich OS”)。在它们的操作中,这些非安全构件可请求安全功能。
- [0006] 通常在可信操作系统中实施应用程序操控的非安全构件请求安全功能的情况下,加载该应用程序,以在需要时要求处理(典型地为加密)安全电子单元。
- [0007] 理解到,为了使用户执行搜索服务,该解决方案有时需要在非安全构件、可信执行环境和安全电子单元中安装应用程序。

发明内容

- [0008] 在本文中,本发明提供如前所定义的电子设备,其特征在于,设置位于安全电子单元外部并且不同于可信操作系统的构件,以触发(启动)第二处理器对应用程序的执行,以及,由第二处理器执行的应用程序设计成请求实施可信操作系统的服务。
- [0009] 而且,由非安全构件触发执行的应用程序将操控安全功能的实施,并在必要时、例如在由应使用于第二处理器操控的处理程序中的可信操作系统管理电子设备的资源时请求可信操作系统的服务。
- [0010] 因此仅使用可信操作系统提供的基本服务,因此不再需要在可信执行环境中安装专用于由用户实施搜索服务的应用程序。
- [0011] 另外,从安全电子单元操控安全功能,安全电子单元提供的安全级别仍大于由可信执行环境实现的安全级别。
- [0012] 根据第一可能性,所述不同的构件为在电子设备中实施的多功能操作系统。可将这种多功能操作系统设计成通过第一处理器执行。
- [0013] 如在接下来的详细描述中所解释的,可设置在基于多功能操作系统的功能和基于可信操作系统之间的功能切换的装置。
- [0014] 在变化形式中,电子设备可包括第三处理器,该多功能操作系统设计成通过所述

第三处理器执行。

[0015] 根据第二实施可能性，所述不同的构件为电子设备的模块，它同样装配有处理器，例如电子设备的通信模块。

[0016] 应注意，所述不同的构件设计成直接控制第二处理器以触发应用程序的执行，或设计成发送触发应用程序执行的命令到可信操作系统，将可信操作系统设计成通过第二处理器控制应用程序的执行。在前一种情况下，可信操作系统的作用被限制于向第二处理器传输触发指令。

[0017] 前面所提及的切换装置设计成将基于多功能操作系统的功能切换到基于可信操作系统的功能，以发送触发命令。

[0018] 通过第二处理器控制服务的实施，包括例如实施电子设备的外设（例如人-机界面）的功能。

[0019] 所述服务可包括在电子设备的人-机界面上返回信息（如显示或发送声音信号，又或激活振动器）和/或接收用户识别信息（例如授权信息）。

[0020] 本发明还旨在提供电子设备实施的方法，该电子设备包括第一处理器和装配有第二处理器的安全电子单元，该电子设备设计成利用可信操作系统的第二处理器的执行来操作，该方法包括如下步骤：

[0021] - 通过位于安全电子单元外部并且不同于可信操作系统的构件触发第二处理器执行应用程序；

[0022] - 通过由第二处理器执行的应用程序来请求可信操作系统实施服务。

[0023] 上面提供的用于电子设备的可选特征还可应用于所述方法。

附图说明

[0024] 参照附图，通过接下来以举例而非限制性方式给出的详细描述将更好理解本发明的组成和怎样实施本发明。

[0025] 在附图中：

[0026] - 图 1 示意性表示实施本发明的主要构件；

[0027] - 图 2 表示根据本发明的在图 1 的系统构件之间的数据交换方法的第一实施例；

[0028] - 图 3 表示根据本发明的在图 1 所示类型的系统中进行的数据交换方法的第二实施例；

[0029] - 图 4 表示可实施本发明的系统的另一实施例；

[0030] - 图 5 表示在图 4 的系统构件之间交换数据的方法的实施例。

具体实施方式

[0031] 图 1 示意性表示实施本发明的主要构件。

[0032] 所述系统包括电子设备 10，在此为终端（例如智能电话，或英文名称为“smart-phone”），其功能（运行）基于两种不同操作系统的使用：多功能操作系统 20（英文为“Rich OS”）和可信操作系统 30（“Trusted OS”），有时命名为安全操作系统（“Secure OS”）。

[0033] 多功能操作系统 20 能够给予用户较大的下载、安装和执行应用程序的自由度。

[0034] 相反,在基于可信操作系统 30 的电子设备 10 的运行范围内,下载和安装应用程序的可能性受限(例如对于已接收特定认证的应用程序),以使可信操作系统的使用能够在电子设备 10 中形成可信执行环境(或 TEE,“Trusted Execution Environment”)。

[0035] 所述可信执行环境例如提供符合公用标准 EAL(“Evaluation Assurance Level”,评估保证级别)的安全级别,对应于 ISO 15408 标准 - 其中级别在 2-7 之间,或对应于 FIPS(“Federal Information Processing Standard”,联邦信息处理标准)140-2 标准。

[0036] 在此处所描述的实施例中,多功能操作系统 20 和可信操作系统 30 由电子设备的同一处理器执行,例如系统芯片型处理器(Soc,“System on Chip”)。除了处理器,系统芯片包括具有不同功能的另外电子构件,尤其是一个或多个存储器(例如,只读存储器或 ROM,即“Read Only Memory”,随机存取存储器或 RAM,即“Random Access Memory”,和非易失性可重写存储器,例如 EEPROM,即“Electrically Erasable Programmable Read Only Memory”);其中至少一个存储器的一部分预留给可信操作系统 30(即,该存储器部分仅被可信操作系统 30 读取和 / 或写入)。

[0037] 在该情况下,如下文所述的,基于多功能操作系统 20 的电子设备 10 的运行和基于可信操作系统 30 的电子设备 10 的运行之间的切换过程为,使电子设备 10 在每一时刻基于这两个操作系统 20、30 中的单独一个运行。

[0038] 在变化形式中,可使多功能操作系统 20 和可信操作系统 30 分别实施为两个专用处理器,这两个专用处理器例如均被嵌入系统芯片。

[0039] 电子设备 10 还包括装配有处理器的安全电子单元 40,该安全电子单元 40 例如为安全整合电路(SE,“Secure Element”,安全构件),它可选地焊接在电子设备 10 上(称为 eSE,“embedded Secure Element”,嵌入式安全构件),或微电路卡(UICC,“Universal Integrated Circuit Card”,通用集成电路卡)。

[0040] 所述安全电子单元例如符合 EAL 通用标准,对应于 ISO 15408 标准 - 其中级别在 2-7 之间,或 FIPS 140-2 标准。

[0041] 发送到电子单元 40 的命令例如为 APDU 类型的(例如见下面的步骤 E13)。如图 1 示意性示出的,电子单元 40 还可将命令发送到可信操作系统 30,该命令例如为 STK(“SIM ToolKit”)类型的。

[0042] 电子设备 10 最后包括用户界面或人 - 机界面(IHM)50(或 UI,“User Interface”,用户界面),例如触摸屏,在此当用户触碰显示于触摸屏上的构件(如虚拟按键)时,该触摸屏可以向用户显示信息和接收用户的指令或信息。

[0043] 在变化形式中,用户界面可使用其它类型的输入 - 输出装置,以交换电子设备与用户之间的信息,例如扬声器、麦克风或生物识别传感器。

[0044] 图 1 呈现的系统包括远程服务器 60(例如属于商业网站),其可通过箭头 A 示意性表示的通信装置与电子设备 10 交换数据,该通信装置尤其可包括电话网络(此处为移动电话网络)和数据网络,例如互联网这样的计算机网络。

[0045] 图 1 的系统可选地另外包括银行服务器 70,即由银行管理的服务器,通常在银行中,用户为银行帐户持有人。

[0046] 图 2 示出根据本发明的在图 1 的系统构件之间交换数据的方法的第一实施例。

[0047] 所述方法开始于步骤 E0,在远程服务器 60 和浏览器 24(例如互联网浏览器或“web

“browser”）之间交换数据，由电子设备 10 的处理器在由多功能操作系统 20 定义的环境范围内执行。

[0048] 由浏览器 24 接收的数据被显示在电子设备 10 的触摸屏上。为此，在步骤 E1 中通过人 - 机界面（或 IHM）管理模块 22 控制浏览器 24。如图 1 所示，该 IHM 管理模块 22 是由多功能操作系统 20 提供的服务的一部分。

[0049] IHM 管理模块 22 在步骤 E2 中控制触摸屏 50 上的请求显示。

[0050] 然后用户选择（通过触碰例如触摸屏 50 上的虚拟按钮）需要在安全内容中实施的功能（例如付款）。

[0051] 在步骤 E3 中，该选择（实际上是用户手指在触摸屏 50 指定位置上的定位）被传送到 IHM 管理模块 22，它在步骤 E4 与浏览器 24 相关联。

[0052] 由于这次选择，浏览器 24 在步骤 E5 中控制实施专用于该功能的模块 26，例如扩展模块（或插入式模块，“plug-in”）。浏览器 24 还可与关联控制功能的信息专用模块 26 相通信，此处为付款信息如交易金额、交易者身份标识、交易日期和产品代码。

[0053] 在步骤 E6，专用模块 26（由电子设备 10 的处理器执行）要求活动的（起作用的）操作系统（在适当情况下为多功能操作系统 20）向基于另一可选操作系统（此处为可信操作系统 30）的电子设备 10 的功能切换，即向可信操作执行环境（或 TEE）中的功能切换。

[0054] 多功能操作系统 20 还在步骤 E7 控制可信操作系统 30 的启动。该可信操作系统 30 在步骤 E8 中确认接收，这引起步骤 E9 中的多功能操作系统 20 的关闭。电子设备 10 在可信操作系统 30 的基础上运行。

[0055] 专用模块 26 向可信操作系统 30 发送可信应用程序 36 的选择命令（或 TA，“Trusted Application”，也可为“trustlet”），这可在电子设备基于可信操作系统 30 运行时（步骤 E10）通过该电子设备 10 的处理器执行。

[0056] 所述选择命令例如伴有可信应用程序 36 的识别，如通用唯一识别码（UUID，“Universal Unique Identifier”）。

[0057] 在步骤 E11 中，可信操作系统 30 选择所请求的可信应用程序 36（即，实际上可信操作系统 30 通过电子设备 10 的处理器开启可信应用程序 36 的执行）。

[0058] 在步骤 E12 中，专用模块 26 可向与用户命令的功能相关联的可信应用程序 36 发送信息（此处为付款信息）。

[0059] 可信应用程序 36 控制安全电子单元 40 中的小应用程序 42 的启动。为此，在步骤 E13 中，可信应用程序 36 向安全电子单元 40 发送选择命令，伴有小应用程序 42 的识别（AID，“Application IDentifier”，应用标识符）。该命令例如为 APDU（“Application Protocol Data Unit”，应用协议数据单元）型的命令。安全电子单元 40（更确切地是通过安全电子单元 40 的处理器执行的操作系统）通过该安全电子单元 40 的处理器启动执行被识别的小应用程序 42（步骤 E14）。

[0060] 然后在步骤 E15 中，可信应用程序 36 向小应用程序 42 发送与用户请求功能相关联的信息（此处为付款信息）。

[0061] 如现在所描述的，在由安全电子单元执行付款验证之前（如下面的描述），小应用程序 42 实施用户授权（用户通过触摸屏 50 提供授权信息）。

[0062] 为此，小应用程序 42 请求可信操作系统 30 实施由可信操作系统提供的服务库中

的服务 34(步骤 E16)。

[0063] 所述服务例如对应于在触摸屏 50 上显示请求用户输入识别码（例如 PIN 码，“Personal Identification Number”，个人识别码）这样的消息，以及等待用户通过触摸屏 50 的虚拟键盘输入代码。

[0064] 在变化形式中，可在触摸屏 50 上显示请求用户识别符号或图片的消息，可选地，以特定顺序，或将其手指放置在触摸屏 50 上的指定位置处，以检测用户的指纹。

[0065] 在这些实施例中，识别代码、识别符号（或图片）和指纹分别形成用户的授权信息。

[0066] 以通常的方式，用户识别数据经过输入外围设置（键盘、触摸屏、生物传感器等）由可信操作系统 30 接收。

[0067] 然后可信操作系统 30 启动所请求的服务 34(步骤 E17)。所述服务 34 向 IHM 安全管理模块 32(步骤 E18) 请求，IHM 安全管理模块 32 在步骤 E19 中控制在触摸屏 50 上进行按要求的显示（即在上面提及的实施例中显示要求输入识别代码或的消息或显示要求放置手指的消息）。如图 1 所示，所述 IHM 安全管理模块 32 作为可信操作系统 30 的一部分。

[0068] 在变化形式中，可设置将由安全电子单元 40 的处理器执行的小应用程序 42 直接指向安全管理模块 32，以请求在触摸屏 50 上进行显示。

[0069] 通过用户界面 50（此处为触摸屏）从用户得到的识别或授权信息被在 IHM 安全管理模块 32 位置处确定（步骤 E20），然后可选地通过可信操作系统 30 传送到小应用程序 42（步骤 E21 和 E22）。

[0070] 小应用程序 42 可验证所接收的识别和授权信息是否与用户相关联（例如通过与安全电子单元 40 中存储的信息相对比）。

[0071] 如果小应用程序 42 验证了所接收的识别和授权信息与所有存储的信息相对应，则小应用程序 42 准备授权消息（例如利用存储在安全电子单元 40 中的密钥来标识该消息）并将该授权消息发送到在步骤 E23 中由电子设备 10 实施的可信操作系统 30。（如果验证出不对称，可例如使小应用程序 42 发送取代授权消息的错误消息）。

[0072] 然后可信操作系统 30 向专用模块 26 发送授权消息（步骤 E24）。在步骤 E26 中，该授权消息还被浏览器 24 获取（步骤 E25）以传送到远程服务器 60，从而通知远程服务 60 有效实施用户要求的功能，此处为用户在步骤 E3 中开始的付款验证。

[0073] 应当注意，在上面描述的方法中，所有的用户识别或授权处理步骤均由可信操作系统 30 和安全电子单元 40 的配合进行实施。而且，识别或授权处理由安全电子单元 40 的处理器执行的小应用程序 42 主动实施，其中的安全级别仍大于由可信操作系统 30 确保的安全级别。还保证了识别或授权处理不被要获取用户授权信息的黑客的恶意软件（“malware”）实施。

[0074] 可信操作系统 30 的作用还在于限制与安全电子单元 40 的数据交换和将服务（尤其是针对访问触摸屏 50 的电子设备 10 的外围设备）提供给安全电子单元 40，而无需操控功能的运行（例如交易运行），该操控已被委托给安全电子单元 40。

[0075] 图 3 示出根据本发明在图 1 类型的系统中的数据交换方法的第二实施例。

[0076] 所述方法开始于步骤 E100，其中用户例如通过在触摸屏 50 上选择与购买应用程序相关联的图标来启动在线购买应用程序。在由多功能操作系统 20 形成的环境中执行在

线购买应用程序。在线购买应用程序还尤其请求多功能操作系统 20 提供的服务。

[0077] 在步骤 E101 中, 在线购买应用程序访问存储在远程服务器 60 中的远程内容 (例如通过呼叫多功能操作系统 20 的专用服务和经过图 1 的箭头 A 表示的通信方式)。所述远程内容被显示在触摸屏 50 上 (图 3 未示出的显示步骤), 以能够例如使用户例如通过触碰显示在触摸屏 50 上的产品图像旁边显示的图标来选择其希望购买的产品。

[0078] 一旦用户选择了产品 (图 3 未示出选择步骤), 例如通过触碰显示在触摸屏 50 上的付款虚拟按钮, 用户通过在触摸屏 50 上的特写激活来启动为所选产品付款 (步骤 E102)。

[0079] 由于该步骤 E102 (实际上由于用户已将其手指安置在付款虚拟按钮的显示位置处), 多功能操作系统 20 接收付款启动信息, 并在步骤 E103 中, 控制存在在安全电子单元 40 中的付款应用程序的启动 (即由安全电子单元处理器执行)。

[0080] 由安全电子单元 40 的处理器执行的付款应用程序设置用户授权处理。

[0081] 为此, 在安全电子单元 40 中执行的付款应用程序在步骤 E104 中控制实施可信操作系统 30 的服务。所述服务旨在获得用户利用用户界面输入外围设备 50 (此处为触摸屏) 提供的授权信息, 例如上面所解释的密码、个人识别码 (PIN 码) 或诸如指纹的生物信息。

[0082] 服务例如命令在触摸屏 50 上显示专属用户的提示或消息, 请求用户提供请求授的信息 (图 3 未示出显示步骤)。

[0083] 在步骤 E105 中, 用户提供请求授权信息 (通过在触摸屏 50 上的激活), 还将授权信息传送到可信操作系统 30。

[0084] 在步骤 E106 中, 可信操作系统 30 将这些授权信息传送到安全电子单元 40, 以使安全电子单元 40 可以验证这些授权信息, 例如通过与存储在安全电子单元 40 中的对应数据进行对比来进行验证。

[0085] 如果安全电子单元 40 检测到从用户处获得的授权信息不准确, 则不会完成付款, 并且安全电子单元 40 向多功能操作系统 20 发送例如错误消息 (图 3 未示出该步骤)。

[0086] 反之, 如果安全电子单元 40 验证从用户处获得的授权信息准确, 安全电子单元 40 准备交易授权消息 (例如利用存储在安全电子单元 40 中的密钥标识的消息), 并在步骤 E107 中将该授权消息发送到在多功能操作系统 20 中执行的在线购买应用程序。

[0087] 应注意, 在步骤 E104 到步骤 E106 中使用可信操作系统 30 能够使安全电子单元 40 利用电子设备 10 (此处为触摸屏 50) 的资源, 这发生于由可信操作系统 30 而形成的可信操作环境 (TEE) 中。利用电子设备 10 的资源获得的信息 (此处为授权信息) 因此可被安全电子单元 40 中执行的应用程序 (此处为付款应用程序) 使用。

[0088] 在接收到授权消息 (上面描述的步骤 E107) 之后, 在步骤 E108 中, 在线购买应用程序根据银行通过与银行服务器 70 交换数据、尤其通过向银行服务器 70 传送授权消息 (例如由已指示的安全电子单元 40 标识) 来触发付款。

[0089] 在利用前一步骤已完成交易时, 通过请求专用于多功能操作系统 20 的服务 (步骤 E109), 在线购买应用程序例如命令用户在触摸屏 50 上显示虚拟确认。

[0090] 图 4 示出可实施本发明的另一系统实施例。

[0091] 所述另一系统包括电子设备 80 和读出器 90, 该电子设备 80 在此为终端、例如智能电话, 该读出器 90 配备有例如访问安全区域的转门。为了授权通过转门, 用户应向读出器 90 呈现包括授权数据的电子设备, 例如电子设备 80。

- [0092] 该电子设备 80 包括控制模块 82、通信模块 88 和诸如触摸屏的人 - 机界面 84。
- [0093] 该控制模块 82 包括处理器以及存储器（例如随机存取存储器、只读存储器和可重写的非易失性存储器），并管理电子设备的主要功能。更具体地，控制模块 82 管理人 - 机界面 84：该控制模块 82 可发送在触摸屏 84 上显示的命令和接收来自触摸屏 84 的信息，特别地，使用者的手指在触摸屏 84 上的位置可被用户特殊指令来解释（根据实施于触摸屏 84 上的显示，例如虚拟按钮的显示）。
- [0094] 控制模块 82 可基于可信操作系统运行（即，通过在控制模块 82 的处理器上执行可信操作系统来实施控制模块运行基础的功能），这能够产生可信执行环境或 TEE。
- [0095] 以任选的方式，如上面参照图 1 描述的，控制模块 82 还可基于多功能操作系统运行。
- [0096] 通信模块 88 连接到天线 89 并且还可设置成与读出器 90 的小范围无接触通信。通信模块 88 例如为 CLF（“ContactLess Frontend”，非接触前端）型的，并且例如能设置成 NFC（“Near Field Communication”，近场通信）型通信。所述通信模块 88 包括处理器和可选的存储器，例如随机存取存储器和可重写的非易失性存储器。
- [0097] 例如通过串联或通过数据总线联接控制模块 82 和通信模块 88。
- [0098] 电子设备 80 还具有安全电子单元 86，例如安全集成电路（SE，“Secure Element”，安全构件），此处的安全集成电路被焊接在电子设备的印刷电路 80（eSE，“embedded Secure Element”，嵌入式安全构件）上。在变化形式中，可作为被安置在电子设备中的微电路卡（UIICC，“Universal Integrated Circuit Card”，通用集成电路卡）。
- [0099] 安全电子单元 86 于此处同时联接到通信模块 88（例如通过 SWP（“Single Wire Protocol”，单线协议）型协议或 12C（“Inter Integrated Circuit”，内部集成电路）型协议）和控制模块 82（同样例如通过 SWP 或 12C 型协议）。
- [0100] 安全电子单元 86 包括处理器和存储器，例如随机存取存储器和可重写的非易失性存储器。可重写的非易失性存储器存储授权数据（其能如上面提示的允许用户通道穿过转门）或能够使安全电子单元 86 产生读出器 90 所等待的授权数据的数据，如接下来所解释的。
- [0101] 读出器 90 包括连接到天线 91 的处理器 92。
- [0102] 当电子设备足够接近时（例如，当它们的天线 89、91 的距离小于 5cm 时），电子设备 80 的天线 89 受到由读出器 90 利用天线 91 生成磁场的作用，这能在读出器 90 的处理器 92 和通信模块 88 的处理器之间交换数据，例如符合 ISO/IEC 14443 标准。
- [0103] 图 5 示出在图 4 的系统构件之间交换数据的方法的实施例。
- [0104] 考虑到用户已接近配备有转门的读出器 90 的终端 80，如前所示的，这引起如在通信模块 88 和读出器 90 的处理器 92 之间实施通信会话。
- [0105] 在开始会话步骤后（未示出），在步骤 E202 中，读出器 90 的处理器 92 向通信模块 88 传送命令，该命令（例如 SELECT AID 型）指定安全电子单元 86 的小应用程序。
- [0106] 在步骤 E203 中，通信模块 88 向安全电子单元 86 传送命令，这能够执行在安全电子单元 86 中指定的小应用程序。所有这些之后的命令均被传送到选定小应用程序。
- [0107] 在准备授权数据之前，安全电子单元 86 将操控电子设备 80 的用户授权处理。
- [0108] 为此，由于小应用程序的执行，在步骤 E204 中，安全电子单元 86 将目标命令发送

到由控制模块 82 的处理器执行的可信操作系统,以使用户可授权并在触摸屏 84 或另一电子设备的输入 - 输出装置、如生物传感器的位置处产生授权信息。授权信息例如为用户在触摸屏 84 呈现的虚拟键盘上输入的密码或识别代码 (PIN 码)。在变化形式中,可作为利用触摸屏 84 或上面提及的生物传感器获得的生物数据。

[0109] 在步骤 E205 中,用户呈现的授权信息被从触摸屏 84(或在变化形式中从另一输入 - 输出装置) 传送到控制模块 82 的处理器执行的可信操作系统。

[0110] 然后授权信息从可信操作系统传送到安全电子单元 86(步骤 E206)。

[0111] 然后安全电子单元 86 验证授权信息是否对应于用户输入的信息 (例如被存储在电子单元的非易失性存储器),如果对应,准备授权数据。(在否的情况下,自然结束处理器而不准备授权数据和因此不授权用户访问)

[0112] 如已说明的,这些授权数据可为被存储在安全电子单元 86 的非易失性存储器中或由安全电子单元 86 例如根据询问 - 响应 (“challenge-response”) 技术获得的数据,例如通过将存储在非易失性存储器中的密钥应用到读出器接收的数据 (例如联合到步骤 E202 的命令)。

[0113] 安全电子单元 86 可将所准备的授权数据传送给通信模块 88(步骤 E207),通信模块 88 将这些授权数据传送给读出器 90 的处理器 92(步骤 E208)。

[0114] 在所接收的授权数据基础上,读出器 90 的处理器 92 通过释放转门的旋转而向用户授权访问。

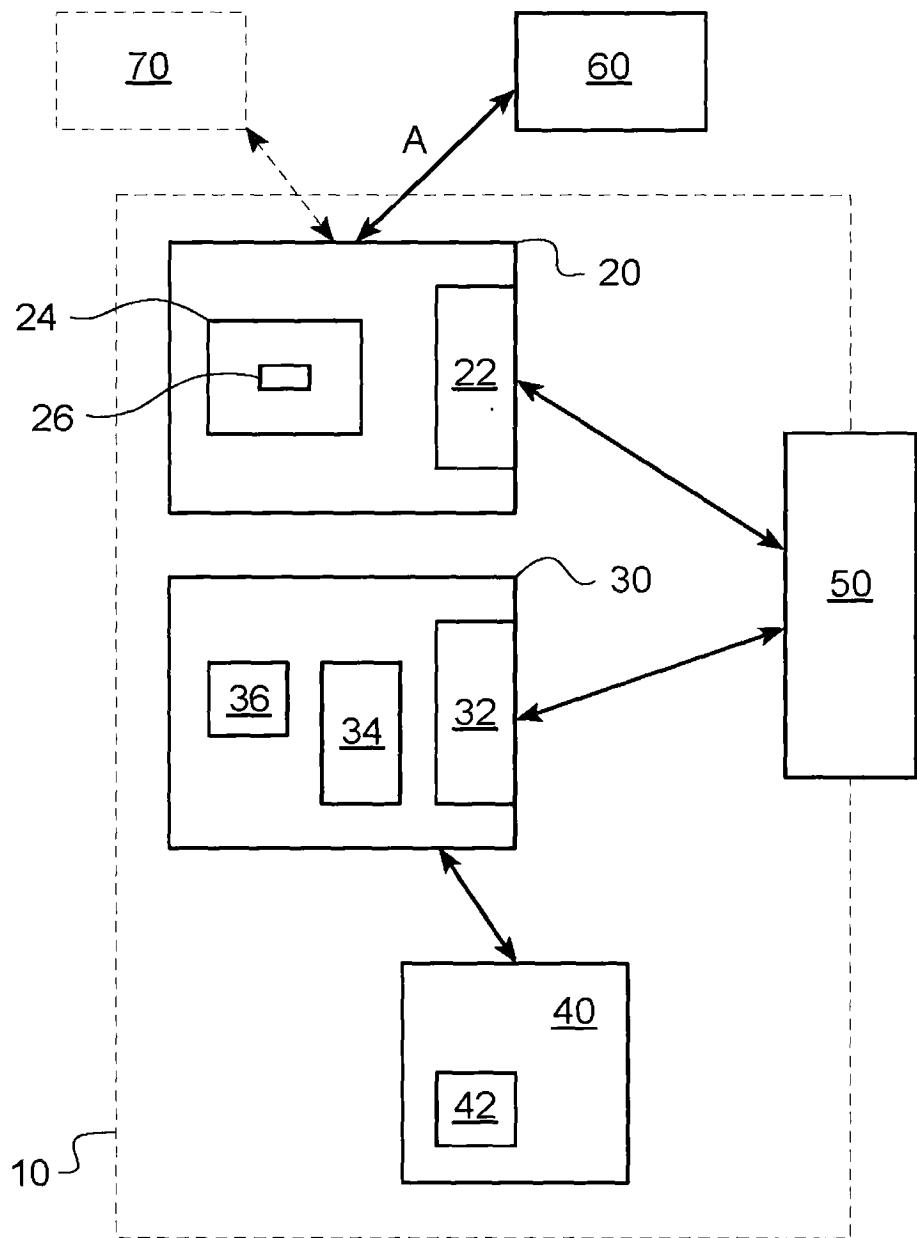


图 1

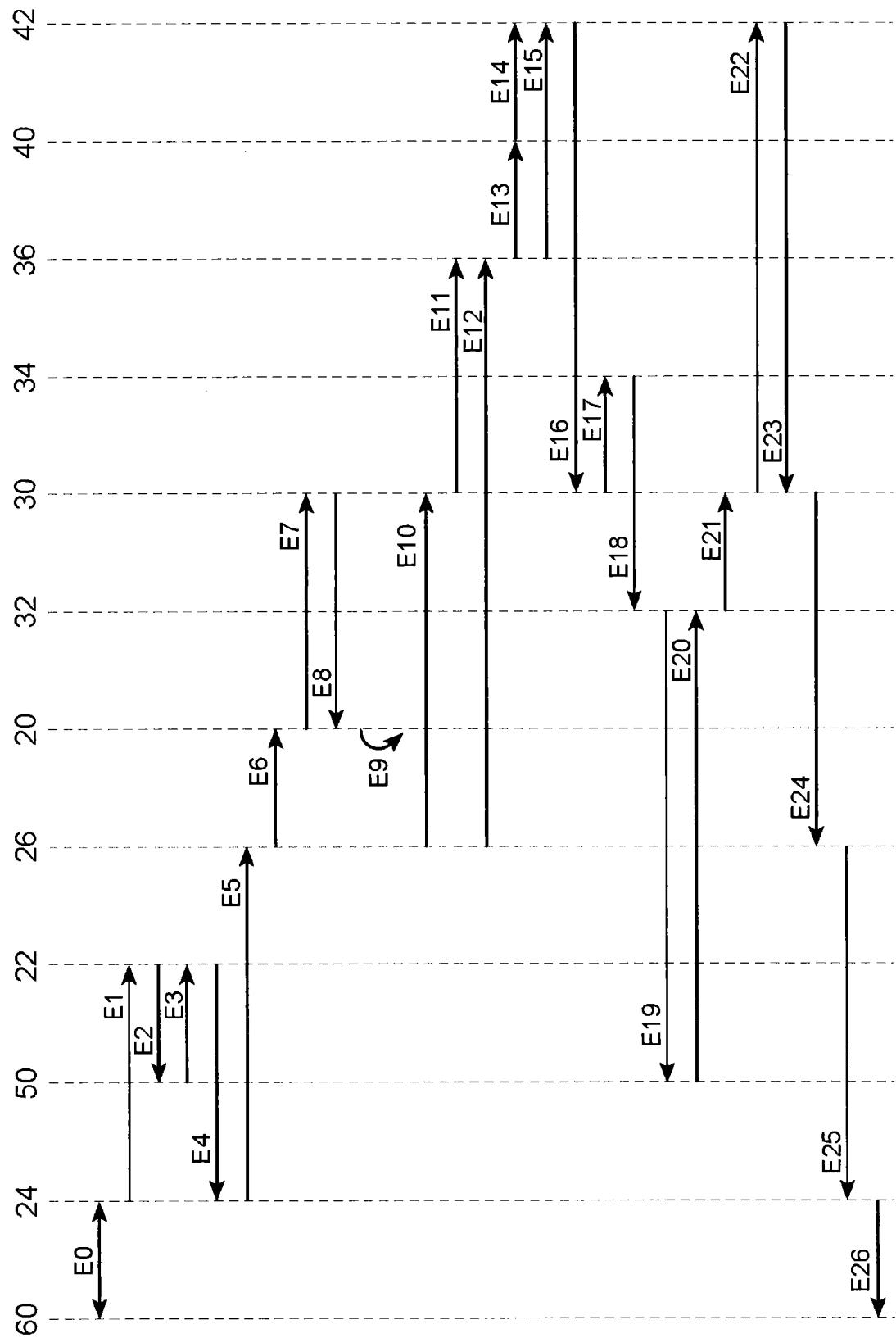


图 2

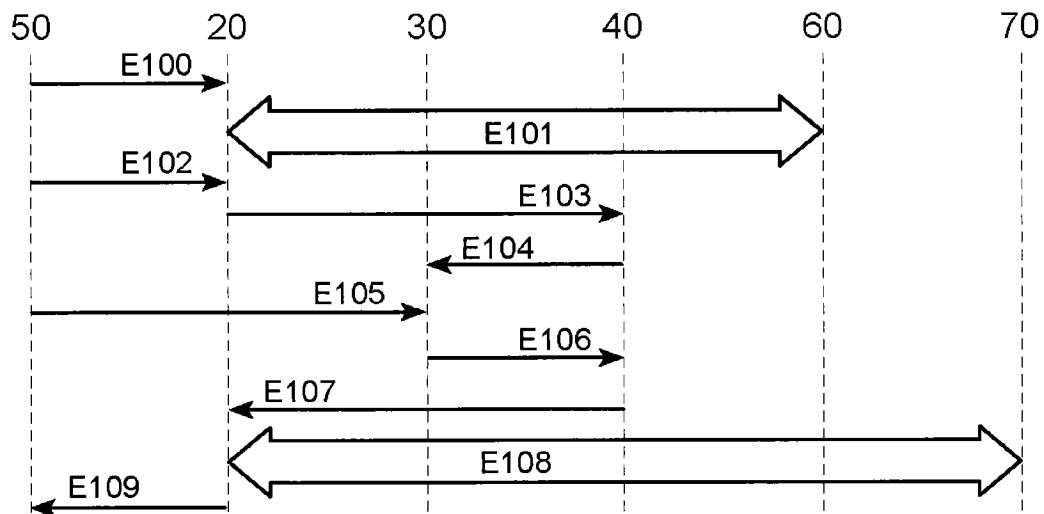


图 3

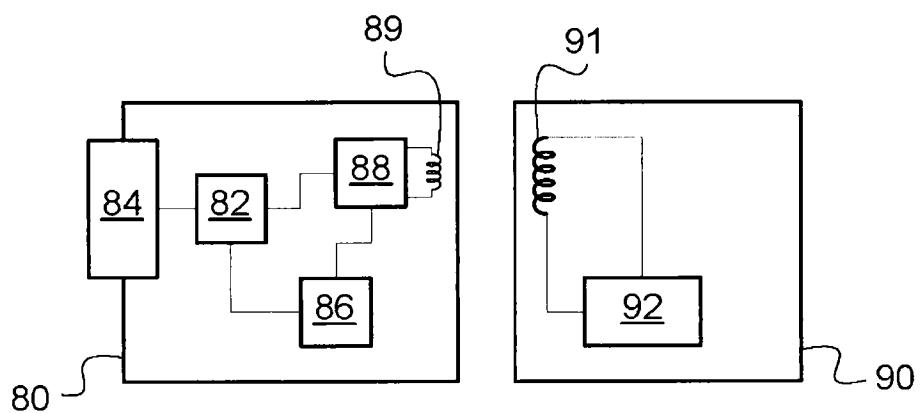


图 4

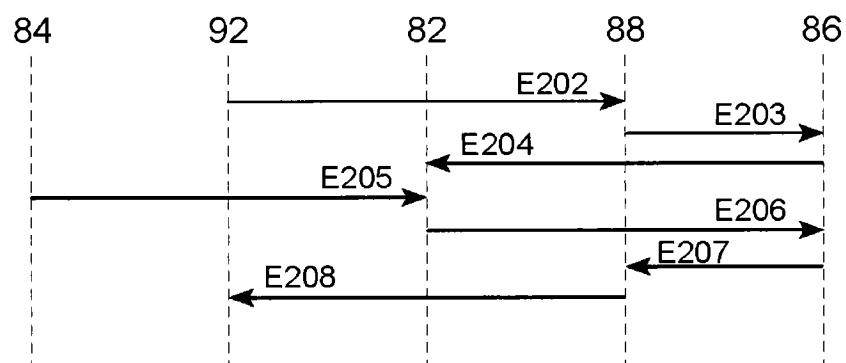


图 5