(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 103155010 B
(45)授权公告日 2016.12.14

(21)申请号 201180042772.6

(22)申请日 2011.08.10

(65)同一申请的已公布的文献号
申请公布号 CN 103155010 A

(43)申请公布日 2013.06.12

(30)优先权数据
10305956.4 2010.09.06 EP

(85)PCT国际申请进入国家阶段日
2013.03.05

(86)PCT国际申请的申请数据
PCT/EP2011/063786 2011.08.10

(87)PCT国际申请的公布数据
WO2012/031848 FR 2012.03.15

(73)专利权人 格马尔托股份有限公司
地址 法国默东

(72)发明人 P·吉拉尔 H·舒克里

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 殷瑞剑 刘春元

(51)Int.Cl.
G07F 7/10(2006.01)

(56)对比文件
US 2009031408 A1,2009.01.29,
US 2010058068 A1,2010.03.04,
US 2009049306 A1,2009.02.19,
US 5745571 A,1998.04.28,
DE 10117445 A1,2002.07.11,
US 2005071282 A1,2005.03.31,
CN 1914603 A,2007.02.14,
US 5721781 A,1998.02.24,
WO 9918533 A1,1999.04.15,
WO 0074007 A1,2000.07.12,
US 2003163688 A1,2003.08.28,

审查员 魏小丽

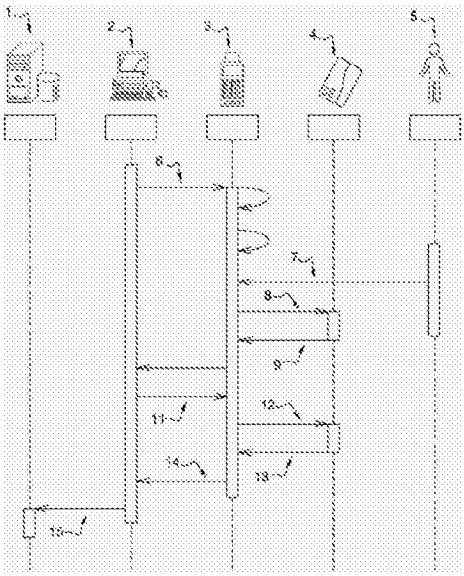
权利要求书2页 说明书6页 附图1页

(54)发明名称

用于对智能卡进行个人化的简化方法以及相关联的设备

(57)摘要

本发明涉及一种用于使用可适于标准认证装置的加密设备对电子设备进行个人化的方法。所述加密设备使得有可能确保秘密代码从用户至可能的个人化服务器的传送的保密性。



CN 103155010 B

1.一种用于由用户向个人化程序提供/传输秘密代码来对目标电子设备进行个人化的方法,使用安全终端(3)以及能够执行计算机程序的通信电子设备(2)对所述目标电子设备进行个人化,所述计算机程序被称为“个人化程序”,所述通信电子设备(2)被称为“计算机”,其特征在于,所述方法包括以下步骤:

-将不同于所述目标电子设备的安全电子设备插入到所述安全终端(3)中;

-所述个人化程序发送请求(6),所述个人化程序通过所述请求(6)请求所述安全终端向所述安全电子设备提交代码;

-用户(5)使用所述安全终端(3)的键盘来输入秘密代码,所述秘密代码被称为“所提供的代码”(7),并且,通过请求REQ(8)将所述所提供的代码传输至所述安全电子设备(4);

-将所述所提供的代码(7)保存在所述安全电子设备(4)的存储器中;

-所述个人化程序通过所述安全终端(3)将“得到加密后的Pin”命令(12)发送至所述安全电子设备(4);

-所述安全电子设备(4)使用密码算法ALG和密钥K来对所述所提供的代码(7)进行加密,以获得“加密后的所提供的代码”;以及

-将所述加密后的所提供的代码(13)传输至所述个人化程序,

-所述加密后的所提供的代码被进一步传输到负责所述目标电子设备的最终个人化的远程个人化服务器(1)。

2.根据权利要求1所述的用于由用户向个人化程序提供/传输秘密代码来对目标电子设备进行个人化的方法,其特征在于,所述请求REQ(8)是验证所述所提供的代码(7)的命令。

3.根据权利要求1至2之一所述的用于由用户向个人化程序提供/传输秘密代码来对目标电子设备进行个人化的方法,其特征在于,所述方法还包括验证步骤,在所述验证步骤期间,当所述安全电子设备(4)接收到所述所提供的代码(7)时,分析至少一个安全性规则。

4.根据权利要求3所述的用于由用户向个人化程序提供/传输秘密代码来对目标电子设备进行个人化的方法,其特征在于,所述安全电子设备(4)根据所述安全性规则的应用的结果,通过所述安全终端(3)向所述个人化程序回送不同的响应。

5.根据权利要求3所述的用于由用户向个人化程序提供/传输秘密代码来对目标电子设备进行个人化的方法,其特征在于,所述安全性规则包括验证所述所提供的代码的格式。

6.一种安全电子设备(4),其配置成被插入到安全终端中,并且所述安全电子设备(4)包括非易失性存储器、密码密钥K、密码算法ALG,其特征在于,所述安全电子设备(4)具有用于执行以下操作的装置:

-在验证所提供的代码的命令的构架内,将所述所提供的代码保存在所述非易失性存储器中;

-通过应用所述算法ALG和所述密钥K来对所述所提供的代码进行加密,以便获得“加密后的所提供的代码”;以及

-响应于“得到加密后的pin”命令,发送所述“加密后的所提供的代码”。

7.根据权利要求6所述的安全电子设备(4),其特征在于,所述安全电子设备(4)包括用于改变上下文的装置,其中专用于所述验证所提供的代码的命令的处理验证与所述上下文中的每一个相关联的所述所提供的代码的精度。

8.根据权利要求6或7中任一项所述的安全电子设备，其特征在于，所述安全电子设备在非易失性存储器中包括至少一个安全性规则。

9.根据权利要求8所述的安全电子设备，其特征在于，所述安全性规则包括验证所述所提供的代码的大小被包括在预定义边界Bmin和Bmax内。

10.根据权利要求8所述的安全电子设备，其特征在于，所述安全性规则包括验证组成所述所提供的代码的字符不相同。

11.根据权利要求8所述的安全电子设备，其特征在于，所述安全性规则包括验证组成所述所提供的代码的字符未形成因子1算术序列。

用于对智能卡进行个人化的简化方法以及相关联的设备

技术领域

[0001] 本发明涉及一种用于对智能卡进行个人化的简化方法。

[0002] 本发明更具体地涉及一种使得有可能在维持最高安全级别的同时通过标准智能卡读取器输入个人化信息的方法。

背景技术

[0003] 移动电子设备知道伴随着小型化的扩充。现今，电子设备可以是手持的，并且与已出现几年的旧台式计算机相比，具有更强的计算能力。

[0004] 对设备进行小型化并增强其容量时的这种伴随而来的演进在应用方面开辟了新视野。

[0005] 现今，移动电话或音乐播放器可以执行密码操作并对信息进行编码或解码。

[0006] 作为嵌入式电子设备的演进的先锋，微芯片在其应用中经历了这种演进。

[0007] 微芯片目前被嵌入到大量设备中。这些微芯片当然可以见于智能卡中，并且还可以见于电子身份证件中、智能自粘标签中等等。

[0008] 这种微芯片(还通称为“计算单元”)提供特别高的安全性能，当然，这使得它有可能将对其的利用集中于安全性或至少安全应用。

[0009] 因此，微芯片常用于政府或银行业务等。

[0010] 所有这些应用基于特别重要的步骤：个人化。该步骤是这样的一个步骤：在该步骤期间，将数据以及更特别地将秘密插入到芯片中。

[0011] 这些秘密中的一些可以与最终用户关联起来。例如，这种秘密还可以是秘密代码。该秘密代码(也被称为PIN CODE(代表“个人识别号码CODE”))使合法用户能够利用芯片进行识别。在银行卡的情况下，在交易之前请求用户给出他/她的秘密代码是一般惯例，以便确保他/她有权请求所述交易。

[0012] 为了执行这种操作：

[0013] -将卡插入到终端中；

[0014] -终端提示用户输入他/她的秘密代码；

[0015] -终端将输入代码发送至卡并从卡请求所述代码的识别；

[0016] -卡验证所述代码并向终端通知这种验证的结果。

[0017] 为了能够验证所提交的所述代码，卡必须知道这种代码的全部或部分。在单纯的实施方式中，卡由此知道所述代码，并将其与输入代码进行比较。在更先进的实施例中，卡具有与所述代码(例如，基于散列的代码)有关的一些信息并在输入代码中搜索相同信息。

[0018] 在任何情况下，卡需要知道所述代码的全部或部分以便能够验证它。

[0019] 电子设备及其应用的相当多数量的多样化引起每个用户要记忆的秘密代码的数目的显著增加。此外，该现象倾向于用户必须自己选择其秘密代码，以便更容易记忆这些秘密代码。

[0020] 那么，问题在于使用户参与极安全的个人化过程，最常集中在受保护的地方。

[0021] 第一个所考虑的解决方案在于:在个人化中心与用户之间建立远程通信。对于该步骤,由于用户一般处于分支(例如,银行或政府分支)中,所以这意味着在个人化中心与所有分支之间建立安全通信。

[0022] 该解决方案不久后被丢弃,这是由于安全个人化系统的如此多的潜在入口势必造成较大风险。

[0023] 第二个所研究的解决方案是每个分支具有安全加密单元(一般被称为HSM(代表“硬件安全性模块”))的设备。这种硬件安全性模块使得有可能在安全环境中对数据进行加密,并从而能够随后传输该数据。

[0024] 在较宽的意义上,HSM(硬件安全性模块)是被视为防篡改、提供密码功能的设备。该设备是提供安全性服务的设备的电子条目,安全性服务一般包括生成、存储、使用和保护密码密钥。

[0025] 在这种情况下,要加密的数据是由最终用户提供的数据,例如,他/她的秘密代码。

[0026] 在将数据传输至个人化中心之后,个人化中心具有用于对这些数据进行解密的资源(最通常的是另一HSM),并因此可以分析和处理该数据。

[0027] 该解决方案所遇到的问题在于这种HSM的极高成本。

[0028] 此外,在个人化链中使用新设备需要所述链的新认证。事实上,将这种极安全的过程提交至测试和证实的集合(被称为“认证”)。这种“标签”保证了专家检验整个系统的安全性的所有参与者。

[0029] 然而,将HSM或任何其他设备插入到这种链中需要新认证,这是极其昂贵的。

发明内容

[0030] 因此,本发明旨在提供一种在不修改个人化链中的设备的情况下的个人化方法,包括最终用户。

[0031] 首先,本发明描述了一种用于使用安全终端以及能够执行计算机程序(也被称为个人化程序)的通信电子设备(也被称为计算机)对电子设备(也被称为目标电子设备)进行个人化的方法,这种方法包括以下步骤:

[0032] -将不同于所述目标电子设备的安全电子设备插入到所述终端中;

[0033] -通过所述个人化程序发送其请求所述安全终端向所述安全电子设备提交代码的请求;

[0034] -用户使用所述终端的键盘来输入秘密代码(也被称为“所提供的代码”),并且,通过请求REQ将所述秘密代码传输至所述安全电子设备;

[0035] -将所提供的代码保存在所述安全电子设备的存储器中;

[0036] -所述个人化程序通过所述安全终端将《得到加密后的Pin(Get-encrypted-Pin)》命令发送至所述安全电子设备;

[0037] -所述安全电子设备使用密码算法ALG和密钥K来对所述所提供的代码进行加密,以获得“加密后的所提供的代码”;

[0038] -将加密后的所提供的代码传输至所述个人化程序。

[0039] 所述请求REQ可以是验证所提供的代码的请求。

[0040] 然后,可以将这种加密后的所提供的代码传输至远程个人化服务器。

[0041] 所述个人化方法还可以包括验证步骤，在所述验证步骤期间，当所述安全电子设备接收到所提供的代码时，分析至少一个安全性规则。

[0042] 所述安全电子设备可以根据安全性规则的应用的结果，通过所述终端向所述个人化程序发送回不同的响应。例如，这种安全性规则可以包括验证所提供的代码的格式。

[0043] 其次，本发明还描述了一种安全电子设备，包括非易失性存储器、密码密钥K、密码算法ALG，其特征在于，所述安全电子设备具有用于执行以下操作的装置：

[0044] -在验证所提供的代码的命令的构架内，将所提供的代码保存在内部存储器中；

[0045] -通过应用算法ALG和密钥K来对所提供的代码进行加密，以便获得“加密后的所提供的代码”；

[0046] -响应于《得到加密后的pin》命令，发送“加密后的所提供的代码”。

[0047] 这种设备可以包括下面这样的装置：使得有可能改变上下文(context)，使得有可能验证所提供的代码的精度与所述上下文中的每一个相关联的专用于命令的处理。

[0048] 这种设备还可以包括在非易失性存储器中的至少一个安全性规则。例如，这种安全性规则可以包括通过验证组成所提供的代码的字符不相同，或者通过验证组成所提供的代码的字符未形成因子1(factor one)算术序列，来验证所提供的代码的大小落入预定义边界Bmin和Bmax内。

[0049] 本发明的一个优势在于：可以针对非常低的成本对根据本发明的个人化链进行适配。事实上，管理设备(也被称为加密设备)以及更特别地智能设备(如果该格式是优选的)的成本与所有分支的具有HSM的设备完全不同。

附图说明

[0050] 在参照附图的同时，在指示性而非限制性的以下描述中详述提及本发明的其他特性和优势，在附图中：

[0051] -图1示出了示意根据本发明的方法的序列图。

具体实施方式

[0052] 现在，已经为易于实现根据本发明的个人化方法的几乎所有销售点提供了计算机2、智能卡读取器3和数字连接。

[0053] 本发明提供了对安全电子设备4(也被称为“加密设备”，例如，智能卡)的利用。这种加密设备能够接收至少2个命令：使得有可能验证所提供的代码7的精度的命令8；以及《得到加密后的pin(get-encrypted-pin)》命令12。

[0054] 例如，验证命令8可以是“验证pin(verify pin)”命令(ISO 7816-4)：

[0055] 该验证Pin命令在卡内发起由接口设备发送的验证数据与卡中存储的参考数据(例如，密码)的比较。

[0056] 《得到加密后的pin》命令12将使卡能够回送13所提供的代码7的加密后的值。

[0057] 优选地，这种命令将由计算机2通过读取器3来发送。如果需要这样，则将在读取器的一般命令中密封该命令，以实现与卡的通信。

[0058] 在一个实施例中，当且仅当事先已经执行验证命令8时，得到加密后的Pin命令才能够回送加密后的PIN。

[0059] 然而，加密设备4能够以原始方式处理这些命令。

[0060] 事实上，在根据本发明的一个所谓的个人化实施例中，所述加密设备在接收到“验证pin”命令时，将所提供的pin代码作为参数保存在内部存储器中。所述加密设备利用任意答复(例如“OK”)来回应，这意味着已经正确执行“验证pin”并且结果是肯定的。

[0061] 在接收到得到加密后的Pin命令12时，加密设备使用密码算法ALG和密钥K来对所述所提供的pin代码7进行加密。

[0062] 这种加密可以是使用本领域技术人员已知的任何加密装置(更特别地使用对称或非对称算法)来执行的。

[0063] 对称密码术或秘密密钥密码术基于两个参与者对秘密的共享了解。

[0064] 所使用的算法(诸如例如，DES、3DES、AES、……)基于以下事实：当你知道消息的加密时，几乎不可能在不知道用于加密的密钥的情况下找到明文消息。

[0065] 非对称密码术或公共密钥密码术基于不可逆函数的存在。

[0066] 因此，公共密钥密码术是使用密钥对的非对称密钥系统。这种密钥(一般被称为“公共密钥”和“私用密钥”)被如此设计以使得已利用一个密钥加密的内容仅可以被第二个密钥解密。

[0067] 应当注意，不可能根据公共密钥猜到私用密钥。

[0068] 生成公共密钥/私用密钥对不是本发明的目的。现有技术中描述的所有方法或者使得有可能获得这种密钥对的未来方法适用于本发明。

[0069] 使得有可能将几个私用密钥与一个公共密钥相关联的“组加密”类型的密钥(其中，每个密钥都使得有可能对已利用公共密钥加密的内容的全部或部分进行解密)可以完美适用于本发明。

[0070] 因此，作为对得到加密后的pin命令的答复，加密设备回应所述加密后的所提供的pin代码。

[0071] 在优选实施例中，加密设备4包括使得有可能验证用户的身份的安全性和认证机制，例如本领域技术人员已知的那些机制。

[0072] 特别适于本发明的解决方案在于利用上下文创建。事实上，在登录时(例如，当对加密设备上电时)，《验证pin》命令具有所谓的标准操作(标准上下文)，该标准操作遵守7616-4(或者ETSI102-221)标准中对其的描述。当用户的认证成功时，设备可以自动地或按照所提出的标准来切换至根据本发明的所谓的加密上下文。在该实施例中，“验证pin”命令根据本发明进行操作，如上所述。

[0073] 在图1所示的示例性利用中，例如，用户5去往银行的柜台，以选择未来银行卡的pin代码。

[0074] 负责该个人化操作的金融顾问将他/她自己的加密卡4插入到智能卡读取器3中。

[0075] 在所述智能卡读取器所连接至的计算机2上执行根据本发明的个人化程序。

[0076] 该程序向卡读取器发送pin代码6验证命令(验证pin)。读取器切换至安全模式，并等待候选pin代码。

[0077] 用户5在卡读取器的安全键盘上输入他/她希望插入到他/她的未来银行卡中的pin代码7。

[0078] 将所提供的pin代码7作为pin代码验证命令8的参数传输至加密卡。

[0079] 然后，加密卡4将所提供的pin代码7保存在其内部存储器中。

[0080] 在本发明的简单实施例中，加密卡回送任意答复9(例如OK)。

[0081] 在本发明的更先进实施例中，有利地，卡可以包含所提供的pin代码验证规则的集合，以便确保遵守预定义的安全性规则。例如，卡可以验证组成所提供的pin代码的数字的数目落入预定义Bmin边界和Bmax边界内。这种边界可以是在安全性规则中预定义的，或者是通过在所述计算机上执行的个人化程序来传输的，例如作为验证pin命令的参数。

[0082] 这种安全性规则还可以验证组成所提供的代码的所有数字是不相同的，或者这些数字未形成平凡(trivial)数学序列，例如因子1算术序列等。

[0083] 在该实施例中，卡响应于pin代码验证命令(如果遵守规则，则为OK；如果不遵守规则，则为KO)而回应。卡读取器将该答复传输至在计算机上执行的根据本发明的个人化程序。

[0084] 在一个实施例中，进一步对于pin代码的肯定验证，加密卡可以切换至第三上下文，即，确认上下文。

[0085] 在该上下文中，卡将等待至少新pin代码验证命令，并验证所提供的pin代码确实相同。如果所提供的pin代码确实与事先提供的pin代码相同，则该新pin代码验证将被视为成功。出于优化目的，以及在将安全性规则应用于所提供的pin代码的情况下，有利地，可以将这种规则仅应用于第一个所提供的pin代码，只是接下来的所提供的pin代码必须与所述第一个所提供的pin代码相同。

[0086] 这种上下文使得有可能避免在输入pin代码时键入差错。

[0087] 出于安全原因，本发明的优选实施例在该方法的该阶段处包括向标准上下文的返回，以便再一次确认持有加密卡的雇员的身份。

[0088] 然后，在计算机2上执行的个人化程序通过智能卡读取器3来做出《得到加密后的pin代码》请求11、12。在接收到这种命令时，加密卡4回送利用密码算法和密钥而加密13的所提供的pin代码。

[0089] 有利地，可以实现本领域技术人员已知且使得有可能优化加密安全性的所有机制。更特别地，导出密钥，以便不系统地使用相同密钥，将变量插入到加密计算中，或者在所述加密中利用OTP(“一次性密码”)。OTP是仅使用一次的所生成的值。

[0090] 可以实现在保证由被授权设备对数据条目的后续解密的同时使得有可能增强系统安全性的所有机制。

[0091] 这种加密有可能使所输入的pin代码决不会在卡外以明文示出。因此，用户是知道这种pin代码的值的仅有的人。执行操作的金融顾问无法获得该值。

[0092] 加密卡将加密后的pin代码13传输至智能卡读取器，智能卡读取器进而将其传输14至在计算机上执行的个人化程序。

[0093] 然后，计算机可以将加密后的pin代码传输15至负责未来智能卡(被称为目标电子设备)的最终个人化的数据处理服务器1。这种服务器1具有在最优安全条件下对所述pin代码进行解码所需的密码装置。与该服务器相连接的HSM(硬件安全性模块)特别适于该方法的这种步骤。

[0094] HSM是安全电子设备，并确保对隐私和安全性的最安全保证。

[0095] 这种传输可以由本领域技术人员已知的任何装置执行，以实现对数字数据的交

换。在优选实施例中，这种传输是通过网络在安全模式中执行的。

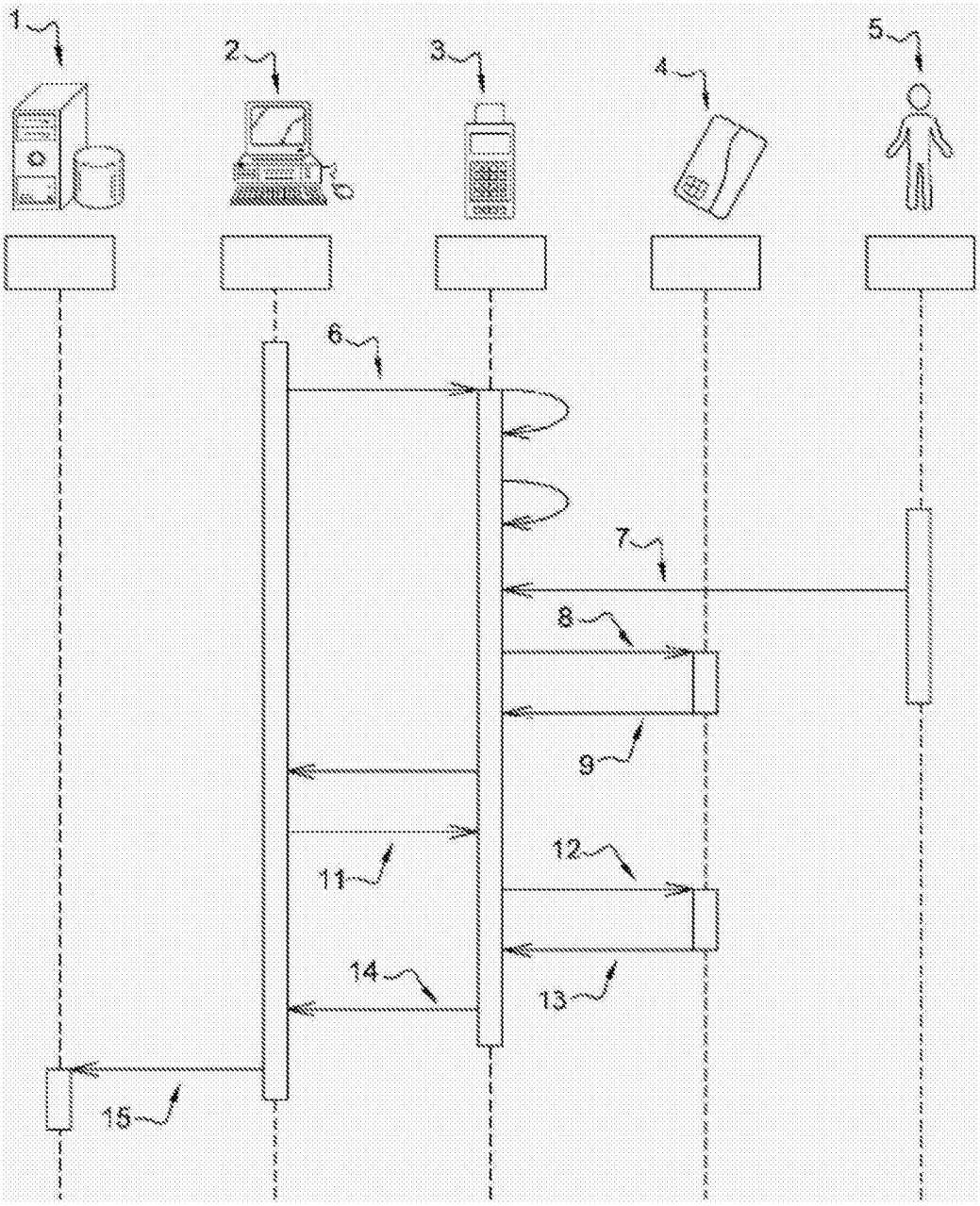


图1