(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 105119902 A
(43)申请公布日 2015.12.02

(21)申请号 201510431114.6
(22)申请日 2008.10.17
(30)优先权数据
07/07331 2007.10.19 FR
(62)分案原申请数据
200880112113.3 2008.10.17
(71)申请人 自然安全公司
地址 法国里尔
(72)发明人 比诺特·库洛贝尔 埃里克·牧里耶 克德里克·霍萨尼 查克彼·嘉琪 杰克库·艾斯蒂耶尼
(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 王达佐 王艳春
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 4/00(2009.01)

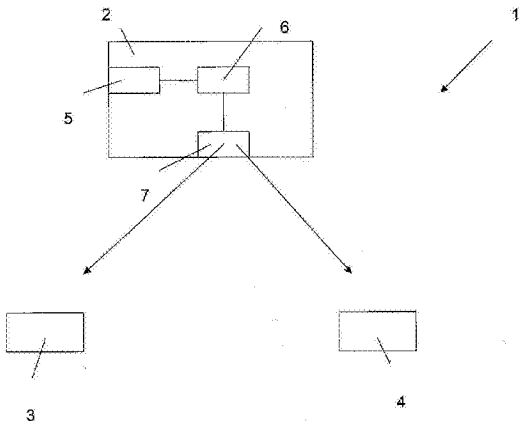
权利要求书3页 说明书10页 附图4页

(54)发明名称

非接触式生物特征身份验证系统和身份验证方法

(57)摘要

本发明涉及一种身份验证系统(1),该系统包括:一个或多个个人身份验证装置(3,4);终端(2),包括:生物特征装置(5,6),适于产生使用者的生物特征信息;无线通信装置(7),适于在个人身份验证装置(3,4)与终端(2)之间没有任何接触的情况下向个人身份验证装置(3,4)传输生物特征信息;一个或每个个人身份验证装置(3,4)包括:存储器,用于存储个人身份验证装置(3,4)的持有者的生物特征信息;处理装置(11),用于对生物特征信息和生物特征数据进行比较,以对使用者进行身份验证;其特征在于,无线通信装置(7)适于向多个个人身份验证装置传输生物特征信息,每个个人身份验证装置(3,4)包括无线通信装置(8),无线通信装置(8)用于在生物特征信息与生物特征数据之间是肯定比较的情况下向终端(2)无接触式传输肯定的身份验证数据,从而能够对使用者进行身份验证,其中,终端适于仅对已经传输肯定的身份验证数据的一个或多个个人装置打开交易会话。



CN 105119902 A

1.一种身份验证系统，包括：

多个个人身份验证装置；以及

终端，包括：

存储器，用于存储私人密钥/公共密钥对；

生物特征装置，设置为生成使用者的生物特征信息；

无线通信装置，设置为在所述多个个人身份验证装置的每一个和所述终端之间都没有任何物理接触的情况下，将生物特征信息传输给所述多个个人身份验证装置的每一个；

所述多个个人身份验证装置的每一个都包括：

存储器，设置为存储所述多个个人身份验证装置的各个个人身份验证装置的持有者的生物特征数据、与所述各个个人身份验证装置相关的多个应用、以及私人密钥/公共密钥对；

处理装置，设置为对所述使用者的生物特征信息和所述各个个人身份验证装置的持有者的生物特征数据进行比较，从而执行所述使用者的身份验证；以及

无线通信装置，设置为响应于所述使用者的生物特征信息和所述各个个人身份验证装置的持有者的生物特征数据之间的肯定的比较，在没有任何接触的情况下，进行将肯定的身份验证数据传输至所述终端或从所述终端传输肯定的身份验证数据中的至少一种，从而能够进行对所述使用者的身份验证；

其中，所述终端和所述多个个人身份验证装置被设置成使得：

所述多个个人身份验证装置的每一个与所述终端交换公共密钥以便打开所述多个个人身份验证装置的每一个和所述终端之间的各个安全通信通道；

所述终端通过所述各个安全通信通道将所述生物特征信息传输至所述多个个人身份验证装置的每一个；

所述多个个人身份验证装置的每一个都将所述生物特征信息与其生物特征数据进行比较，并且响应于所述生物特征信息和所述生物特征数据之间肯定的比较，通过所述各个安全通信通道将肯定的身份验证数据传输至所述终端，从而能够进行对所述使用者的身份验证；以及

所述终端根据与所述各个个人身份验证装置相关的所述多个应用，选择将所述肯定的身份验证数据传输至所述终端的所述多个个人身份验证装置中的一个，以便与所述各个个人身份验证装置进行交易；

其中，所述生物特征信息和所述生物特征数据为能够进行对所述使用者的身份验证的生物特征指标，并且其中，在打开所述终端和所述多个个人身份验证装置的每一个之间的各个安全通信通道之前，所述终端和所述多个个人身份验证装置的每一个都被设置成使得：

所述终端由其生物特征指标计算得出生物特征证书；

所述终端将所述生物特征证书传播至所述多个个人身份验证装置的每一个；以及

所述个人身份验证装置的每一个都由其生物特征指标计算得出生物特征证书，将计算得出的生物特征证书与由所述终端传播的生物特征证书进行比较，如果计算得出的生物特征证书与由所述终端传播的生物特征证书相匹配，则将表明比较为肯定的未编码应答传输至所述终端。

2. 根据权利要求 1 的系统，其中，所述多个个人身份验证装置的每一个都具有：

第一模式，在所述第一模式下，所述多个个人身份验证装置的每一个都不向所述终端传输数据，以及

活动模式，在所述活动模式下，所述多个个人身份验证装置的每一个都与所述终端通信。

3. 根据权利要求 2 的系统，其中，响应于所述使用者的生物特征信息和所述各个个人身份验证装置的持有者的生物特征数据之间的否定比较，所述各个个人身份验证装置被设置成切换至所述第一模式。

4. 根据权利要求 2 的系统，其中，响应于所述使用者的生物特征信息和所述各个个人身份验证装置的持有者的生物特征数据之间的肯定的比较，所述各个个人身份验证装置被设置为保持在所述活动模式下。

5. 根据权利要求 4 的系统，其中，所述多个个人身份验证装置的每一个都具有：

倾听模式，在所述倾听模式下，所述多个个人身份验证装置的每一个都检测由所述终端传输的信号，以及

待命模式，在所述待命模式下，所述多个个人身份验证装置的每一个都运行时间延迟。

6. 根据权利要求 5 的系统，其中，所述多个个人身份验证装置的每一个都被设置为在第一预定时间 T_1 之后，从所述待命模式切换至所述倾听模式。

7. 根据权利要求 6 的系统，其中，所述多个个人身份验证装置的每一个都被设置为在第二预定时间 T_2 结束之前，当所述多个个人身份验证装置的每一个都检测到由所述终端传输的信号时，从所述倾听模式切换至所述活动模式。

8. 根据权利要求 1 的系统，其中，所述生物特征装置包括生物特征读取器和处理装置，其中，所述生物特征读取器被设置为获取所述使用者的生物特征图像，所述处理装置被设置为由所述生物特征图像生成所述使用者的生物特征信息。

9. 根据权利要求 8 的系统，其中，所述生物特征装置的处理装置被设置为从所述生物特征图像检索细节特征，并且其中，所述使用者的生物特征信息包括所述细节特征的凝聚。

10. 根据权利要求 1 的系统，其中，所述生物特征装置包括生物特征读取器，所述生物特征读取器被设置为获取所述使用者的手指或手的静脉网络的图像。

11. 根据权利要求 1 的系统，其中，所述终端的无线通信装置被设置为根据包含于 50 厘米和 300 厘米之间的距离，将所述使用者的生物特征信息传输给所述多个个人身份验证装置的每一个。

12. 根据权利要求 1 的系统，其中，所述多个个人身份验证装置的每一个的无线通信装置能够根据包含于 50 厘米和 300 厘米之间的距离，与所述终端进行通信。

13. 根据权利要求 1 的系统，其中，所述多个个人身份验证装置的每一个都包括所述多个应用的列表，并且所述终端通过以下步骤中的至少一个，来选择所述多个个人身份验证装置中的选定的个人身份验证装置和所述多个个人身份验证装置中的选定的个人身份验证装置的、所述多个应用中的选定的应用，从而执行交易：将所述终端未识别的应用从所述多个应用的每个接收到的列表中删除的步骤；或者应用所述终端内的或存在于所述多个应用的每个接收到的列表中的优先原则的步骤。

14. 身份验证的方法，包括：

在多个个人身份验证装置的每一个和终端之间交换公共密钥，以便打开所述多个个人身份验证装置的每一个和所述终端之间的各个安全通信通道；

通过生物特征装置生成使用者的生物特征信息；

通过终端的无线通信装置，将所述使用者的生物特征信息经过所述各个安全通信通道传输至所述多个个人身份验证装置的每一个；

通过所述多个个人身份验证装置的每一个的处理装置，对所述使用者的生物特征信息和所述多个个人身份验证装置的各个个人身份验证装置的持有者的生物特征数据进行比较，并且响应于所述使用者的生物特征数据和所述持有者的生物特征信息之间的肯定的比较，生成肯定的身份验证数据，从而识别所述使用者；

通过各个个人身份验证装置的无线通信装置，响应于所述肯定的比较，将所述肯定的身份验证数据通过所述各个安全通信通道传输至所述终端；

通过所述终端，打开与已经传输所述肯定的身份验证数据的各个个人身份验证装置的交易会话；

通过所述终端，请求所述终端打开所述交易会话的各个个人身份验证装置的多个应用的列表；以及

通过所述终端，根据多个应用的列表，选择所述多个个人身份验证装置中的选定的个人身份验证装置以执行交易，其中，所述列表包含于所述多个个人身份验证装置中的选定的个人身份验证装置，其中，选择包括选自以下步骤组的一个或多个步骤，所述步骤组包括：

将未识别的应用从所述多个应用的每个接收到的列表中删除；

应用所述终端内的、或者存在于所述多个应用的每个接收到的列表中的优先原则；

通过所述使用者的动作或所述多个个人身份验证装置中的选定的个人身份验证装置，提供所述多个个人身份验证装置中的选定的个人身份验证装置以及所述多个个人身份验证装置中的选定的个人身份验证装置的、所述多个应用中的选定的应用的选择；

在所述终端和所述多个个人身份验证装置的每一个之间的各个安全通信通道打开之前，经由作为生物特征指标的所述生物特征信息和所述生物特征数据，能够进行对所述使用者的身份验证；

经由所述终端，由生物特征指标计算得出生物特征证书；

经由所述终端，将所述生物特征证书传播至所述多个个人身份验证装置的每一个；

所述个人身份验证装置的每一个都由其生物特征指标计算得出生物特征证书，将所计算得出的生物特征证书与通过所述终端传播的生物特征证书进行比较，并且如果计算得出的生物特征证书与由所述终端传播的生物特征证书相匹配，则将表明所述比较为肯定的未编码应答传输至所述终端。

非接触式生物特征身份验证系统和身份验证方法

技术领域

[0001] 本发明涉及一种身份验证系统，其包括：

[0002] - 多个个人身份验证装置中的一个；

[0003] - 一个终端，包括：

[0004] - 生物特征装置，被设置为产生使用者的生物特征信息；

[0005] - 通信装置，被设置为向个人身份验证装置传输生物特征信息；

[0006] - 每个可能的个人身份验证装置或该个人身份验证装置包括：

[0007] - 存储器，被设置为存储个人身份验证装置的持有者的生物特征数据；

[0008] - 处理装置，被设置为对生物特征信息和生物特征数据进行比较，从而进行使用者的身份验证。

背景技术

[0009] 从 WO-A-2004/100083 号 PCT 申请中得知这种系统。在该 PCT 申请中，该装置是身份验证卡，生物特征信息被传输至身份验证卡的存储器。该 PCT 申请并未教导生物特征信息如何被传输至身份验证卡。现在，当终端被设置为例如通过将身份验证卡插入终端中而将生物特征信息传输至身份验证卡时，身份验证需要对使用者具有约束的步骤。使用者必须将他或她的卡取出并将其插入接触式读取器中，以使得身份验证可以进行。

发明内容

[0010] 本发明的一个目的是在上述系统中便于使用者的身份验证。

[0011] 文献 WO 2005/078647 教导了一种如上所述的系统，其中通信装置是无线通信装置，该无线通信装置被设置为在装置与终端之间无任何接触的情况下将生物特征信息传输至个人装置。

[0012] 然而，文献 WO 2005/078647 并未考虑若干个人装置可位于无线通信装置的范围内的事实。

[0013] 事实上，该文献限于特定个人装置与终端之间的一对一 (1:1) 类型的连接，这样使得使用者必须将唯一的个人装置放置在邻近于该装置，以执行该方法。现在，有利的是，可以在若干个人装置处于终端所及的范围内时执行该方法，更具体地可以在通信装置的范围相对较大，例如在 50 厘米与 300 厘米之间时执行该方法。

[0014] 更具体地，例如当环境是共同存在若干终端的百货商店环境时，个人装置可由若干终端同时选择。类似地，终端可在其中具有属于或不属于不同携带者的若干卡。

[0015] 本发明的一个目的是提供可以在无线通信装置具有相对较大范围时操作的身份验证方法和系统，使得若干个人装置可以位于该无线通信装置的范围内。

[0016] 根据本发明，由于如上述所述的系统达到了该目的，其中，无线通信装置被设置为向多个个人身份验证装置传输生物特征信息，并且每一个个人身份验证装置均包括无线通信装置，无线通信装置被设置为在生物特征信息与生物特征数据之间是肯定比较的情况下

以无接触的方式向终端传输肯定的身份验证数据，从而能够进行对使用者的身份验证，其中，终端被设置为仅对已经传输肯定的身份验证数据的一个或多个个人装置打开交易会话。

[0017] 因此，终端可以在其无线通信装置的范围内向所有个人装置发送生物特征信息并仅对来自终端的轮询进行肯定应答的装置打开交易会话。从而，如果若干装置处于终端的无线通信装置的范围内但并不与已进行生物特征获取的使用者相对应，那么将不通过终端打开任何交易会话。因而可以对处于终端的范围内的若干个人装置的存在进行管理。这使得甚至当存在若干装置时获得满意和安全的身份验证成为可能。

[0018] 因此，使用者可以通过使用终端的生物特征装置借助一个动作对他自己或她自己进行身份验证，而不必对他或她自己的个人身份验证装置进行处理。例如，当个人身份验证装置呈身份验证卡片的形式时，使用者可以对他自己或她自己进行身份验证而无需例如从他或她的钱包中取出卡片，并且卡片将对生物特征信息与存储器中的生物特征数据进行比较，而无需由携带者对卡片进行操作。从而由于生物特征比较而方便了身份验证并为身份验证保持了满意的安全水平，并且还考虑了若干使用者可能位于终端的范围内的事实。因而本发明相当良好地适合于百货商店中若干使用者可能同时前往付款台的情况或者一个或若干使用者持有若干个人装置的情况。

[0019] 现在对本发明的有利实施方式进行描述。

[0020] 优选地，终端无线通信装置被设置为根据包含在 50 厘米与 300 厘米之间的距离向个人身份验证装置传输生物特征信息。

[0021] 因而，使用者不必如同采用 NFC“近场通信 (Near Field Communication)”标准的非接触式方案中那样将他或她的个人身份验证装置放置的更近，其中 NFC 标准仅实现在一对一模式下几个厘米处的通信。

[0022] 类似地，个人身份验证装置的无线通信装置还优选地设置为根据包含在 50 厘米与 300 厘米之间的距离与终端进行通信。

[0023] 根据本发明的一个实施方式，生物特征装置包括生物特征读取器和处理装置，生物特征读取器被设置为获取使用者的生物特征图像，处理装置被设置为由生物特征图像产生生物特征信息。该实施方式的优点在于能够使所传输的生物特征信息适合于个人身份验证装置的存储能力和计算能力。更具体地，处理装置可以使得仅有少量的生物特征信息被传输到个人身份验证装置，只要与存储在个人身份验证装置中的数据的肯定比较确保以充分的安全性对已经使用生物特征读取器的使用者进行识别。例如可以根据本发明的应用和由终端授权的交易类型来采用这种安全水平。

[0024] 更具体地，根据本发明的具体实施方式，处理装置被设置为从所述生物特征图像检索细节特征，并且生物特征信息包括细节特征的凝聚。例如通过使用可以应用于终端和个人身份验证装置的散列函数来进行该凝聚。

[0025] 优选地，生物特征读取器被设置为获取使用者的手指或手的静脉网络的图像。这样更具体地使得在不追踪使用者的情况下提供生物特征成为可能。

[0026] 根据本发明的一个实施方式，个人身份验证装置可具有第一模式和活动模式，在第一模式下，个人身份验证装置可以不向终端传输数据，在活动模式下，个人身份验证装置可以与终端进行通信。

[0027] 在该情况下，在个人装置中的生物特征信息与生物特征数据之间是否定比较的情况下，该个人装置可被设置为切换到第一模式，使得在所终端与该个人装置之间未打开任何通信会话。

[0028] 优选地，在个人装置中的生物特征信息与生物特征数据之间是肯定比较的情况下，该个人装置可被设置为保持在活动模式下，使得在终端与该个人装置之间不会进行交易。

[0029] 个人装置还可具有倾听模式和待命模式，在倾听模式下，个人装置可以检测到由终端传输的信号，在待命模式下，个人装置仅可以进行时间延迟。

[0030] 在该情况下，个人装置可被设置为在第一预定时间 T_1 后从待命模式切换到倾听模式。

[0031] 个人装置还可被设置为当个人装置在第二预定时间 T_2 结束前检测到由终端传输的该信号时从倾听模式切换到活动模式。

[0032] 在所有上述实施方式中，在终端从多个个人装置接收到肯定的身份验证数据的情况下，终端可被设置为选择唯一的个人装置以进行交易。

[0033] 在该情况下，个人装置可以包括应用，并且终端可被设置为根据在已经传输肯定的身份验证数据的多个个人装置中包括的应用选择唯一的个人装置。

[0034] 类似地，已经传输肯定的身份验证数据的个人装置可包括多个应用，终端可被设置为选择唯一的应用以进行一个交易。

[0035] 在该情况下，终端可被设置为根据优先原则或者根据能够识别的应用选择唯一的应用。

[0036] 在所有上述实施方式中，终端的无线通信装置和该个人装置或每个个人装置的无线通信装置可具有包含在 30 厘米与 300 厘米之间的通信范围。

[0037] 本发明还涉及一种通过实施如上所述的系统进行身份验证的方法，该方法包括以下步骤：

[0038] - 使用者使用生物特征装置以产生生物特征信息；

[0039] - 无线通信装置向多个个人身份验证装置传输生物特征信息；

[0040] - 每个个人装置的处理装置对生物特征信息和生物特征数据进行比较并在生物特征数据和生物特征信息之间是肯定比较的情况下产生肯定的身份验证数据，以对使用者进行识别；

[0041] - 个人装置的无线通信装置对于肯定的数据身份验证传输至终端；

[0042] - 终端仅对已经传输肯定的身份验证数据的一个或多个个人装置打开交易会话。

[0043] 根据上述方法的实施方式，个人身份验证装置还可传输与能够由个人身份验证装置实施的至少一个应用相关联的至少一个标识符。

[0044] 因而，可以确保在终端与个人装置之间进行的交易适合于由应用所限定的个人装置的能力。

[0045] 优选地，终端的无线通信装置可通过先前建立的安全的通信通道向多个个人身份验证装置传输生物特征信息。

附图说明

[0046] 现在参照附图对本发明的至少一个实施方式进行描述，在附图中：

[0047] - 图 1 示出了根据本发明的身份验证系统；

[0048] - 图 2 示出了包括在图 1 的固定身份验证系统中的个人装置；

[0049] - 图 3 示出了图 1 的身份验证系统的功能示意图；以及

[0050] - 图 4 示出了图 1 的系统的实施方式的功能示意图。

具体实施方式

[0051] 如图 1 所示，根据本发明的身份验证系统 1 包括终端 2，该终端 2 例如与商店中的销售点中的终端 2 相对应。终端 2 包括可以获取使用者的生物特征图像的生物特征读取器 5（例如用于获取使用者手指静脉系统的图像的读取器），以计算图像的细节特征。终端 2 还包括计算器 6，以对生物特征图像以及所获得的细节特征进行处理。这种处理例如对应于对散列函数的应用，以产生细节特征的凝聚。终端 2 还包括无线通信装置 7，从而将信息传输至个人身份验证装置 3 和 4。接下来更详细地对该装置 3 和 4 进行描述。

[0052] 无线通信装置 7 包括基于 ISO 标准，更具体地基于 ISO 18000-6 的射频模块。该标准使得具有在包含于 50 厘米与 3 米之间的距离上的无线通信成为可能。对于 ISO 标准 18000-6 而言，所使用的频率是处于 865MHz 频带内的超高频率。该频率非常适于在包含于 50 厘米与 3 米之间的距离上的通信。

[0053] 无线通信装置 7 还集成了防碰撞算法，使得终端 7 可以与多个装置 3 和 4 对话。

[0054] 现在，参照图 2 对装置 3 进行更详细地描述。例如，装置 3 是呈支付卡形状的卡片。其包括连接至微处理器 11 的射频接口 8 以及也连接至微处理器 11 的接触接口 12。微处理器 11 连接至 EEPROM 存储器 10。电池 9 可以供应装置 3 所需的射频发射能量，使得装置 3 可以与终端 2 进行对话。电池 9 可以在接口 12 与接触式读卡器接触时最终再放电。

[0055] 存储器 10 存储了卡片 3 的持有者的生物特征数据。可使该生物特征数据适合于可由终端 2 产生的信息。更具体地，如果终端 2 包括读取器，以获取使用者手指的静脉网络图像，那么存储器 10 包括当装置 3 接收到来自该手指静脉网络图像的信息时对使用者进行身份验证所需的生物特征数据。该数据可以与静脉网络的细节特征的数据相对应或者与例如从与在终端 2 所应用的散列函数类似的散列函数获得的该图像的凝聚相对应。

[0056] 该数据还可以与关于虹膜或面部形状的数据相对应，以实现对这些生物特征成分的识别或者对任何其它生物特征元素的识别或者对若干生物特征元素的组合进行识别。

[0057] 在客户预订卡片、续展他 / 她的卡片或为现有客户建立新卡片时，该生物特征指标被记录在他 / 她的卡片 3 上。

[0058] 对微处理器 11 进行编程，以在存储器 10 中存储的生物特征数据与通过射频接口 8 从终端 2 接收的生物特征信息之间进行比较。

[0059] 根据定义，这种比较是一对一 (1:1) 类型的：其仅涉及确保所提供的生物特征样本与在携带者所拥有的个人身份验证装置 3（芯片卡、移动电话的 SIM 卡、…）中存在的指标相对应。例如，这与在数据库中进行搜索的相应指标的一对任意 (1 :N) 类型相反。

[0060] 如果存储器 10 中存储的生物特征数据与通过射频接口 8 从终端 2 接收的生物特征信息之间比较是肯定的，那么装置 3 将肯定的身份验证数据传输至终端 2，以向终端 2 表明，正在使用生物特征读取器的使用者确实是装置 3 的持有者。

[0061] 现在，参照图 3 对以上所述的系统 1 的操作进行描述。接下来将参照图 4 对本发明的具体实施方式中使用者的身份验证进行描述。

[0062] 当使用者希望在付款台 13 处支付给定的金额时，付款台系统 13 向终端 2 传输 20 该金额。然后，终端 2 显示例如消息，以使得使用者将他或她的手指或者他或她的手放置在生物特征读取器上。当终端 2 产生生物特征信息时，终端 2 将该生物特征信息发送 13 至处于其环境中的装置。然后该生物特征信息由处于终端 2 传输范围内的所有个人装置 3 和 4 接收。接收到该生物特征信息后，装置 3 将所接收到的生物特征信息与存储在其存储器内的生物特征数据进行比较 41。装置 4 也进行这种比较 42。

[0063] 假设在图 3 中，装置 4 的持有者是正在使用终端 2 的生物特征读取器的使用者，且装置 3 的持有者并不是正在使用终端 2 中生物特征读取器的使用者。在这种情况下，由装置 3 所进行的比较给出否定的结果，并且没有任何身份验证数据由装置 3 传输至终端 2。然后，装置 3 将对与终端进行的交易保持沉默。相反，由装置 4 所进行的比较给出肯定的结果，并且装置 4 将肯定的身份验证数据传输 50 至终端 2，以通知终端 2 正在使用终端 2 的生物特征读取器的使用者是个人身份验证装置 4 的真正持有者。

[0064] 当完成身份验证时，在终端 2 与装置 4 之间打开 60 了安全的交易通道。然后，可以在该安全交易通道上进行安全的交易。由于存在上述的无线通信装置 2 和装置 4，因此可以在装置 4 保持位于装置持有者的钱包、钱夹或口袋中的情况下进行身份验证。然后，例如通过使用 PKI 型证书、公共密钥和私人密钥，在终端 2 与装置 4 之间以原本公知的方式进行安全交易。

[0065] 对于例如 EMV 型的电子支付交易，终端 2 对电子支付身份验证服务器 14 进行轮询 70，以进行交易 EMV。然后，将交易的进行通知 81 终端 2，终端 2 接着通知 82 装置 4 交易已经完成。

[0066] 终端 2 还通知 90 付款台系统交易已经完成。

[0067] 当交易完成时，终端 2 与装置 4 之间的安全通信完成。

[0068] 现在，对上述实施方式的可替换方案进行描述。

[0069] 同一使用者可以是例如呈如上述若干卡片形式的若干个人装置 3 或 4 的持有者。

[0070] 然后，在以上参照图 3 所描述的方法中，对于使用者就是持有者的所有装置将进行肯定的比较，并将肯定的身份验证数据传递至终端 2。在这种情况下，终端 2 可以被设置为实现对已经对比较进行肯定应答的各种装置进行选择。这种选择可以由终端 2 根据终端 2 与已经对比较进行了肯定应答的一个或多个装置之间兼容性自动地进行。

[0071] 例如，如果终端 2 是 EMV 型终端，并且装置中仅有一个可以进行根据标准 EMV 的交易，那么终端 2 将自动地选择该装置并将利用该装置打开安全交易通道。

[0072] 为此，已经对比较做出肯定应答的装置被设置为将可由该装置实现的应用的标识符与例如肯定的身份验证数据一起传输至终端 2。类似地，终端 2 可以在其与装置的交换过程中对终端 2 可以实施的服务的标识符进行传输。

[0073] 此外，当同一个个人身份验证装置包括多个应用时，这些应用的一个标识符与肯定的身份验证数据一起被传输，使得终端可以确定可作为可在装置上获得的应用的功能而提供的服务。

[0074] 此外，已经描述了个人身份验证装置 3 和 4 可具有支付卡的形状。应该理解，还可

以将该装置插入移动电话中，更具体地是插入该移动电话的 SIM 卡中或简单的钥匙链中或任何其它支撑物中。

[0075] 此外，根据本发明的一个实施方式，可将终端 2 的生物特征读取器 5 和无线通信装置 7 插入可例如通过 USB 连接而连接至个人计算机的盒体中。因此，希望例如在互联网上进行安全支付的使用者可将该盒体连接至他或她的个人计算机，并且该使用者可通过使用盒体的生物特征读取器 7 对他或她自己进行身份验证，这仍然由于终端 2 与个人身份验证装置 3 之间存在无线通信，而无需将他或她的个人身份验证装置取出。

[0076] 终端 2 可用于进行需要使用者身份验证的所有类型的交易，更具体地可用于该使用者的支付或向该使用者分配的服务。

[0077] 更具体地，对与例如超级市场的商店中的付款台系统相关联的示例性终端 2 进行描述。该终端可包括：

[0078] - 实施所需处理的处理器；

[0079] - 临时存储存储器；

[0080] - 文字显示器；

[0081] - 键盘；

[0082] - 信用卡单据打印输出；

[0083] - 软件模块，例如应用的选择、设定、和警报的传输。

[0084] 该终端 2 连接至授权银行服务器并与例如在下文所描述的付款台连接。

[0085] 该付款台可更具体地包括：

[0086] - 与付款台工作人员的人 - 机界面；

[0087] - 账单打印机；

[0088] - 票据打印机；

[0089] - 文字显示器；

[0090] - 条码扫描；

[0091] - 用于计算金额和选择支付方法的软件模块；

[0092] - 付款台键盘。

[0093] 该付款台系统与终端 2 连接并与商店中的中央系统连接。

[0094] 现在对呈卡片 3 形式的个人装置 3 的实施方式进行描述。在该实施方式中，卡片 3 包括：

[0095] -CPU 处理器；

[0096] - 存储器；

[0097] - 唤醒装置，在下文中对唤醒装置的操作进行描述；

[0098] - 所谓的私人手动控制或“隐私”，其使使用者可以完全切断卡片的提供（隐私模式）或再次提供卡片；

[0099] - 电源；

[0100] - 在卡片上执行的软件模块，例如信号的检测、应用的管理。

[0101] 现在对卡片 3 与终端 2 之间的传输通道进行更详细的描述。

[0102] 传输通道更具体地包括：

[0103] - 非接触式通信通道，包括位于卡片 3 和终端 2 上的无线电通信电路；

[0104] - 在卡片 3 和终端 2 上接触的通信接口；

[0105] - 软件模块，在卡片 3 和终端 2 上执行，例如是接触式或非接触式通信驱动的形式。

[0106] 该传输通道唤醒卡片 3、提供数据的发出和接收、并提供安全的通信通道的打开和关闭。

[0107] 根据本发明的系统还包括电子支付和服务子系统，以提供支付交易，以及更具体地提供任何服务交易。该子系统更具体地管理与银行服务器的关系。

[0108] 电子支付和服务子系统包括在卡片 3 和在终端 2 上执行的软件构件。

[0109] 其更具体地执行以下功能：授权或拒绝支付、执行支付交易以及更具体地执行服务交易。

[0110] 优选地，根据本发明的系统还包括安全子系统，该安全子系统旨在保护客户、零售商和服务提供者，以免受到可能的欺诈、假冒以及在没有交易授权、身份验证功能、保密性、完整性（非变更）和认可的情况下进行的交易。该安全子系统包括在卡片 3 和终端 2 上执行的软件构件并且在需要的情况下还包括专用的密码电路。

[0111] 该子系统使以下成为可能：

[0112] - 对生物特征数据进行加密或解密；

[0113] - 相对于终端 2 对卡片 3 进行身份验证；

[0114] - 相对于卡片 3 对终端 2 进行可选的身份验证；

[0115] - 交换的加密和解密；

[0116] - 交换的签名。

[0117] 此外，安全子系统提供了对其它子系统中的安全需求的考虑。

[0118] 现在对卡片 3 或 4 的操作进行更详细的描述。

[0119] 处于“丧失隐私”状态的卡片可以处于在下文中描述的被称为“待命”、“倾听”和“活动”的三个模式中的一个模式下。在待命模式下，卡片的消耗被减小到进行持续时间为 T_1 的时间延迟所需的最小程度，其中持续时间 T_1 是待命模式的持续时间。

[0120] 在倾听模式下，卡片倾听处于一个或若干确定的频率上或者处于确定的频率范围的外部无线电信号（如果有的话）。

[0121] 该倾听频率不必与接下来将用于卡片与终端之间通信的频率相同。

[0122] 卡片上唯一提供的且有源的电路是用于信号的接收和检测以及经过持续时间为 T_2 的时间延迟所要求的电路，其中持续时间 T_2 是倾听模式的最大持续时间。

[0123] 在活动模式下，提供了卡片上的所有的电路。

[0124] 处于待命、倾听、和活动模式下的卡片各自的平均消耗分别被称为 P_v、P_e、和 P_a，并且符合不等式 $P_v < P_e < P_a$。

[0125] 时间延迟的持续时间 T_1 和 T_2 被调整为一方面使消耗最小化，另一方面能够对终端的请求快速做出应答。

[0126] 在以下情况下卡片切换到待命模式：

[0127] - 当卡片先前处于倾听模式下、时间延迟 T_2 已经过去并且未检测到任何信号时；

[0128] - 当与终端的通信会话异常结束时；

[0129] - 当该通信会话因以下原因而结束时：

[0130] - 使用者的生物特征身份验证阶段（“卡上匹配”）导致否定的结果；

[0131] - 卡片的选择阶段和应用的选择阶段导致放弃所述卡片；

[0132] - 例如当卡片离开范围时出现传输错误，并且宣称该传输错误不可挽回。

[0133] 当卡片之前处于待命模式且时间延迟 T_1 已经过去时，卡片切换到倾听模式。

[0134] 当卡片先前处于倾听模式时且一旦在时间延迟 T_2 结束之前已经在该模式下检测到终端的信号，卡片切换到活动模式。然后切断该时间延迟。

[0135] 当卡片以接触的方式被引入读卡器时，卡片切换到活动模式。

[0136] 因而在无外界电磁信号的情况下，卡片可选地且有规律地在由具有持续时间 T_1 的待命模式和具有持续时间 T_2 的倾听模式组成的循环中切换。

[0137] 在存在外界电磁信号时，该循环中断并且卡片切换到活动模式。

[0138] 该操作模式具有两个目的：一方面使卡片的消耗最小化并因此延长内部电源（电池）的寿命，另一方面使使用者受到的电磁辐射最小化。

[0139] 现在对根据本发明的系统的操作更详细地进行描述。在操作中，根据本发明的系统逐个执行以下步骤：

[0140] - 开始通信会话并在环境中唤醒卡片；

[0141] - 对使用者进行身份验证；

[0142] - 对待使用的卡片和应用进行选择；

[0143] - 支付或服务交易；

[0144] - 结束通信会话。

[0145] 现在对这些步骤逐个进行描述。

[0146] 可以通过特定的控制（例如压下键盘中的键）使根据本发明的通信会话开始，其中特定的控制由卡片携带者在终端上进行、或通过携带者的确定的动作（例如他或她的手或者他或她的一个或多个手指在生物特征读取器上出现）而由付款台工作人员在终端上进行、或通过这两个动作的组合在终端上进行。

[0147] 该开始使得终端 2 发出也被称为唤醒信号的无线电信号。

[0148] 位于终端环境中并处于倾听模式下的卡片检测到该信号然后切换到活动模式。

[0149] 从而为了将位于读取器范围内且不处于隐私模式下的所有卡片唤醒，有必要使终端以大于 T_1 的最小持续时间发出该信号。

[0150] 可以考虑两个选项：

[0151] - 该信号传送由生物特征指标更具体地计算得出的生物特征证书，而生物特征指标本身则在使用者的生物特征获取步骤过程中所获得的生物特征信息计算得到。该选项需要在该信号发出前进行生物特征信息的获取；

[0152] - 该信号不传送任何信息且仅简单地倾向于唤醒卡片；然后生物特征证书接着可以被传输。

[0153] 参照图 4，以下描述使用者的身份验证。

[0154] 由终端 2 从生物特征获取所计算得到的生物特征指标与存在于卡片 3、3A、3B 上的生物特征指标之间的比较进行身份验证。这种比较在卡片上进行（卡上匹配）。

[0155] 出于安全和隐私保护因素，生物特征指标以加密的方式从终端 2 被传输到卡片或多个卡片 3、3A、3B。

[0156] 可选地，执行传输生物特征指标之前的步骤，该步骤用于使终端向环境卡片传输

未编码的生物特征证书。

[0157] 通过携带者的确定动作（例如他或她的手或者他或她的一个或多个手指在之前由终端激活的生物特征读取器上出现），开始使用者的身份验证。

[0158] 该动作引起了通过与所使用的生物特征技术相对应的生物特征装置进行生物特征信息的获取。例如这可以是一个或若干手指的指纹或者手或者一个或若干手指中的静脉网络的图像。

[0159] 其还导致了对由生物特征装置或者由终端进行的、从所获取的生物特征信息产生的生物特征指标进行计算。该步骤旨在获得携带者的生物特征，该生物特征的量比生物特征信息的量少，并且因而能够以所要求的可靠程度对携带者进行识别。

[0160] 可选地，终端还可以计算生物特征证书，尤其是由生物特征指标计算。该可选的步骤旨在为过程的后续部分除去不合格卡片的最大部分，不合格卡片是这样的卡片，对于该卡片，存储在存储器中的生物特征指标的证书与由终端计算出的证书不匹配，而并不发出未编码的生物特征指标。

[0161] 如果已经执行了计算生物特征证书的可选步骤，那么终端 2 将该未编码的生物特征证书向环境中的卡片 3、3A、3B 传播 100、101、102。

[0162] 如果位于环境的终端中的卡片 3、3A、3B 之前已由来自终端且不带有任何信息的信号唤醒，那么这些卡片切换到活动模式并可接收来自包含生物特征证书的终端的新信号。

[0163] 如果位于终端的环境范围内的卡片之前未由来自终端且不带有任何信息的信号唤醒，那么包含生物特征证书的信号扮演唤醒信号的角色。因而，有必要使信号以至少等于 T_1 的持续时间（待命时期的持续时间）反复传输，以等待卡片切换到倾听模式然后切换到活动模式。

[0164] 因而被唤醒且位于该范围内的卡片 3、3A、3B 将所接收到的生物特征证书与从存储在卡片的存储器中的生物特征指标计算得出的生物特征证书相比较，或者直接与存储在卡片的存储器中的生物特征证书相比较。

[0165] 所进行的比较是否定的卡片，即两个证书不匹配的那些卡片，保持沉默并切换回到待命模式。在图 4 中，假设卡片 3B 进行否定比较并因而不发回任何肯定的比较信号。

[0166] 所进行的比较是肯定的卡片 3 和 3A，即两个证书匹配的那些卡片，保持在活动模式中，并将表明比较为肯定的未编码应答向终端 2 传输 110、111。

[0167] 在终端 2 与在第一步骤中进行肯定应答的卡片 3A、3B 中的每一个之间存在公共密钥 120、121 的交换。因而所有卡片和所有终端都必须在其自身的存储器中具有私人密钥 / 公共密钥对，以使得在每个卡片与终端之间打开安全的通信终端成为可能。

[0168] 然后，终端 2 将从生物特征获取计算得到的生物特征指标传输 130、131 到已在之前步骤中进行应答的所有卡片 3、3A。

[0169] 这些卡片对所接收到的生物特征指标进行解密并将其与卡片在其存储器中所具有的生物特征指标进行比较。

[0170] 所进行的比较是否定的一个或多个卡片保持沉默（或可选地这些卡片向终端发回否定的比较信号）并切换回到待命模式。在图 4 中，假设卡片 3A 执行否定的比较，使得卡片 3A 并不发回肯定的比较信号。

[0171] 相反，所进行的比较是肯定的一个或多个卡片向终端发回肯定的比较信号，并保持在活动模式下。在图 4 中，假设卡片 3 进行这种肯定的比较。可选地，它们可以与肯定的比较信号同时发回 140 它们所具有的候选应用的列表，以对卡片选择和应用选择的后续步骤进行准备。

[0172] 为指标的传输所打开的安全通信通道接着可用于终端 2 与已经进行了肯定的比较的卡片 3 之间的会话的结束 150。

[0173] 同一使用者可以拥有若干卡片，并且每个卡片可以包括若干应用。类似地，每个应用可以提供若干服务。在该情况下，需要能够对待使用的卡片以及该卡片的应用进行选择。卡片的选择和应用的选择同时且以如下方式进行。该步骤以由已经对卡片 3 的“候选列表”（即卡片所拥有的应用的列表）的生物特征比较进行肯定应答的每个卡片 3 向终端 2 进行传输而开始。

[0174] 因而例如可以通过相互不排斥的以下不同方式在该列表中进行选择：

[0175] - 除去未被终端识别的应用；

[0176] - 应用终端内部的或存在于“候选列表”中的优先原则；

[0177] - 通过由使用者或工作人员做出的动作进行应用的选择。

[0178] 在完成选择卡片和应用的步骤后仅选择了一个应用，并且根据具体情况，只有一个服务与该应用相关联。

[0179] 除选择卡片和应用的步骤以外且根据具体情况，必须实施该服务。

[0180] 如果该服务是支付服务，那么根据更具体地是当前的国际通行银行标准：EMV：欧洲支付 (Europay)、万事达卡 (Mastercard)、威士卡 (Visa)，对该服务进行实施。

[0181] 如果该服务是服务交易，那么交易的执行具体为所考虑的服务。

[0182] 还可以在同一安全交易终端内将若干应用交易相连。例如，可以在支付之后进行忠诚交易 (loyalty transaction)。

[0183] 如果出于任何原因无法完成服务交易，那么考虑具有在交易之前返回初始状态的可能性。

[0184] 完成支付或服务交易之后，卡片切换回到待命状态。

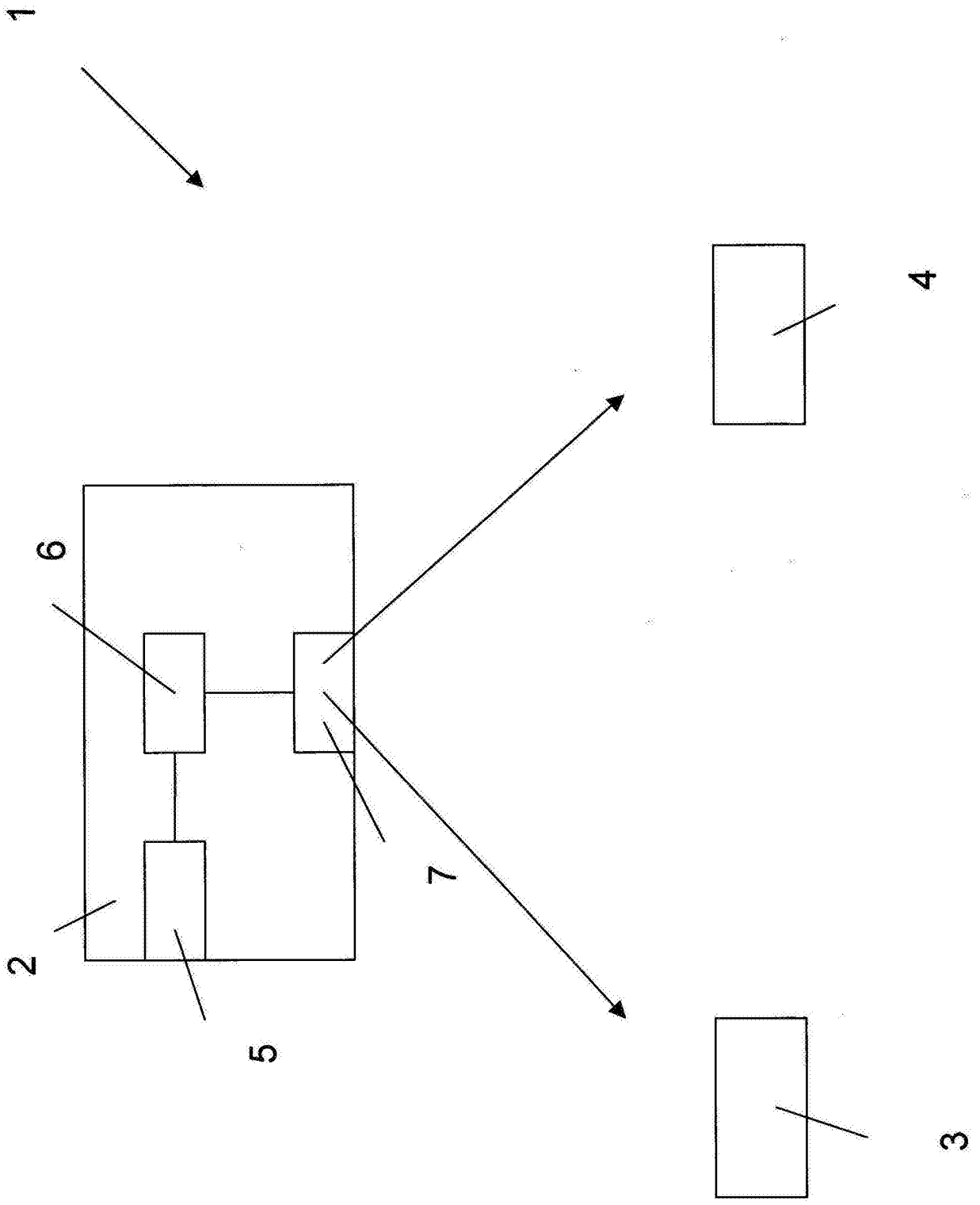


图 1

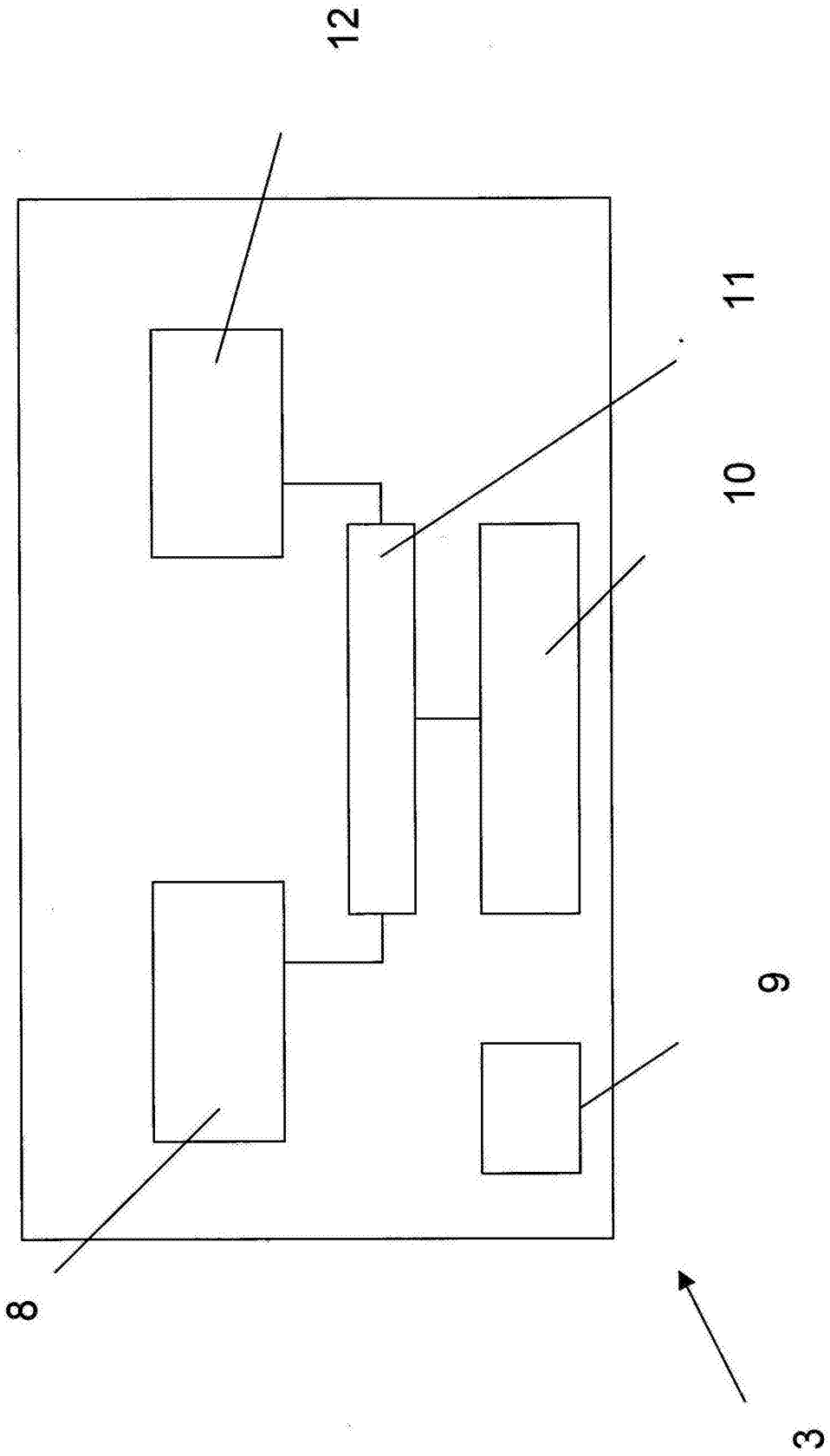


图 2

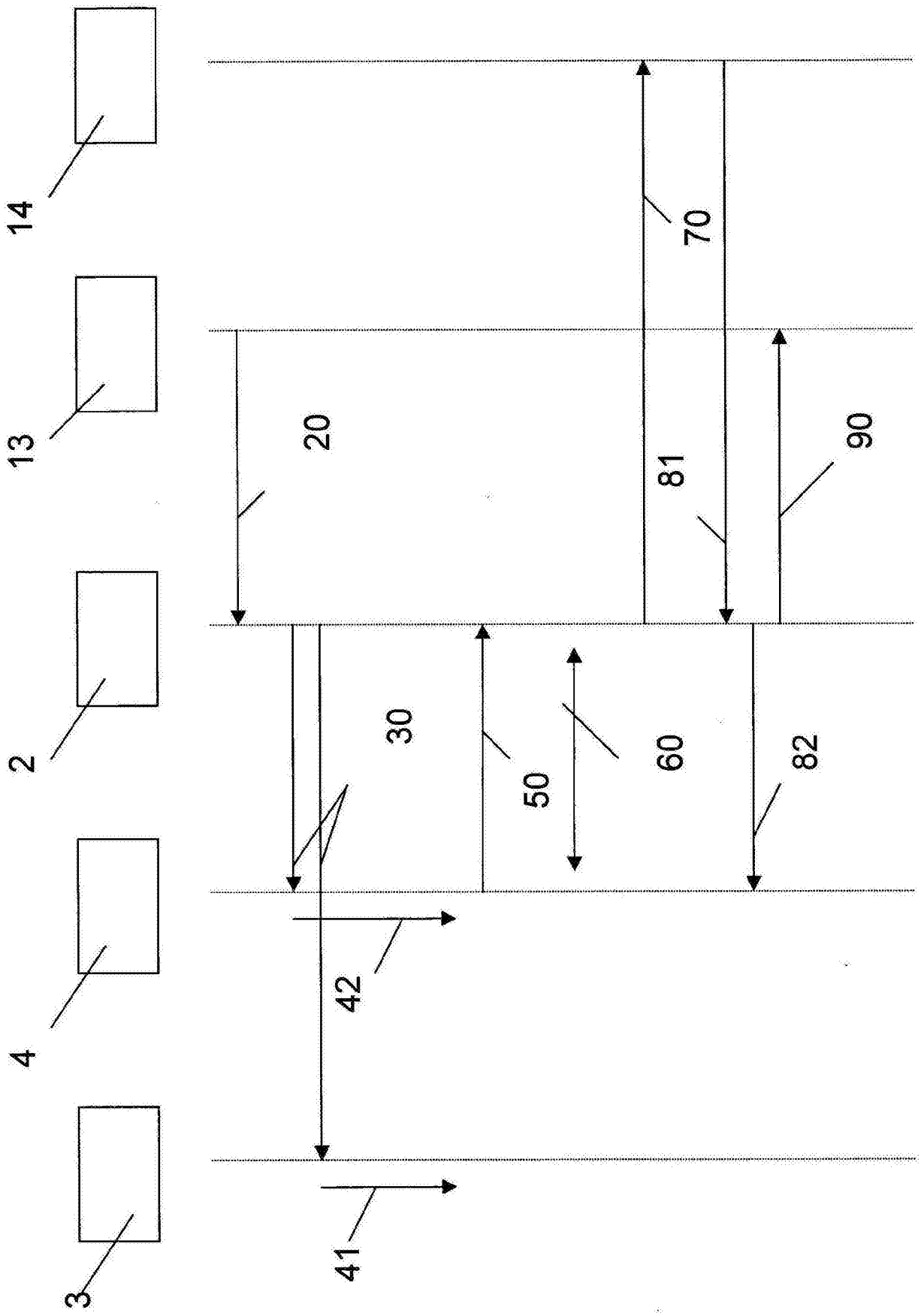


图 3

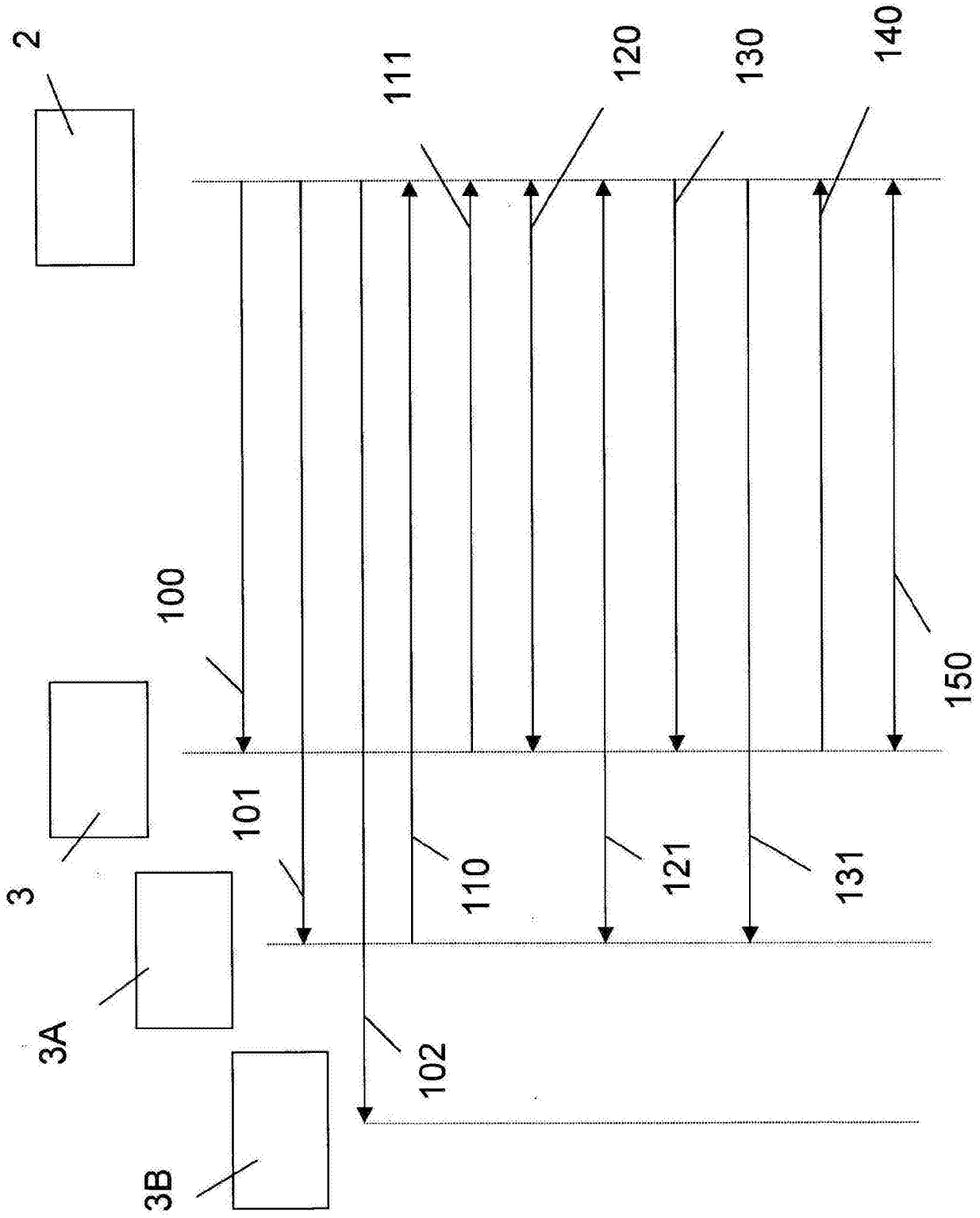


图 4