[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
G07F 7/10

[12]发明专利申请公开说明书

[21]申请号 98809469.X

[43]公开日 2000年10月25日

[11]公开号 CN 1271449A

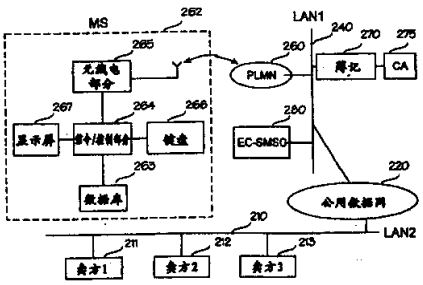
[22]申请日 1998.9.25 [21]申请号 98809469.X
[30]优先权
[32]1997.9.25 [33]FI [31]973788
[86]国际申请 PCT/FI98/00761 1998.9.25
[87]国际公布 WO99/16029 英 1999.4.1
[85]进入国家阶段日期 2000.3.24
[71]申请人 诺基亚网络有限公司
地址 芬兰埃斯波
[72]发明人 莱西·西伯拉宁
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 王以平

权利要求书3页 说明书14页 附图页数2页

[54]发明名称 电子支付系统

[57]摘要

用来在电子支付系统中确认交易的装置和方法，所述电子支付系统包括用来提 供与收到的支付相应的电子收据的第一处理装置(211、212、213; 47)，用来接收所述收据的第二处理装置(270;49)，以及用来在所 述第一和第二处理装置以及所述第一支付装置之间传送所述收据的传送装置(210、220、240、280;46、48)。用一种公共密钥算法对所 述电子收据或其某些部分进行加密，加密时将受款人的专用密钥用作加密密钥，对收据解码时也利用公共密钥算法，并将受款人的公共密钥用作解码密钥，如 果所述收据的受票人希望确认收据的真实性，他就用受款人的公共密钥对加密 的收据解码。用受款人的专用密钥进行的数字加密可以准确无误地证明收据的来源。只要收据是加密格式，如果不确切地知道受款人，则收据不可能被读出，对收据的伪造也是不可能的。电子收据能够轻易地在不同的目的地之间读出和 传送。



ISSN1008-4274

00.03.24

权 利 要 求 书

1. 一种电子支付系统，包括用来生成与收到的支付相应的电子收据的第一处理装置(211、212、213；47)、用来接收所述收据的第二处理装置(270；49)，以及用来在所述第一和第二处理装置之间传送所述收据的传送装置(21、220、240、280；46、48)，其特征在于：

如果需要的话，所述第一处理装置(211、212、213；47)用来对要生成的电子收据或其一部分进行加密，加密时使用一种公共密钥算法，并将受款人的专用密钥用作加密密钥；

所述第二处理装置(270；49)用来对接收到的收据解码，解码时利用公共密钥算法，并将受款人的公共密钥用作解码密钥。

2. 如权利要求 1 所述的电子支付系统，其特征在于，所述支付系统还包括用来以电子形式进行支付的第一支付装置(262；41)，该支付装置能够接收电子收据，并能通过所述传送装置传送所收到的电子收据。

3. 如权利要求 2 所述的电子支付系统，其特征在于，所述第一处理装置(211、212、213；47)用来根据所作出的支付将生成的电子收据发送给所述第一支付装置(262；41)，所述第一支付装置用来将所述收据传送到所述第二处理装置(270；49)。

4. 如权利要求 3 所述的电子支付系统，其特征在于，必要时，所述第二处理装置(270；49)用来将与所接收到的收据相应的金额转到所述第一支付装置(270；49)。

5. 如权利要求 1 到 4 之任何一项所述的电子支付系统，其特征在于，所述第一处理装置(211、212、213；47)由卖方的收款系统构成，所述第二处理装置由所述收据的最终受票人的收款系统(270；49)构成。

6. 如权利要求 5 所述的电子支付系统，其特征在于，所述第一支付装置包括一个存储卡或者一个智能卡(41)，所述传送装置包括所述卡的与收款系统相连的读写接口(46、48)。

7. 如权利要求 5 所述的电子支付系统，其特征在于，所述第一支付装置包括一个移动站，所述传送装置包括下列装置的至少一种：一个与所述移动站相连的移动通信网(260)、公用数据网(220)、与所述第一或第二处理装置相连的局域网(210、240)。

8. 如权利要求 7 所述的电子支付系统，其特征在于，所述传送装置还包括一个连接到所述移动通信网的短消息服务中心(280)，用来借助于短消息服务向所述移动站(262)传送电子收据。

9. 如前述权利要求之任何一项所述的电子支付系统，其特征在于，所述系统包括至少一个签证管理文件(275)，用来维护连接到所述系统的装置的公共密钥。

10.如权利要求 9 所述的电子支付系统，其特征在于，连接到所述系统的所述装置中的一个或者多个维护一个其自身的签证管理文件(275)。

11.如前述权利要求之任何一项所述的电子支付系统，其特征在于，所述第一处理装置(211、212、213；47)用来将交易输入一个记录表，并具有一个标识，根据该标识，对于被加密的所述电子收据，能够从所述记录表中检索出交易来。

12.如权利要求 11 所述的电子支付系统，其特征在于，所述第一处理装置(211、212、213；47)如此设计，使得在所述电子收据的加密部分包括一个标示支付额的部分。

13.一种在电子支付系统中确认交易的方法，所述电子支付系统包括用来提供相应支付的电子收据的第一处理装置(211、212、213；47)，用来接收所述收据的第二处理装置(270；49)，以及在所述第一和第二处理装置之间传送所述收据的传送装置(21、220、240、280；46、48)，其特征在于：

所述电子收据或部分电子收据被加密，加密时使用一种公共密钥算法，并将受款人的专用密钥用作加密密钥；

对所述电子收据解码时，使用一种公共密钥算法，并将受款人的公共密钥用作解码密钥。

14.如权利要求 13 所述的方法，其特征在于，电子收据被发送给第一支付装置(262; 41)，后者能够接收电子收据并将先前接收到的电子收据通过所述传送装置传送到所述第二处理装置(270; 49)。

15.如权利要求 14 所述的方法，其特征在于，必要时，将与所接收到的电子收据相应的金额转到所述第一支付装置。

16.如权利要求 15 所述的方法，其特征在于，所述电子收据借助于短消息服务在所述移动通信系统中传送。

17.如权利要求 13 到 16 之任何一项所述的方法，其特征在于，将交易输入一个记录表，并在所述电子收据的要加密的部分包括由所述第一处理装置提供的所述标识，根据该标识能够从所述记录表中检索出所述交易来。

18.如权利要求 17 所述的电子支付系统，其特征在于，在所述电子收据的加密部分包括一个标示支付额的部分。

19.用来处理电子交易的装置(211、212、213; 47)，包括用来生成与支付相应的电子收据的装置，其特征在于:

所述装置(211、212、213; 47)用来对所生成的电子收据或其一部分进行加密，加密时使用一种公共密钥算法，并将受款人的专用密钥用作加密密钥。

20.用来处理电子交易的装置(270; 49)，包括用来接收电子收据的装置，其特征在于:

所述装置(270; 49)用来对接收到的收据解码，解码时利用公共密钥算法，并将受款人的公共密钥用作解码密钥。

00·03·24

说　　明　　书

电子支付系统

发明背景

本发明涉及通信网络中的电子支付方式，尤其是电子支付系统，包括用来生成与收到的支付相应的电子收据的第一处理装置、用来接收所述收据的第二处理装置，以及用来在所述第一和第二处理装置之间传送所述收据的传送装置。

由于通信网络使用的上升，电子支付方式的使用已变得更加普遍。在不久的将来，对各种服务、有形货物或者信息的支付将在买方和卖方之间越来越经常地以电子货币的形式进行。它们通常称为电子代用币。

由于安全方面的不确定性，电子支付系统的采用已经有所延迟。在协议层，标准的拟订已经有了很大的进展，例如，SET(Secure Electronic Transaction)标准(电子交易安全标准)将很快投入使用，该标准包括若干加密和鉴别功能，借助于这些功能，与交易有关的数据传输能够可靠地进行。

在协议层之上的应用层，操作规程和实际应用依然多种多样。所以已经有几个国家制定了制度和条例，来保护消费者免受与电子交易有关的错误和权利滥用的侵害。例如，美国已经颁布了 E 条例，规定，用于电子交易的系统必须提供系统所执行的所有交易的收据，并定期为用户提供书面的交易清单。对于这种要求通常是这样执行的：在每次交易之后，系统就向存储用户电子代用币的装置发送一个记录，作为电子收据。

对于利用电子支付系统来进行简单的个人支付的普通用户来说，这样的收据完全足够了。但是，有大量的用户其支付交易更为复杂，所以登记的顺畅、收据的传送和鉴别就显得更为重要。例如，可能事后请求雇主支付特定费用的雇员，或者同时有多个项目而要单独对每

个项目收费的顾问，就或者是必须有单独的装置(此后称为“钱包”)来存储各个开单目的地的电子代用币，或者是被迫浪费时间来对开给不同目的地的收据进行存储、确认、转换和传输。前一种方式随着“钱包”数目的增加很快就会变得难以管理。而后一种方式浪费时间，使得用户不能享用先进的数据传输所带来的好处。

另一方面，收据的最终收据人(end-receiver)，例如雇主、顾客或者接受扣税票据(tax-deductible bills)的税务机关，需要确认收据是有真实的交易基础的，确实是由受款人开出的。但收据的分别签证难以实现，而在电话接洽的小单业务(small telephone bills)的情况下，分别签证甚至是无利可图的。基于银行报表(bank statement)的签证继而会削弱开票人的信息安全，因为在这种情况下，接收所述清单的人同时会接收到与所述用户“钱包”有关的所有交易的信息。

发明方案概述

本发明的一个目的是提出一种电子支付系统，其中，交易时用到经签证的、准确无误的电子收据，所述电子收据易于传输，使用这种电子收据，当收据被传输时，相对于其他的支付活动，本付款人的信息安全能够得到保护。一张电子收据主要包括以电荷或磁荷强度表示的信息单元，这些单元可由电子装置读写。

本发明的目的是由在引言部分所描述的电子支付系统实现的，其特征在于，如果需要的话，第一处理装置用来对要生成的电子收据或其一部分进行加密，加密时使用一种公共密钥算法，并将受款人自己的密钥用作加密密钥；第二处理装置用来对接收到的收据解码，解码时利用公共密钥算法，并将受款人的公共密钥用作解码密钥。

本发明还涉及一种如权利要求 13 所述的方法，用来在所述电子支付系统中确认一项交易，所述电子支付系统包括用来提供相应支付的电子收据的第一处理装置，用来接收所述收据的第二处理装置，以及在所述第一和第二处理装置之间传送所述收据的传送装置。该方法的特征在于，所述电子收据或部分电子收据被加密，加密时使用一种公共密钥算法，并将受款人的专用密钥用作加密密钥；对所述电子收据

解码时，使用一种公共密钥算法，并将受款人的公共密钥用作解码密钥。

本发明作为基础的系统包括加密装置，用来对电子收据利用一种公共密钥算法完全地或部分地加密。加密是利用受款人的专用密钥进行的，这样，加密就相当于所述收据上的电子印签。如果收到收据的人想要确认收据的真实性，他就可以用受款人的公共密钥解码。所述收据是电子形式的，因此容易读取，并易于在各目的地之间传输。用受款人专用密钥进行的数字加密可以准确无误地证明收据的来源。只要收据是加密状态，如果不确切地知道受款人是谁，它就不能被读出，而且，包括在收据的加密部分中的信息也是不可能被伪造的。

收据的要被加密的部分最好包括一个交易标识、支付金额以及对支付原由的说明。卖方可以根据所述标识来区分他自己的交易记录表中的各次交易。加密文本最好还包括一个校验区，用它来核实加密是否被正确执行。加密也可以是可选的，这样，仅当收据需要经签证的时候才使用加密功能。

本发明的所述方法和系统的一个优点是，通过维护签证级别，该电子支付系统的用户能够提供经签证的准确无误的交易收据，并能传输所述收据以供进一步处理。要被转移到各个不同的目的地以供存储或者入帐(crediting)的支付额能够从同一个电子“钱包”支出，而不管最终付款人是谁，也不必损害与金额的入帐有关的“钱包”的信息安全。

图面简要说明

下面参照附图结合优选实施例对本发明作更为详细的说明，附图中：

图 1 是一个框图，用以大体上说明本发明的基本思想；

图 2 是一个功能框图，用以说明本发明的一个优选实施例；

图 3 是一个信号图表，用以说明本发明的另一个优选实施例；

图 4 是一个框图，用以说明本发明的另一个优选实施例；

图 5 是一个流程图，用以说明本发明的与图 4 所示实施例有关的

方法。

本发明的详细说明

下面参照图 1 的方框图对本发明的基本原理加以说明，然后再用更具体的例子对所述原理进一步说明。电子收据是一项电子交易的一部分，在电子交易中，支付以电子代用币的形式通过通信网络 11 在卖方 10 和买方 12 之间进行。在交易之后，买方 12 希望将收据传输到目的地 13 作进一步处理。对于本发明的基本思想，所述卖方 10 和买方 12 的装置、网络 11 的具体结构以及要使用的协议本身都不是相关的，条件是，必须有一个支持基于公共密钥的加密的电子系统。

在现有技术的解决方案中，接受买方 12 的支付之后，卖方 10 生成一个电子收据，通常是一个记录，该收据被传送到买方 12 的存储电子代用币的装置亦即“钱包”。当买方 12 希望将收据传送到目的地 13 时，他就例如打印出他“钱包”中的一个记录或者所有记录的清单，将硬拷贝发送到所述目的地，或者电子传输所述记录的一个拷贝到所述目的地 13。但是，显然，这样的未经签证的收据只能在基于相互信任的交易中使用，而且这样做对于簿记来说是没有法律效力的。而对硬拷贝的处理又会不必要地增加维护一个“钱包”所需的工作量。

在本发明的解决方案中，卖方 10 生成一张收据，并最好在该收据上提供一个标识，该标识例如可以是一个流水号、一个时间戳或者另一个字符串，利用该标识，事后就可以在该买方的记录表中找到对应于该收据的登记项。该收据最好还显示出转移的金额以及对该笔交易的说明。然后，卖方的服务器将该收据或选择其一部分加密，加密时用卖方的专用密钥用作加密密钥。被加密的部分最好至少包括所述标识以及转移的金额。

用公共密钥进行加密的数学基础是单向陷门函数。这种函数在一个方向容易求解，在相反的方向则极难求解，但是在难解方向，经过选择的加密的特别信息可以显著地简化求解过程。加密中使用两个密钥：一个专用密钥和一个公共密钥。根据公共密钥通过计算来确定专用密钥实际上是不可能的。在普通加密中，拥有公共密钥的人使用的

是函数的易解方向，能够用该公共密钥对信息加密，但是不能够对加密的信息解码。所述专用密钥就是所述的特别信息，利用该专用密钥，可以在所述难解方向解出所述函数，并能够利用该专用密钥对加密文本解码。

在某些公共密钥算法中，加密可以用公共密钥或专用密钥进行，解码则可用另一个密钥进行。这样的算法的一个例子就是广泛使用的RSA(Rivest, Shamir and Adleman)算法。如果用专用密钥对文本加密，则可以公共密钥解码，对文本的加密就用作了可靠的电子印签。这种电子印签要在本发明的电子收据中使用。

卖方 10 将用作收据并经卖方专用密钥加密的一个记录 11 通过网络 11 传送给买方 12。该买方 12 可以将收据以加密形式存在“钱包”中，或者，买方 12 可以将其解码，象通常那样在需要的时间内将明文的收据存在其“钱包”中。利用本发明，买方 12 还可以将收据以加密形式直接传输到目的地 13，在该目的地，用卖方的公共密钥作为解码密钥对其解码。如果解码正常地成功，目的地 13 就知道有关收据是由卖方 10 发出的收据，并且，至少收据加密部分的信息都是绝对正确的，该信息最好包括卖方专用的标识、支付的说明以及支付的额度。

另一方面，买方能够可靠地传输收据，并自动地检索已经与交易相关联的贷方金额。如果买方 12 将电子“钱包”的全部内容都传送到了目的地 13，则该目的地 13 只能对来自该钱包的下面这些收据解码：目的地知道该“钱包”所属的卖方，从而也知道该卖方的公共密钥。对于其他的支付，信息是安全的。如果费用的转帐是连续的(例如雇主或者顾客)，就可以在所述买方和所述目的地之间确定一个操作，通过它，目的地的簿记惯例所需的任何额外的说明都可以直接添加到所述收据上，并且，这样的话所述支付就能够直接登记到正确的目的地。使用这种电子支付系统允许进行例如匿名支付，这样，有关最终付款人的信息就不需要与交易关联。同时，可以尽量减少金额入帐的延迟。

对公共密钥的管理是应用用途专有的选择，而不属于本发明的基本原理部分。买方 12 可以同收据一起将卖方的公共密钥传送到目的地

13，或者，目的地 13 的服务器可以将准备接收其收据的这些卖方的公共密钥存储起来。如果必要的话，负责管理公共密钥、由某个可靠的机构维护的一个独立的签证管理文件 CA 可以连接到网络中。

如上所述，本发明可应用于任何支持基于公共密钥的加密的电子支付系统。本领域的技术人员可以以多种不同的方式实现所述电子收据。例如，所述电子收据可以是一个记录，可以通过一个读写装置存储在一个存储卡中。所述电子收据也可以由一个或多个通过通信网络传输的信号构成。由于所述收据的可传输性和易于进一步处理性是本发明最为鲜明的优点，下面将结合移动通信系统对本发明作更详细的说明，但本发明并不局限于所描述的组织结构，连接的形式或者所提及的支付协议仅作为例子而已。下面，将通过一个应用于数字 GSM 移动通信系统中的支付系统对本发明的一个优选实施例进行详细说明。至于对所述 GSM 系统的更为准确的说明，请参看 GSM 推荐技术标准以及《用于移动通信的 GSM 系统》(*The GSM System for Mobile Communications*, M. Mouly and M.B. Pautet, Palaiseau, France, ISBN: 2-9507190-0-7)。

图 2 概要示出了一种电子支付系统的功能框图，按照本发明的原理，该系统能够在卖方 211、212 和 213、一个买方 261 以及一个目的地 270 之间通过网络 210、220、240 传输可靠的电子收据。

所述卖方 211、212 和 213 通过一个局域网 LAN 210 连接到一个公用数据网 220。图 2 的框图示出了卖方的计算机或者收款系统(cash systems)，卖方就通过所述计算机或收款系统处理他们的电子交易。在本发明的方案中，所述计算机和收款系统最好用一个公共密钥算法对选择的文本加密。如果卖方的终端装置不能执行加密操作，可以向所述局域网 210 连接一个服务器，由该服务器在收据通过所述公用数据网 220 发送到买方 261 之前对该收据加密。

买方 261 有一个移动站 MS 262 供其支配，该移动站通过一个公用移动通信网(公用地面移动通信网，Public Land Mobile Network, PLMN)，例如 GSM 移动通信网，连接到一个局域网 LAN1 240，并

通过该局域网连接到所述公用数据网 220。所述局域网 LAN1 240 可以是例如一个 PLMN 操作者自身的局域网。与所述局域网 LAN1 一起，有一个独立的电子货币短消息服务中心 EC-SMSC，在本实施例中，就通过该中心进行与用户 261 的交易有关的信号传输工作。

在移动通信系统中，在某个基站和某个移动站之间有一条用于数据或者语音传输的业务信道 TCH，以及用于信令的控制信道 SDCCH(独立专用控制信道)和 SACCH(慢关联控制信道)。移动通信系统的所述控制信道能用来在所述移动站和连接到系统的短消息服务中心 SMSC 之间传输短小的数字数据消息，亦即短消息。所述短消息服务中心是一个连接到所述移动通信系统的中心，通过它传送短消息，并能在其中存储所述短消息，以便在接收方没有收到的情况下在稍后重发。由所述短消息服务中心发出的短消息由移动站服务交换中心接收，后者用作所述 GSM 系统的短消息服务网关 MSC，从归属位置寄存器询问路由和短消息信息，并将要发的短消息发送到接收者的访问者位置寄存器。在所述 GSM 系统中，例如，一条短消息的最大长度为 140 字节。一条短消息可以是一次移动站终接短消息传输 MT，或者是一次移动站始发短消息传输 MO。

如果所述移动站 MS 262 连接到所述业务信道 TCH，短消息则在所述控制信道 SACCH 上传输。在别的情况下，短消息在所述控制信道 SDCCH 上传输。移动通信系统的用户寄存器用来在移动通信网中为短消息选定路由，基本上就同通话路由选定的方式一样。在 MT 的情况下，按照一种电子支付协议从所述公用数据网 220 到移动站用户的消息首先经由所述局域网 LAN1 240 发送到所述短消息服务中心 EC-SMSC 250，后者将所述短消息转换为所述移动通信系统 PLMN 260 的短消息，并将其以上述形式发送到用户。在 MO 的情况下，消息经由所述移动通信网 PLMN 260 发送到所述短消息服务中心 EC-SMSC 250，从该处，经过可能有的转换之后，所述消息再经由所述公用数据网发送到用户给定的地址。

在本实施例中，所述移动站 MS 使用的是某种广泛使用的支付协

议，该协议也是卖方所使用的协议。本申请人的在前的芬兰专利申请955354 公开了另一种方案，其中，在有关方之间连接有用来传送交易的独立的网关装置，该网关装置执行不同支付服务接口之间的协议转换。本领域的技术人员能够以多种不同的方式选择并提供所要使用的支付协议之间的接口。对于本发明来说，所述问题与此无关，所以对其不作详细说明。

在图 2 中，包括方框 262 的图面部分图示了一个移动站 MS 的简单结构。无线电部分 265 包括形成无线电通路的发射和接收部件，比如一个无线电收发器、调制器、信道编码器和解码器等。信令和控制部分 264 控制该移动站的整个操作。当与用户通信时，该信令和控制部分就生成所需的消息，并使消息显示在一个显示屏 267 上。相应地，所述信令和控制部分解释并执行用户从键盘 266 输入的命令。另外，该移动站还包括至少一个数据库 263，该数据库包含各种用户专用的数据。

在图 2 中，所述移动站 MS 262 包括一个数据库 DB 263，其中存储有与用户专用的支付服务有关的信息，例如用户可支配的电子货币量(现金或者信贷)的信息，以及与交易有关的收据的信息。所述数据库 263 中的所述数据群就称为一个“电子钱包”。在本实施例中，信息最好存储在所述移动站 MS 的识别单元中，即存在 SIM 卡中。

用户识别模块 SIM 是一个例如按照 GSM 推荐技术标准在其中存储所有与某个移动站用户有关的并包含在该移动站 MS 262 中的所有信息的单元。SIM 可以是一个智能卡，其与外部的接口遵守与 IC 卡有关的 ISO 标准，即 ISO 7816 系列。对于便携式无线装置来说，标准尺寸的 IC 卡 SIM 可能太大了，因此也可以使用插入式 SIM，这种 SIM 在 GSM 系统中是一种完全标准化的专用存储体，半永久性地安装在移动站装置中。

在所述 GSM 系统中，是根据 SIM 卡中的信息识别移动站用户的。除了 GSM 的专门服务和专有特征数据之外，SIM 卡的存储容量可以允许存储并管理与移动站用户有关的额外信息。借助于数字公共密钥

算法和存储容量的支持，SIM 卡尤其适合实现本发明。

图 2 所示的将电子钱包设置在移动通信网中的方式仅是许多种可能方式中的一种。例如，在本申请人在此之前的芬兰专利申请 955354 中，由连接到所述局域网 240 的网关服务器的控制单元来管理买方的支付服务数据库，所述电子钱包连接到所述网关装置，而不直接连接到所述移动站。所述电子钱包也可以包含在用户的存储卡或者智能卡中，用户可以用公用的或者专用的读写装置使用所述卡。具体实现电子钱包的方式与本发明无关，但对于每一种应用，本领域的技术人员都可以具体实现所述电子钱包。最基本的是，用户要有一个电子钱包供其支配，在其中可存储关于交易的信息，并且，存储在其中的信息可以用一个可与之连接的接口装置读出、临时或永久地删除。

下面，针对所述用户 262 从卖方 212 订购一项服务或者一批货物的情况，对本发明作进一步的说明。卖方 212 的计算机或者收款系统向收自买方 262 的网络地址发出一条支付一笔与所述服务的价值相应的金额的提示消息。由于该网络地址的作用，所述消息经由所述局域网 LAN2、公用数据网 220 和局域网 LAN1 而发送到在用户 262 的移动通信系统中工作的所述短消息服务中心 EC-SMSC 250. 该短消息服务中心将所述消息转换为一条短消息，将其经由所述公用移动通信网 PLMN 260 发送到所述移动站 MS 262. 该移动站的操作系统包括一个支付协议接口，通过该接口执行与交易有关的功能。该移动站的控制单元查看所述数据库 263，看买方的电子钱包中是否有充足的货币以供支付所请求的金额。如果货币数量不足，所述控制单元就生成一条拒付消息，经由网络发送给卖方 212。如果数据库 263 中有充足的货币，控制单元就生成一条包含支付请求的消息输出到显示屏上。用户通过键盘 266 接受支付请求，这样，控制单元就按照买方和卖方之间使用的支付协议经由所述网络从所述数据库 DB 263 向所述卖方 212 转移所需数目的货币。

接收到所述支付之后，卖方 212 生成一张收据，该收据基本上按照所述使用的支付协议生成，并包括关于该交易的主要信息。收据上

的信息可以随用途而变，但最好包括一个交易标识、交易说明、金额以及指示解码是否正确的校验区。所述交易标识 ID 是一串字符，系由卖方附加到收据上的，根据该标识，可以从卖方的记录表中准确地将该收据检索出来。该标识可以基于例如时间戳、流水号或者其组合而确定。对支付的说明是一串明文或者编码的字符，用来描述交易的主题。这样的说明可以针对每一次交易具体选择，但也可以是典型化的例如“旅馆帐单”、“出租车费”或者预先为各种用途选定的编码。所述校验区最好包含一个预先确定的值或者所述字符串的某项特征，基于该值或该特征，通过比较解码所得到的校验区与预先确定的值，可立即推断解码是否成功。

在生成所述收据之后，卖方 212 使用一种公共密钥算法对收据加密。这样的公共密钥算法例如是广泛使用的 RSA 算法。为了确保加密可准确无误地签证收据上的印签，卖方 212 的收款系统对收据加密时用卖方的专用密钥作为加密密钥。完成加密后，收据经由局域网 210 和公用数据网 220 发送到所述移动通信系统的所述短消息服务中心 EC-SMSC 250，从这里，所述收据作为一条短消息经由所述移动站系统发送到所述移动站 MS 262。检测到接收到的收据时，移动站 MS 262 的所述信令和控制部分就在该移动站的显示屏 267 上生成一条消息，通知买方 262 收到了所述收据，并请求输入对所述收据作进一步处理的指令。买方用其键盘 266 键入指令，决定是否将收据存在该移动站的数据库 DB 263 中供以后使用，或者是否立即进行进一步的处理。

要将一张加密的收据解码成明文格式需要一个公共密钥。下面，把在其中存储卖方的标识以及与这些标识有关的公共密钥的文件称作签证管理文件 CA。本领域技术人员可以以任意方式专门针对每一项应用实现一个签证管理文件。该文件例如可以由与所述电子钱包相联的支付系统的用户维护，或者可以作为某个可靠的机构提供的一项服务，甚至作为官方所提供的服务。在本实施例中，所述签证管理文件与所述支付系统的用户(买方和卖方)的装置(移动站、收款系统)安排在一起。但是，本发明并不局限于这种方案。

如果收据未作进一步处理，则将其以加密格式存在所述电子钱包 DB 263 中，以便以后能够检索出来作进一步处理，如果需要的话。为了使收据在所述电子钱包的记录表中可被辨别，可以向所述收据添附可自由选择的明文标识。该标识可以是例如一个文本串、与交易有关的缩写、或者支付的金额。卖方可以在他发出的消息中建议一个在买方的记录表中使用的标识，接到收据后，买方可以接受也可以拒绝该标识。

如果用户 261 已经针对某个票据进行了电子支付，他希望将该票据过户以记入其办公室簿记 270 的贷方，那么，该用户就用其键盘发出命令，所述控制单元根据该命令生成一条包含记入贷方的请求的消息并将其发送到办公室网络地址。如果簿记 270 接受该请求，同意将该金额记入贷方，则将加密格式的收据以及卖方的标识发送到目的地 270. 所述簿记可支配一个签证管理文件 CA 275，根据所述卖方标识从该签证管理文件检索出卖方的公共密钥。用该公共密钥对收据解码。如果用所述公共密钥对收据的解码成功，收据中可能含有的所述校验区就应该是预期的值，则所述簿记就接受该收据，发出与所述金额价值相应的电子代用币，记入所述用户 261 的电子钱包 263 的贷方。

图 3 的信号图表示出了上述过程。用卖方 S 的公共密钥利用 RSA 算法对字符串 T 进行的处理在该图表中用 S(T)表示，用卖方的专用密钥利用 RSA 算法对所述字符串进行的处理用 $S^{-1}(T)$表示。基于前述，显然有:

$S(S^{-1}(T)) = T$.

当进行交易时，买方 261 以电子货币的形式向卖方 212 支付(信号 3.1)。卖方生成一张收据，并用其专用密钥对之数字化加密，所述专用密钥对于其他任何人而言都是完全保密的。卖方将该加密的收据发送给买方(信号 3.2)，买方又将所述加密收据以及卖方的标识转发到所述目的地(信号 3.3)，也就是转发到买方办公室的簿记 270。该簿记 270 将所述卖方标识发送给所述签证管理文件 CA 275(信号 3.4)，后者将卖方的公共密钥返回给所述簿记(信号 3.5)。簿记将所述收据解码，如

果解码成功，收据的校验区就会给出一个值，根据该值可以推断加密的收据已被正确地解码，相应于应被记入买方的贷方的金额的一笔电子货币就转到了买方的帐上(信号 3.6)。转移的金额存储在买方 261 的移动站的所述电子钱包 263 中。

如果买方不需要记入贷方，而是想过户扣税收据以添加到其税务申报表(tax return)中，过程与上述过程(信号 3.1-3.5)大抵相似。买方支付(3.1)，卖方生成收据(3.2)，买方将收据以及卖方标识转送到目的地(3.3)，该目的地在此为存储在税务部门数据库中的税务机关的纳税人专用文件。税务机关将所述卖方标识发送到所述签证管理文件(3.4)并接收返回的卖方公共密钥(3.5)。税务机关将所述收据存储下来，当信息最后被传送到纳税人税务信息中时，就将收据解码。

另一种存储扣税收据的方案是建立一个与银行、税务机关相联的电子收据包，或者在另一个可靠的地方建立一个电子收据包。在纳税年度，纳税人将扣税收据送入该收据包中。在该收据包中，收据可以存为加密格式。可以对所述加密进行解码。当提交税务申报表时，可对所有的收据打印出一个经过保管者签证的明细单。

本发明的一种实施例是电子收据的经核准的硬拷贝。本发明的方案中可以添加一个可靠的机构，例如银行。为了收到一个硬拷贝，可以将加密的收据发送给该银行。由该银行来执行与所述目的地有关的功能(信号 3.4-3.5)。收据打印出来后，由银行对打印件进行签证。在完成打印工作后，银行将电子收据销毁。

本发明的方法示于图 4 的方框图和图 5 的流程图中。图示的例子描述了这样一种情况：买方用其自己的卡支付了其雇主应付的费用，然后要向其雇主收回所述费用。在图 4 所示的方案中，卖方有一个收款系统 47 供其支配，并有一个能够处理卖方的卡的读写装置 46 与所述收款系统相连。在支付时，买方用其自己的卡 41 作为向卖方支付的手段，卖方读出该卡 41 中的电子钱包 42 中的内容，从该钱包 42 中收取一笔特定的金额。同时，卖方的系统 47 生成一张对应于所述金额的收据，并用其专用密钥作为加密密钥对收据加密，然后将加密的收据

存储在买方的电子钱包 42 中。当买方下次去办公室时，他将其自己的卡交给雇主，雇主用一个与其系统相连的读写装置读出存储在所述卡 41 中的所述电子钱包 42 中的收据，在其认可该项支付之后，就将该收据相应的金额记入买方电子钱包 42 的贷方。

图 5 的流程图示出了本发明的方法应用到上述例子中的情况。在步骤 510，卖方请求从买方的电子钱包支付对应于一定金额的一定数目的电子代用币。接收到所述支付之后，卖方生成一张对应于所述金额的收据(步骤 515)，将所述收据或其被选择的某些部分加密，加密时用卖方的专用密钥作为加密密钥(步骤 520)，然后将该收据存到买方的电子钱包中(步骤 525)。在图中，折线表示该方法的各步骤之间长度可能会变化的时间段。该方法的各步骤可能一步紧接另一步，或者，取决于买方的行为，各步骤之间可能会经过较长的时间。

如果买方想收回其已支付的金额(步骤 530)，他就将他的卡交给其雇主，雇主用一个连接到其系统的读写装置读出该卡中的电子钱包的内容(步骤 535)。由于收据被加密了，雇主如果没有特别的信息就不能读出收据。从买方收到卖方标识后，雇主可以从其系统的数据库，或者从一个由某个可靠的机构维护的外部数据库中检索出卖方的公共密钥(步骤 545)，以对收据进行解码(步骤 550)。仅当收据系由买方所标示的卖方开出时，雇主才能够解开收据的密码。根据被解码的明文收据，雇主可以判断所涉及的费用是否要记入所述雇员的贷方(步骤 555)。记入贷方的操作是这样执行的：将与所述收据相应的一定数目的电子代用币存入所述买方的电子钱包中(步骤 560)。

一种可能的方案是为所述卖方和所述办公室系统提供一个读写装置。该读写装置能够连接到所述买方的计算机或者移动站，这样，交易活动和有关的数据传输就能够例如以图 2 所示的方式通过所述公用数据网进行。

本说明书中所述的经签证的电子收据也可以设计为可选择的，这样，买方就能够结合交易的情况决定他是想要一张经签证的电子收据，还是要普通的明文收据就足够了。本发明中的用一种公共密钥算法签

证的收据仅当付款人请求时才提供。

根据上文所述，显然，对于本领域的技术人员来说，本发明的基本思想随着技术的发展能够以多种不同的方式实现。因此，本发明及其具体实施并不局限于上述例子，而可以在所附权利要求的范围内进行各种变化。

说 明 书 附 图

图1

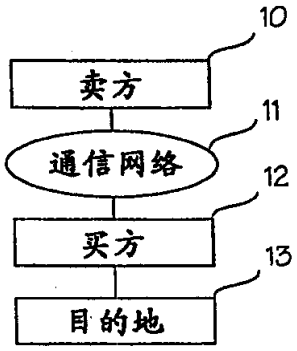


图2

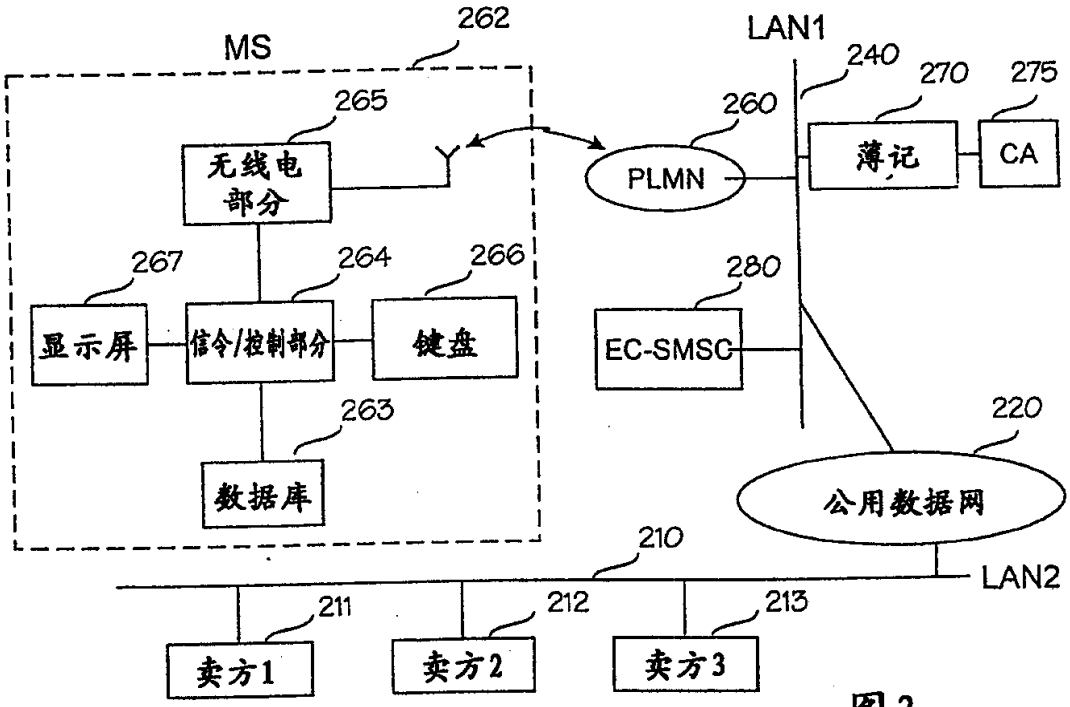


图3

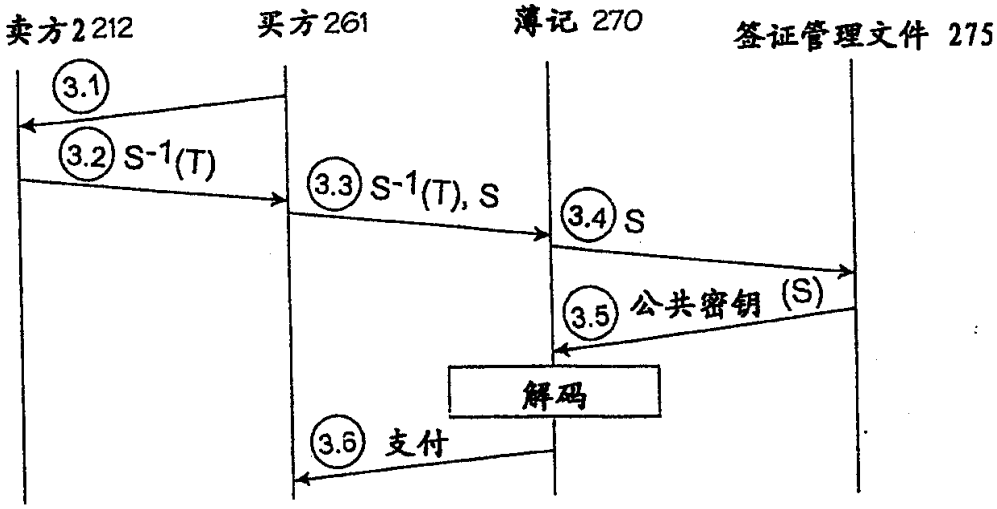


图 4

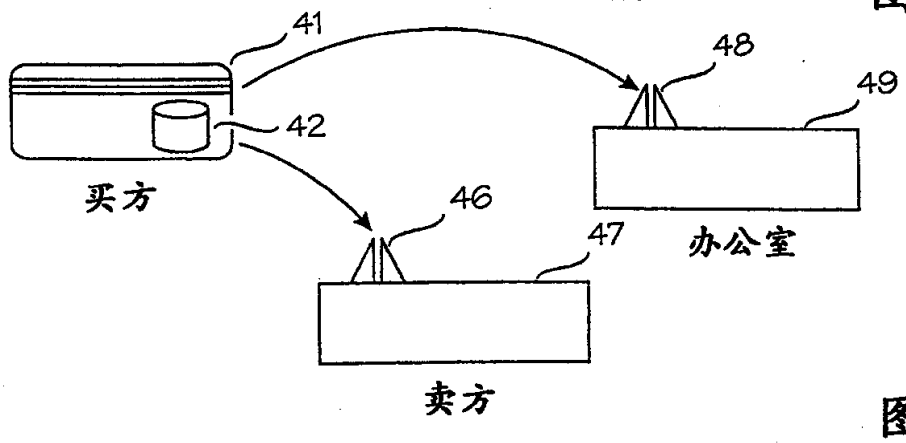
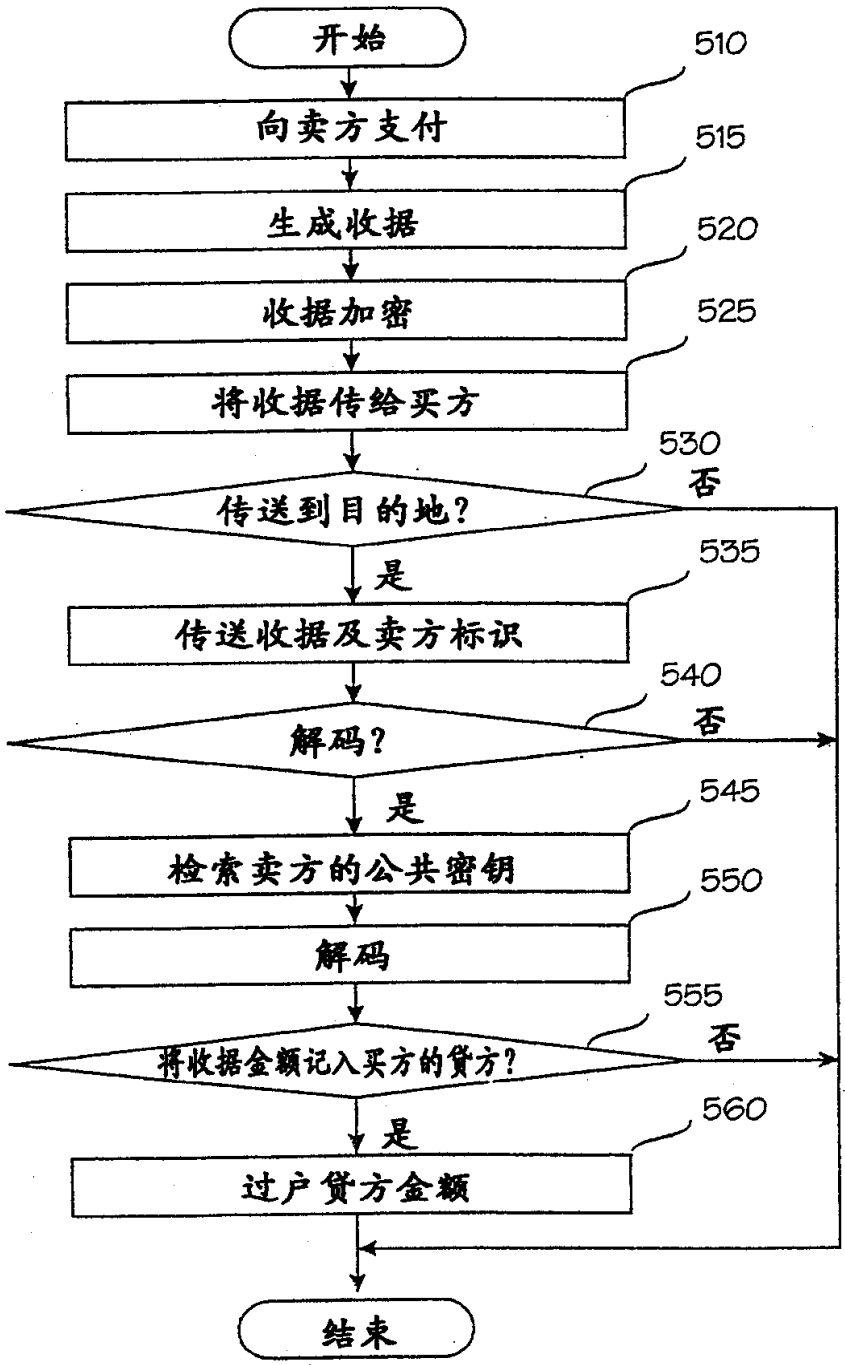

41
42
买方
48
49
办公室
46
47
卖方

图 5


开始
510
向卖方支付
515
生成收据
520
收据加密
525
将收据传给买方
530
传送到目的地?
否
是
535
传送收据及卖方标识
540
解码?
否
是
545
检索卖方的公共密钥
550
解码
555
将收据金额记入买方的贷方?
否
是
560
过户贷方金额
结束