

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G07F 19/00 (2006.01)

G06Q 20/00 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 03827012.9

[43] 公开日 2006年10月18日

[11] 公开号 CN 1849632A

[22] 申请日 2003.7.2 [21] 申请号 03827012.9

[86] 国际申请 PCT/ES2003/000329 2003.7.2

[87] 国际公布 WO2005/004069 西 2005.1.13

[85] 进入国家阶段日期 2006.3.2

[71] 申请人 莫比培国际公司

地址 西班牙阿尔科文达斯

[72] 发明人 L·加西亚鲁阿诺

G·桑彻斯桑托斯

I·德卡索巴斯特雷彻亚

A·斯门尼斯桑彻斯

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 程天正 梁永

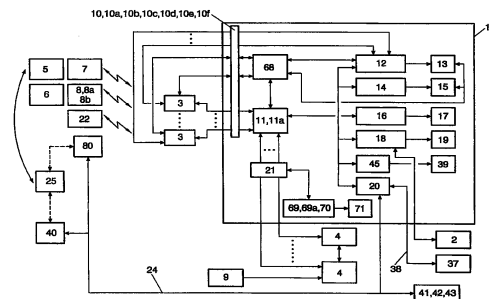
权利要求书 26 页 说明书 80 页 附图 15 页

[54] 发明名称

数字移动电话交易和支付系统

[57] 摘要

该系统允许使用任何类型的移动电话作为使用在任何与该系统相连的国家中采用了任何技术的移动电话网络的支付设备的启动设备。该系统包括不同国家中的一组支付和操作处理中心(1)，这些支付和操作处理中心(1)通过国际寻址处理装置(2)互连，以完成在相同或不同国家中与该系统相关的用户-付款人和收款人之间的交易和支付。该中心(1)具有特殊的结构以便允许不同类型的购物、查询、修改和对支付设备的验证。本发明允许交换的所有不同消息使用语音消息。另外本发明还允许使用收款人/销售商的移动电话作为 POS(22) 以完成交易。



1. 通过移动电话处理与该系统相关的用户 - 付款人 (5) 和收款人 (6) 之间的支付和交易的支付和交易系统, 至少一种支付方式与具有至少一个与金融实体处理装置 (4) 相关的金融实体的帐户相关; 至少用户 - 付款人 (5) 以及选择性地收款人 (6) 属于一个移动电话网络 (3); 通过数字移动电话使用至少一种通信; 金融实体处理装置 (4) 之间相互连接并与金融实体互连; 其中该支付和交易系统包括不同国家的多个支付和操作处理中心 (1, 1'), 各个国家中的用户 - 付款人 (5) 和收款人 (6) 属于各自国家的支付和操作处理中心, 并且这些支付和操作处理中心之间通过国际寻址处理装置 (2) 互连以完成从相同和不同国家选择的相关用户 - 付款人和收款人之间的支付和交易; 支付和操作处理装置 (1, 1') 包括:

电信控制器 (10), 具有支持不同移动电话技术的不同技术的多个移动电话网络 (3), 用户 - 付款人 (5) 和选择性的收款人 (6) 与这些移动电话网络相关联, 并且有选择地与用户 - 付款人 (5) 的移动电话 (7) 通信, 所述移动电话由从电话号码和与此相关的号码选择的号码标识; 并且有选择地与收款人的通信设备 (8, 8a, 8b, 22) 通信, 收款人的通信设备由通信设备标识符标识; 该电信控制器装置 (10) 包括多个通信控制器 (10a - 10f);

通信控制器装置 (21), 具有一个国家的用户 - 付款人和收款人所关联的不同金融实体处理装置 (4), 与从相关用户 - 付款人 (5) 的金融实体处理装置 (4) 和相关收款人 (6) 的金融实体处理装置 (4) 中选择的处理装置进行通信;

操作处理装置 (11), 与从电信控制器装置 (10) 和通信控制器装置 (21) 中选择出的控制器装置通信, 并通过电信装置接收从与相关用户 - 付款人 (5) 有关的第一标识数据中选出的数据, 除了第一数据之外, 还接收与相关收款人 (6) 有关的第二标识数据, 除第一数据之外还通过控制器装置 (10) 接收与相关收款人 (6) 有关的第三数据; 操作处理装置 (11) 生成从对相关用户 - 付款人 (5)、相关收款人 (6)、索引或以上组合的确认请求选出的确认请求;

操作处理装置 (11) 包括识别装置 (11a), 除了从第一、第二和第三数据中选择的数据外, 用于识别接收到的涉及不同支付和交易形

式的数据;

钱夹处理装置(12),它与操作处理装置(11)相连并访问第一存储装置(13),第一存储装置(13)至少存储了每个相关用户-付款人(5)的第一标识信息,第一标识信息涉及从分配给各个用户-付款人的移动电话(7)的电话号码和其相关号码中选择的号码;以便处理在对相关用户-付款人的确认请求中接收到的相关用户-付款人(5)的第一标识数据,并生成对相关用户-付款人的确认消息;第一存储装置还包括关于各个相关用户-付款人的支付方式的第二标识信息,所述第二标识信息与第一信息相关联,并且与各种支付方式所关联的金融实体处理装置(4)的标识相关联;

销售商处理装置(14),它与操作处理装置(11)相连,并访问第二存储装置(15),以处理在对收款人的确认请求中接收到的相关收款人的第二标识数据,并生成对相关收款人的确认消息,第二存储装置(15)至少存储了各个相关收款人的第一标识信息,该第一标识信息还与各个相关收款人的各个通信设备的识别代码有关;第二存储装置(15)还包括标识各个相关收款人的支付方式的第二信息,第二信息与各个相关收款人的第一标识信息和各个相关收款人的支付方式所关联的金融实体处理装置(4)的相关标识相关联,以便操作处理装置获得相关收款人的确认消息,选择性地还一并获取所述相关收款人的支付方式以及所述相关收款人所关联的金融实体处理装置的标识;

索引处理装置(16),它与操作处理装置(11)相连,并访问第三存储装置(17),以处理在索引确认请求中接收到的索引的第三标识数据,并生成索引确认消息,索引确认消息包括从价格/货币选择的标识、从产品和服务选择的标识、相关收款人的标识、相关收款人的通信设备的标识符以及以上的任意组合,第三存储装置(17)至少存储了多个索引的第一标识信息,每一个标识信息至少与相关收款人的标识相关,并且与从产品和服务选出的价格/货币的标识或通信设备的标识符相关联;

钱夹处理装置(12)包括:

第一检测器装置(12a₁),以获得从相关用户-付款人(5)和相关收款人(6)的支付方式中选择的支付方式以及相关用户-付款人

(5) 和相关收款人(6)的公共支付方式,并在已经生成从对相关用户-付款人和相关收款人的确认消息选出的消息时,或是在已经生成对相关用户-付款人、相关收款人和相关索引的确认消息时,生成交易验证请求消息;有选择地将所述验证请求消息发送到相关用户-付款人的移动电话(7);该验证消息包括从相关用户-付款人和相关收款人的支付方式选择出的方式以及相关用户-付款人和相关收款人的公共支付方式;引入安全参数的请求;从相关用户-付款人的至少一种支付方式以及相关用户付款人和相关收款人的公共支付方式中选择的选择请求;相关收款人的标识;从产品和服务选出的信息;以及从相关收款人的产品价格和选出的服务价格中选择出的价格;

第二检测装置(12a₂),用于获得对所发送的验证消息的响应消息,响应消息包括安全参数和选择性的与之相关的加密序列,以及至少由相关用户-付款人选择的支付方式;所述第二检测装置访问第一存储装置(13),第一存储装置(13)还包括第三标识信息,第三标识信息从涉及相关用户-付款人(5)的金融实体处理装置(4)中的验证、通过相关收款人的金融实体处理装置(4)在相关用户-付款人的金融实体处理装置(4)的验证以及支付和操作处理装置(1,1')中的委托验证的实现;该验证包括对安全参数与由用户-付款人选择的至少一种支付方式相关的加密序列进行选择检查,对与相关用户-付款人的第一标识信息相关的所述至少一个选择出的支付方式的检查,以及随后的交易授权;以便通过金融实体处理装置(4)完成交易,并将交易结果发送到相关用户-付款人的移动电话和相关收款人的通信设备;

第一存储装置(13)包括与远程支付和操作处理装置(1')相关的用户-付款人的第四标识信息,所述第四标识信息由钱夹处理装置(12)访问,一旦处理第一数据并检测到与远程支付和操作处理装置(1')相关的用户-付款人的标识,就生成路由消息,该路由消息至少包括第一数据、对与远程支付和操作处理装置相关的用户-付款人的确认和验证请求以及相关收款人的支付方式;第三存储装置(17)包括与远程支付和操作处理装置(1')相关的索引的第二标识信息,以便当索引处理装置(16)处理在索引验证请求中接收到的第三数据时,一旦检测到与远程支付和操作处理装置(1')相关的索引的标识,就生

成至少包括该第三数据和该相关用户 - 付款人的确认结果的路由消息;

支付和操作处理装置还包括路由处理装置 (18) 用于处理路由消息, 路由处理装置 (18) 与操作处理装置 (11) 相连并访问第四存储装置 (19), 以从所述处理装置将该路由消息发送到远程支付和操作处理装置 (1'), 第四存储装置 (19) 包括至少一个国际寻址处理装置 (2) 的至少一个第一标识信息, 其中从选择性的确认与远程支付和操作处理装置 (1') 相关的用户 - 付款人、索引和收款人中选择出的操作处理验证并生成一个路由消息, 该路由消息包含从确认和验证请求消息、确认和验证结果以及交易中选择出的消息;

支付和操作处理装置 (1), 包括一个技术检测处理装置 (68), 它选择性地访问第一存储装置 (13) 或第二存储装置 (15), 第一存储装置 (13) 包括涉及各个相关用户 - 付款人 (5) 的移动电话网络 (3) 和相关技术的第五标识信息, 以及涉及各个相关用户 - 付款人的移动电话 (7) 的技术的第六标识信息, 并且涉及相应用户 - 付款人的电话号码; 第二存储装置 (15) 包括关于与各个相关收款人 (6) 相关的移动电话网络和其中的相应技术的第三标识信息, 并且有选择的访问关于与各个相关收款人的通信设备 (22, 8, 8a, 8b) 相关的技术的第四标识信息, 以便允许通过用户 - 付款人或收款人与之相关的移动电话网络 (3) 与用户 - 付款人的移动电话 (7) 或与收款人的通信设备 (22, 8, 8a, 8b) 进行通信;

支付和操作处理装置还包括发票和交易管理处理装置 (45), 它与第七存储装置 (39) 相连以存储完成的不同交易的标识, 每个交易标识与交易中完成的操作类型、交易中涉及的用户 - 付款人的标识、交易数额、交易货币、以及交易中涉及的相关收款人的标识有关。

2. 根据权利要求 1 的系统, 其中不同技术的移动电话网络是从 GSM (全球移动电话系统)、CDMA (码分访问)、TDMA (时分访问)、2.5G、3G 例如 GPRS、EDGE (增强数据 GSM 演进)、CDMA 1、UMTS (统一移动通信系统) 和 CDMA2000 中选择的。

3. 根据权利要求 1 的系统, 其中相关用户 - 付款人的移动电话 (7) 可以从具有 WAP (无线应用协议)、STK (SIM 应用程序工具包)、J2ME (Java 2 平台, 微型版)、BREW (无线二进制运行时间环境) 以

及它们的组合的移动电话中选择，由此向移动电话提供用于存储从相应应用程序（WAP、STK、J2ME 或 BREW）或其组合中选择的信息的存储装置。

4. 根据权利要求 2 的系统，其中各个相关收款人的通信设备选自常规销售终端（POS）（9）、装备了移动通信终端的蜂窝 POS（8，8a，8b），其中所述移动通信终端选自 GSM、CDMA、TDMA 和 2.5G、3G 例如 GPRS、EDGE（增强数据 GSM 演进）、CDMA 1、UMTS（统一移动通信系统）和 CDMA 2000、作为 POS（22）的移动电话，所述移动电话是从支持 WAP（无线应用协议）、STK（SIM 应用程序工具包）、J2ME（Java 2 平台，微型版）、BREW（无线二进制运行时间环境）以及它们的组合的移动电话中选择的，由此向所述作为 POS 的移动电话提供用于存储从相应应用程序（WAP、STK、J2ME 或 BREW）和其组合选择的信息的存储装置；以及通过不同于移动电话网络的通信网络（24）访问支付和操作处理装置的通信设备（40、41、42、43、80）。

5. 根据权利要求 4 的系统，其中相关收款人的蜂窝 POS（8，8a，8b）是从自动售货机（8a）、接收打印机（8b）和允许启动交易的 POS（8）中选择的，以完成选自查询、修改、退货和现场购物的操作，其中用户 - 付款人是通过所述蜂窝 POS 的相关收款人的前提。

6. 根据权利要求 1 的系统，其中相关收款人（6）的金融实体处理装置（4）在直接接收到来自相关收款人的通信设备（9）的交易请求时，将带有相关收款人的标识连同它的支付方式以及相关用户 - 付款人的第一标识数据的消息发送到支付和操作处理装置（1），该交易请求选择性地包括相关用户 - 付款人的第一标识数据、产品、产品的价格以及相关收款人的标识；支付和操作处理装置（1）在交易完成后直接将结果发送到相关收款人的通信设备（9）。

7. 根据权利要求 1 的系统，其中除了第一数据之外，多个索引的第三标识数据在由相关用户 - 付款人的移动电话生成的交易请求中接收到；并且其中涉及相关收款人标识的第二数据是从相关索引的确认消息中获得的。

8. 根据权利要求 1、3 或 7 的系统，其中相关用户 - 付款人的第一标识数据包括从相关用户 - 付款人的移动电话号码和与从分配给该系统的各个支付和操作处理装置的 PAN（专用帐户号码）和 EAN 代码（条

码格式的 PAN) 中选择的代码相关的号码中选择的号码。

9. 根据权利要求 1 的系统, 其中收款人的各个移动设备 (8, 8a, 8b, 22, 40, 41, 42, 43, 80) 的标识符是从电话号码、涉及电话号码的号码、因特网代码、表示因特网代码的代码、email 地址以及基于 email 地址的代码中选择出的。

10. 根据权利要求 1 的系统, 其中各个相关用户 - 付款人 (5) 的各种支付方式与各种支付方式的安全参数相关; 并且其中第一存储装置包括与钱夹处理装置 (12) 相关的安全参数的标识, 以完成委托验证和购物、以及第一存储装置中包含的信息的查询和修改等操作。

11. 根据权利要求 1 的系统, 其中相关用户 - 付款人的各种支付方式与安全参数有关, 对于各个相关用户 - 付款人安全参数是不同的, 并且其中第一存储装置包括与钱夹处理装置 (12) 相关的安全参数的标识, 以完成委托验证、对第一存储装置中包含的信息的查询和修改。

12. 根据权利要求 1 的系统, 其中与不同金融实体处理装置通信的通信控制器装置 (21) 包括在将验证请求直接发送到相关用户 - 付款人 (5) 的金融实体处理装置或者通过相关收款人 (6) 的金融实体处理装置 (4) 发送到用户 - 付款人 (5) 的金融实体处理装置时将与安全参数有关的加密序列加密以完成加密的装置。

13. 根据权利要求 1 的系统, 其中当已经在相关用户 - 付款人 (5) 的移动电话 (7) 或者在相关收款人 (6) 的通信设备 (8, 22) 中生成交易请求消息时, 交易的结果消息被通过电信控制器装置 (10) 发送到相关收款人的通信设备 (8, 8a, 8b, 22) 和相关用户 - 付款人的移动电话 (7)。

14. 根据权利要求 1 的系统, 其中第三存储装置 (17) 中包括的多个索引的标识信息与下列服务有关: 移动电话充值服务、移动电话内容下载服务、自动售货机 (8a)、预付费购物 (定单购物)、个人之间的支付方式、因特网购物、目录购物、电话销售、发票和交付的支付、票据、付费节目和电子签名。

15. 根据权利要求 14 的系统, 其中在处理第三数据时, 索引处理装置 (16) 在检测到移动电话充值服务时, 它涉及充值价格和收款人的标识, 这是由第三存储装置 (17) 的多个索引标识的第一信

息中的移动电话网络(3)确定的;并且其中操作处理装置的识别装置(11a)检测要充值的电话号码,该号码被包括在标识相关用户-付款人的第一数据或者包括在对验证消息的响应消息中,包括输入要充值的电话号码的请求,并且已经由相关用户-付款人输入,以便在完成对要充值的移动电话号码的所述检测后,生成和发送一个检验请求消息以确认检测到的移动电话号码允许在该移动电话网络的运营商中充值。

16. 根据权利要求15的系统,其中移动电话网络(3)的运营商检验该移动电话号码是否允许充值,生成一个消息并将它发送到操作处理装置(11),以便在除了第一数据之外还接收到要充值的移动电话号码时完成验证或者当在验证消息的响应消息之外还接收到要充值的移动电话号码时完成交易。

17. 根据权利要求16的系统,其中当操作处理装置接收到交易结果时,向检测到的要充值的移动电话的运营商生成充值命令,接收充值结果并通过钱夹处理装置(12)将它发送到相关用户-付款人(5)的移动电话(7)。

18. 根据权利要求1的系统,其中当操作处理装置(11)在索引确认中检测到收款人的通信设备标识时,操作处理装置(11)生成对收款人的确认请求以及对收款人通信设备的确认请求,该请求被发送到销售商处理装置(14),销售商处理装置(14)生成对收款人的通信设备的确认以允许建立与收款人通信设备的通信,该确认包含关于所述收款人通信设备的数据。

19. 根据权利要求5、14和18的系统,其中当索引处理装置(16)处理关于检测到与自动售货机(8a)相关的索引的第三数据时,生成包括该自动售货机(8a)的标识符的索引确认消息,以便操作处理装置(11)生成一个消息并将它发送到所述自动售货机(8a)以启动该次购物,该消息至少包括通过指示用户-付款人通过自动售货机上的屏幕选择产品的消息或者是包括相关用户-付款人的标识的启动购物的消息;并且其中自动售货机(8a)包括检测装置以检测购物启动消息,以便将选择请求消息显示在所述自动售货机的屏幕上,该选择请求消息可以包括相关用户付款人的标识,并在所述选择之后生成产品选择消息并将它发送到操作处理装置(11)以生成验证请求消息,该产品

选择消息至少包含由钱夹处理装置(12)的第一检测装置检测到的数额和货币。

20. 根据权利要求19的系统,其中当自动售货机(8a)接收到有效交易的结果时它吐出所选产品,或者在交易无效情况下生成错误消息。

21. 根据权利要求14的系统,其中第三存储装置(17)包括与带有定位符的索引相关的第三信息,以便当索引处理装置(16)处理第三数据并检测到带有定位符的索引时访问该第三信息以获得可能是随机的定位符。

22. 根据权利要求5、18和21的系统,其中预付费购物的标识涉及定位符、产品、价格以及接收打印机(8c)的标识。

23. 根据权利要求5、18和21的系统,其中预付费购物的标识涉及定位符、产品、价格以及从入场票、票和租费选择的预订方式的通信设备的标识。

24. 根据权利要求21或22的系统,其中当从操作处理装置接收到预付费购物的有效交易结果时,它生成至少包括交易结果、定位符、产品或服务的预付费购物消息,并将该消息发送到相关用户-付款人(5)的移动电话(7),并发送到接收打印机(8c)进行打印。

25. 根据权利要求14-24的系统,其中第三存储装置(17)包括第四信息以检验有效性,第四信息涉及索引过期时间并与多个索引的第一标识信息以及标识与远程支付和操作处理装置相关的索引的第二信息相关。

26. 根据权利要求14系统,其中在操作处理装置(11)的识别装置(11a)检测到个人操作之间的支付操作时,其中收款人是相关的用户-付款人,所述用户-收款人在钱夹处理装置(12)中进行确认。

27. 根据权利要求26的系统,其中第一存储装置(13)包含的关于验证的第三可选标识信息可能涉及从以下验证中选择出的验证的实现:在用户-付款人所关联的金融实体处理装置(4)中对用户-付款人的验证和在收款人所关联的金融实体处理装置(4)中对收款人的验证,所述验证涉及个人之间的延迟支付的操作,以便在操作处理装置(11)的识别装置(11a)检测到通过电信控制器(10)接收到的个人之间的延迟支付操作时完成验证。

28. 根据权利要求 27 的系统, 其中在从相关用户 - 付款人的移动电话 (7) 接收到个人之间的延迟支付操作时, 第二检测装置 (12a₂) 检测到在用户 - 付款人所关联的金融实体处理装置 (4) 中对用户 - 付款人的验证, 将验证结果发送到所述相关用户 - 付款人的移动电话 (7), 同时操作处理装置 (11) 生成与个人之间的延迟支付操作相关的索引生成请求, 从而索引处理装置 (16) 生成所述索引并将它连同交易数据一起存储在第三存储装置 (17) 中, 并将它发送到相关收款人的移动电话 (7), 该收款人是相关的用户 - 付款人。

29. 根据权利要求 27 或 28 的系统, 其中操作处理装置 (11) 通过电信控制器 (10) 接收到与个人之间的延迟支付相关的索引, 以便钱夹处理装置 (12) 生成验证消息并将它发送到相关收款人的移动电话 (7), 该验证消息中的支付方式是相关收款人的支付方式, 该收款人是相关的用户 - 付款人; 并且在收款人、也是相关用户 - 付款人所关联的金融实体处理装置 (4) 中完成对收款人的验证、完成交易并将结果发送到相关收款人的移动电话, 所述收款人是相关的用户 - 付款人。

30. 根据权利要求 1 的系统, 其中操作处理装置 (11) 的识别装置 (11a) 检测到用户 - 付款人 (5) 所关联的金融实体处理装置 (4) 中的查询操作, 以便钱夹处理装置 (12) 在确认了相关用户 - 付款人之后生成验证消息, 该验证消息包含用户 - 付款人的支付方式、输入安全参数的请求、选择至少一种支付方式的请求以及输入要查询的参数的请求; 并且其中操作处理装置的识别装置 (11a) 在确认了相关用户 - 付款人并生成验证消息后检测到钱夹处理装置 (12) 中的查询操作, 该验证消息包含用户 - 付款人的支付方式、输入安全参数的请求、选择支付方式的请求以及输入要查询的参数的请求。

31. 根据权利要求 14 的系统, 其中操作处理装置 (11) 的识别装置 (11a) 检测到对与相关用户 - 付款人相关的数据的参数化操作, 在这种情况下, 钱夹处理装置在确认了相关用户 - 付款人之后生成验证消息, 该验证消息在用户 - 付款人的支付方式、输入安全参数的请求和选择至少一种支付方式的请求之外还包括对要修改的参数的请求。

32. 根据权利要求 1 或 14 的系统, 其中支付和操作装置 (1, 1')

包括因特网处理装置(20),其包括:与不同于移动电话网络的电信网络(24)的连接接口(28、34、35),以便连接到相关收款人的通信设备(40-43,80)或者系统运营商的通信设备(37);与操作处理装置(11)、索引处理装置(16)、和销售商处理装置(14)的连接接口(36);可能还包括识别装置(26),用于识别从收款人的通信设备(40-43,80)接收到的请求,可能是响应、对接收的确认、索引生成请求、一组索引请求、对第二和第三存储装置的查询请求以及对第二和第三存储装置的修改请求;还包括识别装置(26)用于从操作处理装置接收到的请求,可能是交易结果的通知和对相关收款人的至少一种产品的库存水平的查询。

33. 根据权利要求32的系统,其中第二存储装置(15)包括第五标识信息,可能是与相关收款人的第二标识数据有关的因特网地址或电子邮件地址。

34. 根据权利要求32的系统,其中因特网处理装置(20)的所述可选识别装置包括与访问控制模块(30)相连的查询模块(26),查询模块(26)访问销售商处理装置(14)以获得相关收款人的数据。

35. 根据权利要求32的系统,其中访问控制模块(30)包括用于验证相关收款人的装置以完成从下列验证中选择的验证:对相关收款人的验证,包括确认在来自相关收款人的通信设备的请求中接收到的该收款人的标识以及口令;对支付和操作处理装置的运营商的验证,包括确认在来自系统运营商的通信设备的请求中接收到的运营商的标识和口令。

36. 根据权利要求32-34的系统,其中当操作处理装置(11)接收到操作结果时,向因特网处理装置(20)的查询模块(26)生成对通知所述操作结果的请求,以获得相关收款人的数据和其email地址;查询模块(26)与加密模块(29)和email管理器(27)相连以加密该通知请求,将其转换成适当的电子邮件格式;并通过与不同于移动电话网络的通信网络的连接接口(24)中包括的email控制器(28)将它发送到与相关收款人的设备(40-43,80)相关的email地址。

37. 根据权利要求32-34、36的系统,其中在接收到操作结果后操作处理装置(11)向因特网处理装置(20)的查询模块(26)生

成对所述操作结果的通知请求，以获得相关收款人的数据以及与所述收款人相关的因特网地址；并且其中与不同于移动电话网络的通信网络的连接接口（24）包括与查询模块（26）相连的因特网控制器（34），以便发送所述通知请求到与该收款人的设备（40-43，80）相关的因特网地址，并接收确认接收到交易结果通知的响应，查询模块（26）将该响应交付给操作处理装置（11）。

38. 根据权利要求 32-35 的系统，其中索引生成请求被通过因特网控制器（34）接收到，以便由查询模块（26）处理，索引生成请求包括相关收款人、产品、服务、价格、数字签署的文档或者它们的组合的标识，查询模块（26）生成对相关收款人的验证请求，并在接收到对相关收款人的所述验证后，将索引生成请求发送到索引处理装置（16）。

39. 根据权利要求 38 的系统，其中索引处理装置（16）配备了用于生成一个索引和一组索引的生成装置，以在接收到索引生成请求后生成与收款人、数额或货币相关的一组索引；将该信息存储在第三存储装置（17）中，并通过查询模块（26）、因特网控制器（http/https）（34）或 SMTP 控制器（简单邮件传输协议）（28）将它发送到相关收款人的设备（40-43，80），或者将它发送到相关用户-付款人的移动电话（7）。

40. 根据权利要求 32、34、36 和 39 的系统，其中在处理索引确认请求中包含的第三数据时，索引处理装置（16）检验它是根据索引生成请求而创建的索引，生成该索引是由它所关联的收款人请求的确认请求，将该确认请求通过操作处理装置（11）发送到查询模块（26）以获得相关收款人的数据，并通过因特网控制器（34）将该请求发送到相关收款人的通信设备（40-43，80），并接收来自相关收款人的通信设备（40-43，80）的响应；将该响应交付给操作处理装置（11）。

41. 根据权利要求 32-34 的系统，其中销售商处理装置（14）在由钱夹处理装置（12）生成对相关用户-付款人的验证请求消息之前，生成相关收款人是否有库存产品的确认请求，并通过操作处理装置（11）将它发送到查询模块（26），以获得所述相关收款人的数据，通过因特网处理装置（34）将该请求发送到相关收款人的通信设备（40），并从相关收款人的通信设备（40）接收响应；将该响应交付

给操作处理装置(11)。

42. 根据权利要求32的系统,其中因特网处理装置(20)包括与因特网控制器(34)相连的Web贸易处理装置(32),以允许在因特网上访问相关收款人的通信设备(40-43,80)的因特网处理装置(20),并且其中该Web贸易处理装置(32)与访问控制模块(30)相连以检测下列请求:对第二存储装置(15)的查询或修改请求以及对第三存储装置(17)的查询或修改请求,完成对相关收款人的验证,选择性地处理对销售商处理装置(14)或索引处理装置(16)的请求,销售商处理装置(14)或索引处理装置(16)完成查询或修改,并通过访问控制模块(30)、Web贸易处理装置(32)和因特网控制器(34)将结果发送到相关收款人的通信设备。

43. 根据权利要求42的系统,其中因特网处理装置(20)中不同于移动电话网络的通信网络的连接接口包括与销售商数据管理模块(33)相连的专用网络控制器(35),销售商数据管理模块(35)存储了提供给相关收款人的不同服务,以允许通过专用网络(38)访问系统运营商的通信设备(37);并且其中销售商数据管理模块(33)与访问控制模块(30)相连,以检测第二存储装置(15)中的插入、查询或修改请求或者第三存储装置(17)中的修改请求;完成对运营商的通信设备的验证,并且处理对销售商处理装置(14)的请求,其中执行对服务的查询操作或修改操作并将结果发送到系统运营商的通信设备(37)。

44. 根据权利要求42或43的系统,其中Web贸易处理装置(32)是一个图形接口,通过它用于查询或修改的不同可用选项被显示给相关收款人,并且其中销售商数据web管理模块(33)包括图形接口,该图形接口将涉及支付和操作处理装置提供给不同相关收款人的服务的不同修改或查询选项显示给系统运营商。

45. 根据权利要求32-34的系统,其中对访问控制模块(30)然后对销售商处理装置(14)的访问或者对索引处理装置(16)的访问是通过应用程序服务器模块(31)完成的,以便建立因特网或专用网络与所述处理装置(14,16)之间存在的关系。

46. 根据权利要求34的系统,其中第三存储装置(17)中包含的多个索引的第一标识信息涉及在因特网上的服务购买或产品购买,

以通过因特网处理装置将交易结果发送到由从因特网地址和电子邮件地址选择的方向所标识的用户或收款人的设备。

47. 根据权利要求 46 的系统，其中收款人是软件文件提供商，并且其中索引生成请求还包括软件文件的解密索引的生成请求，并且该解密索引和交易结果被一起发送到用户 - 付款人的移动电话。

48. 根据权利要求 14、32 - 42 或 45 - 47 的系统，其中收款人的通信设备是发票生成器 (41)，它生成并发送至少包含涉及发票类型、交易额、货币和截止日期的信息的索引生成请求。

49. 根据权利要求 14、32 - 42 或 45 - 47 的系统，其中收款人的通信设备是付费电视解码器控制器 (42)，并且其中索引与电视节目相关。

50. 根据权利要求 14、32 - 42 或 45 - 47 的系统，其中相关收款人的通信设备是可下载到与该系统相关的移动电话中的内容的服务器。

51. 根据权利要求 14、32 - 42 或 45 - 47 的系统，其中相关收款人的通信设备是交付票据提供者 (43)，它生成并发送至少包含涉及交付产品和服务的信息的索引生成请求；并且其中交易请求表示预付交货票据或货到付款票据的交付，这是由操作处理装置 (11) 的识别装置 (11a) 在接收到交易请求时检测到的。

52. 根据权利要求 51 的系统，其中当操作处理装置 (11) 的识别装置 (11a) 检测到预付交货票据的支付时，交易被执行，并且在操作处理装置 (11) 的识别装置 (11a) 检测到货到付款票据的支付时，生成与货到付款支付相关的索引生成请求以发送到相关收款人的通信设备 (43)，并且其中在由索引处理装置 (16) 检测到与货到付款支付有关的索引时交易被执行。

53. 根据权利要求 32 - 52 的系统，其中索引处理装置包括管理模块 (16c)，管理模块 (16c) 通过接口 (16d) 与第三存储装置 (17) 和操作处理装置 (11) 相连以接收索引并确认它们，还和销售商处理装置 (14) 相连以根据接收到的索引传递相关收款人的标识，或者发送/接收与远程支付和操作处理装置相关的索引；管理模块 (16c) 通过接口 (16d) 还与路由处理装置 (18) 相连，以完成对来自远程支付和处理装置的索引或发往远程支付和处理装置的索引的访问；通过管

理模块(16c)与访问第三存储装置(17)的自动维护模块(16a)相连,以检测并消除过期的索引;与编码模块(16b)相连以根据定义的算法对索引编码并将它们存储在第三存储装置(17)中。

54. 根据权利要求1的系统,其中钱夹处理装置(12)包括管理模块(12a),该管理模块(12a)包括第一检测器装置(12a₁)和第二检测器装置(12a₂),它们与第一存储装置(13)和接口(12d)相连,通过接口(12d)与操作处理装置(11)相连以完成对支付方式的添加、删除和修改;钱夹处理装置(12)配备了消息处理装置(12b),消息处理装置(12b)与管理处理装置(12a)、第一存储装置(13)以及接口(12d)相连,通过接口(12d)连接到技术检测处理装置(68)和电信控制器装置(10),以完成对技术的检测以及和相关用户-付款人的移动电话的通信;钱夹处理装置(12)还包括验证处理装置(12c),验证处理装置(12c)与第一存储装置(13)、管理处理装置(12a)以及接口(12d)相连,以允许完成对相关用户-付款人的验证、对涉及钱夹处理装置的安全参数的验证、委托验证,以及将对与远程支付和操作处理装置相关的用户-付款人的验证请求发送到国际寻址处理装置(2)。

55. 根据权利要求1的系统,其中当生成包含对与远程支付和操作处理装置相关的用户-付款人的验证和确认请求以及相关收款人的支付方式的路由消息时;在接收到对相关用户-付款人(5)验证和确认结果时,在已经确认了相关收款人之后,完成交易并生成带有交易结果的路由消息。

56. 根据权利要求55的系统,其中当在确认了收款人和索引后生成包含第三数据的路由消息时,其中该第三数据标识与支付和操作处理装置(1)相关的收款人的索引,生成包含与远程支付和操作处理装置相关的用户-付款人的确认和验证请求的路由消息,并且生成包含与远程支付和操作处理装置(1')相关的用户-付款人的验证和确认请求的路由消息。

57. 根据权利要求55或56的系统,其中当相关用户-付款人(5)不在他们的移动电话网络(3)的范围内时(漫游),所述用户-付款人与它的移动电话网络(3)的通信是通过所述用户-付款人所在国家的移动电话网络(3)完成的。

58. 根据权利要求1的系统, 其中第一存储装置(13)中包括的关于与远程支付和操作处理装置(1')相关的用户-付款人(5)的第四标识信息包含: 所述移动电话和用户-付款人所关联的支付和操作处理装置所属国家的移动电话号码的国家代码、或者远程支付和操作处理装置所属国家的PAN代码的国家代码、或EAN代码的国家代码的标识。

59. 根据权利要求1的系统, 其中第三存储装置(17)中包括的关于与远程支付和操作处理装置相关的索引的第三标识信息还可能包含该索引所关联的支付和操作处理装置的国家代码的标识。

60. 根据权利要求58或59的系统, 其中国际寻址处理装置(2)包括到多个路由处理装置(18)的连接和访问控制器(23), 通过路由管理器(24)管理连接和访问控制器(23), 路由管理器(24)访问第五存储装置(25), 第五存储装置(25)至少包括关于与远程支付和操作处理装置相关的用户-付款人的国家代码标识的第一标识信息、关于与远程用户-付款人相关的索引的第二信息以及关于发送/接收路由消息要遵循的路径的第三标识信息。

61. 根据权利要求1或权利要求55-59的系统, 其中第一(13)和第二(15)存储装置包括关于各个相关用户-付款人和收款人的语言的标识信息, 以便与相关收款人的移动设备或相关用户-付款人的移动电话的通信接收适当语言的相关数据。

62. 根据前述任一权利要求的系统, 当没有发出对用户-付款人、收款人或相关索引的确认消息时, 验证没有通过或者交易没有完成时, 生成一个拒绝消息。

63. 根据权利要求1和4的系统, 其中第二存储装置(15)包括关于与相关收款人的第一标识信息相关的安全参数的第六标识信息, 以便当操作处理装置(11)检测到来自充当POS的移动电话(22)的交易请求时, 它生成相关收款人的验证消息, 该验证消息包括收款人的标识、安全参数的输入请求, 该验证消息被发送到收款人的充当移动电话的POS, 并且当操作处理装置检测到响应时, 请求钱夹处理装置(12)验证, 钱夹处理装置通过访问第二存储装置(15)完成所述验证。

64. 根据权利要求63的系统, 其中来自充当POS(22)的移动电

话的交易请求可以是购物操作、退货、以及对完成的交易的查询。

65. 根据权利要求 4 和 64 的系统，其中当操作处理装置 (11) 接收到来自作为 POS (22) 的移动电话的对完成的交易的查询操作时，生成消息以获取相关用户-付款人的标识数据、交易的数额、货币、相关收款人的安全参数或者还有交易日期；所述数据被发送到交易和发票管理处理装置 (45)，交易和发票管理处理装置 (45) 访问第七存储装置 (39) 以确认该交易已经被完成，将查询结果发送到相关收款人的充当 POS (22) 的移动电话。

66. 根据权利要求 5 的系统，其中当操作处理装置 (11) 从蜂窝 POS (8) 接收到对已完成交易的查询操作时，在获得了相关用户-付款人的标识数据、交易的数额、货币可能还有交易日期；所述数据被发送到交易和发票管理处理装置 (45)，交易和发票管理处理装置 (45) 访问第七存储装置 (39) 以确认该交易已经被完成，将查询结果发送到相关收款人的蜂窝 POS (8)。

67. 根据权利要求 4 和 64-65 的系统，其中当通过识别装置 (11a) 检测到来自充当 POS (22) 的移动电话的交易请求时，该充当 POS (22) 的移动电话的标识符是由一可选消息序列相关的电话号码确定的，该可选消息序列请求数据以建立操作处理装置与充当 POS (22) 的移动电话的消息交换并获得涉及要完成的操作的数据，所述数据可以是相关用户-付款人的标识数据、价格、货币、或者相关收款人的安全参数。

68. 根据权利要求 36 的系统，其中识别装置 (11a) 检测到电子签名证书的注册操作，并且为相关用户-付款人生成一个公共密钥和一个私有密钥，通过销售商处理装置 (14) 和第二存储装置 (15) 获得与支付和操作处理装置 (1) 相关的证明授权中心 (CAC) 的菜单，将它连同选择所述证明授权中心之一的请求以及选择并输入电子签名安全参数的请求一起发送到用户-付款人的相关移动电话，相关用户-付款人通过他/她的移动电话发送包含所请求数据的响应，从而当操作处理装置计算所述安全参数的散列并且用散列结果对私有密钥编码时，存储加密数据并生成与所述加密数据相关的定位符；并且其中操作处理装置通过通信控制器 (21) 将相关用户-付款人的公共密钥连同定位符以及相关用户-付款人的标识数据一起发送到所选择的证明授权中心；并且各自的证明授权中心识别出相关用户-付款人之后，所述授权

中心生成包含该相关用户-付款人的公共密钥的电子签名证书并将它发送到操作处理装置(11),所述电子签名证书被存储下来。

69. 根据权利要求 68 的系统,其中相关收款人的通信设备是电子签名 POS(80),它生成涉及电子签名和要签署的文档可能还有相关用户-付款人选择的其中的敏感部分的索引生成请求,当该索引生成请求被索引处理装置(16)处理时,索引处理装置(16)生成所述索引并将它连同文件可能还有敏感数据一起存储在第三存储装置中,并将所有这些发送到电子签名 POS(80),以使用户-付款人借助于通过它的移动电话发送生成的索引而启动电子签名操作;并且其中操作处理装置检测到关于接收所生成的索引的电子签名操作时,并且在确认了用户-付款人、收款人和索引之后,钱夹处理装置(12)生成验证请求消息,该验证请求消息包括输入电子签名的安全参数的请求、文档的散列可能还有敏感部分,以便当操作处理装置(11)接收到该电子签名的安全参数时,它计算散列、解密相关用户-付款人的私有密钥并计算文档的散列,并将其连同所述证书一起发送到电子签名 POS(80),所述文档是被用该相关用户-付款人的所述私有密钥加密的;并将交易结果发送到相关用户-付款人和收款人。

70. 根据权利要求 69 的系统,其中当操作处理装置(11)接收到电子签名的定位符时,它检测所签署的文档上的查询操作。

71. 根据权利要求 6 或 32 的系统,其中来自虚拟 POS(40)的交易请求包含查询与用户-付款人相关的支付方式验证查询请求,由此虚拟 POS(4)先前查询金融机构的支付方式目录,从中获得涉及支付和操作处理装置的 URL(统一资源定位符),该支付和操作处理装置的因特网处理装置(20)通过所述 URL 通信以接收检验请求;并且其中在钱夹处理装置(12)中生成的验证请求消息包括输入与支付方式相关的安全参数以及检验过的支付方式的请求。

72. 根据权利要求 1 的系统,其中当处理涉及存在控制的交易请求时,在支付和操作处理装置(1)中完成委托验证,以允许通过支付和操作处理装置(1)对从建筑、房屋和地面选择的地点的准入控制。

73. 根据权利要求 1 的系统,其中电信控制器装置(10)包括 USSD(无结构辅助服务数据)控制器(10a),它包括第一存储装置(10a1)、协议转换器(10a2)、交换设备(10a3);第一存储装置(10a1)存

储了支付和操作处理装置(1, 1')的功能信息; 协议转换器(10a2)将USSD帧转换成支付和操作处理装置(1)所用的协议或者进行反向的转换, 以检测所接收的信息是否被发送到操作处理装置(11)或钱夹处理装置(12); 交换设备(10a3)访问存储了接收信息要遵循的路线的第二存储装置(10a4), 并根据建立的路线将接收的信息发送到操作处理装置(11)和钱夹处理装置(12)。

74. 根据权利要求73和63-66的系统, 其中当操作处理装置(11)在来自充当POS(22)的移动电话的USSD会话中检测到交易请求时, 在销售商处理装置(14)中确认了收款人之后, 发送具有不同可用操作的选择菜单; 并且一旦相关收款人选择了可用操作之一, 选择就被发送到操作处理装置, 操作处理装置接着发送一个新的菜单请求完成所选交易所需的数据, 该菜单包括输入相关收款人的安全参数的请求, 在USSD会话中重复该过程, USSD会话保持开放直到获得了完成交易所需的数据; 并且其中对用户-付款人的验证消息和交易结果被通过建立USSD的钱夹处理装置(12)发送到相关用户-付款人的移动电话。

75. 根据权利要求1的系统, 其中电信控制器装置(10)包括SMS控制器(10b), SMS控制器(10b)包括第一存储装置(10b1)、协议转换器(10b2)、交换设备(10b3); 第一存储装置(10b1)存储了支付和操作处理装置(1, 1')的功能信息; 协议转换器(10b2)将SMS消息转换成支付和操作处理装置(1)所用的协议或者进行反向的转换, 以检测所接收到的信息是否被发送到操作处理装置(11)或钱夹处理装置(12); 交换设备(10b3)访问存储了接收信息要遵循的路线的第二存储装置(10b4), 并根据建立的路线将接收到的消息发送到操作处理装置(11)或钱夹处理装置(12)。

76. 根据权利要求75、63-66的系统, 其中充当POS(22)的移动电话或者用户-付款人的移动电话包括STK功能, 在所述电话中存储了涉及支付和操作处理装置的功能的STK应用程序, 所述应用程序被通过OTA(空中)服务器(91)从STK应用程序服务器或从SMS消息中心(76)下载, 以便在请求交易时显示要执行的交易的选择菜单以及输入完成交易所需数据的请求菜单; 并且其中STK应用程序通过前摄命令与充当POS(22)的移动电话或者用户-付款人的移动电话

通信。

77. 根据权利要求 76 的系统，其中从支付和操作处理装置发到移动电话 POS(22)或用户 - 付款人的移动电话或从移动电话 POS(22)或用户 - 付款人的移动电话发送到支付和操作处理装置的消息是通过 SMS 消息中心(76)用短消息发送的。

78. 根据权利要求 76 和 77 的系统，其中在充当 POS(22)的移动电话与支付和操作处理装置(1)之间交换的消息被用 3DES(三元数据加密标准)用对称密钥密码进行了加密，对称密钥密码中的一个存储在支付和操作处理装置中并且与各个相关收款人的安全参数相关，另一个被存储在充当 POS(22)的移动电话中，由 16 个密钥组成，其中只有一个被从操作处理装置激活，被激活的密钥随时间改变；并且其中在用户 - 付款人的移动电话与支付和操作处理装置之间交换的短消息被用对称密钥密码以 3DES(三元数据加密标准)过程进行了加密，在对称密钥密码对中，一个存储在支付和操作处理装置中并与各个相关用户 - 付款人的安全参数相关，另一个在用户 - 付款人的移动电话(7)上，涉及 IMSI(国际移动用户身份)。

79. 根据权利要求 63-66 及 76、77 和 78 的系统，其中相关收款人通过充当 POS(22)的支持 STK 的移动电话启动交易，STK 应用程序选择性地请求用户 - 付款人的标识、数额、相关收款人的安全参数，并用所述数据生成一个 SMS 消息，它将该 SMS 消息发送到支付和操作处理装置(1)，支付和操作处理装置(1)一旦检测到该 SMS 消息就在完成交易之后将交易结果用 SMS 消息发出。

80. 根据权利要求 76、77 和 78 的系统，其中交易由相关用户 - 付款人通过支持 STK 的移动电话(7)启动，STK 应用程序以菜单形式显示不同的可用操作，一旦相关用户 - 付款人选择了可用操作之一，STK 应用程序就请求完成所选交易需要的数据，并且生成并发送包含一个验证请求的 SMS 消息，该验证请求通过其显示请求输入安全参数和支付方式的菜单激活 STK 应用程序，STK 应用程序用输入的参数生成一个 SMS 消息并将它发送到支付和操作处理装置，重复将交易结果发送到移动电话(7)的过程。

81. 根据权利要求 1 的系统，其中电信控制器装置(10)包括与 IVR(交互式语音响应)设备(61)相连的 IVR 控制器(10c)，IVR

设备(61)配备了存有支付和操作处理装置(1, 1')的功能信息的第一存储装置(61a)和基于TCP/IP协议(传输控制协议/互联网协议)的具有安全Ipsec连接的连接接口(61b);并且其中IVR设备(61)与PABX交换机(专用自动小型交换机)相连,以和不同的移动电话网络(3)通信,并通过语音消息传递将来自支付和操作处理装置(1, 1')的语音消息发送到相关用户-付款人的移动电话(7)和收款人的通信设备(8, 8a, 8b, 22),所述移动电话和通信设备配备了语音识别机制。

82. 根据权利要求81和63-66的系统,其中当操作处理装置(11)在来自充当POS(22)的移动电话的IVR会话中检测到交易请求时,在销售商处理装置(14)中确认了收款人之后,发送具有不同可用操作选项的语音菜单;并在相关收款人通过键盘或者语音指令选择了想要的可用操作之后,选择被发送到操作处理装置,操作处理装置接着打开新的语音菜单以请求所选交易需要的数据,包括输入相关收款人的安全参数的请求,在IVR会话中重复该过程,IVR会话保持开放直到接收到交易需要的所述数据;并且其中用户-付款人的验证消息以及交易结果被通过钱夹处理装置(12)发送到相关用户-付款人的移动电话。

83. 根据权利要求1的系统,其中电信控制器装置(10)包括智能网控制器(10d),智能网控制器(10d)包括协议转换器装置(10d₁)以将智能网使用的协议转换成支付和操作处理装置(1, 1')所用的协议或者进行反方向的转换,以便支付和操作处理装置(1, 1')和CDMA/TDMA技术移动电话网络(3)的智能网(63)的SCP(服务控制点)(62)通信,SCP包含支付和操作处理装置(1)的功能信息;并且其中相关用户-付款人的移动电话(7)或者通信设备(8, 8a, 8b, 22)生成智能网的触发以发送交易请求,交易请求在智能网(63)上的MSC(66)(移动交换中心)中被检测到并将它发送到支付和操作处理装置(1, 1'),以在智能网上令支付和操作处理装置(1, 1')和相关用户-付款人的移动电话(7)或相关收款人的通信设备(8, 8a, 8b, 22)通信;由蜂窝POS(8, 8a)组成的通信设备的触发信号包括从相关用户-付款人的信息、产品、服务或者产品或服务的价格中选择的标识信息。

84. 根据权利要求 83 的系统, 其中智能网 (63) 的 IP (64) (智能外设) 包括向相关用户-付款人的移动电话 (7) 或相关收款人的通信设备 (8, 8a, 22) 请求所需各种数据的预先记录的语音消息。

85. 根据权利要求 81 的系统, 其中当从相关用户-付款人的移动电话 (7) 或相关收款人的通信设备 (8, 22) 建立通信时, 会接收到呼叫音和个性化的欢迎消息以确保对 IVR 的验证。

86. 根据权利要求 85 的系统, 其中当识别装置 (11a) 检测到由 IVR 设备 (61) 处理的交易请求时, 操作处理装置 (11) 生成请求数据的选择性消息序列以建立语音交换指令, 这些语音指令涉及有选择地获取涉及要完成的交易的数据的交易菜单。

87. 根据权利要求 75 和 83 的系统, 其中 SMS 控制器 (10b) 与智能网 (63) 的 SMS 中心 (65) 相连, 以向相关用户-付款人的移动电话 (7) 或相关收款人的通信设备 (8a, 8b, 22) 请求涉及交易的不同数据。

88. 根据前述任一权利要求的系统, 其中销售商处理装置 (14) 包括与第二存储装置 (15) 和连接到操作处理装置 (11) 的接口 (94) 相连的管理模块 (92), 以便由支付和操作处理装置的分析员或金融实体处理装置的分析员执行对相关销售商的标识符和它们的相关支付方式的添加、删除和修改; 销售商处理装置 (14) 还包括验证处理装置 (93), 它与第二存储装置 (15)、管理处理装置 (92) 和接口 (94) 相连, 以允许完成对相关收款人的确认和对涉及相关收款人的安全参数的验证。

89. 根据权利要求 1 的系统, 其中第一存储装置 (13) 中包括的每个第五信息涉及与各个相关用户-付款人相关的移动电话网络 (3) 的标识和技术, 每个第六信息涉及各个移动电话 (7) 的技术, 第二存储装置 (15) 中包括的每个第三信息涉及各个相关收款人的移动电话网络 (3) 的标识, 以及每个第四信息涉及各个通信设备 (8, 8a, 8b, 22) 的技术, 此时标识代码是电话号码或与其相关的号码, 该相关号码在 GSM 网络中是 IMEI (国际移动设备标识符)。

90. 根据权利要求 1 的系统, 其中第一存储装置 (13) 中包括的每个第五信息涉及与各个相关用户-付款人相关的移动电话网络 (3) 的标识和技术, 每个第六信息涉及各个移动电话 (7) 的技术, 以及第

二存储装置(15)中包括的每个第三信息涉及相关收款人的移动电话网络的标识,每个第四信息涉及各个通信设备(8, 8a, 8b, 22)的技术,此时标识代码是电话号码或与之相关的号码,该相关号码在采用CDMA或TDMA技术的移动电话网络中是ESN(电子序列号)。

91. 根据权利要求89或90的系统,其中电信控制器装置(10)包括HTTP控制器(10e)(超文本传输协议),以用技术检测装置(68)和各个移动电话网络(3)通信,技术检测装置(68)访问第一存储装置(13)上的第五和第六信息以及第二存储装置(15)上包含的第三和第四信息,以更新所述第三、第四、第五和第六信息,这些信息具有更新时间表或过期日期。

92. 根据权利要求91的系统,其中在钱夹处理装置(12)与相关用户-付款人(5)的移动电话(7)的通信之前或在操作处理装置(11)与相关收款人(6)的通信设备(8, 8a, 8b, 22)的通信中;所述钱夹处理装置(12)和所述操作处理装置(11)向技术检测处理装置(68)生成请求以获得移动电话网络(3)的技术标识、可能还有相关用户-付款人的移动电话技术的标识、或者相关收款人的通信设备(8, 8a, 8b, 22)的技术标识,技术检测处理装置(68)随后访问第一存储装置(13)上的第五和第六信息或者第二存储装置(15)上的第三和第四信息,以获得所述信息并将它发送到钱夹处理装置(12)或操作处理装置(11),钱夹处理装置(12)或操作处理装置(11)根据检测到的技术选择上述那些电信装置控制器中的一种电信装置控制器(10a, 10b, 10c, 10d, 10e, 10f)。

93. 根据权利要求89的系统,其中技术检测装置(68)检查第五和第六信息的过期日期或者第三和第四信息的过期日期,当所述信息还没有过期时将所述信息发送到钱夹处理装置(12)或操作处理装置(11),或者生成请求以检测移动电话网络的技术、移动电话(7)的技术或者通信设备(8, 8a, 8b, 22)的技术以更新第五和第六信息或第三和第四信息。

94. 根据权利要求89-93的系统,其中移动电话网络(3)周期性地生成并发送更新后的第五和第六信息或第三和第四信息,并且其中技术检测处理装置(68)将更新结果返回到移动电话网络(3)。

95. 根据权利要求89-94的系统,其中获得移动电话网络(3)的

技术和相关用户-付款人的移动电话(7)的技术的请求涉及第一存储装置中的多个第五和第六信息;并且其中获得移动电话网络的技术和相关收款人的通信设备(8, 8a, 8b, 22)的技术的请求涉及多个第三和第四信息;并且其中来自移动电话网络的响应包括多个更新后的第五和第六信息或第三和第四信息。

96. 根据权利要求3的系统,其中第一存储装置(13)中包括的标识各个相关用户-付款人的移动电话(7)的技术的第六信息涉及与表示选择用于通信的技术的优先级相关的多个技术。

97. 根据权利要求1的系统,其中第一存储装置(13)中包括的关于各个相关用户-付款人的支付方式的第二标识信息与最大购物额度和本地授权中心(69)的标识相关,以便在确认了与钱夹处理装置(12)相关的相关用户-付款人之后,生成包括指示存在至少一种支付方式与最大额度相关的确认;并且其中第二存储装置(15)中包括的标识各个相关收款人的第一信息与最大额度或收款人的如下授权特征之一相关:表示不允许委托授权的在线授权,表示只允许在特定额度之下的委托授权和交易的离线授权,或者表示交易额在指定额度之上或之下时允许所述授权之一的在线和离线授权的混合,以便在确认相关收款人时钱夹处理装置(14)生成包括收款人的授权特征指示的确认消息。

98. 根据权利要求97的系统,其中在检测到相关用户-付款人的确认消息表示它有至少一种与最大额度相关的支付方式,并且收款人的确认消息表示所述收款人的授权特征是在线时,生成的验证消息包括收款人允许的支付方式和与最大额度相关的付款人的支付方式的匹配,以便在接收到对验证消息的响应时检测与最大额度相关的支付方式,并且在钱夹处理装置(12)中生成委托验证请求,还在根据与最大额度相关的所选择的支付方式的标识所识别的本地授权中心(69)中生成委托授权请求,本地授权中心(69)包括第一存储装置(69a)以接收委托授权消息并完成所述授权,并发送结果到相关用户-付款人的移动电话和收款人的通信设备,所述第一存储装置存储了与各个相关用户-付款人相关并与最大额度有关的支付方式的第二标识信息;该授权中心(69)还包括用于从最大额度减去在支付和操作处理装置(1, 1')中包括的第七存储装置(71)中预先设置的一个特定时间段中进

行的支付以获得与所进行的扣除对应的可用净余额，并在交易额超过所述净余额时生成拒绝消息的装置。

99. 根据权利要求 98 的系统，其中本地授权中心（69）包括与第七存储装置（71）相连的批处理装置（70），以存储在预先设定的时间段内完成的不同交易，在预设的时间段结束时该批处理装置（70）通过通信控制器（21）发送不同交易到相应的金融实体处理装置，由该金融实体处理装置完成对用户-付款人的帐户扣除和对收款人的帐户存入。

100. 根据权利要求 3 的系统，其中相关用户-付款人的移动电话（7）可以支持 STK、J2ME 和 BREW，并且可能包含该用户-付款人相关的支付方式的标识，并且其中第一存储装置中的第六信息与存储了所述支付方式标识的移动电话（7）有关，以生成输入安全参数和相关收款人的支付方式的验证请求，以便当在移动电话（7）中接收到时，它能够确认相关用户-付款人和相关收款人的公共支付方式。

101. 根据权利要求 100 的系统，其中相关用户-付款人的移动电话（7）包括用于安全参数的激活密钥、随机参数和密码密钥的存储装置，所有这些都预先生成并可能存储在相关用户-付款人的金融实体处理装置（4）中，以在金融实体处理装置（4）或本地授权中心（69）中完成验证；移动电话（7）还包括用于对密钥和随机参数加密以生成包含该密钥和该随机参数的加密序列的装置；该加密序列被存储在本地授权中心或相关用户-付款人的金融实体处理装置中，以便通过确认所存储的加密序列与从移动电话（7）接收到的加密序列一致而完成验证。

102. 根据权利要求 101 的系统，其中移动电话（7）包括根据激活密钥生成输入安全参数的请求的装置，安全参数在输入之后被存储下来；以便在输入安全参数后生成加密序列，该加密序列被响应验证请求消息而发送到支付和操作处理装置（1）。

103. 根据权利要求 101 的系统，其中钱夹处理装置（12）在通过相关收款人的金融实体处理装置发送对相关用户-付款人的金融实体处理装置中的验证请求消息的响应时，再次对该加密序列加密。

104. 根据权利要求 100-103 的系统，其中该电信控制器装置（10）包括 WAP Push 控制器（10f），以通过 WAP 网关（89）和任何移动电

话网络(3)用WAP和WML消息与移动电话(7)通信,WAP Push控制器(10f)包括用于与支付和操作处理装置(1)的功能相关联的WAP(无线应用协议)应用程序的存储装置(10f1),还包括要以WML(无线标记语言)发送的文本消息;其中在WAP Push控制器(10f)和WAP网关(89)之间使用的协议是PAP(Push访问协议),在WAP网关(89)和移动电话(7)之间使用的协议是POVAP(Push空中协议)。

105. 根据权利要求104的系统,其中支付和操作处理装置(1)生成常规Push请求,以发送信息到至少一个移动电话(7),所发信息的内容是WML编程的,用常规元素p表示应该显示在移动电话屏幕上的句子,用常规元素输入允许输入安全参数。

106. 根据权利要求105的系统,其中WML语言脚本用来在每个移动电话中确认输入的安全参数的格式有效并避免不正确的数据串的传输。

107. 根据权利要求100和104的系统,其中交易请求包含分配给支付和操作处理装置的WAP地址,以便当移动电话发送所述交易请求时它显示一个WML页面,该页面显示对要完成的操作的和输入所选操作需要的数据的选择菜单,常规元素p、选择和选项用来选择所述想要的选择,所请求的信息被以WML显示。

108. 根据权利要求107的系统,其中WAP栈的基于SSL(安全套接字层)的安全标准协议WTLS(无线传输层系统)被用于建立移动电话和WAP Push控制器(10f)之间的通信,其中所述安全协议WTLS根据所需要的安全性可以支持加密和PKI(公共密钥基础结构)、WIM或者WPKI。

109. 根据权利要求100的系统,其中支持STK、J2ME或BREW的移动电话(7)存储了要完成的操作的选择菜单和涉及所执行操作的数据输入的选择菜单。

110. 根据权利要求1的系统,其中交易请求选择性地包括操作代码、支付和操作处理装置的标识代码、安全参数、支付方式、电话号码或它们的组合;并且支付和操作处理装置通过引导菜单请求交易请求中没有包括的所述代码和参数。

111. 根据权利要求1的系统,其中与一个国家相关的支付和操作处理装置(1)被通过通信控制器装置(21)连接到其它国家的金融实

体处理装置，并且其中电信控制器装置（10）与和该支付和操作处理装置（1）属于不同国家的运营商的移动电话网络的网关相连，以便充当其它国家中的支付和操作处理装置，为此所述国家中的相关用户-付款人和收款人必须与该支付和操作处理装置相关联。

112. 根据前述任一权利要求的系统，其中与支付和操作处理装置（1，1'）的发票和交易管理处理装置（45）相连的第七存储装置（39）包括在该支付和操作处理装置（1，1'）中完成的不同发票和操作的记录。

数字移动电话交易和支付系统

技术领域

所讨论的发明适用于移动电话技术、身份验证、数字签名领域中的电子交易产业领域，涉及贸易和支付系统。

背景技术

在本领域的现有技术中，已知在商业设施中借助于用户或付款人的移动电话使用支付系统和过程，所述的商业设施装备了销售终端（POS）（包括数字移动电话）以完成交易。。

在这点上，应该注意到欧洲专利申请 EP-00202720.9 说明了一种交易过程，该交易过程允许使用任何类型的移动电话作为使用 GSM（全球数字移动电话系统）移动电话网络的不同购物形式中的支付手段，并且不需对移动电话做出任何修改，这使得拥有移动电话的任何用户都能够签订所有的功能和支付服务，并且都不需要有信用卡。因此，它构成了具有与移动电话网络中通常存在的相应通信设备进行通信的不同移动电话通信能力的支付交易中心，并且该支付交易中心还包括识别进行支付的移动电话的类型的装置，并由此允许该支付及交易中心使用移动电话网络和任意类型的移动电话建立通信，而这在上述申请里提到的任何现有技术中都是不允许发生的。

应该注意的另一专利是未公开的西班牙专利，专利号为 200200576，它说明了一种使用移动电话并且另外还允许使用任何移动电话的交易和支付系统，该交易和支付系统允许利用采用了 GSM（全球数字移动电话系统）技术的各种移动电话网络进行操作。

没有任何现有技术或者提到的文档说明了这样一种系统：它除了允许用任何类型的移动电话进行支付之外，还允许使用来自任何国家或采用与所述移动电话不同技术的不同移动电话网络完成交易，以便该系统能够包容任何国家的任何移动电话用户，而不管现与之签约的移动电话网络、该网络所采用的技术或者所使用的支付和交易中心。

因此，目前不存在任何系统允许通过移动电话在国际间进行支付和交易。

发明内容

所讨论的发明的目的是通过如下系统克服现有技术的不便：该系统允许将任何类型的移动电话作为支付方式的启动装置，并允许对使用任何国家中与该系统相连的采用任何技术的任何移动电话网络的工具的使用，借此我们预见到不同国家中的多个操作和支付处理中心，每个国家的用户-付款人和收款人都与各自国家的操作和交易处理中心相关联，并且这些操作和交易处理中心通过国际寻址处理装置在它们自己之间互连，用来完成相同或不同国家的用户-付款人和收款人之间的交易和支付，以及识别每个用户的移动电话网络技术及用来进行相应支付的移动电话类型的装置。

本发明允许进行不同类型的购物，其中产品或服务被关联到一个索引（reference），它允许从自动售货机进行购物、购物后对待取货品的提前支付、个人之间的支付、充值并下载移动电话内容、因特网购物、目录购物、电话销售、发货和运送的付费、付费电视甚至是电子签名。

本发明的另一目的是允许小额支付，即非常小额的支付。

本发明所使用的系统还允许收款人通过因特网对支付方法、与产品或服务相关联的索引和与每个收款人相关联的数据进行查询和修改。

这个系统还允许用户-付款人通过移动电话对支付方法和每个相关用户-付款人的数据进行查询和修改。

本发明可以用于的另一操作是对支付的验证。它还可用于要进行的退货。

本发明还允许交换的消息使用语音消息。

另外，本发明还允许收款人使用移动电话作为销售终端（POS）。

为了实现前面所述目的，本发明提供了一种系统来处理与这个系统相关联的用户-付款人和收款人之间的支付和交易，以及至少一种由与金融实体处理装置相关联的至少一个金融机构的帐户所支持的支付方式。另外，用户-付款人与一个移动电话网络签定协议，这个条件对收款人不是必须的，收款人可以属于或可以不属于这样一个网络。但是，在任何情况下，必须通过使用借助于数字移动电话与金融处理装置之间建立的至少一个通信进行交易和支付，所述金融处理装置由常规手段在它们自己之间互连并与金融机构相连。金融机构通过常规手

段在它们自己之间通信并且和金融处理中心通信以交换数据。

本发明的特征是包括不同国家中的多个操作和支付处理中心，各个国家中的用户-付款人和收款人与它们相关联，并且它们通过国际寻址处理装置在它们自己之间互连，以通过下述装置实现相同或不同国家中的相关用户-付款人和收款人之间的交易和支付：

具有支持不同移动电话技术的大量不同技术移动电话网络的电信控制器装置，用户-付款人和收款人有选择地与其相关联，并且它与由电话号码或其它索引标识的任何用户-付款人的移动电话通信，或者与由特定的通信设备标识符所标识的收款人的通信设备通信，每个电信控制器装置包括多个通信控制器；

通信控制器与不同金融实体处理装置相连（任意国家的用户-付款人和收款人与它们相关联）以有选择地与相关用户-付款人的金融实体处理装置或相关收款人的金融实体处理装置通信；

操作处理装置，通过它可以有选择地与电信控制器装置或通信控制器装置通信，并可能首先接收相关用户-付款人的标识数据，随后又通过电信装置接收标识相关收款人的第二层数据，或者通过电信控制器装置另外接收标识与相关收款人有关的索引的第三层数据，操作处理装置有选择地生成对相关用户-付款人、相关收款人、产品索引或它们的组合的验证请求；

该操作处理装置包括对除上述第一、第二和第三信息之外有选择地接收到的涉及不同交易和支付方式的数据的识别装置；

钱夹处理装置，与操作处理装置相连，访问至少存储了各个相关用户-付款人的标识数据的存储装置，并将相关用户-付款人的标识数据链接到分配给各个相关用户-付款人的移动电话号码或索引号码，该钱夹处理装置用来处理在相关用户-付款人的验证请求中接收到的相关用户-付款人的标识数据，并生成确认相应的用户-付款人的消息；该存储装置除了标识数据之外还包含关于与各个相关用户-付款人对应的支付方式的数据，支付方式数据链接到标识数据并与各种支付方式所关联的金融机构标识处理装置相联；

销售商处理装置，与操作处理装置相连，它访问第二存储装置以处理在来自收款人的验证请求中接收到的相关收款人的第二层标识数据，并生成相关收款人的确认消息，第二存储装置至少存储了标识各

个相关收款人的第一层信息并将该信息链接到各个相关收款人的各种通信设备单元的标识代码；该第二存储装置还包括各个相关收款人的标识支付方式的第二信息，该信息与标识各个相关收款人的第一层信息以及各个收款人的支付方式所关联的金融实体处理装置的标识相关联，以便操作处理装置模块能够有选择地获得相关收款人的确认消息以及所述相关收款人的支付方式；并与收款人所关联的金融实体处理装置的标识相关联；

产品索引处理装置，与操作处理装置相连，它访问至少存储了多个产品索引的第一标识信息的第三存储装置，每一个产品索引标识信息都与相关收款人的标识相关联，并且有选择地至少与产品或服务的价格/货币标识相关联或者与收款人的通信设备标识符相关联，以处理在索引验证请求中接收到的产品索引标识的第三层数据，并生成产品索引验证消息，产品索引验证消息有选择地包括收款人的标识、产品或服务的价格/货币、相关收款人的标识或者相关收款人的通信设备的标识符或者以上几种的任意组合；

钱夹处理装置包括：

第一检测装置，用来获得相关收款人的支付方式，或者相关用户-付款人的支付方式，或者相关收款人和相关用户-付款人的公共支付方式，以在每当生成相关收款人或相关用户-付款人的验证消息或每当有关于相关用户-付款人、相关收款人或相关联产品索引的验证消息已经被生成时选择生成交易验证请求消息，或者选择性地发送所述验证请求消息到相关用户-付款人的移动电话；验证请求消息选择性地包括对相关用户-付款人的支付方式的验证消息、对相关收款人的支付方式的验证消息、或者对相关用户-付款人和相关收款人的公共支付方式的验证消息、从所述用户-付款人的支付方式或相关用户-付款人和相关收款人的公共支付方式中选择一种的请求、相关收款人的标识、以及相关收款人的产品或服务或者产品或服务的价格；

第二检测装置，用来获取所发送的验证消息的响应消息，响应消息包括安全参数（例如密码）或与之相关联的加密序列，至少还包括相关用户-付款人选择的支付方式；所述第二检测装置访问第一存储装置，第一存储装置还包括从相关用户-付款人的金融实体处理装置直接涉及验证实现的验证、通过相关收款人的金融实体处理装置的相

关用户 - 付款人的金融实体处理装置中的验证或者钱夹处理装置中的委托验证中所选验证的第三标识信息; 验证包括至少与用户 - 付款人所选择的支付方式相关联的安全参数或加密序列的确认, 并且对所选支付方式的确认与标识相关用户 - 付款人的第一信息相关联; 以便选择性地, 一旦核实了验证数据后, 能够进行委托验证从而确认所选择的支付方式能够支持该交易、在金融实体处理装置中完成该交易并将结果发送到相关用户 - 付款人和收款人;

第一存储装置包括标识与由钱夹处理装置访问的远程支付和操作处理装置相关联的用户 - 付款人的第四信息, 以处理第一层数据并检测与远程支付和操作处理装置相关联的用户 - 付款人的标识, 生成路由消息, 生成的路由消息至少包括与远程支付和操作处理装置相关联的用户 - 付款人的第一数据、确认请求、验证以及相关收款人的支付方式; 第三存储装置包括与远程支付和操作处理装置相关联的产品索引的第二标识信息, 以在产品索引处理装置处理产品索引确认请求中接收到的第三层数据, 以及检测到与远程支付和操作处理装置相关联的产品索引标识时生成至少包括相关用户 - 付款人的第三层数据和验证结果的路由消息;

支付和操作处理装置还包括路由处理装置以处理路由消息, 路由处理装置与操作处理装置相连, 并访问存储了至少国际寻址处理装置的至少第一标识信息的第四存储装置, 并从那里发送路由消息到远程支付和操作处理装置, 并由此确认与该远程支付和操作处理装置相关联的用户 - 付款人产品索引或收款人, 并处理所述验证或生成包含了验证请求消息的路由消息, 产生确认和验证或交易;

支付和操作处理装置包括技术检测器处理装置, 以能够通过用户 - 付款人或收款人所属的移动电话网络与用户 - 付款人的移动电话或收款人的通信设备进行选择性通信, 技术检测处理装置选择性地访问第一存储装置, 第一存储装置包括标识各个相关用户 - 付款人所用移动电话网络 and 技术的第五信息以及标识各个相关用户 - 付款人的移动电话技术并将之链接到相关联电话号码的第六信息; 或访问第二存储装置, 第二存储装置包含标识每个相关收款人所关联的移动电话网络和它的技术的第三信息, 以及标识与各个相关收款人的相关联的通信设备的技术的第四信息。

支付和操作处理装置还包括发票和交易管理处理装置，发票和交易管理处理装置与存储了所进行的不同交易的标识的第七存储装置相连，每个交易标识与相应的操作类型、进行交易的用户 - 付款人的标识、交易额、货币以及交易中涉及的相关收款人的标识有关。还应该注意的，按照惯例，在验证之后要完成对交易的授权，以使付款人（发起实体）的金融机构确认支付方式能够支持该交易以授权该交易，但本说明书没有考虑这个环境，因为它是在金融机构之间以常规方式完成的，并且也不是本发明的目标。还有一种可能性是可以在支付和操作中心内的本地授权处理装置中以委托方式进行授权，对此将针对小额支付情况进一步说明。

因此每次进行验证时其后总是跟随着相应的授权，这里除了小额支付情况之外都没有包括具体说明。

另外，当我们说在金融实体处理装置中进行验证时，意味着验证是由所述处理装置或所述金融机构进行，视具体情况而定，这对本发明根本没有影响。这是为什么我们交替使用术语金融实体处理装置或金融机构以简化说明书的原因。

通过使用所说明的结构，相同国家中的用户 - 付款人和收款人之间的支付事务是通过与用户 - 付款人和收款人都关联的所述国家的支付和操作处理装置完成的。因此，不同国家的用户 - 付款人和收款人之间的交易是通过与它们各自的国家相对应的并且他们与之相关联的支付和操作处理装置完成的，并且这些处理装置通过国际寻址处理装置彼此互连。

还有一种可能性是一个国家的支付与操作处理装置可以与其它国家的金融实体处理装置相连，并且通过漫游网关与这种国家的移动电话网络相连，这使得他们能够充当特定区域范围内的处理装置。例如，一个国家中的处理装置可以在一个或多个国家中操作，因此，这种国家的用户 - 付款人和收款人必须与管理该国的支付和操作处理装置相连。

在这两种情况的任一种情况下，完成交易或支付必须进行的最小移动电话通信包含任何移动电话技术和任何类型的移动电话，因此可以在任何国家中使用该系统，而不考虑它们的移动电话网络所采用的技术，也不考虑用户 - 付款人所使用的移动电话的类型和技术，因为

由技术检测器处理装置识别该通信所使用的网络和移动电话的技术，下面将更详细地对此进行说明。

因此，检测器将在 GSM 网络中所用的各种移动电话通信技术之间进行选择，包括 GSM（全球数字移动电话系统）、CDMA（码分多路访问）、TDMA（时分多路访问）和像 GPRS、EDGE（增强数据 GSM 演进）、CDMA 一代、UMTS（通用移动通信系统）和 CDMA 2000 的 2.5G 和 3G 系统。

移动电话自身的技术可以是目前技术水平下存在的那些技术中的任意一种。就 GSM 网络来说，终端或移动电话的技术可以是具有 USSD（无结构辅助服务数据）、MAP（移动应用部分）版本一或版本二功能的类型，或者是具有 STK（SIM 应用工具包）功能的移动电话。除了上述网络类型中的任何类型之外，终端或移动电话还可以具有使用 WAP（无线应用协议）、J2ME（Java 2 平台，微型版）、BREW（用于无线的二进制运行时间环境）以及它们的组合的应用程序，这将为所述终端带来用于存储关于相应应用程序（WAP、STK、J2ME 或 BREW）的信息的存储装置。由移动电话组成的相关收款人的通信设备中也存在相同特征。

另外，如果单个移动电话包括不同功能或通信应用程序，该系统将检测到它，后面对此会有更详细的说明。

标识相关用户 - 付款人的第一数据包括其电话号码或别的标识终端或用户的方式，例如分配给该系统中的每个支付和操作处理装置的 PAN 代码（私有帐号）或 EAN 代码（条码形式的 PAN）。

现在我们将说明本发明的系统进行相同国家中（即与相同支付和操作处理装置相关联）的用户 - 付款人和收款人之间的支付和交易的不同运行模式。但是，所有这些运行模式都适用于进行不同国家（即与不同支付和操作处理装置相关联）的用户 - 付款人和收款人之间的交易，下面将对此进行详细说明。

依照本发明的一个实施例，收款人的设备由常规 POS（销售终端）组成，它通过常规方式与它所关联的金融实体处理装置相连。常规 POS 与支付和操作处理装置并没有直接连接，并且通常由第三方管理，例如它通过常规陆上通信线路或无线连接与之通信的金融实体处理装置。

在这种情况下，如果用户 - 付款人通过这个 POS 进行购物，收款人输入该用户 - 付款人的标识及交易数据，并发送交易请求消息到它所关联的金融实体处理装置，该金融实体处理装置检测出该收款人所约定的支付方式，并且随即验证该收款人，产生收款人的验证消息，验证消息包括支付方式以及相关用户 - 付款人的第一标识数据。

这个验证消息被通过通信控制器装置发送到操作处理装置，并且该数据在钱夹处理装置中被用来确认该用户 - 付款人，钱夹处理装置随后发出上述验证消息。

在完成了交易之后，由金融实体处理装置将结果直接发回相关收款人的常规 POS，而相同的结果还被通过上述支付和操作处理装置的钱夹处理装置发送到用户 - 付款人。

还可以通过输入与相关收款人的标识有关的索引并输入至少产品或服务的标识或所述产品或服务的价格而在用户 - 付款人的移动电话中生成交易请求，交易请求被通过拨打支付和操作处理装置的标识号码而在移动电话网络上发送到支付和操作处理装置。另外，交易请求包括用户 - 付款人标识，这是在移动电话网络上进行的通信中被检测出来的，就像按常规为发送交易请求所进行的通信一样。这样，交易请求由操作处理装置通过电信控制器装置接收到，并根据哪个收款人被识别出而在索引处理装置中完成对索引的验证。接下来，完成对用户 - 收款人的验证以检测索引确认消息的钱夹处理装置；收款人和用户 - 付款人生成验证请求消息并在接收到验证请求的响应之后以上述方式完成交易。

还应该注意的是本发明计划将各个相关用户 - 付款人的各种支付方式与不同的安全参数相关联，或者相反地将各个用户 - 付款人的各种支付方式与相同的安全参数相关联，明显地对各个相关用户 - 付款人来说安全参数必须不同。另外第一存储装置包括与钱夹处理装置相关联的安全参数的标识，以完成委托验证并允许对该第一存储装置进行添加、删除、查询和更改。

因此，有两种类型的非常不同的安全参数：涉及金融实体处理装置中的验证的那些安全参数，以及涉及钱夹处理装置的那些安全参数。

收款人的通信设备可以由蜂窝 POS 组成，它主要由和移动电话网

络之间有无无线连接的销售终端组成，并通过该无线连接与支付和操作处理装置相连以完成由 POS 自己或用户 - 付款人的移动电话发起的交易。

在这种情况下，关于交易的响应消息被通过电信控制器装置发送到收款人的蜂窝 POS 以及用户 - 付款人的移动电话，而不管交易请求由收款人的蜂窝 POS 或用户 - 付款人的移动电话生成。同样，蜂窝 POS 发起的交易也是通过电信控制器装置接收的。

在本发明的一个实施例中，第三存储装置中所包括的多个索引的第一标识信息与移动电话充值服务有关，从而当发送了一个包含有与充值服务有关的索引的交易请求时，索引处理装置会检测该交易请求，索引处理装置检测出收款人标识，在这种情况下收款人是移动电话网络/运营商。另外，索引可以与充值价格相关联，并且所述价格可以被包括在交易请求中以便完成对收款人和用户 - 付款人的确认，并且生成验证请求消息。沿着这些线路，应该注意到操作处理装置必须知道要充值的移动电话号码，所以可以将所述号码包括到交易请求以及对验证请求的响应消息中，从而在这种情况下验证消息进一步包括输入要充值的电话号码的请求。

一旦操作处理装置以上述两种方式中的任意一种检测到要充值的电话号码，它可以选择生成并发送请求验证所检测到的移动电话号码允许由移动电话网络运营商充值的消息。

当运营商已经确认该电话号码允许充值时，它生成一个消息并发送给操作处理装置以完成对要充值的电话号码是否已经接收到交易请求的验证，或者当要充值的电话号码除了响应消息之外还接收到验证请求时完成交易。

在接收到交易结果之后操作处理装置马上生成由移动电话运营商执行的充值命令，并接收充值结果，以通过钱夹处理装置发送到相关用户 - 付款人的移动电话。

相同的运行方式还适用于用户 - 付款人想要下载移动电话内容的情况，但是在这种情况下，在接收到交易结果时开始通过移动电话网络从对应的服务器到交易请求中或验证请求响应消息中检测到的移动电话号码的下载。明显地，没有验证是否允许充值。

依照本发明，为了建立来自支付和操作处理装置和收款人的通信

设备的连接，必须知道其中的操作系统。为此，索引处理装置在验证索引时将在所述验证中包括与所述索引相关联的通信设备的标识，以便它在被操作处理装置检测到时生成该收款人的通信设备的验证请求连同收款人验证请求；这个请求被发送到销售商处理装置，销售商处理装置生成所述收款人的确认和该收款人的通信设备的确认，收款人的通信设备的确认包括涉及所述通信设备的操作系统的数据库以与之建立适当的通信。

需要验证通信设备的一个例子是收款人的设备由自动售货机组成时，其中用户 - 付款人可以进行购物，并且因此向蜂窝销售终端提供移动电话连接或允许自动售货机与支付和操作处理装置通信的设备。在这种情况下，第三存储装置中包括的多个索引的标识和该自动售货机关联在了一起，以便在检测到包括与这种自动售货机相关联的索引的交易请求时，索引处理装置生成包括自动售货机标识符的验证消息，并且操作处理装置生成一条消息并将其发送到自动售货机以启动这次购物，该消息至少包括通过该自动售货机的屏幕呈现给用户 - 付款人以选择要购物的产品的消息，该消息还包括相关用户 - 付款人的标识。为此，该自动售货机包括检测该消息的装置以通过在它的屏幕上显示请求选择商品的消息而启动该次购物，该消息可能还包括相关用户 - 付款人的标识，以便在该用户 - 付款人进行了所述选择之后该自动售货机生成表示选择已完成以及至少还有数额和货币或产品代码的消息并将它发送到操作处理装置。这个消息由钱夹处理装置的第一检测装置检测到，钱夹处理装置以已经说明过的方式生成验证请求消息和随后的交易。

交易结果被发送到自动售货机，自动售货机在检测到有效交易后发送请求和产品，或者如果交易未被许可就生成错误消息。

还可以将产品代码包括在操纵自动售货机的收款人的支付和操作处理装置的遥测服务中。这些服务包括，例如，产品价格的远程维护和操作画面（使用 web 界面）上的查询以及产品短缺报告、故障报告等等。

本发明的系统还将允许进行预付费购物。为此，第三存储装置中包括的标识多个索引的第一信息与预付费购物服务相关联，第三存储装置还包括与具有定位符的索引有关的信息以便操作处理装置检测到

预付费购物中的有效交易结果，生成包含交易结果、定位符、以及选择性地还有产品和服务在内的预付费购物消息。这个定位符可以是随机的。

在这种情况下收款人的通信设备由具有接收打印机的蜂窝 POS 组成，操作处理装置将获得的定位符和交易结果发送给蜂窝 POS。为此，当操作处理装置接收到有效交易结果时，它一方面将对该预付费购物的确认发送给用户 - 付款人，还至少将交易结果和定位符发送给用户 - 付款人。

另外，它将预付费购物消息发送给接收打印机，该消息至少包括交易结果、定位符和索引，可能还有产品或服务的额外信息，所有这些都打印出来。

这样，用户 - 付款人可以收集在相关收款人的零售市场上购买的产品，收款人在确定定位符一致后将产品交付给用户 - 付款人。还可以由支付和操作处理装置通过因特网建立通信，对此将有进一步的说明。

还可以用通信设备对旅游预约、休闲活动门票、租赁等进行预付费购买，这样定位符和交易结果都被同样发送到通信设备以使用户 - 付款人可以接收到门票、旅游证件、或者根据定位符购买或租用的其它物品。

根据这个说明，可以看到由自动售货机组成的蜂窝 POS 以及接收打印机都不会启动交易请求，但也不是所有交易请求都由用户 - 付款人启动。

在本发明的另一实现中，收款人的设备由通过不同于移动电话网络的其它方式（例如因特网）与支付和操作处理装置相连的虚拟销售终端组成。因此，支付和操作处理装置包括：具有与其它通信网络相连的所有相应接口的因特网处理装置；与操作处理装置的连接接口、与索引处理装置的连接接口以及与销售商处理装置的连接接口；从涉及响应、接收、请求的收款人的通信设备接收到的请求的选择性标识装置，以生成一个索引或一组索引、对第二和第三存储装置中数据的查询请求或对第二和第三存储装置中数据的更改请求；因特网处理装置还包括从操作处理装置接收到的请求（涉及对交易结果的通知、对原先已经由收款人请求过并被关联在第三存储装置中的购物索引的确

认通知、或者对相关收款人的至少一种产品的库存水平的查询)的选择性标识装置。

第二存储装置还包含因特网和 e-mail 地址(被链接到标识相关收款人的第二层数据)的选择性标识的第五信息,以用因特网以在线方式或通过 e-mail 以离线方式与收款人的通信设备通信。

因特网处理装置的选择性标识装置包括一个与访问控制模块相连的查询模块,访问控制模块访问销售商处理装置以获得相关收款人的数据。另外,访问控制模块包括对相关收款人的验证装置以验证所述收款人,所述验证包括确认收款人的身份以及在来自该相关收款人的通信装置的请求中接收到的密码。

这种结构允许在操作处理装置接收到操作结果(例如交易结果)时向因特网处理装置的查询模块生成对所述操作结果的通知请求,并由此获得相关收款人的数据,它的 email 地址或它的 IP 地址。在检测到 email 地址时,查询模块与加密模块和 email 发生器相连以加密与 email 消息的适当格式相适合的通知请求,并通过 email 控制器(包括在与不同于移动电话网络的通信网络的连接接口中)将该通知请求以及标识相关收款人的第二层数据发送到相应的 email 地址。

在操作处理装置生成关于操作结果的通知请求的情况下,该通知请求涉及因特网地址,查询模块获得相关收款人的数据和 IP 地址。在这种情况下,与不同于移动电话网络的通信网络的连接接口由因特网控制器组成,因特网控制器与该查询模块相连以由此发送通知请求到收款人的通信设备的相关因特网地址,并接收识别出接收到所述交易结果通知的响应,查询模块将该响应传递到操作处理装置。

这种配置允许通过收款人的通信设备进行购物,收款人的通信设备由虚拟销售终端组成,用户-付款人通过通信设备例如个人计算机获得对虚拟销售终端的访问。这样,一旦选择了要购买的产品,就有两种可能性:该产品与一个索引相关联,在这种情况下用户-付款人通过他的移动电话发送所述索引以及包含所述索引的交易请求;或者所选择的产品不与任何索引相关联,在这种情况下收款人的通信设备生成索引生成请求,该索引生成请求在因特网处理装置被接收到,因特网处理装置在验证了收款人之后,以上述方式将它发送到索引处理装置,索引处理装置生成所请求的索引并将其关联到该收款人、该产品

以及所指定的价格，并将所述索引存储在第三存储装置中，并通过查询模块和因特网控制器将它发送到相关收款人的通信设备，该索引随后被收款人的通信设备接收到，收款人的通信设备随后通知用户-付款人。

另外，本发明的系统提供了在交易请求中接收索引的可能性，当索引处理装置检测到已经根据索引生成请求创建了索引时，它能够确认所述索引生成请求是由所述索引所关联的收款人的通信设备发送。为此，当处理索引确认请求中包含的第三层数据时，索引处理装置检验索引是否是基于索引生成请求被创建的，并生成确认该索引是由它所关联的收款人所请求的确认请求，通过操作处理装置将所述索引发送到查询模块以获得相关收款人的数据，并通过因特网控制器将该请求发送到相关收款人的通信设备。从相关收款人的通信设备接收到的响应被传递到操作处理装置，在该响应表明所述被检测的索引确实是由该收款人的通信设备所请求时，操作处理装置以上述方式执行该交易。

另外，本发明的系统允许确认产品（正处理的交易所相关的产品）在收款人的库存中存在，换句话说，所述产品是可得到的。这种情况在通过虚拟销售终端购物时尤其有用，但在需要时也同样可以用在各种情况下。

为此，在钱夹处理装置生成用户-付款人验证请求消息之前，销售商处理装置生成关于相关收款人是否有所需要的产品可供购买的确认请求，通过操作处理装置将所述请求发送到因特网处理装置的查询模块以获得相关收款人的数据，接着通过因特网控制器将该请求发送到所述收款人的通信设备，并从相关收款人接收响应并将该响应传递到操作处理装置，以便如果后者检测到该收款人没有该产品时交易可以按照上述方式继续进行。

这种结构允许在因特网上进行购物，标识第三存储装置中包含的多个索引的第一信息被链接到通过因特网购买产品或服务的购买行为，在这种情况下交易请求是在因特网处理装置上被以上述方式接收到的，在完成了交易之后，所述交易的结果被根据上述因特网地址或 email 地址发送到收款人的设备。

因特网处理装置的结构还允许收款人是软件提供商，这样在请求

生成索引的情况下，它除了索引生成请求外还将包括对软件解密的需求，这个请求是通过钱夹处理装置与交易结果一起被发送到用户-付款人的移动电话的。因此，销售商将要交付的文件用解密密钥加密并下载到通信设备（用户-付款人的个人计算机），用户-付款人随后可将下载的文件解密或解锁。

所述结构还允许与因特网处理装置通信的收款人通信设备构成发票开具装置，它生成并发送索引生成请求，该请求还包括关于发票类型、数额、货币和到期日的信息，从而能够生成与这个数据相关联的索引，并由此允许根据所获得的索引支付发票。

这还适用于收款人的通信设备由付费电视解码控制器组成的情况，在这种情况下索引被关联到电视节目，以便在接收到交易结果时它能够激活解码器并允许观看相关的电视节目。

收款人的通信设备还可以由具有可下载移动电话内容的服务器组成，这样获得与所述内容的下载相关联的索引允许以上述相同的方式进行所述下载。

另一情况是收款人的通信设备与生成并发送索引生成请求的交付服务相关联，所述索引生成请求至少包括关于要交付的产品和价格的信息，以便完成该交付记录/发票的支付。

在这种情况下，可以采用两种途径进行支付，可以预付交付记录/发票，即在交付产品之前支付，或者货到付款，即在用户-付款人实际接收到产品时支付。因此，为了以这种方式进行支付，用户-付款人发送包含与交付记录相关的索引和要进行的支付的类型的交易请求。

当检测到预付交付记录时，以已经说明过的方式执行交易，在检测到货到付款时，发出与该货到付款相关联的索引生成请求，该请求被发送到相关收款人的通信设备，从而当索引处理装置检测到货到付款索引时它以已经说明的方式执行交易。

本发明还允许为进行的所有购物完成退货事务。该功能与为购物所说明的相同，区别仅在于操作处理装置在确认了用户-付款人之后检测退货操作并且收款人完成验证和后续交易。在退货操作中还有不对用户-付款人进行验证的可能。

在本发明的一种实施例中，相关收款人的通信设备由用于电子签名的虚拟销售终端组成，该虚拟销售终端为数字签名生成索引生成请

求。因此，首先必须生成数字签名证书，这是由相关用户-付款人启动的操作。当操作处理装置检测到数字签名证书注册操作时，就为相关用户-付款人生成一个公共密钥和一个私有密钥，通过销售商处理装置从第二存储装置获得与支付和操作处理装置相关联的认证授权中心（Cas）的菜单，该支付和操作处理装置向用户-付款人的移动电话发送选择所述认证授权机构之一的请求以及输入数字签名安全参数的请求，并在接收到所述用户-付款人发送的包含所请求数据的响应时，操作处理装置计算安全参数的散列，并用散列结果编码私有密钥并存储加密数据、生成了相连的定位符以发送加密的数据。

此后，操作处理装置通过通信控制器将相关用户-付款人的公共密钥以及相关用户-付款人的定位符和标识数据一起发送到所选择的认证授权机构。相关用户-付款人以所述授权机构指定的方式用各自的认证授权标识它们自己，例如，通过定位符来标识，并且所述授权机构生成包含相关用户-付款人的公共密钥的数字签名证书，并发送该电子签名证书到操作处理装置。

这时，通过相关收款人的通信设备完成对电子签名的实现，该通信设备例如是生成数字签名连同要签署的文档（可能还有相关用户-付款人所选择的其中的有关部分）的索引生成请求的数字签名销售终端。在索引处理装置中处理这个数据，索引处理装置生成索引并将它连同文档（可能还有相关数据）一起存储在第三存储装置中，将所有这些发送到数字签名销售终端，从而用户-付款人能够通过用他或她的移动电话发送所生成的索引而启动数字签名操作。操作处理装置在接收到生成的索引时检测到数字签名操作，在确认了用户-付款人、收款人和索引之后，钱夹处理装置生成验证请求消息，该消息包括输入数字签名的安全参数的请求、文档的散列（可能还有其中的敏感部分），从而在操作处理装置接收到数字签名的安全参数时计算出散列、将相关用户-付款人的私有密钥解密并用相关用户-付款人的所述私有密钥为加密的文档计算散列、并将它和证书一起发送到销售终端。交易结果随后被发送到该用户-付款人和相关收款人。

用数字签名生成的定位符可以用来查询所签署的文档。当操作处理装置接收到数字签名定位符时，它检测出文档查询操作，并通过展示由此识别出的所签署的文档而响应。

这样，本发明的系统可以用于第三方的验证，例如在电子签名的情况中。

第三方验证的另一例子是 Visa 3 区域验证模型，它由从支付和操作处理装置请求验证与特定用户-付款人相关联的支付方式组成，为此，由虚拟销售终端组成的收款人的通信设备生成包含与用户-付款人相关联的支付方式验证请求的交易请求。虚拟销售终端首先查询金融机构的支付方式目录，从那里获得支付和操作处理装置的 URL（统一资源定位符），支付和操作处理装置的因特网处理装置使用所述 URL 通信以接收验证请求，并且在这种情况下在钱夹处理装置中生成的验证请求消息由输入安全参数和验证过的支付方式的请求组成。这样，当支付和操作处理装置通过因特网处理装置接收到对支付方式的检验请求时，在确认了用户-付款人以及希望进行检验的支付方式之后，支付和操作处理装置发送请用户-付款人输入支付方式的安全参数的验证请求，验证所述支付方式，并将结果发送到收款人的虚拟销售终端。

另外，因特网处理装置还允许对第二和第三存储装置的查询和修改，由此因特网处理装置包括与因特网控制器相连的电子商务处理装置以允许通过先前说明的通信设备之一访问因特网处理装置。电子商务处理装置与访问控制模块相连，以检测对第二或第三存储装置的查询或修改请求，并随后执行对相关收款人的验证，并通过销售商处理装置或索引处理装置处理请求，销售商处理装置或索引处理装置借助于访问控制模块、电子商务处理装置和因特网控制器执行查询或修改并将结果发送到相关收款人的通信设备。

为了提供这个功能，电子商务处理装置由图形用户界面组成，图形用户界面在相关收款人的设备上显示查询或修改的不同可能性。

可以由系统分析员或管理员完成相同的功能，为此他们必须拥有与支付和操作处理装置的因特网处理装置相连的通信设备。在这种情况下，系统管理员的通信设备的连接是通过专用网络控制器实现的，该专用网络控制器构成了因特网处理装置与不同于移动电话网络的通信网络的连接接口的一部分。

另外，在这种情况下，该专用网络控制器与销售商数据网管理模块相连，以允许通过专用网络从系统管理员的通信设备访问，销售商数据网管理模块存储了提供给相关收款人的不同服务。

在这种情况下还必须执行对系统管理员的通信设备的验证，并且销售商数据网管理模块必须与访问控制模块相连，以检测由系统管理员的通信设备发起的在第二或第三存储装置中创建新表项、查询或修改的请求，以允许在所述验证后进行查询或修改。

销售商数据网管理模块由一个图形用户界面组成，该图形用户界面向系统管理员展示了支付和操作处理装置提供给相关收款人的不同查询和修改选项。

在上述任意操作中，其中因特网处理装置的访问控制模块访问销售商处理装置或索引处理装置，应该注意到这是通过应用服务器或模块完成的，以在因特网和专用网络以及所述销售商或索引处理装置之间建立连接。

本发明的系统允许的其它操作包括允许在个人之间进行支付和交易，即在用户-付款人之间进行，在这种情况下收款人是相关的用户-付款人。在这种情况下，对所述收款人的验证是通过钱夹处理装置完成的，一旦操作处理装置通过它的标准识别装置检测出这是个人之间的支付操作，就以已经说明过的方式完成该交易。在这种情况下，用户-付款人输入收款人的标识以及要支付的数额以生成交易请求。

个人之间的支付还有第二种形式，这种形式由允许在个人之间进行延迟支付组成，在这种情况下交易是在两个不同阶段中完成的。

在第一阶段中，只进行对用户-付款人的验证，在第二阶段中以下述方式完成对收款人的验证。

为此，第一存储装置中包含的选择性验证标识的第三信息涉及他或她所关联的金融实体处理装置中对用户-付款人验证的实现，或者他或她所关联的金融实体处理装置中对收款人的验证，所述验证被链接到个人之间的延迟支付操作，以便在操作处理装置识别出通过电信控制器接收到的个人之间的延迟支付操作的方式时完成所述验证之一。

因此，当用户-付款人用他或她的移动电话发送个人之间的延迟支付交易请求并在所述请求中包括收款人标识和支付数额时，钱夹处理装置的第二检测装置检测到用户-付款人所关联的金融实体处理装置中对用户-付款人的验证，金融实体处理装置在该交易完成时将验证结果发送到相关用户-付款人的移动电话，同时操作处理装置生成与个人之间的延迟支付相关联的索引生成请求，该请求被发送到索引处理装

置执行，所产生的索引和涉及个人之间延迟支付操作的数据一起被存储在第三存储装置中。所述索引和交易数据一起被发送到相关收款人的移动电话，收款人在这种情况下，如前所述，也是相关的用户-付款人。

这样，当相关收款人生成包含了在索引处理装置中生成并被关联到个人之间延迟交易的索引的交易请求时，第二阶段就开始了，这样在操作处理装置接收到交易请求时它使得钱夹处理装置生成验证消息并将验证消息发送到所述收款人，该消息中的支付方式是相关收款人的支付方式，从而他或她能够选择他或她希望用来接收所述延迟支付的那种支付方式，以便对所述收款人的验证能够在他或她所关联的金融实体处理装置中完成，并且随后利用被发送到相关收款人的移动电话的结果执行该交易。

相关用户-付款人还可以用他们的移动电话向他或她所关联的金融实体处理装置查询这种项目，例如最近的活动或特定支付方式上的可用余额，由此他或她将生成查询交易请求，该查询交易请求由操作处理装置的识别装置检测到，随后钱夹处理装置验证用户-付款人并生成验证消息，所生成的验证消息包括所述相关用户-付款人的支付方式、输入安全参数的请求、选择至少一种支付方式的请求以及输入要进行的查询的参数的请求。随后在金融实体处理装置中完成该交易，金融实体处理装置将所述查询/交易的结果发送到操作处理装置，以便钱夹处理装置能够将该结果发送到用户-付款人的移动电话。

本发明所允许的另一操作是通过移动电话对与用户-付款人相关联的不同数据进行修改的能力。在这种情况下，所述交易请求由允许进行更改的参数化操作的标识组成，例如与钱夹处理装置相关的安全参数、用于通信的语言、缺省支付方式或请求向用户-付款人发送额外的确认消息的标识。这个交易在操作处理装置的识别装置中被检测到，操作处理装置验证用户-付款人，并且钱夹处理装置生成验证消息，该验证消息由用户-付款人的支付方式、输入安全参数的请求、选择至少一种支付方式的请求以及对要修改参数的请求组成，从而对该验证请求消息的响应消息包含交易中要修改的参数，这些参数被发送到用户-付款人所关联的金融实体处理装置，以便在所述修改之后该响应可以被以已经说明过的形式发送到相应用户-付款人的移动电话。因

此，这个特征允许安全参数、支付方式或所涉及的任意其它操作的变化。

在这种情况下，安全参数被链接到钱夹处理装置，钱夹处理装置完成所述验证。为此，第一存储装置包括与钱夹处理装置相关联的安全参数的标识，以完成委托验证以及对第一存储装置中包含的信息的查询和修改。

用户-付款人还可以用他们的移动电话对钱夹处理装置进行查询，例如最后的活动或一种支付方式的可用余额。在这种情况下，操作处理的识别装置检测出钱夹处理装置中的查询操作，钱夹处理装置在验证了相关用户-付款人之后生成验证消息，该验证消息包括该用户-付款人的支付方式、输入安全参数的请求、选择至少一种支付方式的请求以及输入要查询的参数的请求。

在这个操作中，验证过的安全参数还是与钱夹处理装置相关联的安全参数。

为了完成上述所有功能，索引处理装置包括了管理模块、自动维护模块和编码模块，管理模块通过接口与第三存储装置和操作处理装置相连以接收索引并验证它们，并通过接口和销售商处理装置相连以根据接收到的索引传送相关收款人的标识，或者发送/接收与远程支付和操作处理装置相关联的索引，另外，管理模块通过接口与路由处理装置相连，以完成对来自远程支付和操作处理装置或到远程支付和操作处理装置的索引访问；自动维护模块通过管理模块访问第三存储装置，以检测并消除过期的索引；编码模块用定义好的算法将索引编码并将它们存储在第三存储装置中。

从本说明书中可以看出，很明显有不同类型的索引，例如可以根据以下因素而归类：

- 功能

- 操作索引：这些索引用特定的相关价格标识对一种或多种产品或服务的购买操作。这覆盖了（例如）对在因特网上进行的操作（下定单、充值电话、知识产权下载）的需求。

- 销售终端索引：这些索引标识充当销售终端的终端或设备，其数据和操作系统被存储在索引处理装置（16）中。这些索引涉及用户在哪里发起交易的销售终端的特定类型，例如自动售货机。

操作索引同时也可根据以下因素分类：

- 生成的起点和时间：

- 预先-生成的：此时销售商使用 Web 管理工具请求它。生成的索引被发送到了销售商，销售商在他们的系统中包括了这些索引并将这些索引提供给用户以进行支付。在预先知道产品或服务的价格时可以使用这些索引。

- 在线生成的：不是用 Web 管理工具生成，而是销售商（例如虚拟 POS）在接收到来自用户的任意购物请求时，与支付和操作处理装置（1）通信并通过提供必要数据（销售商标识、交易额、货币、等等）请求生成一个索引，并且支付和操作处理装置返回一个索引（如果合适的话，还有前面说明的定位符），销售商随后将它传送给用户。例如，这被用在虚拟销售点中，例如电子商务购物车，那里不必知道最终价格。

- 根据性能：

- 单次使用，在交易后过期并被从第三存储装置删除以重新分配给其它销售商。例如，这些索引可以和产品（例如可下载的音乐）的单个副本或一组产品（例如在线购物车）相关联。

- 多次使用；用户-付款人总是使用相同的索引进行支付，该索引同时与特定的产品或服务相关联。例如，有为在线书店的当月畅销书或饭店显示屏上的超豪华汉堡包发布的索引。产品的交付可能需要使用定位符。

- 根据地理范围：

- 国内使用的索引，限国内使用，不允许国际购物，因此必须被限制在本地索引处理装置中。

- 国际索引：用于由本发明的系统内的任何用户-付款人的购物而不管交易发起人来自哪个国家。

- 多国索引：上述索引的子群，用来在当付款人和销售商属于不同国家中的支付和操作处理装置时帮助用移动电话进行通话。在这种情况下，支付和操作处理装置生成索引，索引被发送到具有完成对支付方式和安全参数的请求所需的信息的其余支付和操作处理装置。这样，当用户用不属于该支付和操作处理装置的索引启动交易时，如果所述索引被注册为外部（多国）索引，对支付方式和安全参数的请求

就被直接处理并且该操作随即被转发到受让方的支付和操作处理装置，受让方的支付和操作处理装置管理该交易的环境。

出于功能原因，在线完成的索引生成请求只能是单次使用，并且出于效率原因，将只允许多国索引用作多次使用索引。

除了所有上述功能外，账户处理装置还包括了管理模块，它由第一和第二检测装置组成，该管理模块与第一存储装置和一个接口相连，以便由支付和操作处理装置的系统分析员或金融实体处理装置的系统分析员或管理员执行对支付方式的添加、删除和修改。另外，钱夹处理装置包括消息传递处理装置，该信息传递处理装置与第一存储装置、管理处理装置和一个接口相连，该信息传递处理装置通过该接口连接到技术检测处理装置以及用于和用户-付款人的移动电话通信的电信控制器装置。钱夹处理装置还包括验证处理装置，该验证处理装置与第一存储装置、管理处理装置和一个接口相连，以让它能够完成与和钱夹处理装置有关的安全参数验证相关联的用户-付款人的验证、委托验证，并将对与远程支付和操作处理装置相关联的用户-付款人的验证请求发送到国际寻址处理装置。

还要注意到本发明可能需要有涉及许可控制的交易。当操作处理装置的识别装置检测到许可控制交易时，钱夹处理装置生成支付与操作处理装置中的委托验证请求，该验证请求由输入该钱夹处理装置的安全参数的请求组成，这将允许对建筑、娱乐场所或地面的许可控制。

所有前面的操作都能够在不同国家的用户-付款人和收款人之间完成。为此，当钱夹处理装置检测到用户-付款人与相应的支付和操作处理装置不关联时，它生成一个路由消息，该路由消息包含对与远程支付和操作处理装置相关联的用户-付款人的确认和验证请求，所述请求还包括相关收款人的支付方式，以便能够在远程支付和操作处理装置中完成验证，远程支付和操作处理装置通过国际寻址处理装置将确认验证请求的结果发送到相关收款人所关联的支付和操作处理装置。根据这些结果，该支付和操作处理装置执行该交易，并在完成时用交易结果生成一个路由消息以通过他或她所关联的支付处理装置传送到用户-付款人。

在这种情况下，消息被发送到用户-付款人的移动电话，从用户-收款人所关联的移动电话网络借助通常称作漫游的系统经由收款人所

在国家的移动电话网络到达。

这种结构允许通过收款人的业务从海外进行购物，其中交易请求发自所述收款人的通信设备。

还可以有这种情况：交易请求来自目前位于他或她自己的国家之外的用户-购买者的移动电话。这个请求通过在收款人的国家或地区中存在并可由该用户-付款人在所述漫游系统下使用的移动电话网络之一到达该用户-付款人的远程支付和操作处理装置。在这种情况下索引处理装置检测到它是与远程支付和操作处理装置相关联的索引，并生成包含与远程支付和操作处理装置相关联的收款人的第三标识数据的路由消息。这个路由消息被通过国际寻址处理装置发送到所述远程支付和操作处理装置，该远程支付和操作处理装置确认该索引并生成还包含了相关收款人的支付方式的确认请求消息，以用上述方式完成该确认验证。另外，还值得注意的是，该过程与用户-付款人在他或她自己的国家中并从另一国家的相关收款人进行购物的情况中的过程相同，在这种情况下消息只穿过他或她所属的移动电话网络发送到该用户-付款人的移动电话。

第一存储装置中所包括的与远程支付和操作处理装置相关联的用户-付款人的第四标识信息包含关于所讨论的移动电话的对应发起国家的移动电话号码的国家代码、或该用户-付款人与之相关联的支付和操作处理装置的国家代码、或远程支付和操作处理装置的 PAN 代码的国家代码和 BAN 代码的国家代码的标识，以允许所生成的路由消息检测到国家代码。

同样，第三存储装置中所包括的与远程支付和操作处理装置相关联的索引的第三标识信息包含该索引所关联的支付和操作处理装置的国家代码的选择性标识，以在由此检测到国家代码时生成路由消息。

为了让所有上述功能都成为可能，国际寻址处理装置包含了一个连接和访问控制器，连接和访问控制器具有多个路由处理装置，路由处理装置是通过访问第五存储装置的路由管理器控制的，第五存储装置至少包括关于与远程支付和操作处理装置相关联的用户-付款人的国家代码的国际标识的第一信息、关于与该远程用户-付款人相关联的索引的第二信息以及关于发送/接收上述路由消息所遵循的路径的第三标识信息。

在国际交易和支付的情况下，第一和第二存储装置必须包括每个相关用户 - 付款人和收款人的语言的标识信息，以便能够与相关收款人的通信设备或相关用户 - 付款人的移动电话进行的有选择性的通信以正确的语言接收到相关联的数据。

语言和货币的标识还可以应用到通过单个支付和操作处理装置进行交易和支付的情况，也就是说用户 - 付款人和收款人在相同国家内的情况。

在所有上述形式中，当没有发出对用户 - 付款人或收款人的确认消息时、相关联的索引无效时、不能核实验证数据或不能完成交易时都会生成一个拒绝消息。

如上所述，本发明还允许相关收款人的通信设备由移动电话组成，构成这里所谓的 POS（由移动电话号码标识），并且有选择性地与和第三存储装置中包括的第一信息相关联的索引有关，所述第一信息又与请求数据的选择性消息序列相关联，以在通过识别装置检测到来自充当销售终端的移动电话的交易请求时或者来自涉及充当 POS 的移动电话的用户 - 收款人的移动电话的交易请求时建立操作处理装置；并与移动电话 POS 交换消息，并且有选择性地获取涉及要完成的操作的数据、相关用户 - 付款人的第一标识数据、相关收款人的安全参数、产品或服务的价格以及可用货币。

为了获得收款人的安全参数，本发明需要第二存储装置包括第六标识信息，第六标识信息是与相关收款人的第一标识信息相关联的安全参数的标识信息，以便当操作处理装置检测到发起自移动电话 POS 的交易请求时生成对相关收款人的验证消息，该验证消息包括收款人标识以及输入安全参数的请求，该请求被发送到了收款人的 POS。当操作处理装置检测到响应时，它请求销售商处理装置验证它，销售商处理装置通过访问第二存储装置进行验证。

发起自充当 POS 的移动电话的交易请求可以是购物操作、退货操作或对所完成的交易的查询。

当操作处理装置接收到发起自充当 POS 的移动电话的对所完成交易的查询操作时，以上述方式确认并验证收款人，在获得了相关用户 - 付款人、数额、货币或者可选择地还有交易日期的标识之后；所有这些都发送到了交易和发票管理处理装置，交易和发票管理处理装置

访问第七存储装置以确认该交易已经被完成，并将结果发送到相关收款人的移动电话 POS。

这样，在收款人想要通过他或她的移动电话 POS 产生交易请求的情况下，所述收款人输入了代表该移动电话 POS 的操作代码以与支付和操作处理装置通信，其中完成了对收款人的确认，与该移动电话 POS 交换了消息以获得涉及相关用户 - 付款人的数据、用于验证所述收款人的相关收款人的安全参数以及涉及交易的数据（例如产品或服务的价格，或者货币）。

同样，当用户 - 付款人想要请求涉及作为 POS 的移动电话的交易时，它生成涉及所述移动 POS 的交易，并且操作处理装置在对该用户 - 付款人进行确认之后生成到该移动电话 POS 的连续的消息，以请求涉及该交易的数据，将这些数据输入他的移动电话作为响应发送消息。一旦已经接收到所有的交易数据，包括要完成验证的收款人的安全参数，就如上所述执行该交易。

蜂窝 POS 还可以执行对先前的交易的查询，在这种情况下操作处理装置将接收到发自蜂窝 POS 的对早先交易的查询。在获得了相关用户 - 付款人的标识数据、数额、货币或者可选择地还有交易日期之后，该信息被发送到发票和交易管理处理装置，发票和交易管理处理装置访问第七存储装置以确认该交易是否完成，并将结果发送到相关收款人的蜂窝 POS。因此，在这种情况下，没有对相关收款人进行任何验证。

在这一节的开始我们讲述了电信控制器由多个通信控制器组成，在本发明的一个实现例子中，这多个通信控制器包括一个 USSD（无结构辅助服务数据）控制器和一个交换设备，该 USSD 控制器包括第一存储装置（其中存储了支付和操作处理装置的运行信息）、协议转换器（将 USSD 结构转换成支付和操作处理装置所用协议或进行相反的转换），以检测所收到的信息是否应该被发送到操作处理装置或钱夹处理装置；该交换设备访问第二存储装置和接收信息要遵从的路线，并根据所建立的路线将信息发送到操作处理装置或钱夹处理装置。

这允许使用 GSM 网络上采用的 USSD 字符串交换消息。

当操作处理装置检测到从移动电话 POS 启动的 USSD 会话中的交易请求时，在销售商处理装置中确认了收款人之后，操作处理装置具有不同可用选项的选择菜单，并且一旦相关收款人选择了选项之一并响

应,操作处理装置发出请求完成所选交易所需数据的新菜单,重复 USSD 会话中的过程, USSD 会话保持开放直到获得了所需数据, USSD 会话包括输入相关收款人的安全参数以完成验证的请求,并且其中用户-付款人的验证消息以及交易结果被通过与相关用户-付款人的移动电话建立 USSD 会话的钱夹处理装置发送到所述用户-付款人的移动电话。

同样,为了允许 GSM 网络上的通信,本发明需要电信控制器装置包括 SMS 控制器,以检测接收到的信息是否被发送到了操作处理装置或者钱夹处理装置,该 SMS 控制器由第一存储装置和协议转换器组成,第一存储装置中存储了运行支付和操作处理装置的信息,协议转换器将 SMS 消息转换成该支付和操作处理装置所用协议并进行反方面转换。另外,该 SMS 控制器装备有交换设备,该交换设备访问第二存储装置和要遵从的路线,并根据建立的路线发送从操作处理装置或钱夹处理装置接收到的信息。

在移动电话充当销售终端或者用户-付款人的具备 STK 功能的移动电话的情况下,该电话具有涉及支付和操作处理装置运行的 STK 应用程序。这个应用程序是通过 OTA 服务器(空中(Over the Air))和 SMS 消息中心从 STK 应用程序服务器下载的。这个应用程序显示了带有可用交易的菜单,并且一旦选择之后,会有另一个提示,提示输入完成所选择的交易所需的数据。如果需要的话,这个数据可以包括相关收款人的安全参数。该 STK 应用程序通过主动命令与移动电话 POS 或用户-付款人的具备 STK 功能的移动电话通信。

从支付和操作处理装置发往移动电话 POS 或用户-付款人的移动电话或反方向发出的每个消息都采用了 SMS 消息传递能力。

另外,该 STK 应用程序可以在用作 POS 的移动电话或用户-付款人的移动电话的 SIM 卡的存储器中存储信息,当然用户-付款人的移动电话是具备 STK 功能的,由此允许用户-付款人和收款人随时查询这个信息,例如先前的交易。

在移动电话 POS 及支付和操作处理装置之间交换的消息被用 3DES (三元数据加密标准)利用一个对称密钥密码和另一由 16 个密钥组成的密码进行了加密,该对称密钥密码存储在支付和操作处理装置中并被链接到各个相关收款人的安全参数,所述由 16 个密钥组成的密码中只有一个密钥可以从操作处理装置选择性地激活,并且随着时间被随

机改变。

在用户-付款人的移动电话以及支付和操作处理装置之间交换的消息被用 3DES (三元数据加密标准) 利用一个对称密钥密码以及移动电话自身上的由 IMSI (国际移动用户身份) 组成的另一密码进行了加密, 所述对称密钥密码存储在支付和操作处理装置中并被链接到各个相关用户-收款人的安全参数。

因此, 当相关收款人通过用作销售终端的具备 STK 功能的移动电话启动交易时, 该应用程序选择性地请求用户-付收款人的标识、数额以及相关收款人的安全参数。它随后用输入的数据生成一个 SMS 消息并将它发送到支付和操作处理装置, 支付和操作处理装置一旦检测到该消息就在完成交易后也用 SMS 将结果发回。

在由用户-付款人通过具备 STK 功能的移动电话启动交易的情况下, 该应用程序显示带有不同可用操作选项的菜单, 一旦输入了选择, 就打开另一菜单以请求完成所选交易所需的数据。它随后生成并发送包含激活该 STK 应用程序的验证请求的 SMS 消息, 并显示请求输入支付方式和安全参数的菜单, 用输入的信息生成一个 SMS 消息并将它发送到支付和操作处理装置, 支付和操作处理装置一旦检测到该 SMS 消息并且完成了交易就通过 SMS 消息中心将结果发回。

另外, 不管是在 GSM 网络以及 CDMA/TDMA 网络上, 本发明允许从操作处理装置发出的消息是语音而非文本, 收款人或用户-付款人通过用键盘或语音输入所请求的各种数据而响应这些消息。因此, 电信控制器装置包括与常规 IVR 设备相连的 IVR (交互式语音响应) 控制器, IVR 控制器唯一装备了存有支付和操作处理装置运行信息的第一存储装置以及基于 TCP/IP 协议 (传输控制协议/因特网协议) 的具有安全连接的连接接口。IVR 设备与 PBX 交换机 (专用自动交换机) 连接, 以和不同的移动电话网络通信并与相关用户-付款人的不同移动电话以及具有语音识别机制的收款人通信设备交换消息。

当从用户-付款人的移动电话或收款人的通信设备同 IVR 进行通信时, 会接收到一个呼叫音以及个性化欢迎消息以确保对 IVR 的验证。

因此, 操作处理装置在检测到由 IVR 设备处理的交易请求时, 生成请求数据的选择性序列以建立涉及交易菜单的语音指令, 以有选择性地获得完成交易所需的数据。在移动电话被用作 POS 的情况下, 它

还请求收款人输入他或她的安全参数以根据已经说明的方式进行验证。

当操作处理装置检测到来自移动电话 POS 的 IVR 会话中的交易请求时，在销售商处理装置中确认了收款人之后，它发送一个具有不同的可用操作的语音选择菜单。在收款人用键盘或语音指令选择了想要的操作之后，该选择被发送到操作处理装置，操作处理装置随后打开一个新的语音菜单以请求所选交易需要的数据并在 IVR 会话中重复该过程，IVR 会话保持开放直到接收到所述所需数据，包括对相关收款人的安全参数的输入，以及用户 - 付款人的验证消息。交易结果被通过钱夹处理装置发送到用户 - 付款人的移动电话。

为了完成上述所有功能，销售商处理装置包括与第二存储装置相连的管理模块以及与操作处理装置的连接接口，以便它能够完成对相关收款人标识符和相应的支付方式的添加、删除和修改。这可以由支付和操作处理装置的系统分析员或金融实体处理装置的系统分析员或管理员完成。另外销售商处理装置包括与第二存储装置、管理处理装置以及接口相连的验证处理装置，以允许它执行对相关收款人的确认以及对涉及相关收款人的安全参数的验证。另外，它还允许通过高级 CDMA/TDMA 移动电话网络的智能网进行通信。为此，电信控制器装置包括智能网控制器，它包含了协议转换以将支付和操作处理装置所用的协议转换成智能网的协议或者进行相反方向的转换，由此允许支付和操作处理装置与包含该支付和操作处理装置运行信息的智能网服务控制点 (SCP) 之间的通信。在这种情况下，为了通过智能网完成通信，用户 - 付款人的移动电话和收款人的通信设备必须能够为智能网生成触发点以发送交易请求（交易请求被智能网上的移动交换中心检测到），并将它发送到支付和操作处理装置，以允许相关用户 - 付款人的移动电话或相关收款人的通信设备在智能网上和支付及操作处理装置通信。发起自相关收款人的通信设备（由蜂窝 POS 组成）的触发信号包含了相关用户 - 付款人的标识信息、产品和服务以及产品和服务的相应价格。

智能网的智能外设 (IP) 可能包括从相关用户 - 付款人请求各种数据的预先记录的消息，还可能包括从相关收款人的通信设备请求数据的预先 - 记录的消息，以用和上述 IVR 设备相同的方式根据预先 -

记录的语音指令发送该消息。

还有一种可能性是上述 SMS 控制器与智能网的 SMS 中心相连，以通过发送 SMS 消息从相关用户 - 付款人的移动电话或者从相关收款人的通信设备请求各种数据。

另外，如前所述，为了与各种不同技术的移动电话网络以及与各种不同类型的移动电话通信，必须通过这一节开始说明的技术检测器检测出相应的技术。

为此，应该注意第一存储装置中包括的第六信息涉及与各个相关用户 - 付款人相关联的移动电话网络的标识，并且每个第六信息涉及各个相关用户 - 付款人的各个移动电话的技术，另外第二存储装置中包括的每个第三信息涉及各个相关收款人的移动电话网络的标识，并且第四信息涉及各个相关收款人的各个通信设备的技术，此时标识代码是电话号码或所涉及的别的号码，或者是 GSM 网络的国际移动设备标识符 (IMEI)，GSM 网络中的每个移动电话由电话制造商分配作为唯一标识符的一个 IMEI 号码标识。

对 CDMA/TDMA 网络也存在这种情况，但在这种情况下国际标识符是唯一标识与 CDMA/TDMA 移动电话网络相关联的各个移动电话的电子序列号 (ESN)。

IMEI 和 ESN 都被存储在移动电话网络的一个结点上，该结点是标准，以便在建立通信时可以访问这些结点以更新与终端或移动电话技术、各个相关用户 - 付款人和相关收款人的网络的技术有关的信息。

为此，电信控制器装置包括一个 HTTP (超文本传输协议) 控制器，以便支付和操作处理装置的技术检测控制器能够与各个移动电话网络通信，所述处理装置访问第一存储装置上包含的第五和第六信息或第二存储装置上包含的第三和第四信息以更新第三、第四、第五和第六信息，这些信息有选择地与终止日期和更新进度相关联。

本发明还提供了一种可能性，即在钱夹处理装置与相关用户 - 付款人的移动电话的任何通信或操作处理装置与相关收款人的通信设备的任何通信之前，所述钱夹处理装置或所述操作处理装置必须首先生成一个请求，请求从技术检测处理装置获得相关用户 - 付款人的所述移动电话的移动电话网络的技术标识或者相关收款人的通信设备的移动网络的技术标识，技术检测处理装置随后访问第一存储装置上的第

五和第六信息或者第二存储装置上的第三和第四信息以获得所述信息，并将它适当地发送到钱夹处理装置或操作处理装置，钱夹处理装置或操作处理装置随后根据所检测到的技术选择上述那些中的一个通信装置控制器。

技术检测处理装置检验第五和第六信息或第三和第四信息的过期日期，假设所述信息还没有过期，技术检测处理装置就将所述信息适当地发送到钱夹处理装置或操作处理装置；否则，它生成一个要检测该移动电话和通信设备的技术和移动电话网络的技术的请求，以适当地更新所述第五和第六信息或第三和第四信息。

本发明提供的另一种可能性是移动电话网络适当地生成并发送涉及第五和第六信息或第三和第四信息的更新过的信息，其中技术检测处理装置将更新结果返回该移动电话的网络。

不管检测技术的形式如何，存在以下可能性，获取相关用户 - 付款人的移动电话或移动电话网络的技术或者相关收款人的通信设备或移动电话网络的技术的请求涉及多个第五和第六或第三和第四信息，以便能够同时完成对用户 - 付款人和/或收款人的更新，这种情况下来自移动电话网络的响应包括第五、第六或第三和第四信息的多个更新过的信息。

第一存储装置中包括的标识各个相关用户 - 付款人的移动电话技术的第六信息涉及多个与优先级相关联的技术，这样做是为了表明，在任何时候检测到移动电话与多种技术相关联时选择出最高优先级的技术与相关用户 - 付款人的移动电话通信。

在这一节的开始我们还提到了存在支付和操作处理装置完成委托授权的可能性，这种情况下它必须已经完成了支付和操作处理装置中的委托验证。为了完成委托授权，支付和操作处理装置包括一个本地授权中心，以便授权被发送到所述本地授权中心而不是金融实体处理装置。

这个授权对进行小额支付（即支付额非常小）的情况尤其有用。为此，第一存储装置中包括的与各个相关用户 - 付款人的支付方式有关的第二标识信息必须与一个最大购物额度和本地授权中心的标识关联在一起，以便在接收到交易请求并确认相关联的用户 - 付款人时，钱夹处理装置生成包括与最大额度相关联的至少一个支付方式的存在

指示的确认。另外，收款人必须接受小额支付，为此第二存储装置中包括的标识各个相关收款人的第一信息与最大额度或者收款人的授权特征相关联，收款人的授权特征涉及：表示委托授权不被允许的在线授权，表示只有低于一定数额的交易的委托授权被允许的离线授权，或者表示交易额在指定额度之下或之上的一个或另一授权被允许的混合在线和离线授权，以便在确认相关收款人时销售商处理装置生成包括了所述收款人授权特征指示的确认消息。

因此，当交易额不超过所建立的最大额度并且销售商授权该交易时，在本地授权中心进行授权，或者相反地，如果交易额超过所述最大额度或者销售商不授权带有委托验证的交易，就在金融实体处理装置中进行授权。

因此，为了进行本地授权，当检测到相关用户 - 付款人的确认消息表示至少一个支付方式与一个最大额度相关联，并且收款人的确认消息表示所述收款人的授权特征是在线授权时，钱夹处理装置生成一个验证消息，该验证消息包括验证该收款人允许的支付方式与和最大额度相关联的用户 - 付款人的支付方式的匹配，以使用户 - 付款人可以选择一个与最大额度相关联的支付方式。

在对上述验证消息的响应消息中检测到与最大额度相关联的支付方式时，就在根据所选择的与最大额度相关联的支付方式的标识识别出的本地授权中心产生一个委托授权请求。

本地授权中心接收到该委托授权请求，并检验关于各个用户 - 付款人所关联的支付方式（与最大数额相关联）的第二标识信息在第一存储装置中的状态，以完成所述委托验证和授权并将交易结果发送给用户 - 付款人和收款人。

另外，本地授权中心还配备了从最大允许额度减去预定时间周期内进行的所有的交易的装置，以便购物不会超出由销售商建立并授权的最大额度，或者如果交易额超出所建立的最大额度或者销售商不授权具有委托授权的交易，就在金融实体处理装置中完成交易。所述授权中心访问支付和操作处理装置中包括的第七存储装置，以获得可用的净余额、周期内最近的交易，并在交易额超过所述净余额时生成拒绝消息。因此，该授权中心不允许支出超过所建立的预定周期（例如一天）内的最大额度。

本地授权中心包括一个与第七存储装置相连的批处理装置，以存储在预定时间周期内完成的各个交易，该批处理装置在预定周期结束时通过通信控制器将各个交易发送到对应的金融实体处理装置，所述金融实体处理装置分别为用户 - 付款人和收款人记入借方和记入贷方。

在移动电话技术中，如上所述，包括具有 WAP、STK、J2ME 和 BREW 应用程序的那些移动电话技术，分别标识在第一和第二存储装置中的第五、第六或第三、第四信息中。

移动电话技术包括包含了 WAP、STK、J2ME 和 BREW 应用程序的移动设备，这些应用程序执行分配给支付和操作处理装置的一些功能（例如，支付方式的匹配）以简化其运行，以便具有上述技术的移动电话包含用户 - 付款人所关联的支付方式的信息以接收验证请求，所述验证请求包括输入安全参数和相关收款人的支付方式的请求。因此，正是用户 - 付款人的移动电话建立由相关用户 - 付款人和收款人共享的公共支付方式。

为此，第一存储装置中的第六信息与具有所述技术以及本地存储的支付方式信息的移动电话的标识联系在一起，以生成验证请求。

另外还有一种可能性，即前面所述技术的移动电话允许对安全参数的验证，借此目的它们具有存储安全参数的激活密钥、随机参数和加密密钥的能力，所有这些信息都已预先生成并被有选择地存储在用户 - 付款人的金融实体处理装置中，以在金融实体处理装置中或本地授权中心中完成有选择的验证。为此，用户 - 付款人的移动电话必须具有用随机参数加密密钥的装置，以生成包含密钥和标准参数的加密序列，该加密系统被存储在钱夹处理装置的第一存储装置或相关用户 - 付款人的金融实体处理装置中，以通过所存储的加密序列与从移动电话接收到的加密序列一致的确认完成验证。因此，可以通过确认该加密序列与金融实体处理装置中的相对应或相同，而在用户 - 付款人所关联的钱夹处理装置中以委托的方式完成验证。

另外，具有所指出的技术的移动电话具有根据激活密钥生成输入安全参数的请求的装置，安全参数在输入之后被存储下来，以便在请求输入时响应验证请求消息将一个加密序列发送给支付和操作处理装置。这样利用只发送加密序列，安全参数就只为用户 - 付款人所知，

并且被存储在用户 - 付款人的移动电话中。

在由相关用户 - 付款人的金融实体处理装置通过相关收款人的金融实体处理装置完成验证时，通信控制器装置在发送验证时将已经加密的序列再次加密。

在具有 WAP 功能的移动电话的情况下，应该注意到为了建立上述各种功能电信控制器装置必须包括 WAP（无线应用协议）Push 控制器（它包括用于与支付和操作处理装置的运行相关联的 WAP 应用程序的存储装置，包括要以 WML（无线标记语言）发送的文本消息）以通过 WAP 网关和任意移动电话网络用 WAP 和 WML 消息与移动电话通信，假定 WAP 协议独立于载波和所用的移动电话网络。WAP Push 和 WAP 网关之间的协议已知是 PAP（Push Access Protocol），而 WAP 网关和移动电话之间所用协议已知为 POVAP（Push over the Air Protocol）。

当支付和操作处理装置需要发送消息到一个或多个移动电话时，它生成以 WML 所写的常规 Push 请求，用常规元素 p 表示应该显示在移动电话屏幕上的语句，并用常规元素输入以允许安全参数的引入。

标记语言 WML 脚本用来在特定的移动电话中确认输入的安全参数具有有效的格式并避免不正确的数据链的传输。

当移动电话生成交易请求时，所述交易请求包含分配给支付和操作处理装置的 WAP 地址，以便当移动电话发送该请求时它显示具有要完成的操作的选择菜单的 WML 页面，随后显示用于利用常规元素 p 和选项输入所选操作所需要的数据的 WML 页面，所请求的信息以 WML 显示。

该系统使用基于 SSL（安全套接字层）的 WAP 栈的标准安全协议 WTLS（无线传输层安全）建立对移动电话和 WAP Push 控制器的验证。WTLS 协议基于所需安全级别选择性地支持加密和 PKI（公共密钥结构）、WIM 和 WPKI。

关于具有 STK、J2ME 和 BREW 功能的移动电话，应该注意到这些移动电话存储了要完成的操作、输入涉及所执行操作的数据、以及将功能委托给特定移动电话的选择菜单。

本发明还提供了一种可能性，即交易请求包括操作代码、操作处理装置中支付网关的标识代码、安全参数、支付方式、以及以上的组合，其中支付和操作处理装置以所说明的方式完成对用户-付款人、销

售商和索引的确认，唯一的区别是必须发送给用户-付款人的消息数量有所下降。没有包括的代码和参数由支付和操作处理装置通过引导菜单请求。

还有一种可能性是可以使用其它具有无线通信功能的移动设备代替移动电话，例如 PDA 和手提计算机。

在支付和操作处理装置与金融实体处理装置之间的通信中，使用了三种协议，具体为：PRICE（集成连接建立过程（Procedures for the Integrated Connection of Establishments））、PUC（统一商业协议（Unified Commercial Protocol））和 PUM（统一移动协议（Unified Mobile Protocol）），这些协议都是基于 ISO（国际标准化组织）的推荐。

PRICE 和 PUM 被用在对来自信用卡和签帐卡的使用的计帐交易的处理中。

PRICE 协议使用过程以结合常规收款人的设备，这也是基于 ISO 8583。

PUM 协议已被指定来定义交换的消息和使用移动电话作为交易的激励器的支付方式的操作。这是特别的进步。

这三种协议使用了所谓的位图概念，在这个概念下每个数据元素都被分配了一个控制域或位图中的位置指示符。一个数据元素在特定消息中的存在由所分配位置中的“1”表示。而不存在则由“0”表示。

这三种协议所标识的每个消息包括下列序列：消息类型标识符、一个或两个位图以及按照由位图表示建立的顺序的一系列数据元素。

消息类型指示符是一个数字字段，其中表示了消息的版本号、消息类别、消息功能和交易发起者。

该消息的第二部分是一个或两个位图，其中每个位表示消息中与这个特定位相关联的数据元素存在或不存在。主位图总是存在并且表示最经常使用的数据元素。次位图表示不太经常使用的数据元素。

该消息的第三部分是数据元素。数据元素的存在由位图或消息类型表示。

PUM 协议在消息类型标识符之前包括对话控制报头，以控制并同步对话跟随接口两端的应用程序。

以协议“PRICE 和 PUC”定义的消息如下：

- 计帐请求/响应，用于授权、批准或确保计帐交易的资金。
- 计帐通信/响应，用于以本地模块传递对计帐交易的授权（销售和返回）。
- 取消通信/响应，用于通知计帐操作的取消。
- 建立通信/响应，用于建立计帐会话。
- 管理请求/响应，用于会话总体。
- 管理通知，用于通知接收到无法识别的消息。
- 验证请求/响应，用于请求在支付和操作处理装置中的验证，这在不与支付和操作处理装置直接相连的收款人的通信设备中进行。
- 管理通知，用于用户/付款人和收款人的操作的确认。
- 会话控制消息。

另外，PUM 协议包括下列消息：

- 用于对移动电话充值、请求余额和移动和改变安全参数的授权的请求/响应。如果充值是通过与移动电话网络管理员连接的管理员而不是直接连接到支付和操作处理装置的所述管理员完成。
- 取消通信/响应，用于取消充值的电话中的安全参数变化。
- 对用于验证帐户持有者和支付方式的管理响应的请求。
- 管理通知，用于确认用户 - 付款人和收款人的操作。
- 管理请求/响应，用于请求对索引的管理。
- 用于在线更新文件以管理对用户 - 付款人和支付方式的添加、修改和删除的请求/响应。
- 会话控制消息。

在支付和操作处理装置中完成的所有操作都在所述支付和操作处理装置中包括的发票和交易管理处理装置进行了注册，以便能够开具发票和获取帐户历史并让支付和操作处理装置能够访问不同的数据处理装置。

附图说明

图 1 示出了在一个国家内的支付和操作处理装置的功能框图，该支付和操作处理装置与相同国家范围内采用不同技术的多个移动电话网络以及所述国家内用户 - 付款人和收款人所关联的多个金融实体处理装置相连，以允许国际和本地交易和支付。

图 2 示出了允许在因特网上进行购物和交易的因特网操作处理装

置的可能实现示例的功能框图。

图 3 示出了索引处理装置的一种实现的功能框图。

图 4 示出了钱夹处理装置的一种实现的功能框图。

图 5 示出了一个解释用户 - 付款人在他或她自己的国家之外时进行的购物的示意图，并因此该购物是从与不同于所述用户 - 付款人的支付和操作处理装置的支付和操作处理装置相关联的销售商进行的，并且其中收款人的通信设备是蜂窝 POS (8)。

图 6 示出了与上述相似的示例，区别在于收款人的通信设备是常规销售终端 (9)。

图 7 示出了国际寻址处理装置的可能配置的功能框图。

图 8 示出了一个功能框图，该框图突出显示了支付和操作处理装置中包括的用来支持通过 GSM 移动电话网络通信的电信控制器装置。

图 9 示出了一个功能框图，该框图突出显示了支付和操作处理装置中包括的用来支持通知 CDMA/TDMA 移动电话网络通信的电信控制器装置。

图 10 示出了一个功能框图，其中从支付和操作处理装置到相关用户 - 付款人的移动电话或到相关收款人的通信设备的通信是用语音消息进行的。它还示出了支付和操作处理装置所包括的用来完成这个功能的电信控制器装置。

图 11 示出了一个功能框图，其中移动电话被用作 WAP 终端，通常由支付和操作处理装置完成的功能可以被委托到该 WAP 终端以简化交易。

图 12 示出了与前一个相同的功能框图，但在这个例子中移动电话具有 STK 功能。

图 13 示出了与图 9 和 10 中相同的功能框图，但区别是在这个例子中移动电话具有 J2ME 功能。

图 14 示出的功能框图与 9 到 11 中的相同，但区别是在这个例子中移动电话具有 BREW 功能。

图 15 示出了销售商处理装置的一种实现的功能框图。

具体实施方式

下面我们将通过上述附图说明本发明。

本发明包括多个通过寻址处理装置 (2) 互连的支付和操作处理装

置(1),例如,以便各个支付和操作处理装置(1)被安排在不同国家并且允许通过国际寻址处理装置(2)在它们自己之间进行通信,对此将会有进一步说明。

各个国家的不同用户-付款人(5)和收款人(6)与他们自己国家内的支付和操作处理装置(1)相关联。

各个支付和操作处理装置(1)与属于该支付和操作处理装置所属的相同国家的多个移动电话网络(3)和多个金融实体处理装置(4)相连。

用户-付款人(5)是至少一个移动电话网络(3)的客户并且拥有移动电话(7),收款人(6)可以是移动电话网络(3)的客户或不是,取决于所拥有的通信设备,对此将会有进一步说明。

另外,用户-付款人和收款人是至少一个金融机构的客户,他们与自己所属的金融机构已经签署了与所述金融机构中的银行帐户相关联的至少一种支付方式,所述金融机构与金融实体处理装置(4)相关联。

金融机构和金融实体处理装置(4)以包括网络在内的常规方式相连,它们在网络上通过常规方式交换各种数据。为了简化图1我们只包括了金融实体处理装置(4),此外贯穿本文档的操作都被表示为由金融实体处理装置完成。实际上所述操作可以由所述处理装置或金融机构自己完成,这对本发明没有任何影响。因而,例如当本文档声称在金融实体处理装置内或由金融实体处理装置完成验证时,实际上该操作可以由金融实体处理装置或金融机构完成,这对本发明的运行和操作没有任何影响。

仅仅出于信息目的,应该注意到存在如下的金融机构,所述金融机构发布并操作支付方式或提供其它类型的商品或服务给支付方式的帐户持有者,因此允许用户-付款人接收服务、所购买的商品,并进行和接收支付,或通过由所述金融机构发布的支付方式或在其中的指令下被验证。所述金融机构发行者与用户-付款人(5)的金融实体处理装置(4)相关联,根据前面所述我们已经到处应用的委托涉及金融实体处理装置或金融机构。

我们还应该注意到收款人是其客户的金融机构是购方金融机构,并且允许获取收款人的从用一定支付方式与用户-付款人进行的交易所获得的信贷权利,并且允许收款人通过支付方式提供服务、销售商

品、付款或收款并验证用户-付款人。如同所示那样，购方金融机构与收款人的金融实体处理装置相关联，这也是我们已经在整个文档中出于简化目的而使用的委托，假定金融实体处理装置（4）和金融机构之间的通信是按照常规方式进行并且不代表本发明的目标。

沿着这些线，我们应该澄清每次我们提到支付时，它原本就与结算概念紧密相连，并且是在它们自身间在客户帐户中完成储蓄的金融调整的过程，作为其中产生的信贷的结果，因此不在本发明的系统的范围内，本发明的系统只充当结算支付的激活者但不处理支付或结算。

还有一种可能性是处理装置独立于金融机构，支付和操作处理装置与金融机构通信并且其中付款人是不同于支付方式的卡的帐户持有者，但通信将到那里结束。

这种结构能够在相同或不同国家的用户-付款人和收款人之间完成交易和支付，相同国家内的付款人和收款人之间的交易通过该国家的支付和操作处理装置完成，不同国家的用户-付款人和收款人之间的交易通过他们自己的国家内对应的支付和操作处理装置完成，并且他们之间以将要进一步说明的方式通过国际寻址处理装置（2）互连。

另一种可能性是一个国家的支付和操作处理装置（1）与其它国家的金融实体处理装置（4）相连，并且通过漫游网关与其它国家的移动电话网络相连，由此让它能够充当区域处理装置。这样，支付和操作处理装置（1）可以在一个或多个国家中起作用。

首先，对用户-付款人（5）能够和在单个国家内的收款人（6）进行的不同购物和交易形式进行了说明。因此只涉及了一个支付和操作处理装置（1）。

因此，用户-付款人（5）可以进行现场购物，也就是说在这些购物中他或她前往收款人（6）的公司购买商品或服务。在这种情况下用户是付款人（5）。

收款人（6）可以是移动电话网络的客户或不是，但任何情况下收款人（6）都必须有通信设备，根据一种实现其通信设备由常规POS（销售终端）（9）构成，也就是说与支付和操作处理装置（1）没有直接连接并由第三方（例如金融实体处理装置（4））管理的销售点，在收款人（6）不是移动电话网络的客户的情况下销售点与所述第三方通过

陆上电缆通信，或者通过无线连接通信；或者，在另一实现中，该通信设备由包括移动电话的 POS (8) 构成，下文中称为蜂窝 POS (8)，在这种情况下所述收款人 (6) 应该是移动电话网络 (3) 的客户，它通过该网络与处理装置 (1) 直接通信。收款人 (6) 还可以用移动电话作为 POS (22) (作为 POS 的移动电话)，在这种情况下收款人 (6) 也必须是移动电话网络的客户。

每个付款人 (5) 都被分配了一个由秘密标识密钥构成的安全参数，该密钥通过移动电话号码、或移动站点集成服务数字网络号码 (MSISDN)、或分配到那里的特定号码 (例如系统的 PAN (私人帐户号码) 或 EAN (条码格式的 PAN)) 与付款人的标识相关联，而付款人的标识与由用户 - 付款人和金融机构分别签署的支付方式相关联。

接下来我们说明现场购物，它是对将要说明的后续支付和交易形式的说明的基础。

就现场购物来说，其中收款人配备有蜂窝 POS (8)，付款人 (5) 适当地通知收款人 (6) 他或她的电话号码、PAN 或 EAN，收款人用这些信息生成包括付款人标识、收款人标识、购物数据 (例如产品标识和价格) 的交易请求，为此相关收款人将所述信息输入蜂窝 POS (8) 并通过输入支付和操作处理装置 (1) 的网络号跨越移动电话网络 (3) 将该交易请求发送到支付和操作处理装置 (1)。通过使用常规主叫 ID，收款人的标识在利用移动电话网络进行的通信中是隐含的。

交易请求通过电信控制器装置 (10) 进入支付和操作处理装置 (1)，对电信控制器装置 (10) 将有进一步说明，它将请求传送到操作处理装置 (11)，操作处理装置 (11) 配备有识别操作类型以及始发通信设备类型的装置 (11a) 并启动与操作和 POS 相对应的子过程，也就是说，在这种情况下识别出它是发自蜂窝 POS (8) 的购物操作。操作处理装置 (11) 随后生成对相关收款人的标识的验证请求，下文中称为收款人确认请求，它将该请求发送到销售商处理装置 (14)，销售商处理装置 (14) 向第二存储装置 (15) 访问与该系统中的各个相关收款人相关的至少第一标识信息以及各个相关收款人的各个通信设备的有关标识代码。另外第二存储装置包括关于各个收款人的支付方式的第二标识信息，该信息与各个收款人的第一标识信息相关联，并且与各个所述收款人相关联的对应金融实体处理装置的标识相关

联。因此，在识别出收款人时，销售商处理装置生成一个收款人确认请求，并将它和被确认的收款人的支付方式一起通过操作处理装置（11）发送到钱夹处理装置（12）。

操作处理装置生成确认相关付款人的请求，它将该请求发送到钱夹处理装置（12），钱夹处理装置（12）接着向第一存储装置（13）访问该系统中各个相关付款人的第一标识信息，第一标识信息与各个付款人的移动电话号码（7）、或 PAN 或 EAN 有关，以便根据付款人标识检验该数据并生成付款人确认消息。另外，第一存储装置（13）包括与各个用户（5）签署的支付方式有关的第二标识信息，该第二标识信息与第一标识信息和各个用户的支付方式所关联的金融实体处理装置的标识有关。

钱夹处理装置（12）检测到付款人和收款人的确认消息，并通过第一检测装置（12a₁）获得它们的公共支付方式以生成交易验证请求消息，并利用先前对付款人所属网络的技术以及所述付款人使用的移动电话的技术进行的检测（后面将有进一步说明）通过电信控制器（10）和付款人（5）所属的移动网络（3）将它发送到付款人（5）的移动电话（7）。钱夹处理装置和付款人（5）的移动电话（7）之间的通信总是通过电信控制器（10）执行。

交易验证请求消息包括交易中涉及的付款人和收款人的公共支付方式、输入安全参数的请求、以及选择付款人和收款人的至少一种公共支付方式的请求、以及收款人的标识，还可以在其中包括商品和价格的标识。

付款人通过移动电话（7）接收到验证请求消息，输入所请求的数据，并发送包含所选支付方式中的安全参数的响应消息，以根据下面说明的三种可能的情况完成验证。

为此，钱夹处理装置（12）包括第二检测装置（12a₂），第二检测装置获得响应消息并访问第一存储装置（13），第一存储装置还包含标识要执行的验证的类型的第三信息，该第三信息与关于支付方式的第二标识信息相关联，并且表示直接在付款人的金融实体处理装置（4）中进行的验证、在付款人的金融实体处理装置（4）中通过收款人的金融实体处理装置（4）进行的验证或是钱夹处理装置（12）中的委托验证。

应该注意到在所述验证之后进行对交易的授权。为此，付款人（请求者）的金融机构检验支付方式是否能够支付交易额以对其进行授权。这是由常规装置完成的，并且已被放在本说明书之外，因为它不是本发明的目标。但是，所述授权还可以被委托给支付和操作中心，下面将会就小额支付对其做进一步说明。因此，每次进行验证时，还要执行相应的授权，尽管在本文档中除了对所述小额支付的那些例子之外没有明确指出。

如同所示，不同金融实体处理装置由常规装置互连以在它们之间交换信息。可能会出现收款人的金融实体处理装置（4）和付款人的金融实体处理装置（4）是同一个，这种情况下就不必在金融实体处理装置（4）之间交换信息，但也会出现付款人的金融实体处理装置（4）和收款人不同的情况，这种情况下信息交换就是必须的。

假如检测到必须在付款人的金融实体处理装置中直接进行验证，钱夹处理装置（12）将对验证消息的响应消息连同付款人所选支付方式所关联的金融实体处理装置的标识一起传送到操作处理装置（11），并将验证响应消息发送到通信控制器装置（21），通信控制器装置（21）识别出相应的金融实体处理装置（4），并将验证响应消息发送到识别出的付款人的金融实体处理装置，以便在发送安全参数之前对安全参数进行加密。付款人的金融机构检验所选择的支付方式是否与付款人对应，以便在金融实体处理装置（4）完成了验证之后，将对安全参数的确认结果通过通信控制器返回到操作处理装置，并且和收款人的金融实体处理装置（4）（通过传统的金融网络执行交易）中的验证结果一起处理交易。收款人的金融实体处理装置（4）随后将交易结果发送到通信处理装置（21），通信处理装置将其转发给操作处理装置（11），从那里交易结果又被借助于电信控制器（10）通过移动电话网络（3）发送到收款人（6），同样交易结果还被从那里发送到钱夹处理装置（12），从钱夹处理装置（12）交易结果又被借助于电信控制器（10）通过付款人（5）的移动电话网络（3）发送到付款人（5）的移动电话（7）。

假如检测到必须通过相关收款人的金融实体处理装置在相关联付款人（请求者）的金融实体处理装置中直接进行验证，验证和交易信息以及收款人的金融实体处理装置的标识一起被发送到通信控制器

(21)，通信控制器(21)将安全参数和所选支付方式的标识一起加密以随后传送给收款人(让受人)的金融实体处理装置，收款人的金融实体处理装置使用来自发送它的付款人(请求者)的金融实体处理装置的验证响应中的数据，付款人的金融实体处理装置向它发送了加密的交易数据以及用于交易的验证和授权的安全参数，而清算和结算通过相应的金融机构间定义的方式在请求者和受让人之间处理，将结果发送到付款人的金融实体处理装置，并从那里通过支付和操作处理装置(1)以已经说明的方式发送到付款人和收款人。

假如支付和操作处理装置(1)检测到委托验证，就如前所述在钱夹处理装置中完成验证。随后，操作处理装置与收款人的POS以及移动电话(7)通信以发送对交易结果的通知。

操作处理装置与发票和管理处理装置通信以存储交易结果，发票和管理处理装置是存储交易历史的地方，交易结果至少包含下列信息：操作标识，例如操作号和/或授权号，操作类型，用户-付款人的标识，数额，货币以及相关收款人的标识。

假如操作是退回而非购物，收款人就在POS中输入用户-收款人的标识，以及与要退回的商品对应的数额和货币。

该系统完成的所有交易都由与发票和交易管理处理装置(45)通信的操作处理装置注册在了交易历史中，发票和交易管理处理装置(45)存储了由相关用户和收款人完成的每个交易的记录，而不管其类型，即购物、退回、查询或参数更改。

对这些历史的访问可以用于对商业操作的查询，例如在退回的情况下，尤其是输入到发票和交易管理处理装置中的历史。

还有一种可能性是在现场购物中，收款人(6)配备了由金融实体处理装置管理的常规POS(9)。在这种情况下，收款人(6)向常规POS中输入了相关联付款人的标识，以及涉及交易的数据，例如操作类型、产品和价格，并将这个数据发送到收款人(6)所属的所述金融实体处理装置(4)。

接下来，该金融实体处理装置访问它的数据库，确认该收款人并生成一个确认消息，它将该消息和付款人的标识以及收款人的支付方式一起通过控制器(21)发送到操作处理装置(11)。

随后以已经说明过的方式检验付款人并生成验证请求消息，重复

为蜂窝 POS (8) 所说明的过程, 区别在于一旦交易完成向收款人 (6) 发送交易结果的操作通过直接从金融实体处理装置(4)发送到常规 POS (9) 来执行。

包含交易结果的消息还表示各种交易数据, 例如操作类型、收款人标识、产品和数额等。

本发明系统还允许付款人 (5) 使用他或她的移动电话 (7) 启动交易或购物操作, 在本发明的一个实现例子中这是基于对索引的使用, 对索引的使用由下列字段组成: 格式, 生成索引的索引处理装置, 由生成索引的索引处理装置表示的字段长度, 索引, 可能还有一个控制位, 它是根据通常用于超过四位的索引的、被称作 LUHN 的公式计算出的。

为了能让支付和操作处理装置 (1) 以这种形式运行, 本发明允许索引处理装置 (16) 与第三存储装置 (17) 相连, 第三存储装置 (17) 至少存储了标识多个各种类型的索引的第一信息, 如在题为“发明内容”一节中所描述的那样, 至少各索引与收款人标识有关, 或者还可能根据索引类型 (POS) 至少与产品或服务的价格标识或收款人的通信设备的标识有关, 以便完成交易, 付款人在他或她的移动电话 (7) 中用索引号键入购物操作的标识, 并通过他或她所属的移动电话网络 (3) 将它发送到支付和操作处理装置 (1), 在那里购物操作标识在电信控制器 (10) 中被接收到, 电信控制器 (10) 将购物操作标识传送到操作处理装置 (11), 在操作处理装置 (11) 中第一识别装置 (11a) 由索引编号检测出它是购物操作并继续以已经说明的方式执行对付款人的检验, 如通常所发生的那样根据与移动电话网络的通信进行所述检验。接下来, 它生成对索引的检验请求, 并将它发送到索引处理装置 (16), 索引处理装置 (16) 根据中心建立的标准检查索引的格式 (结构、控制位、长度, 等等) 的正确性以使操作不被拒绝。它随后提取出索引处理装置代码以检验该索引属于这个索引处理装置或别的索引处理装置。如果该索引属于另一可识别的索引处理装置, 就用某种方式 (将有进一步说明) 将该索引发送到该索引处理装置。随后就根据第三存储装置 (17) 中的第一信息的清单检查该索引以查看它是否有效, 同样将进一步说明一个概念, 如果没有找到该索引或者它已经过期, 就拒绝该操作; 如果有效, 就将与它相关联的数据 (例如数

额、货币、收款人标识、收款人设备（POS）的标识和操作系统等）返回以生成包括所述数据的索引确认消息，并将该消息发送到操作处理装置（11），操作处理装置（11）根据索引数据中包括的收款人标识生成收款人确认请求消息，或者生成 POS 标识确认消息。假如索引的确认包括 POS 标识以允许与之进行通信，POS 标识的确认被发送到销售商处理装置，销售商处理装置在确认了收款人之后确认相应的 POS，确认消息返回 POS 的操作系统以允许操作处理装置打开与所述 POS 的会话并在需要时获得剩余的操作数据。

当钱夹处理装置（12）检测到三个所述确认时，它生成上述验证消息。

这时，以上述方式重复该过程直到完成了发送交易结果到付款人或收款人的操作。

在本发明的一种按索引支付形式中，索引涉及到用于充值预付费移动电话卡的 POS，在这种情况下收款人是发行充值卡的移动电话网络运营商（3），并且通过输入要充值的电话号码而标识收款人，如下所述。

在这种情况下付款人（5）输入表示充值操作的索引，并且可以选择输入要充值的电话号码。这个请求由操作处理装置（11）接收到，操作处理装置（11）的第一识别装置（11a）检测出该操作是索引购物并以已经说明的方式执行对付款人、索引和相关收款人的确认。接下来，操作处理装置（11）可以选择生成检验请求消息，以检查检测到的移动电话号码是否允许充值，将所述消息通过控制器（10）发送到移动电话网络运营商（3）。运营商检验接收到的电话号码是否与预付费模式相关联，并生成一个消息，它将该消息发送到操作处理装置（11）以按照前面的例子中已经说明的方式进行一致性验证。

还有一种可能性是在充值操作中，验证消息在包括上述请求这外还包括输入要充值的移动电话号码的请求，在这种情况下这个号码是在对验证请求的响应消息中而不是在交易请求中接收到的，并且此时操作处理装置生成检验要充值的电话号码是否属于预付费模式的消息，并在接收到所述响应消息并且已经向运营商检验了所述电话号码允许预付费时，以已经说明过的方式完成验证和交易。向运营商检验电话号码是否属于预付费模式是可选的。

在任何一种充值情况中，在接收到交易结果时，生成充值序号并将它发送到移动电话网络的运营商/承载者，并在接收到充值结果后通过钱夹处理装置（12）将它发送到已经请求充值的付款人（5）的移动电话（7）。

同样，本发明允许购买可以下载到相关付款人的移动电话的运营商标志符、铃声、游戏和应用程序。在这种情况下其运行与为按索引支付的第一个例子所说明的相同，区别在于收款人是移动电话运营商，这样在接收到交易结果时运营商生成或允许内容下载到付款人（5）的移动电话（7）。

按索引支付的另一形式与蜂窝 POS 相关联，蜂窝 POS 包括具有无线电话连接的售货机（8a），无线电话连接能够与支付和操作处理装置（1）通信。在这种情况下，当操作处理装置（11）检测到它是按索引的购物时，操作处理装置（11）执行对付款人、索引、收款人以及销售点终端的确认。在确认了这些并且检测出是具有无线电话连接的自动售货机后，操作处理装置（11）生成一个消息并跨越相应的移动电话网络（3）将它发送到该自动售货机以启动购物，该消息至少包括消息类型（欢迎、产品选择等），还可能包括付款人标识，自动售货机（8a）能够检测到这个启动消息以将消息类型，可能还有付款人标识以及选择想要产品的请求显示在它的屏幕上。付款人标识可以包括昵称或他或她的移动电话号码的后六位，以便通知所述付款人该消息涉及的是他或她。在付款人进行了想要的选择之后，自动售货机将产品选择结果生成一个消息并将它发送到操作处理装置（11），该消息至少包括消息的类型、指示是否选择了产品的响应代码、数额、货币，可能还有产品代码，该消息由钱夹处理装置（12）的第一检测装置（12a）检测到以生成验证请求消息。

在这种情况下操作处理装置除了生成收款人确认消息外还生成一个消息以确认蜂窝 POS（8），如前所述，这是由操作处理装置执行的，以便允许操作处理装置按照所说明的过程建立与自动售货机（8a）的通信。通常，每当支付和操作处理装置与收款人的 POS 建立通信时这个操作都是必须的。

接下来，以先前说明的方式完成验证和交易，但区别在于当自动售货机接收到有效的交易结果时，它放出所选择的产品，或生成一个

错误消息表示该交易已经被断定为无效交易。

本发明允许的另一种按索引支付的形式需要索引与蜂窝 POS (8b) 相关联, 蜂窝 POS (8b) 允许对以后收取的货物(定单购物)的预付费购物或者对以后才交付的货物预先付费, 例如对在一段时间以后才获得或交付的外卖食品的定购。

在这种情况下, 当操作处理装置通过识别装置检测到该操作是按索引购物时, 它以已经说明过的方式完成对相关付款人、索引、收款人和 POS 的确认, 但区别在于这种情况下 POS 包括与移动设备相连的接收打印机(8b), 这样第三存储装置(17)包括与定位符索引有关的第三信息, 以便在索引处理装置(16)中确认了索引之后, 它访问第三信息以获得定位符索引, 定位符索引可能是随机的。定位符索引与产品、价格以及接收打印机(8b)相关联, 并当操作处理装置(11) (在完成了验证和交易后)接收到有效的交易结果时, 它为晚些时候收取或交付的产品生成预付费购物消息, 该消息至少包括交易结果、产品标识、价格和定位符索引, 将该消息发送到相关付款人的移动电话, 并发送到接收打印机进行打印。这样, 当付款人到达销售商处收取所购产品时, 在确定定位符收条后, 收款人向付款人交付所购产品并完成交易, 该收条标识了所购产品、付款人标识以及该交易已经被正确执行。采用这种方式, 所有定购的产品都已经预先付费, 避免了没有付费的定单的收条。

相同操作对于购买剧院或音乐会门票、旅游票以及通常需要预付费的任何产品也有效, 但在这种情况下 POS 是虚拟的, 对此将会有进一步的说明。

还有一种可能性是在因特网上实现与接收打印机的通信, 对此将有进一步的说明。另一种索引形式适用于因特网上的购物。因此, 支付和操作处理装置(1)还配备了因特网处理装置(20) (图1和图2)并通过不同于移动电话网络的因特网网络(24)连接到相关收款人的通信设备(40)。

本发明的一种实施例还允许收款人的设备是虚拟 POS (40), 由付款人通过通信设备(25) (例如个人计算机)访问它以实现对该虚拟 POS (40) 选择的产品或服务的购买, 通信设备(25)显示了与想要的产品和所述虚拟 POS (40) 有关的索引。接下来, 付款人(5)

输入购物的索引代码和他或她的移动电话(7)的标识,将包含所述数据的交易请求发送到支付和操作处理装置(1)。操作处理装置(11)通过识别装置(11a)检测它是否是涉及虚拟POS的索引交易,并执行早先说明过的过程,即对付款人、POS、索引和相关收款人的确认,对交易的验证、实现,并最后将交易结果通过相关付款人的移动电话(7)传送给相关付款人并传送给收款人(6)。但在这种情况下(使用虚拟POS的情况下),第二存储装置(15)包括标识与相关收款人的第二标识数据有关的因特网地址或email地址,以便操作处理装置(11)接收到由识别装置(11a)识别出的交易结果时,将所述交易的结果发送到因特网处理装置(20),因特网处理装置(20)通过接口(36)接收它并将它传送到查询模块(26),查询模块(26)访问销售商处理装置(14)以获得标识与收款人相关联的因特网地址或email地址的第五信息。如果查询模块检测到一个因特网地址,它就通过加密管理器(29)将交易结果加密,并通过email管理器(27)以及使用SMTP(简单邮件传输协议)的Web控制器(28)将加密后的消息发送到收款人(6)的虚拟POS(40),以便email管理器(27)生成正确的email格式并通过构成与网络(24)的接口的控制器(28)离线发送通知。

假设查询模块(26)检测到虚拟POS(40)与集成因特网操作相关联,就通过HTTP/HTTPS(超文本传输协议/超文本传输协议安全)Web控制器(34)在线发送交易结果消息,使用常规安全机制从Web控制器(34)将交易结果发送到虚拟POS(40)。

在本发明的另一种支付形式中,存在一种可能性是付款人(5)在虚拟POS(40)中选择产品或服务,该虚拟POS(40)与具有由支付和操作处理装置(1)生成的索引的集成因特网操作相关联。在这种情况下虚拟POS(40)在线生成索引生成请求,该请求和收款人标识以及验证收款人的密码一起在因特网上被发送到因特网处理装置(20)。因特网处理装置(20)通过控制器(34)接收到该请求,并将它传送给查询模块(26),查询模块(26)访问访问控制模块(30),其中使用收款人的密码和标识在因特网上以常规方式进行销售商验证。一旦收款人通过验证并且已经检验其被授权请求生成索引,查询模块(26)就接收到验证并将索引生成请求发送到索引处理装置(16),索引是通过第三存储装置(17)获得的,在第三存储装置(17)中索引和产

品和服务数据、价格、货币以及相关收款人的标识存储在一起，并且索引处理装置（16）将索引通过返回路径发送到虚拟 POS（40），以便在付款人（5）的个人计算机中获得索引，付款人（5）的个人计算机借助于他或她的移动电话（7）生成包含该索引的交易请求，重复前面的例子中已经说明的过程，但区别在于在这个例子中在生成验证请求消息之前销售商处理装置（14）可以生成对相关收款人确实拥有所识别出的商品的可用库存的确认请求，该请求通过操作处理装置（11）被发送到查询模块（26），查询模块（26）用已经说明过的方式从相关收款人获得数据，并通过 Web 控制器（34）将库存确认请求发送到所述相关收款人的通信设备（4），以便虚拟 POS（40）检验与接收到的索引相关联的产品的库存级别，并通过返回路径将结果返回给操作处理装置（11），以便如果该收款人库存中有该产品交易以已经说明过的形式继续；否则就拒绝该交易，并通过付款人的移动电话（7）通知他或她。

当查询模块（26）接收到索引生成请求时它生成一个会话代码，将该代码发送到虚拟 POS（40）并将它与正在进行的交易关联起来。所述会话代码被添加到各种信息中，例如生成的索引或者库存确认请求，以让 POS 确认接收到的会话代码与交易开始时接收到的会话代码是否一致。

前面在因特网上进行支付的任意一种情况都可以和预付费形式结合起来，从而以与预付费购物或定单接受模块相同的方式将索引生成请求、定位符生成请求一起发送出去，以便购买剧院或音乐会门票、旅游门票和任何其它类型的门票以及租费等，以便一旦获得了交易结果，就以已经说明过的方式将它们和定位符一起发送到虚拟 POS（40）以及付款人（5）的移动电话（7），付款人随后可以早先说明的方式收取或接收产品。

在本发明的一种实现中，收款人是软件提供商。在这种情况下，一旦付款人选择了想要的文件，虚拟 POS（40）生成索引生成请求连同定位符生成请求，以便一旦以已经说明的方式完成了交易，在虚拟终端中接收到交易通知时，虚拟 POS（40）将该文件连同定位符一起加密并授权下载到付款人，付款人用所述定位符解密移动电话上接收到的文件。

另外，因特网处理装置（20）包括与 Web 控制器（34）相连的电子商务处理装置（32）以允许从相关收款人的通信设备通过因特网访问因特网处理装置，并执行对与其相关联的索引数据的查询或修改，例如对索引编号的添加、删除、查询或修改。为此，该处理装置（32）提供了一个图形用户界面，能够让销售商用户通过安全的连接并使用他们的默认 Web 浏览器访问并管理他们的数据。

当收款人想要执行查询或修改操作时，他或她生成一个详细说明要执行的操作的消息，该消息被处理装置（32）通过 Web 控制器（34）接收到并被传递到访问控制模块（30），访问控制模块（30）以已经描述过的基于收款人标识和其密码的形式执行对相关收款人的验证，并且通过应用程序服务器模块（31）将请求发送到操作处理装置，操作处理装置通过识别装置（11a）检测到操作类型并将数据传递到销售商处理装置（14）、索引处理装置（16）或同时传递到这两者，以完成所请求的操作，并分别访问第二和第三存储装置（15 和 17），以便在完成了所请求的操作之后，将结果通过返回路径发送到虚拟 POS。应用程序服务器（31）在因特网和处理装置 14 和/或 16 之间建立起关系。

还有一种可能性是允许通过系统管理员的通信设备（37）进行这些类型的操作、查询或修改，系统管理员在专用网络（38）上访问，为此目的因特网处理装置（20）包括了 HTTP/HTTPS 专用网络控制器（35），它与销售商数据网管理模块（33）相连，该模块（33）存储了提供给相关收款人的不同服务并且构成了对操作员来说与已经说明过的由处理装置（32）所提供图形用户界面相同的图形用户界面，这样，它同样地通过访问控制模块（30）接收验证管理员的请求，并以为相关收款人说明过的形式重复该过程以修改、查询或为对相关收款人允许的查询和/或修改创建新的访问可能性。在这种情况下，应用程序服务器（31）在处理装置 14 和/或 16 中建立专用网络之间的联系。

另一个例子，对请求生成索引的相关收款人的确认是通过检验是否授权所述收款人进行这种请求而完成的。在按索引购物的功能中，本发明允许涉及帐户、税收或其它费用的发票支付。在这种情况下，收款人的设备是发票开具器（41），它以已经说明的形式生成索引生成请求并在因特网（24）上将该请求发送到因特网处理装置（24），以便第三存储装置（17）存储生成的索引连同发票的数据，并将它发

送到该开具器(41)。当付款人想要支付发票时,他或她输入适当发票的相关索引并生成交易请求,以已经说明过的形式重复该过程,但区别是在这个例子中交易请求还被通过因特网处理装置(20)以已经为前面的例子说明的方式发送到发票开具器(41)。

明显地,可以为目录购物或电话销售的支付采用本发明的系统,在这两种购物形式中产品与预先存储在第三存储装置(17)中的索引编号关联在一起,而第三存储装置(17)与相应的收款人相关联。

在这种情况下,以为按索引购物所说明的第一种情况相同的方式进行交易。

另外,本发明还允许付费电视节目的购买,其中收款人的通信设备是付费电视(42)的解码器,并且其中索引与电视节目相关联,采用遵循按索引购物的第一种情况的相同形式的过程,但区别在于当该通信设备(42)接收到交易结果时,它生成激活该付款人的解码器的信号并由此允许观看该节目。

另一种按索引支付的形式是对用于产品交付的交货票据的支付。在这种情况下收款人的设备是快递公司(43),并且对于先前的情况,收款人的设备生成并发送索引生成请求,该请求至少包含涉及交付产品和价格的信息,以将所述信息和生成的索引连同交货票据数据一起存储在第三存储装置(17)中。

在这种情况下,相关联付款人以已经说明过的形式发送交易请求,交易请求包含与交货票据相关联的索引、支付方式(提前支付或货到付款)、对付款人的确认、索引以及正在确认的收款人。但是,在这种情况下,区别是操作处理装置的识别装置(11a)检测到相关联索引指示符是交货票据并且形式是支付交货票据。这个检测由操作处理装置中的所述装置完成。如果付款人所选形式是预付费,该过程以按索引支付的第一个例子中说明的方式继续。但是,如果付款人选择货到付款,这是由操作处理装置的识别装置检测到的,操作处理装置的识别装置就生成索引处理装置(16)中的与货到付款相关联的索引生成请求。在生成和存储索引连同货到付款的相关联数据之后,索引被发送到相关收款人的通信设备(43)。

当商品被交付给付款人并得到确认时,通过使用与货到付款相关联的索引启动按索引支付过程,该交易以在按索引支付的第一例子中

描述的方式进行。

本发明的系统还允许完成验证服务所需的交易，例如在电子文档的数字签名情况下所需的交易。

这需要一个预先步骤，包括获得数字签名证书的注册，由此用户-付款人用他或她的移动电话输入操作代码，操作代码被发送到支付和操作处理装置，支付和操作处理装置检测出它是数字签名证书的注册操作，并向销售商处理装置查询由支付和操作处理装置(1)认可的并被存储在第二存储装置中的授权证明授权中心(CA)的列表，并发送这个数据以使用户能够选择证明授权中心之一。随后为用户-付款人生成公共密钥和私有密钥，并向用户发送一个消息请求他或她为数字签名选择权限参数。一旦接收到权限参数，就为用户选择的签名的安全参数计算(归纳算法)出散列，并且产生密码和私有密钥。这个数据被加密并存储在第一存储装置(13)中。接下来，操作处理装置(11)请求索引处理装置生成定位符，定位符会被传递给用户。

接下来，支付和操作处理装置(1)将用户的公共密钥连同标识数据和定位符一起发送到用户选择的证明授权中心。在由证明授权中心制定的过程之后，用户通过定位符标识他或她自己，并且证明授权中心随后为用户生成一个证书并将它发送到操作处理装置(1)，已经用用户的公共密钥对该证书进行了加密。该证书被存储在第一存储装置中，假定能够提取公共密钥，这个数据不需要单独维护。

在这种情况下，相关收款人的通信设备由电子签名POS(80)构成，付款人亲自或以已经说明过的方式用个人计算机(25)访问电子签名POS(80)，允许用户察看用户想要的文档和数据以及要签名的文档的散列，并选择通过支付和操作处理装置(1)完成数字签名。从这时起，数字签名POS(80)生成索引生成请求，该请求连同要签署的文档一起被发送到因特网处理装置(20)，因特网处理装置(20)通过因特网控制器(34)接收到该请求，并重复已经为索引接收请求的接收说明的过程，但区别是在这种情况下在生成索引时索引连同接收到的文档一起被存储到第三存储装置(17)中。接下来，索引被发送到数字签名POS(80)以通知所述索引的用户-付款人，该用户-付款人随后启动包括所生成的索引的交易请求。

当操作处理装置(11)接收到所述索引并检测出它是数字签名时，

就以已经说明的方式进行对付款人、索引和收款人的确认并随后生成验证请求消息，该消息包含输入安全参数和要签署的文档的散列的请求以及用户选择的敏感数据（如果有的话）。

这样，用户能够通过散列确认他或她将要签署的文档是展示给销售商的文档，避免文档的任何替换。

当签名安全参数到达支付和操作处理装置时，它被用来计算解密用户的私有密钥所需的散列。在计算出文档的散列并加密了用户的私有密钥（它构成了用户的文档的签名）之后，支付和操作处理装置（1）将伴有上述用户证书的签署的文档传递给签名 POS（80），用户证书确保了由证明授权中心识别出的用户签名有效。在签名过程成功完成时通知用户，另外，可以将定位符传递给用户，以允许所述用户更方便地通过支付和操作处理装置（1）的 Web 界面查询所签署的文档。本发明将所签署的文档存储在充当存储库的发票和交易管理器处理装置（45）中。

另外，本发明的系统允许对金融和其它卡的 PAN 编号的验证能够检查持卡人的真实身份，不管它是否是涉及购物或任何其它类型的操作，例如存在或许可控制、或者验证医疗保险卡的用户等，以避免其否认操作。例如，我们说明了在因特网上进行支付中对卡的验证（Visa 3 域验证模型），由此付款人在通过虚拟 POS（40）进行购物之后，输入对应支付方式的卡号。在响应中虚拟 POS 在所述支付方式的目录中查询该支付方式的发行实体，并获得涉及支付和操作处理装置（1）的 URL（统一资源定位符），以便通过该 URL 以已经说明过的方式通过因特网处理装置（20）与支付和操作处理装置通信，在该通信中发送了对卡号（支付方式，与持卡人的 PAN 相关联）的检验请求，从而该数据以上面已经说明过的方式通过因特网处理装置（20）到达操作处理装置（11），并完成对收款人和付款人的确认，生成验证消息，该消息包含该卡的支付方式以及输入与钱夹处理装置相关联的安全参数的请求。

在接收到该验证请求的响应消息后，检测出该操作是钱夹处理装置（12）中的委托验证，完成该验证并以已经说明的方式通过移动电话向付款人传递验证结果，并通过因特网处理装置（20）向虚拟 POS（40）传递验证结果。这样，虚拟 POS（40）知道所选择的卡确实属

于该收款人并且目前有效。

本发明的系统还允许相关收款人的通信设备仅由用作 POS 的移动电话组成，下文中移动电话被称为 POS。这种可能性是为旅行中的销售商或者操作量和操作费用不值得安装蜂窝 POS 或常规销售终端的情况而特意设计的。

在这种情况下，对于先前的情况，作为 POS 的移动电话必须被登记在支付和操作处理装置（1）中，并且第二存储装置必须以为先前的例子所说明的相同方式包含与收款人和作为 POS 的移动电话相关的各种数据。

在这种情况下，如果收款人发起交易，还生成了交易请求，如同先前的例子，交易请求被通过相应的移动电话网络（3）发送到操作处理装置（11），并由操作处理装置（11）的识别装置（11a）检测出它是发起自作为 POS 的移动电话的操作，并确以先前说明的方式确认相关收款人，但区别是在这种情况下一旦结束了所述确认，操作处理装置就和作为 POS 的移动电话建立了消息交换以获取交易所需的各种数据，如下所述。

还应该注意到作为 POS 的移动电话是由它的电话号码标识的，并且可能与第三存储装置（17）中包含的第一信息中的索引相关联，索引接着与请求数据的选择性消息序列相关联，该请求数据消息序列可选择性地涉及要完成的操作，相关用户-付款人的第一标识，相关收款人的安全参数，产品或服务的价格以及要使用的货币。

在这种情况下，还对收款人进行了验证，为此目的本发明需要第二存储装置包括标识与相关收款人的第一标识信息相关联的安全参数的第六信息，以便操作处理装置检测到发起自作为 POS 的移动电话的交易请求，并为相关收款人生成验证消息，该消息包含收款人的标识以及输入安全参数的请求，该消息被发送到收款人的 POS。当操作处理装置检测到响应时，它请求销售商处理装置（14）验证该响应，销售商处理装置（14）通过访问第二存储装置（15）完成验证。

发起自作为 POS 的移动电话的交易请求可以包括购物操作、退货或对交易历史的查询。

当操作处理装置接收到发起自作为 POS 的移动电话的对早先的交易的查询时，它请求标识该交易的相关用户-付款人、数额、货币，可

能还有交易日期的数据。这个信息被发送到发票和交易管理处理装置，它访问第七存储装置以检验该交易记录是否存在，将结果发送回相关收款人的作为 POS 的移动电话。

这样，在收款人想要通过作为 POS 的移动电话查询先前交易的情况下，他输入表示该移动 POS 的操作代码以和支付和操作处理装置通信，支付和操作处理装置确认该收款人，并启动与作为 POS 的移动电话交换消息的过程以获取涉及相关用户-付款人的数据，验证相关收款人的所述收款人的安全参数，以及涉及交易的数据（例如产品或服务的价格或交易货币）。

同样当用户-付款人想要请求涉及作为 POS 的移动电话的交易时，他或她利用和所述作为 POS 的移动电话相关联的索引生成交易，并在确认了该交易和该用户-付款人之后，操作处理装置生成向作为 POS 的移动电话请求涉及该交易的数据的连续消息，收款人在收到这些消息时将请求的数据输入移动电话而响应这些请求。一旦接收到了该交易的所有所需数据，该过程如前面所说明的那样继续。

在本文中，我们将继续更详细地说明作为 POS 的移动电话的不同交易功能。

蜂窝 POS (8) 也能够完成对先前的交易的查询，在这种情况下当操作处理装置 (11) 接收到发起自蜂窝 POS (8) 的对先前交易的查询构成的事务时，在获得了相关用户-付款人的标识数据、数额、货币，可能还有交易日期之后，相关信息被发送到发票和交易管理处理装置，发票和交易管理处理装置访问第七存储装置以确认该交易记录是否存在，将查询结果发送到相关收款人的蜂窝 POS。因此，在这种情况下，没有进行对相关收款人的验证。

将会更详细地进一步说明，发送到作为 POS 的移动电话的请求消息可以是预先记录的语音消息，以便当由作为 POS 的移动电话接收到它时，收款人输入对接收到的语音消息的响应。

为了让操作处理装置发出不同的消息，它包含的表格/文件具有包括了与移动电话的对话的消息的各种不同可能性的代码。

在这个实现例子中，应该注意到有一种特性是作为 POS 的移动电话不能打印销售收据，所以不能用短消息作为记录单发送交易结果。这限制了作为 POS 的移动电话上可以存储的短消息的数量，因此在这

种情况下销售商处理装置(14)可以在第二存储装置(15)中存储消息,以便能够用上述查询操作从作为POS的移动电话查询它们。

还应该注意到第三存储装置(17)包括标识索引与远程支付和操作处理装置(1')相关联的第二信息,根据该第二信息确定是否能从远程支付和操作处理装置访问索引以实现国际交易和支付,对此将有进一步的说明。另外,第三存储装置(17)包括与涉及索引的到期时间的第一、第二和第三信息相关联的第四信息,以便它们可以建立不同类型的索引,如“对本发明的说明”一节中所示那样。

另外,本发明的系统还允许个人之间的支付,在这种情况下收款人是相关付款人。在这个操作中,相关付款人通过输入收款人的标识以及要支付的数额而从他们的移动电话(7)发起交易,收款人是另一相关联的用户-付款人。这个消息在操作处理装置(11)中被接收到,操作处理装置通过识别装置(11a)检测到它是个人之间的交易,并进行对相关收款人的确认,收款人在这个例子中是另一相关用户-付款人。该确认在钱夹处理装置(12)中完成,它以和确认相关付款人相同的方式访问第一存储装置(13)。

随后,以所说明的方式进行对付款人的确认。

操作的剩余部分与先前所说明的相同,唯一的区别是交易结果通过钱夹处理装置(12)而不是直接从操作处理装置(11)被发送到收款人(用户),因为收款人是另一用户-付款人。

个人之间的另一支付形式是进行延迟交易。在这种情况下,交易被如下分两个阶段完成。在第一阶段,以所说明的方式确认收款人和用户,但在这种情况下操作处理装置(11)通过识别装置(11a)检测到它是个人之间的延迟支付。另外,包括在第一存储装置(13)中的有选择地标识验证的第三信息有选择地涉及对付款人的验证的实现。

对付款人的支付方式的收费和对收款人的支付方式的付帐处于等待执行中,下一步是在操作处理装置(11)中生成验证结果,验证结果被钱夹处理装置以已经说明的方式发送到付款人(5)的移动电话,同时操作处理装置在索引处理装置(16)中生成与个人之间的延迟支付相关联的索引生成请求,索引处理装置(16)生成所述索引并将它和交易数据一起存储在第三存储装置(17)中,然后将它发送到相关收款人的移动电话,该收款人如前所述还是相关用户-付款人。

已经接收到索引的相关收款人现在处在通过生成按索引的交易请求而启动第二步的位置，交易请求被以已经说明过的方式发送到支付和操作处理装置（1），支付和操作处理装置（1）的操作处理装置检测它是否是延迟支付索引，并且对相关收款人（如上所述相关收款人在这种情况下是相关付款人）进行确认，以发送验证消息给相关收款人的移动电话，从而所述收款人可以选择它想要接收付款的支付方式，操作处理装置检测与它相关联的金融实体处理装置中对涉及收款人验证的验证请求的响应，以收款人所选择的支付方式付款，收款人随后在他或她的移动电话中接收到交易结果。

可以通过本发明的系统完成的另一操作是付款人向它所关联的金融实体处理装置进行查询例如查询余额和最近的活动情况。为此，用户-付款人用他或她的移动电话（7）生成表示查询操作的消息，该消息被操作处理装置的识别装置（11a）检测到，以已经说明的方式进行对用户-付款人的确认。所述处理装置随后生成验证消息，其中支付方式只是用户-付款人的支付方式，并且验证消息还包括输入要查询的参数的请求。用户-付款人随后选择要查询的支付方式并输入安全参数和要进行的查询，发送对验证消息的相应响应消息。接下来操作处理装置（11）将查询发送到与所选择的支付方式对应的金融实体处理装置（4），并接收响应连同与用户-付款人所进行的查询相对应的数据，该数据随后被通过钱夹处理装置（12）发送到相关联付款人的移动电话（7）。

可以在钱夹处理装置中完成相同的操作，在这种情况下由它检测用户-付款人的查询操作。在这种情况下，验证是在钱夹处理装置中执行的，钱夹处理装置检验接收到的安全参数是否与第一存储装置中所存储的相一致，并且与所述处理装置的安全参数相一致。接下来，完成查询并将所获得的数据发送到用户-付款人。

本发明的系统能够进行的另一操作包括在与用户-付款人相关联的各种数据上进行的参数更改操作。在这种情况下，用户-付款人发送请求参数更改操作的消息，该消息被操作处理装置的识别装置（11a）检测到，并且以已经说明过的方式完成对该用户-付款人的确认。接下来，生成验证消息，在验证消息中支付方式仅涉及该用户-付款人的钱夹处理装置，并且还包括输入要修改的参数的请求。在用户-付款人

(5)的移动电话(7)中接收到所述验证消息后,所述用户-付款人输入安全参数和他或她想要修改的那些参数,可能包括对安全参数、语言、默认支付方式等的修改。接下来,操作处理装置路由消息到钱夹处理装置(12),在钱夹处理装置(12)中进行修改,并从钱夹处理装置(12)将操作响应消息发送到该付款人(5)的移动电话。

在这种情况下安全参数与钱夹处理装置相关联,通过钱夹处理装置进行验证以允许所需的参数更改。

为了执行为索引处理装置(16)说明的所有功能,索引处理装置配备了对第三存储装置(17)中的信息进行维护的自动维护模块(16a)(图3)以检测并消除过期的索引。这个处理装置还配备了编码模块(16b),以按照早先所标识出的字段并根据定义好的算法对索引进行加密。这些都存储在第三存储装置中。另外,索引处理装置配备了与这里编号为11、12、14、18和20的其它处理装置的连接接口,以及控制索引处理装置(16)运行的管理模块(16c)。

同样,为了让钱夹处理装置(12)能够执行所说明的所有功能,它配备了管理处理装置(12a),该管理处理装置(12a)包括第一、第二和第三检测器装置(上面说明过的12a₁和12a₂),并且实现对第一存储装置(13)中包含的信息的管理操作,以允许对金融实体处理装置的访问从而完成对相关用户-付款人的支付方式的添加、删除和修改。另外,该管理处理装置(12)允许访问发票和交易管理器(45)以在其中存储钱夹处理装置完成的各种操作。

为此,该管理处理装置(12)与接口(12d)相连,通过该接口(12d)它连接到了支付和操作处理装置(1)下包括的各个处理装置。

另外,钱夹处理装置(12)配备了消息处理装置(12b),它与管理处理装置(12a)、第一存储装置(13)以及接口(12d)通信,以便管理处理装置(12a)可以完成对技术的检测,对此将有进一步的说明。

为了通过相应的移动电话网络建立起通信,钱夹处理装置(12)配备了消息处理装置(12b),消息处理装置(12b)与管理处理装置(12a)、第一存储装置(13)和接口(12d)相连,以使它能够发送与用户-付款人的移动电话建立会话和维持对话的消息。

消息处理装置(12b)与接口(12d)的连接使得它能够和技术检

测处理装置（68）以及电信控制器（10）进行通信。

最后，钱夹处理装置（12）包括验证处理装置（12c），其与第一存储装置（13）相连以执行对用户-付款人的验证操作，以及对涉及钱夹处理装置的安全参数的检验，例如就购物操作来说，有余额查询和最近的活动、参数更改以及委托验证。另外，它执行到国际寻址处理装置（2）的选路以及与远程支付和操作处理装置相关联的用户-付款人的验证请求，下面将对此有说明。关于销售商处理装置（14），它包括一个管理模块（92），该管理模块（92）与第二存储装置（15）相连，并通过连接接口（94）与操作处理装置（11）相连，以便由支付和操作处理装置（1）的系统分析员或金融实体处理装置的系统分析员或管理员完成对具有相关联支付方式的收款人的添加、删除和修改。此外，销售商处理装置包括一个验证处理装置（93），该验证处理装置（93）与第二存储装置、管理处理装置（92）和接口（94）相连，以便能够进行对相关收款人的确认和对与相关收款人有关的安全参数的验证。

在由用户-付款人发启的所有操作中，我们已经说明了用户-付款人在被支付和操作处理装置（1）所要求时输入不同交易数据的过程，但还有一种可能性是用户-付款人在一次交易请求中输入完成交易需要的全部或部分数据，以便在只输入部分所述数据的情况下可以用所说明的方式请求剩余的所需数据。

另外，应该注意到第一存储装置（13）存储了涉及单个国家中不同语言的信息，由此允许选择进行操作的语言以及和用户-付款人的移动电话以及收款人的通信设备交换各种数据所用的语言。

下面我们说明在相关联付款人在他或她自己的国家之外的某个国家进行购物或完成交易，或者付款人在他或她自己的国家向在另一国家的收款人进行购物或完成交易，并因此与不同于该付款人的支付和操作处理装置（1）的远程支付和操作处理装置（1'）相关联的情况下该系统的运行。

为了提供这个功能，第一存储装置（13）包括与远程支付和操作处理装置（1'）相关联的付款人的第四标识信息。所述第四信息用来标识国家代码，例如各移动电话属于的国家的移动电话号码的国家代码，并且每个支付和操作处理装置都与一个国家代码相关联。还有一

种可能性是国家代码是标准国家代码，例如由美国银行家协会发布的 ISO/IEC 7812-1:1993 定义的表示每个国家的每个支付和操作处理装置的前缀。这是表示支付和操作处理装置的国家的 PAN 代码并且还可以是上述 PAN 的 EAN 代码的国家代码。

另外，为了提供这个功能，支付和操作处理装置 (1, 1') 包括路由处理装置 (18)，它与第四存储装置 (19) 相连，第四存储装置存储了关于至少一个国际寻址处理装置 (2) 的标识的第一信息。

因而，在付款人从海外进行购物 (图 5) 的情况下，收款人生成的交易请求中付款人标识包括上述前缀之一，以便所述交易请求 (表示蜂窝 POS (8)) 通过移动电话网络 (3) 到达该收款人相关联的支付和操作处理装置 (1) 的电信控制器 (10)。首先，按照已经说明的过程，在与收款人相关联的支付和操作处理装置中完成对该收款人的确认，并将所述收款人的支付方式输入钱夹处理装置 (12)。接下来，由操作处理装置 (11) 获得该请求，操作器处理装置生成对相关付款人的确认和验证请求，该请求被发送到钱夹处理装置 (12)，钱夹处理装置 (12) 通过访问第一存储装置的第四信息检测到该前缀是与另一远程支付和操作处理装置 (1') 相关联的付款人，生成一个路由消息并将它发送到路由处理装置 (18)，该路由消息由对该远程付款人的确认和验证请求以及关于该收款人允许的支付方式的数据组成，路由处理装置 (18) 通过访问第四存储装置 (19) 和国际寻址处理装置 (2) 而发送该路由消息。最后，该消息被从国际寻址处理装置 (2) 发送到该付款人所关联的远程支付和操作处理装置 (1')，发送方式后面将有更详细的说明，在该远程支付和操作处理装置 (1') 该消息被接收到钱夹处理装置 (12) 中，钱夹处理装置 (12) 的识别装置 (11a) 检测出它是一个远程确认和验证请求。在以已经说明过的方式完成了所述确认之后，钱夹处理装置 (12) 生成一个包含验证结果和该付款人所选择的支付方式的路由消息，并将它通过该远程支付和操作处理装置 (1') 的路由处理装置 (18) 并通过国际寻址处理装置 (2) 发送到收款人所关联的支付和操作处理装置 (1)。

付款人的钱夹处理装置 (12) 以已经说明过的形式完成对付款人的确认并以和上述相同的方式完成验证。但是，区别在于验证请求被从远程支付和操作处理装置 (1') 发送到付款人的移动电话网络，并

由该付款人通过收款人所在国家的移动电话网络之一在他或她的移动电话(7)中接收到。因此收款人与付款人所在不同国家的所述移动电话网络通过常规国际漫游网关(90)彼此通信。付款人在他或她的移动电话(7)中输入的响应由他或她所关联的移动电话网络(3)通过国际网关(90)从收款人所在国家的移动电话网络(3)接收到,发送响应到付款人所关联的远程支付和操作处理装置(1'),该远程支付和操作处理装置(1')生成包含结果的路由消息,并通过国际寻址处理装置(2)将它发送到收款人所关联的支付和操作处理装置(1)。

收款人所关联的支付和操作处理装置的操作处理装置(11)接收到验证结果,并向该收款人所关联的金融实体处理装置请求交易。在接收到交易结果之后,它生成包括所述交易结果的路由消息,并将它发送到付款人所关联的远程支付和操作处理装置(1'),并从那里用漫游将该消息发送到相关联付款人的移动电话(7)。

交易结果同时被以已经说明过的方式发送到相关收款人的通信设备。

对于相关收款人的通信设备是常规POS(图5)的情况,所述过程与为这种情况所说明的相同,但区别在于对收款人的确认是以先前例子中所说明的相同方式在金融实体处理装置中完成的,金融实体处理装置将确认结果连同支付方式一起发送到收款人所关联的支付和操作处理装置(1)的操作处理装置(11),支付和操作处理装置(1)随后生成发往远程支付和操作处理装置(1')的对相关联付款人的验证和确认请求,启动对前一种情况所指出的过程,但区别在于交易结果被从收款人所关联的金融实体处理装置发送到该常规POS(9)。

还有一种可能性是付款人向国外收款人请求交易,以先前为付款人和收款人在同一国家的情况所说明的不同方式在他或她的移动电话中输入数据,而不管付款人在他或她自己的国家或别的国家。

这时,应该注意到第三存储装置(17)包括与远程支付和操作处理装置(1')相关联的索引标识的第二信息,以检测远程支付和操作处理装置的相关索引的标识并生成一个路由消息以确认它与该支付和操作处理装置中的索引相关联。

因此,在付款人在国外(图6)并按索引进行购物的情况下,交易请求被通过所述付款人所在国家的移动电话网络(3)之一并通过国际

网关发送到付款人所关联的移动电话网络。交易请求又被从那里发送到付款人所关联的远程支付和操作处理装置(1')，该远程支付和操作处理装置以已经说明过的方式确认付款人，并在检测出该索引与支付和操作处理装置(1)相关联后生成一个包括索引确认请求、该索引以及相关付款人的确认的路由消息。该路由消息被以已经说明过的方式发送到收款人所关联的支付和操作处理装置(1)，在那里确认该索引和相关联的收款人，并且生成包括对付款人的验证请求的路由消息，重复先前说明过的过程，即验证消息被通过寻址处理装置(2)发送到远程支付和操作处理装置(1')，在那里验证该付款人。通信是通过网关(90)以及付款人临时所处国家的移动电话网络(3)之一处理的，在收款人的支付和操作处理装置(1)中接收到验证结果，以已经说明过的方式完成交易，并且用相应的移动电话网络、国际网关(90)和所述付款人临时所在国家的移动电话网络之一通过远程支付和操作处理装置(1')将交易结果发送到相关收款人的通信设备以及相关付款人的移动电话(7)。

对于付款人通过他或她自己国家内的移动电话输入与远程支付和操作处理装置的相关收款人对应的索引的情况，过程与前面的情况相同，唯一的区别在于与付款人的支付和操作处理装置(1')的通信是通过常规移动电话网络直接完成，而不通过常规国际网关(90)也没有其它国家中的其它移动电话网络的参与。

为了完成国际交易，本发明的系统要求第一存储装置(13)和第二存储装置(15)都包括关于相关付款人和收款人的语言的信息，以便能以与各个相关收款人和付款人对应的语言进行交易和表示消息中的相应数据。

对于执行所有上述功能的国际寻址处理装置(2)(图7)来说，它包括与不同支付和操作处理装置(1, 1')的路由处理装置(18)相连的访问控制器(23)，以能够在它们之间进行通信。另外访问控制器(23)由访问第五存储装置(25)的路由管理器(24)控制，第五存储装置(25)至少包括关于与远程支付和操作处理装置相关联的付款人的国际标识和前缀的第一标识信息，关于与远程支付和操作处理装置相关联的付款人的索引的第二信息，以及标识要遵从的路线的第三信息，在接收到路由消息后，如前所述，访问第五存储装置并确定

发送和接收路由消息要遵从的路线。

寻址处理装置(2)包括管理模块(44),其中存储了完成的所有操作。

关于路由处理装置(18),应该注意到它们可以和多个国际寻址处理装置(2)相连,以便在接收到路由消息时,它们访问第四存储装置(19)并识别出应该为该路由消息寻址的寻址处理装置。

另外,路由处理装置(18)与系统管理员的通信设备相连以进行对路线的添加、删除和修改操作,以使系统保持通用并且能够在不同的支付和操作处理装置(1,1')之间进行所有不同的通信。

接下来,我们说明不同的电信控制器装置(10),支付和操作处理装置(1)包括它是为了能够和不同类型的移动电话(7)以及不同技术的移动电话网络(例如GSM网络,TDMA(时分多路访问)和CDMA(码分多路访问)网络)中的通信设备通信。

将对由支付和操作处理装置(1)完成的对每个移动电话的技术检测做进一步说明。在所述检测之后,选择适当的电信控制器,对此也将有进一步的说明。

当移动电话启动操作时,是移动电话网络以常规方式识别出终端或移动电话的技术并与适当的电信控制器装置通信。按照图8所示,我们说明了通过GSM(全球数字移动电话系统)移动电话网络在支付和操作处理装置(1)和相关联付款人的移动电话(7)之间、和由蜂窝POS(8)构成的相关收款人的通信设备之间、以及和作为POS(22)的移动电话之间进行通信的情况,由此控制器(10)包括USSD控制器(10a)(无结构辅助服务数据)和SMS(短消息服务)控制器(10b),以根据移动电话(7)或作为POS(22)的移动电话的技术选择所述控制器10a或10b之一,以后我们将把移动电话(7)和作为POS(22)的移动电话都称作移动电话以简化说明书。

在GSM网络中可以通过不同的移动电话7、22使用的不同技术主要包括支持USSD MAP(移动应用部分)版本1或版本2(如欧洲专利编号EP-00202720所述)的那些技术,以便如果移动电话支持USSD版本2,就选择USSD控制器10a从支付和操作处理装置(1)向移动设备发送USSD堆栈,例如在验证请求以及交易结果的发送中。

在移动电话支持USSD版本1的情况下,从支付和操作处理装置到

移动电话的请求通过 SMS 控制器 10b 进行，以发送 0 类别短消息，该短消息被显示在屏幕上。接下来，支持 MAP 版本 1 的电话启动 USSD 会话，对话在用户-付款人及支付和操作处理装置的钱夹处理装置之间建立起来并通过所述会话完成对话。

USSD 控制器 10a 与移动电话网络 (3) 的 USSD 中心 (77) 通信，SMS 控制器 (10b) 与所述移动电话网络 (3) 的 SMS 中心 (76) 通信以实现先前所说明的功能。没有更详细地说明移动电话网络的结构，因为这不是本发明的目标，并且在本领域的现状中是众所周知的。

为了完成这些通信，USSD 控制器 (10a) 至少配备了第一存储装置 (10a1) 和将 USSD 栈转换成所有支付和操作处理装置内部使用的公共协议或反方向转换的协议转换器 (10a2)，第一存储装置 (10a1) 包括支付和操作处理装置 (1) 的运行信息，所述公共协议在该实现例子中指的是目前技术发展水平中存在的标准协议之一，例如 XML 消息 (可扩展标记语言)。这个信息能够检测出接收到的信息将被通过网络 (3) 分别导向谁，操作处理装置 (11) 或钱夹处理装置 (12)。

另外，USSD 控制器 (10a) 配备了交换模块 (10a3)，该交换模块根据接收到的信息访问包括要遵从的路线信息的第二存储装置 (10a4) 以将它们发送到操作处理装置 (11) 或钱夹处理装置 (12)。

这个配置允许在 USSD 堆栈 (包含涉及验证响应或交易请求等的信息) 被发送到支付和操作器 (1) 时，USSD 控制器分析堆栈并将它和内部协议消息捆绑在一起传递到交换模块 (10a3)，交换模块 (10a3) 借助第二存储装置根据接收到的消息确定要遵从的路线并将它发送到操作处理装置 (11) 或钱夹处理装置 (12)。

在所用移动电话技术是 USSD MAP 版本 2 的情况下，所有通信都是通过 USSD 控制器 (10a) 完成的，与移动电话具有 USSD MAP 版本 1 的情况不同，具有 USSD MAP 版本 1 的移动电话当在移动电话中启动通信时将从 USSD 控制器 (10a) 接收到的 USSD 栈发送出去。在支付和操作处理装置 (1) 启动与移动电话的通信的情况下，例如发送验证请求时，它使用已经说明过的 0 类别的短消息。

关于代表收款人设备的蜂窝 POS (8)，应该注意到这些蜂窝 POS 总是由具有支持 USSD MAP 版本 2 的移动终端的 POS 组成，因此通信总是通过 USSD 控制器 (10a) 完成。

关于具有 USSD 网络菜单的作为 POS 的移动电话，我们将在下面说明作为 POS 的移动电话与支付和操作处理装置的通信。

下面是对消息交换的逐步分解：

收款人从它的移动电话启动 USSD 会话，输入表示交易请求的序列。通过维护交易环境的操作处理装置，这个请求到达销售商处理装置的管理处理装置（92），该管理处理装置（92）检验收款人的数据。如果确定收款人有效，操作处理装置将可用交易（购物、退货、查询）的菜单发送到收款人的移动设备。

收款人为想要进行的交易输入相关联选择。假定收款人输入购物选项，操作处理装置在 USSD 会话中请求收款人输入购物量/销售量。收款人输入该量并将它发送到支付和操作处理装置。支付和操作处理装置通过操作处理装置请求收款人输入购物/销售的交易货币。收款人输入货币选择并将它发送到支付和操作处理装置。支付和操作处理装置通过操作处理装置要求收款人输入付款人标识。收款人输入付款人的移动电话标识符。接下来，以便销售商授权该交易，操作处理装置将通过开放的 USSD 会话发送对收款人的安全参数的请求。收款人输入安全参数，所述信息被传递到操作处理装置，操作处理装置与销售商处理装置（14）的验证处理装置（93）通信以验证该销售商。

支付和操作处理装置通过钱夹处理装置启动付款人的移动电话中的 USSD 会话，显示涉及购物/销售交易的信息。此时，如果付款人希望用默认支付方式完成交易，他或她输入所述默认支付方式的安全参数。如果希望使用另一种支付方式，则通过所述安全参数选择所述支付方式，并且这个选择被发送到支付和操作处理装置。

钱夹处理装置检验用户 - 付款人的数据。

如果所有数据都正确并且已经确认了用户 - 付款人，支付和操作处理装置就通过操作处理装置完成对交易的授权并首先将对交易的确认发送到收款人的充当 POS 的移动电话。支付和操作处理装置（1）通过钱夹处理装置将对交易的确认发送到付款人的移动电话。

在任一种情况下，在 GSM 网络上进行的各种通信包括对移动电话的验证机制以及对 GSM 网络通常使用的通信的加密，这在欧洲专利 EP-00202720.9. 中有说明。

另外，它包括基于 IPsec 的安全机制，这种安全机制也为 USSD 中

心(77)和USSD控制器(10a)之间以及SMS消息中心(76)和SMS控制器(10b)之间的通信经常采用,其包括一系列能够将加密和验证集成到IP(因特网协议)通信的协议。因此,没有对其进行更详细的说明,因为它是经常使用的协议。

关于SMS控制器(10b),它配备了第一存储装置(10b1)和协议转换器(10b2)以检测将接收到的信息发送到操作处理装置(11)或钱夹处理装置(12),第一存储装置(10b1)具有支付和操作处理装置的运行信息,协议转换器(10b2)将SMS消息转换成支付和操作处理装置(1)所用的协议或者进行反方向的转换。

另外,SMS控制器(10b)配备了交换模块(10b3),交换模块访问第二存储装置(10b4)以获得要遵从的路线,并根据所建立的路线将接收到的信息发送到操作处理装置(11)或钱夹处理装置(12)。

在网络使用TDMA或CDMA技术ANSI(美国国家标准协会)版本(41-E)的情况下,在一个实现例子中将通过图9所详细说明的智能网(63)进行通信。

在这种情况下,通信控制器装置(10)配备了智能网控制器(10d),并且可能还使用先前已经说明过的SMS控制器(10b)。

智能网控制器(10d)配备了协议转换装置(10d1),它将智能网所用协议转换成支付和操作处理装置所用的协议或者进行反方向的转换,以便支付和操作处理装置与包含了支付和操作处理装置运行信息的服务控制点(SCP)(62)通信。

智能网的SCP(62)(如通常所知)包含完成从智能网(63)移动到支付和操作处理装置(1)或反向移动操作的网关功能所需的体系结构。因此,在从移动电话(7,22)启动的通信中,例如交易请求中,所述移动设备从用户的移动电话为智能网生成触发,该触发在智能网(63)的MSC(移动交换中心)(66)中被检测到。换句话说,根据对支付和操作处理装置的呼叫号码在MSC中对触发信号编程。在检测到该触发后,它将指令发送给该网络的HLR(归属位置寄存器)(67)以获得呼叫指令。MSC(66)发送到移动电话网络的HLR(67)的参数表示呼叫号码以及所呼叫号码的位。HLR确定它是对位于所确定的SCP(62)中的支付和操作处理装置(1)的呼叫。随即,HLR(67)与SCP(62)通信,发送涉及支付和操作处理装置(1)的信息,作为响应,

SCP (62) 建立与智能网控制器 (10d) 的通信, 根据要完成的操作所述信息被从智能网控制器 (10d) 发送到操作处理装置 (11) 或钱夹处理装置 (12)。

在交易请求从蜂窝 POS (8) 发出的情况下, 过程与先前所述相同。但是, 在这种情况下, POS 发送包含涉及付款人、产品或服务以及产品或服务数量的触发信号。

网络的 STP (服务传输点) 完成对所述不同网元之间通信的交换。

对于 SCP (62) 和智能网控制器 (10d) 之间的通信, 和 IPsec 安全机制一起使用了 TCP/IP 协议。

在这两种情况中的任意一种情况下, 用于智能网的触发可以包括用户完成交易所需的所有数据, 即操作代码、索引、支付方式和安全参数, 这些在启动交易时被直接输入并根据它们生成所述触发, 或者相反地只输入部分所述数据, 剩下的再根据请求输入以便处理交易。

从支付和操作处理装置 (1) 到移动电话 (7, 22) 的通信可以采用两种不同的形式:

- 使用网络 (63) 通常包括的 IP (智能外设) (64) 的 IVR (交互式语音响应) 功能。因此, 例如, 从智能网控制器 (10d) 发送验证请求到智能外设 (64), 智能外设借助于 IP (64) 中存储的预先记录的语音消息通过 MSC (66) 完成和用户的交互, IP 响应能够发送的每个可能的消息。

- 另一种可能性是以已经说明过的方式使用 SMS 控制器 (10b), SMS 控制器 (10b) 与短消息服务中心 (65) 通信, 而短消息服务中心 (65) 则通过 MSC (66) 发送相应的消息。

来自智能网控制器 (10d) 和 SMS 控制器 (10b) 的通信也是使用具有 IPsec 安全机制的 TCP/IP 协议完成的。智能网 (63) 上的通信使用和 GSM 网络相同的形式, 加密和验证机制是通常在 CDMA/TDMA 网络上使用的那些, 但区别是通常是在所述网络进行加密和验证的, 而在这种情况下使用了 CAVE (蜂窝验证语音加密) 验证中心。

不管移动电话网络的技术是 GSM、TDMA 或 CDMA, 本发明允许通过语音消息传递完成从支付和操作处理装置 (1) 到用户 - 付款人的移动电话 (7)、收款人的蜂窝 POS (8) 或移动电话 (22) 的通信。为此, 支付和操作处理装置 (1) 与 IVR (交互式语音响应) 设备 (61) 相连,

如图 10 所示。此外，支付和操作处理装置配备了 IVR 控制器（10c），通过它与 IVR（61）相连，并且如先前的例子，使用具有 IPsec 安全机制的 TCP/IP 协议执行与 IVR 的通信。

为此目的，IVR 控制器（10c）配备了协议转换器（10c1），该协议转换器完成操作处理装置（11）和钱夹处理装置（12）所用协议和 IVR 设备（61）所用协议之间的转换。

在移动电话（7，22）和蜂窝 POS（8）支持 DMTF（双音多频）的那些情况中一向可以使用这个设备，DMTF 是现有技术发展水平中移动电话的标准。

IVR 设备（61）是常规类型并且包含基于上述协议的连接接口（61b），以能够和 IVR 控制器（10c）相连。它还包括第一存储装置（61a），该存储装置包含支付和操作处理装置（1）的运行信息。

另外 IVR 设备（61）与 PABX（专用自动小交换机）（60）相连，通过它能够完成对发自移动电话网络（3）的呼叫的生成和接收，如前所述，移动电话网络（3）可以是任何技术类型的网络。这样，PABX（60）处理呼叫建立信令，用于主要 ISDN（集成服务数字网络）访问的特殊信令或可能使用的任何其它类型的通信链路。

IVR 设备（61）和移动电话网络（3）之间的这些通信由语音操作，在 IVR（61）和如上所述的移动电话网络（3）的 MSC（图 10 中未包括）之间建立了一条或多条链路。

这样，通过 IVR 设备（61）的预先记录的语音声明接收不同的消息，例如请求支付方式、安全参数、要充值或要向其通知交易结果的电话号码，等等。这是由于在这种情况下还允许完全输入交易所需的全部数据，或仅仅输入部分所述数据，以便通过用 IVR 请求已经被排除的交易所需数据而启动导航。

在上述任一情况下，为了在用户-付款人或收款人进行呼叫时确保对 IVR 的验证，该系统并入了一种安全机制，包括为这个操作提供个性化呼叫音并为每个用户-付款人和收款人提供个性化欢迎消息。

下面我们解释了使用移动电话作为 POS 并使用 IVR 的操作情况下的语音菜单。

交易是通过从收款人的移动电话输入呼叫一个电话号码的特定操作链而被启动的。收款人发起呼叫并被连接到一个 IVR 设备。在这种

情况下，对话是被通过电话呼叫维持的，其中收款人将收听到一系列将指导他完成交易的语音指令。下面是对所交换消息的逐步分解：

收款人通过输入标识操作的序列或输入适当的电话号码从他或她的移动电话发起语音呼叫。这个数据被 IVR 收集并转发到支付和操作处理装置 (1)。操作处理装置被改变为维护交易环境，它发送请求到销售商管理处理装置以检验该收款人的数据。如果一切正确，这些数据被按照次序发送到 IVR 设备 (61) 以生成对该收款人的欢迎消息以及可用交易 (购物-销售、退货、查询) 的菜单。收款人输入与想要的操作对应的选项。在这种情况下，可以用键盘或语音进行选择。IVR (61) 识别出这个数据并将它转发到支付和操作处理装置。随即，操作处理装置向 IVR 发出命令以重现对应于请求输入数额的语音指令。

收款人输入该交易的相关数额。IVR 再次识别出这个数据并将它转发到支付和操作处理装置。操作处理装置接着向 IVR 发出一个新的命令，以重现与请求输入交易货币相对应的语音指令。收款人输入想要的货币。IVR 收集到这个数据并将它转发给支付和操作处理装置，支付和操作处理装置像前面的例子一样通过操作处理装置向 IVR 发出命令，以指导收款人输入付款人的标识符。收款人输入付款人的移动电话标识符。IVR 识别出这个数据并将它转发给支付和操作处理装置。此后，为向收款人授权该交易，操作处理装置命令 IVR 指导收款人输入所对应的安全参数。收款人通过 DTMF 语音或键盘输入安全参数。IVR 将这个信息转发到支付和操作处理装置，操作处理装置随后与销售商验证处理装置 (14) 通信以验证该销售商 (收款人)。

下一步，钱夹处理装置命令 IVR 发起对付款人的移动电话的电话呼叫，并另外用购物/销售交易的信息重现语音消息。所述信息包括销售商身份及数额。随后指导付款人选择支付方式并输入与所选择的输入方式相关联的安全参数。IVR 识别出这个数据并将它转发到支付和操作处理装置。钱夹处理装置检验接收到的数据，并且如果一切正确，操作处理装置就授权该操作并命令 IVR 通知收款人交易结果。

钱夹处理装置随后命令 IVR 通知付款人交易结果。另外，在这种情况下，该系统还将采用可用于 GSM、CDMA 和 TDMA 网络的安全机制，如本文前面所述。

CDMA/TDMA 网络的机制可以概括如下：

- 版本“c”之前的 ANSI 网络版本“41”的基于 ESN（电子序列号）和 MIN（移动标识号码）/IMSI（国际移动用户身份）的基本验证过程。

- 全球验证和注册过程（全球询问/基站询问和唯一询问过程）。这些过程基于 CAVE 算法和称为 SSD（共享秘密数据）的 128 位密钥，SSD 在移动电话和网络验证中心两端都被在本地生成。从不在网络上传输 SSD。

- 信令信道的加密过程。基于 CMEA 算法的对语音信道的信令消息加密过程（SME）；基于 CAVE 算法和最后的数据信道的语音保密过程（VP）；基于 ORYX 算法。

下面一节说明了上面提到的技术检测过程，用在根据网络技术和移动电话技术与用户 - 付款人和收款人或销售商的不同通信中。

这个通信要求必须预先检测出用户 - 付款人和收款人的移动电话的技术。

本发明的支付和操作处理装置配备了完成所述检测的技术检测处理装置（68）（图 1）。为此，第一存储装置（13）将包括第五信息和第六信息，第五信息标识与各个用户-付款人相关的移动电话网络和它们的技术，第六信息标识各个相关用户-付款人的移动电话的技术和其相关的电话号码。

应该注意到一部移动电话可以允许不同的技术。为此，将会有第六层信息表示各个相关用户-付款人的各个移动电话所支持的不同技术。

相同的情况就蜂窝 POS（8）和由收款人用作 POS（22）的移动电话来说也有帮助，也就是说，第二存储装置（15）包括与各个相关收款人相关的各个移动电话网络和技术的第三标识信息以及标识与各个收款人的各个通信设备相关的技术的第四信息。

就这一点来说，应该注意到参数化操作可以包括更改各个移动电话的不同技术的优先级以及选择/改变缺省选择的技术。

这个信息的全部都与一个过期日期相关联以允许更新，并且还与其被更新的最近日期相关联。

在通信之前，操作处理装置（11）或钱夹处理装置（12）生成对与它必须与之通信的电话号码相关联的网络和移动电话的技术检测请

求。

这个请求由技术检测处理装置（68）接收到，它以三种可能的方式完成该检测：

1. 实时检测，包括：一旦操作处理装置或钱夹处理装置已经生成了技术检测请求，它们保持在等待状态直到接收到请求的结果。在这个可忽略的时间段内，技术检测处理装置（68）根据该请求是否涉及用户-付款人或收款人的设备而查询第一存储装置（13）或第二存储装置（15）中的数据，并且检查所获得的信息的过期日期，除非通过入口参数另外表明了过期日期。技术检测模块随后不管是否过期直接返回所发现的数据的值。如果数据过期或者入口参数表明其已经过期，技术检测处理装置（68）通过电信控制器装置（10e）发送对指定电话号码的技术更新请求到检测到的移动电话网络。为此，支付和操作处理装置（1）包括通信控制器（10e），它由与移动电话网络通信以处理该请求的 HTTP 控制器（10e）组成。

应该注意到移动电话制造商通常分配一个明确地标识移动电话的号码。这个号码在 GSM 网络的例子中被称作国际移动设备标识符或 IMEI。在 CDMA/TDMA 网络的例子中被称作电子序列号或 ESN。

这个国际标识符与移动电话的技术和各自的功能相关，例如它是支持 WAP（无线应用协议）、STK（SIM 应用程序工具包）、J2ME（Java 2 平台，微型版）或 BREW（无线二进制运行时环境）的（所有这些都涉及智能移动电话）以及它们用于早先提到的 USSD 和 SMS 的能力。

另外，国际标识号码被存储在移动电话网络的一些结点中，并且存储一个国际标识号码的结点与该电话的电话号码有关，以便为讨论中的电话号码检测到的移动电话网络技术可以通过利用该网络自身上可用的资源访问所述国际号码而得到。

例如，就 GSM 移动电话网络来说，获得 IMEI 号码的途径与欧洲专利申请号 EP-00202720.9 中所说明的相同。

同样，在 CDMA/TDMA 网络中，执行相同的过程以访问网络中包含与 MIN/ESN 对相关的信息的那些结点。

ESN/移动电话技术之间的关系必须存在于移动运营商的数据表或移动运营商（MO）的其它委托机构中。MIN/技术对是从两张表的匹配获得的，并且是用于技术检测的数据。

一旦运营商已经完全检测出技术，它响应由技术检测处理装置（68）产生的请求，技术检测处理装置（68）接收到响应并且立即根据所查询的号码在第一存储装置（13）中为相关的用户-付款人更新接收到的技术信息，或者在第二存储装置（15）中为相关收款人更新接收到的技术信息。

2. 对于不是实时的检测，过程与上述相似，但在这种情况下钱夹处理装置（12）或操作处理装置（11）生成技术检测请求并且随即继续所进行的操作。同时，技术检测装置（68）发送请求消息到移动电话网络，并在接收到响应后与操作处理装置（12）或钱夹处理装置（11）通信，并同时以已经说明过的方式更新信息。

3. 最后，还有一种可能性是移动电话网络实现了周期发送更新消息的可能性，或者以可以实现的任何其它方式。在这种情况下，更新由技术检测处理装置（68）接收到，技术检测处理装置（68）根据指定的过期日期更新数据，并随即通过 HTTP 控制器（10e）在一个响应消息中将完成更新的结果发送到移动电话网络。

还应该注意到在上述三种情况中的任何一种情况下，技术检测请求可能涉及要检验的一个或多个电话，数据由此必须被分别更新以提高系统的性能。在这种情况下，来自移动电话网络的响应涉及所查询的不同移动电话号码。

已经提过本发明还能够在钱夹处理装置（12）中完成委托验证之后的委托授权。因此，支付和操作处理装置配备了本地授权中心（69），本地授权中心通过它的通信控制器（21）（图 1）与操作处理装置相连。设计它主要是为了允许小额支付，即小数额支付，以便本地授权中心（69）通过降低处理消耗和交易时间完成对交易过程的简化，这在小型支付的情况下尤其有用。当授权被委托时，验证也被委托。

委托验证是在钱夹处理装置中通过对第一存储装置中存储的安全参数的检验而完成的。在验证之后，在本地授权中心中进行委托授权。

小额支付可以用在前面说明过的所有不同的支付形式中。

在说明其运行之前，应该注意到至少相关的付款人必须被签署到至少一个与最大购物数额相关的支付方式。这个消费限制被反应在第一存储装置（13）中为各个相关付款人所包括的支付方式的第二信息中。为此，上述支付方式的第二标识信息被关联到一个最大消费限制。

钱夹处理装置(12)生成一个确认,它包括与消费限制相关的至少一种支付方式的存在指示,获得所述支付方式连同执行对付款人的确认。另外,在委托授权的情况下,与消费限制相关的每种支付方式都与本地授权中心(69)的标识相关。

此外,销售商或收款人可能接受或拒绝小额支付,这个信息被包括在第二存储装置(15)的第二信息中。在完成对相关收款人的确认操作后,如上所述,销售商处理装置(14)生成一个确认消息,它包括销售商的授权特征,可以是三种类型,具体地说:在线授权(不允许委托授权),离线授权(只允许委托授权以及小于指定数额的交易),或混合离线和在线授权(根据交易额在指定限制之上或之下而允许委托授权)。

当检测来自相关付款人的移动电话或相关收款人的通信设备(包括蜂窝POS(8)或充当POS(22)的移动电话)的交易请求时,如果对付款人和收款人的确认结果表明付款人有至少一种与最大消费限制相关的支付方式,并且收款人的授权特征是离线,并且如果交易额少于与所述收款人相关的最大限制,就生成一个验证消息,该验证消息包括验证由收款人允许的支付方式和与最大数额相关的付款人的支付方式的匹配。在接收到验证消息之后,它检测出与最大数额相关的支付方式并且生成委托验证和授权,根据所选择的支付方式的标识获得本地授权中心(69)的标识。这样,操作处理装置(11)生成授权和验证请求,验证在钱夹处理装置中完成,授权请求被通过通信控制器(21)发送到本地授权中心(69)。

本地授权中心(69)以下面将要说明的方式完成授权,并且将结果发送到操作处理装置(11)并将完成的不同交易存储在第七存储装置(71)中,存储收款人的标识,并且还获得金融实体处理装置和交易数据,所述信息在验证和授权请求中被传递到本地授权中心(69)。另外,本地授权中心配备了批处理装置(70),它定时(例如每天)通过通信控制器(21)将各种交易发送到金融实体处理装置(4)(包括收款人所关联的获取处理装置,以及付款人的支付方式所关联的发行(issuing)处理装置)。所述金融实体处理装置通过常规金融网络完成对收款人的存款以及对付款人的扣款。

假如销售商具有离线授权特征并且交易额超出了所述特征中建立

的限制，就会有拒绝消息生成以拒绝该交易并终止操作。

假如以具有最大消费限制的相同支付方式完成不同的交易，完成验证（以已经说明过的方式检验安全参数），并且随后执行委托授权，为此，在这种情况下，本地授权中心（69）配备了从指定时间段上的总的获批消费限制减去交易额的装置。采用这种方式，每个交易都导致生成净可用余额，这样如果任何单个交易导致所述余额超过最大可用限制，则导致生成拒绝操作并终止交易的拒绝消息。否则，如所示，发送授权结果并为不同交易存储其授权结果。

此外，为了完成所有这些功能，本地授权中心（69）包括存储了与各个相关付款人相关并与最大消费限制有关的支付方式的第二标识信息、与最大数额相关的各个相关收款人的第一标识信息的第一存储装置（69a），以便能够接收委托验证和授权请求消息，并在上述可用余额之外完成委托验证和授权。以支付方式的发行金融机构所规定的方式清除余额并重新建立最大交易额，这可以通过转储金融实体处理装置中的交易而完成，对此将有进一步说明。

假如销售商具有在线授权特征，就以先前说明的方式在金融实体处理装置中完成授权。

第三种形式是折衷的，离线授权和在线授权的混合特征，这种情况下可以根据交易额委托授权由金融实体处理装置完成授权。具体地说，如果交易额超出与收款人相关的最大限制，就生成一个消息以便在金融实体处理装置中按照与支付方式相关的类型完成验证，并且如果交易额少于所述限制，就生成委托授权验证请求并且以已经说明过的方式完成委托授权。

如上所述，相关用户-付款人的移动电话（7）可以是任意类型的，包括 WAP、STK、J2ME 和/或 BREW，因此可以包括存储与各个应用程序（WAP、STK、J2ME 和/或 BREW）对应的信息的能力，因此这些应用程序能够实现不同的功能或者能够简化这里所说明的运行方式的应用程序。

例如，所述存储装置可能包括（可选地）与用户-付款人（5）相关的支付方式。在这种情况下，识别收款人和付款人之间的公共支付方式的将是移动电话（7）。在这种情况下，验证消息只包含相关收款人的支付方式以及输入安全参数的请求。还有一种选择是由付款人的

移动电话(7)完成检验,在这种情况下检验是根据间接表示安全参数的加密序列而完成的,下面将对此进行说明。

在这种情况下,当付款人签署了一种支付方式时,该支付方式所属的金融实体处理装置(4)必须生成与激活密钥相关的加密算法、随机参数(口令)和指定密钥,以便在本发明的系统之外以安全连接将这个数据发送到移动电话,它随即被存储在移动电话中。这样激活密钥生成让付款人输入安全参数的请求,在付款人输入安全参数之后安全参数被存储在移动电话上,并由此验证所述参数,并且只有该用户-付款人知道所述密钥。

这种配置提供了一种可能性:当请求安全参数时,指示用户正确地输入了该序列,然后用密钥加密一个随机参数并生成一个加密序列,并在对验证请求消息的响应消息中将该加密序列发送出去,以便该加密序列到达付款人的金融实体处理装置,付款人的金融实体处理装置确定所述加密序列与存储在所述金融实体处理装置中的集成序列一致。如果这两个加密序列一致,就产生了验证。

在委托验证的情况下,算法和激活密钥以及指定密钥中的安全参数被存储在第一存储装置(13)中,并且交易被通过本地验证处理装置(12c)以已经说明过的方式完成。

假如验证是在付款人的金融实体处理装置中完成的,但在这种情况下是通过收款人的金融实体处理装置,加密序列由付款人的移动电话发送并且在接收到对验证请求的响应消息后由通信控制器装置(21)再次加密。

假如付款人拥有支持WAP的电话(图11),如下所述,这个功能可用WAP协议完成。

为此,电信控制器装置(10)包括存储了常规WAP应用程序的WAP Push控制器(10f),以便支付和操作处理装置(1)通信能够借助通常使用的WAP协议通过WAP网关(WAP Push代理网关)(89)与相关付款人的移动电话(7)通信。WAP Push控制器(10f)和充当网关的WAP网关(89)之间使用的协议是PAP(Push访问协议)。用于移动电话(7)和移动电话网络(3)之间通信的协议称作空中协议之上的Push。

就此来说,应该注意到移动电话网络可以是CDMA、TDMA、GSM以

及 2.5G、3G、GPRS、EDGE（增强数据 GSM 演进）、CDMA 1、UMTS（通用移动通信系统）和 CDMA 2000 等等，其中 WAP 协议独立于移动电话网络（3）所用的载体。

这允许在 WAP 协议消息中包括以 WML（无线标记语言）所写的支付和操作处理装置（1）的机能并包括适当的存储装置（10f1），该存储装置中存储所述信息和要发送的以 WML 所写的不同消息。

因此，当支付和操作处理装置想要发送消息到移动电话（7）时，钱夹处理装置通知 WAP 控制器（10f），已经以先前说明的方式通过技术检测处理装置（68）检验出该电话支持 WAP。

随后，WAP 处理装置生成 PUSH 请求（在想要发送信息到一个或多个移动电话时通常用 WAP 协议发送该请求）。

这个请求包括发往移动电话的内容，例如操作授权请求，以及输入安全参数的请求。这个内容被以 WML 编程，使用元素 p（常规的）以表示应该在付款人的移动电话的屏幕上显示那些语句，并使用元素输入（input）（常规的）以允许输入安全参数。另外，WML 语言的脚本可以用来检验在相同的移动电话中输入的安全参数是否具有有效的格式并且由此避免在网络上传输不正确的数据链。

一旦和终端或移动电话建立起了通信，一旦交易完成，结果被通过发往移动电话的 WML 页面非常简单地发送出去。

相反，当付款人生成交易请求时，访问分配给支付和操作处理装置（1）的特定 WAP 地址。这个地址在移动电话的屏幕上被显示为一个 WML 页面，该 WML 页面具有可以在该系统内执行的各种可用操作的菜单。使用常规元素 p、选择（select）和选项（option），付款人选择需要的选项，输入他或她的安全参数，如果输要的话还输入随后被显示为一个 WML 页面的所需要的信息。

在这种情况下，为了完成上述验证过程的个性化，使用了 WAP 栈的标准安全协议，例如 WTLS（无线传输层安全），以便为数据传输提供安全性，WTLS 是基于 Web 环境中使用的 SSL（安全套接字层）的协议。它允许加密和 PKI（公共密钥基础结构）。这个协议包含建立对移动电话和 WAP 控制器（10f）的验证的服务。如果应用程序需要更强的限制，例如具有公共密钥的证书或数字签名，应该采用这一层支持的另一种安全机制（WIM 或 WPKI）。

下面我们说明 STK 技术，这种情况下用户 - 付款人的移动电话将具有“基于 SIM 工具包的用于支付的特定应用程序”。这个应用程序将被存储在付款人的移动电话的 SIM 卡中。

应用程序被通过使用 OTA 接口 (91) (在无线上) 的 SMS 信息中心 (76) 从 STK 应用程序服务器 (85) 下载到移动电话，如同图 12 所示。STK 应用程序服务器 (85) 可以和用户的 SIM 卡通信，以便不仅完成对基于 STK 的用户支付应用程序的下载，还能够远程地对应用程序进行修改和更新。

假如用户 - 付款人的移动电话 (7) 支持 STK (SIM 工具包) (图 12)，假定所述 STK 应用程序只适用于 GSM 网络，参与激活这个应用程序的控制器被限制为 SMS 控制器 (10b)。

在这种类型的移动电话中，短消息应用程序被通过为 STK 应用程序建立的机制以常规方式相关联。

发送到移动电话的 STK 应用程序包含涉及支付和操作处理装置机能的菜单，并且被存储在支持 STK 的移动电话上。

在这种情况下，所述应用程序在需要时能够存储相关付款人的支付方式，以便如前所述建立付款人和收款人之间的公共支付方式。在这种情况下，这个数据由支付和操作处理装置通过技术检测处理装置 (68) 识别，技术检测处理装置 (68) 访问第一存储装置 (13) 和它上面的第六信息，第六信息与移动电话类型和其不同操作功能相关。

STK 应用程序包括提供了可以用本发明的系统完成的不同可用操作的菜单，如上所述，这些操作有按索引购买、个人之间的支付、查询、余额等等。因此，当付款人想要进行交易请求时，就在所述菜单上进行适当的选择，这个选择引出了请求完成所选择的交易所需信息的一个新菜单。明显地，这两个菜单都被本地存储在付款人的移动电话上的 STK 应用程序中。

STK 应用程序的菜单具有树形结构。当付款人通过支付和操作处理装置选择支付选项时，SIM 工具包应用程序用该领域目前技术发展水平中存在的命令与付款人的移动电话通信，所述命令通常是 SIM 工具包应用程序的前摄 (proactive) 命令。移动电话使用电话的目前技术发展水平中存在的命令与 STK 应用程序通信，例如终端特征、取数据和终端响应。

具体地说，其中由 STK 应用程序使用的最广泛使用的前摄命令是：

“设置菜单”：用户-付款人选择 STK 支付应用程序的这个参数以激活驻留在移动电话内存中的应用程序。

“选择项目”：这个前摄命令允许用户-付款人选择想要的选项，可以支付交易、对电子帐户的查询或修改。一旦选择了一个项目，例如“查询”，STK 应用程序就将可用选择以菜单形式显示在用户-付款人的电话屏幕上，包括对具体支付方式的余额查询，或这里所说明的任何其它操作。

“显示文本”：STK 应用程序的这个前摄命令将信息显示在用户-付款人的电话屏幕上，例如输入索引、请求支付方式、选择要充值的电话号码、选择 PIN。在这一点，应该注意到 STK 应用程序隐藏了用户键入的数字以使它们不会被第三方看到。

“获得输入”：STK 应用程序的这个前摄命令收集用户输入的数据并存储它，例如所选择的支付方式、输入的 PIN、索引、要充值的移动电话，等等。

“获得 Inkey”：用这条前摄命令，应用程序收集与数字相关的选择，以便当 STK 应用程序的命令“显示文本”显示与数字相关的信息时，该应用程序保存用户键入的选择，例如，所选择的支付方式。

客户的移动电话的 STK 应用程序将用户键入的信息写入 SMS 消息。

因此，例如，如果已经选择了按索引购物，菜单将向用户提示输入索引，并且该用户-付款人的移动电话的 STK 应用程序将封装输入的信息，生成 SMS 消息，该 SMS 消息包括支付和操作处理装置所关联的 SMS 中心（76）的号码、以及操作类型的代码、以及索引自身，在这种情况下操作类型是按索引购物，该 SMS 消息被通过 SMS 中心（76）发送到支付和操作中心。支付和操作中心完成对用户-付款人、索引以及与输入的索引相关的收款人的确认过程，所有这些都以先前说明的方式完成。钱夹处理装置与和该交易关联的支付和操作处理装置的 SMS 控制器（10b）通信，该 SMS 控制器（10b）生成一个新的 SMS 消息并将它发送到 SMS 短消息中心（76），以便这个中心接着能够与付款人的移动电话的 STK 应用程序通信。在接收到包含验证请求的所述消息之后，应用程序用为所述目的而建立的前摄命令启动选择支付方式以

及输入安全参数的过程。一旦用户-付款人输入了所需参数，用户-付款人的移动电话的 STK 应用程序再次用所输入的与支付方式和安全参数有关的信息生成一条消息，该消息被通过短消息中心（76）发送到支付和操作处理装置（1）的 SMS 控制器（10b）。该控制器（10b）将所述信息发送到钱夹处理装置，以便钱夹处理装置根据验证模式按照上述方式验证该信息。接下来，一旦已经在相应的授权中心中授权了该交易，通过金融机构的通信处理装置直接授权或被委托给钱夹处理装置，操作处理装置负责交易的管理并与支付和操作处理装置（1）的 SMS 控制器（10b）通信，以便后者能够通过 SMS 消息发出带有交易结果通知的短消息。

另外，STK 应用程序能够将不同记录存储在用户-付款人的移动电话以及支持 STK 的充当 POS 的移动电话的 SIM 卡存储器中。这样，用户-付款人和收款人都可以在他们的电话上查询所述记录，在本地完成对这种信息（例如以前的交易）的查询。

对于交易的所有剩余部分，发送和接收短消息的过程以为按索引购物的例子所说明的相同方式进行。应该注意到在现有技术水平下，SMS 通信是半双工的，这意味着，信息在一个时间只能在一个方向上传输，并且不能在支付与操作处理装置和付款人的移动电话之间建立交互式会话。因此，每次支付和操作处理装置都必须和用户-付款人的 STK 应用程序通信，反之亦然，必须发送一个 SMS 短消息。

在为具有 STK 应用程序的移动电话上的验证和加密所说明的过程中，在移动电话和支付与操作处理装置之间发出和接收到的消息被用常规过程 3DES（三元数据加密标准）加密，不会更详细地说明 3DES，因为它在现有技术发展水平下是众所周知的，并且不是本发明的目标。

下面我们将就收款人的移动电话将充当具有 STK 应用程序的移动电话 POS 的例子说明 STK 技术。收款人将访问“作为基于 SIM 工具包的 POS 应用程序的特定移动电话”。这个应用程序将被加载到收款人的移动电话的 SIM 卡中。

借助图 12 中所示的 OTA（无线上的）接口，应用程序被通过 SMS 短消息中心下载到电话中。应该注意到 STK 应用程序服务器能够和收款人的 SIM 卡通信，以便不仅完成对基于 STK 的用户支付应用程序的

下载，而且还在需要时在远程完成对应用程序的修改和更新。

下面我们说明通过支持 STK 的作为 POS 的移动电话进行购物/销售情况下的 SMS 消息过程。如同对于先前的例子，我们不说明查询交易或退货情况下的操作，假定在这两种情况下支付和操作处理装置以及收款人的移动电话之间交换的消息是相同的。

作为例子，我们将说明用支持 STK 的作为 POS 的移动电话进行的现场购物。在收款人选择移动电话作为 POS 应用时，该 POS 应用程序被存储在电话（22）中，STK 的前摄命令将显示具有可用选项（购物/销售，退货，查询，参数化）的菜单。

在这种情况下，收款人从 STK 应用程序的初始菜单中选择销售选项，STK 应用程序随即请求用户-付款人的标识，这个标识可以是电话号码或相应的 PAN 代码。

如果收款人输入了用户-付款人的标识，STK 应用程序随即将请求输入交易额。

一旦输入了销售额，并且在将带有交易数据的 SMS 发送到支付和操作处理装置之前，收款人的 STK 应用程序请求它的安全参数。如果收款人输入安全参数，SMS 被按照由支付和操作处理装置的 SMS 电信控制器（10b）定义的协议发送出去。如果消息发送成功，STK 应用程序将简要地显示一条消息通知收款人请求已发出。如果通信出了任何问题，将显示一条消息通知收款人请求尚未发出。

一旦由 SMS 应用程序成功地将消息发送到支付和操作处理装置的电信控制器，后者将与操作处理装置通信以便它在销售商处理装置（14）的验证模块中启动验证过程。

接下来，操作处理装置（11）与钱夹处理装置（12）通信，以便后者与用户-付款人通信以完成验证过程和对结果的通知，这两者前面都已说明过。

在完成了该交易之后，操作处理装置通过通信控制器的 SMS 发送关于交易结果的通知消息，该消息包含了这次购物的相关信息。

在用户-付款人的电话和作为 POS 的电话之间交换的 SMS 消息上支持对用户和销售商的 STK 接口的加密。这些消息必须具有用于标识目的的未加密的报头，而消息体包含从点到点加密的交易数据。

所使用的加密是带有对称密钥的 3DES。这个对称密钥由两部分组

成，一部分存储在用户-付款人或收款人的移动电话的 SIM 卡中，第二部分存储在支付和操作处理装置的操作处理装置中。在用户-付款人的 STK 应用程序一端，该密钥由与 IMSI（国际移动用户身份，由移动电话处理的标识）而不是 MSISDN（移动用户集成服务数字网络）相关的数据组成。

就收款人来说，与它的 SIM 卡相关的数据是一系列 16 个密钥，在构成了作为 POS 的手机的初始化和激活一部分的操作中，这些密钥被通过安全过程方式装入手机的 SIM 中。在这 16 个密钥中，在任何时间只有一个有效，支付和操作处理装置能够以它自己的判断改变在任何给定时间上哪个密钥有效，在为所述目的发送的任何消息的字段中将选择传递给作为 POS 的手机的 STK 应用程序。

所述对称密钥的另一部分分别涉及用户的安全参数和收款人的安全参数。

假如用户-付款人（5）的移动电话（7）支持 J2ME（图 13），允许访问驻留在 J2ME 内容服务器（86）上的 J2ME 应用程序，J2ME 服务器包括依照 J2ME 应用程序的支付和操作处理装置（1）的机能，以便当用户订购时，该应用程序被下载到付款人的移动电话。

有三种下载应用程序的可能途径通常应用于这种类型的应用程序，通过 WAP 网关（88）、短消息中心（76）或者通过 CBDD（单元广播数据下载）消息。事实上，已知可以在任何移动电话载体上执行 J2ME 应用程序，移动电话网络（3）可以是任何类型的技术。为此，第一存储装置中包含的第六信息标识用于通信的电信装置（10a-10f）。

一旦用户已经安装了与支付和操作处理装置的功能对应的应用程序，如同前面的例子中那样，该应用程序将显示各种菜单用于选择选项和输入每个操作需要的数据。

同样，J2ME 应用程序可以包括付款人的支付方式，并因此获得并识别出所述付款人和相关收款人之间的公共支付方式。

关于验证，应该注意到在这种情况下，下载过程的安全需要使用 Java 加密中指定的用于 MIDP 平台（移动信息设备特征）的 J2ME API（应用程序编程接口），例如“Bouncy Castle”。

就支持 BREW 的移动电话来说，已知 BREW 也是与载体无关，所述过程与前面的例子相同，但在这种情况下区别在于不是使用 J2ME 内容

服务器（86），而是使用 BREW 内容服务器（87）（图 14）。

在这种情况下，通过使用 QIS（Qualcomm Internet Services）处理安全问题，QIS 允许安全测试、验证和下载。这些应用程序携带一个数字签名。

另外，还应该注意注意到发票和交易管理处理装置（45）顺序存储了支付和操作处理装置（1，1'）中完成的不同操作，以提供对操作历史的访问。

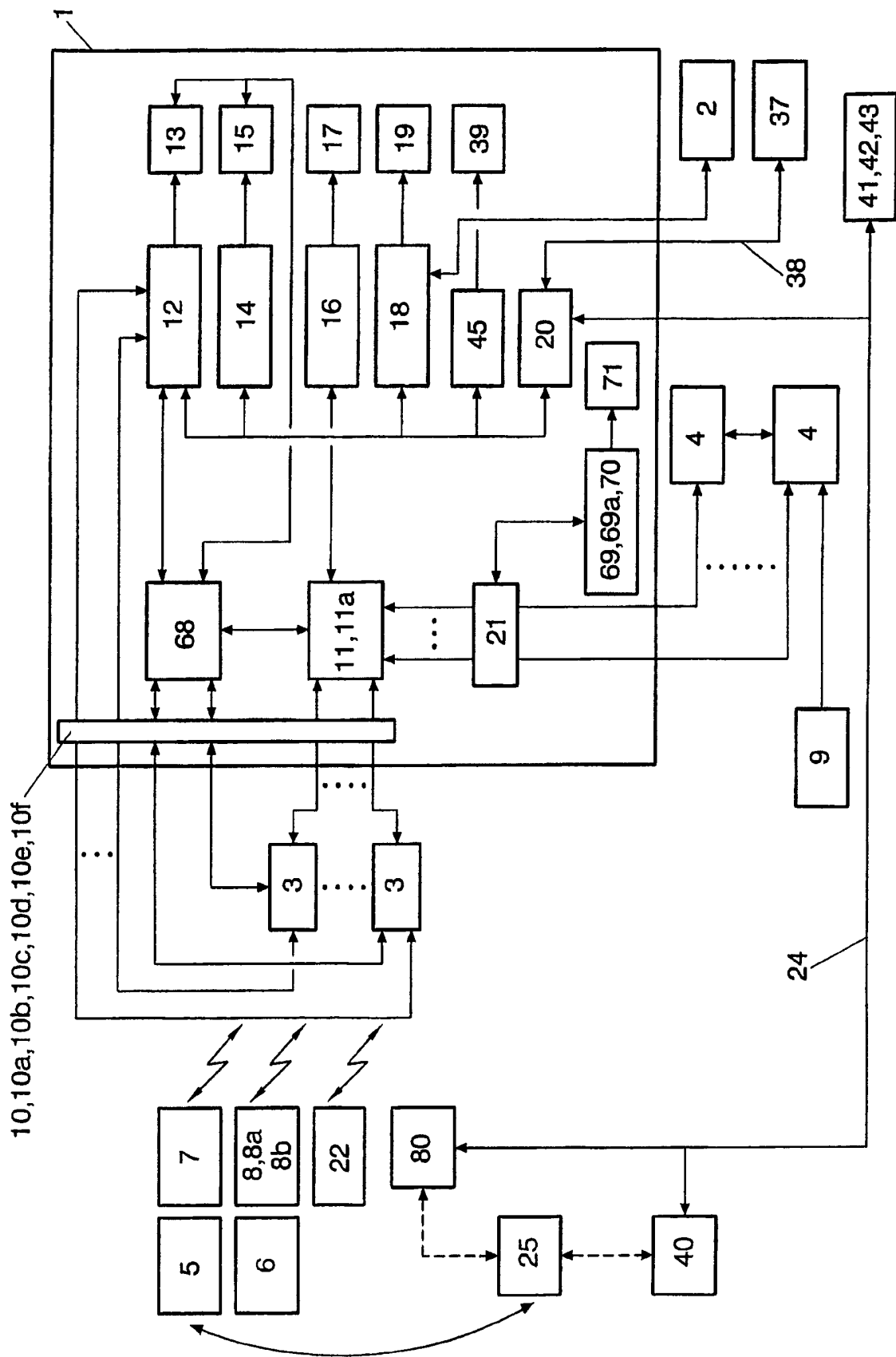


图 1

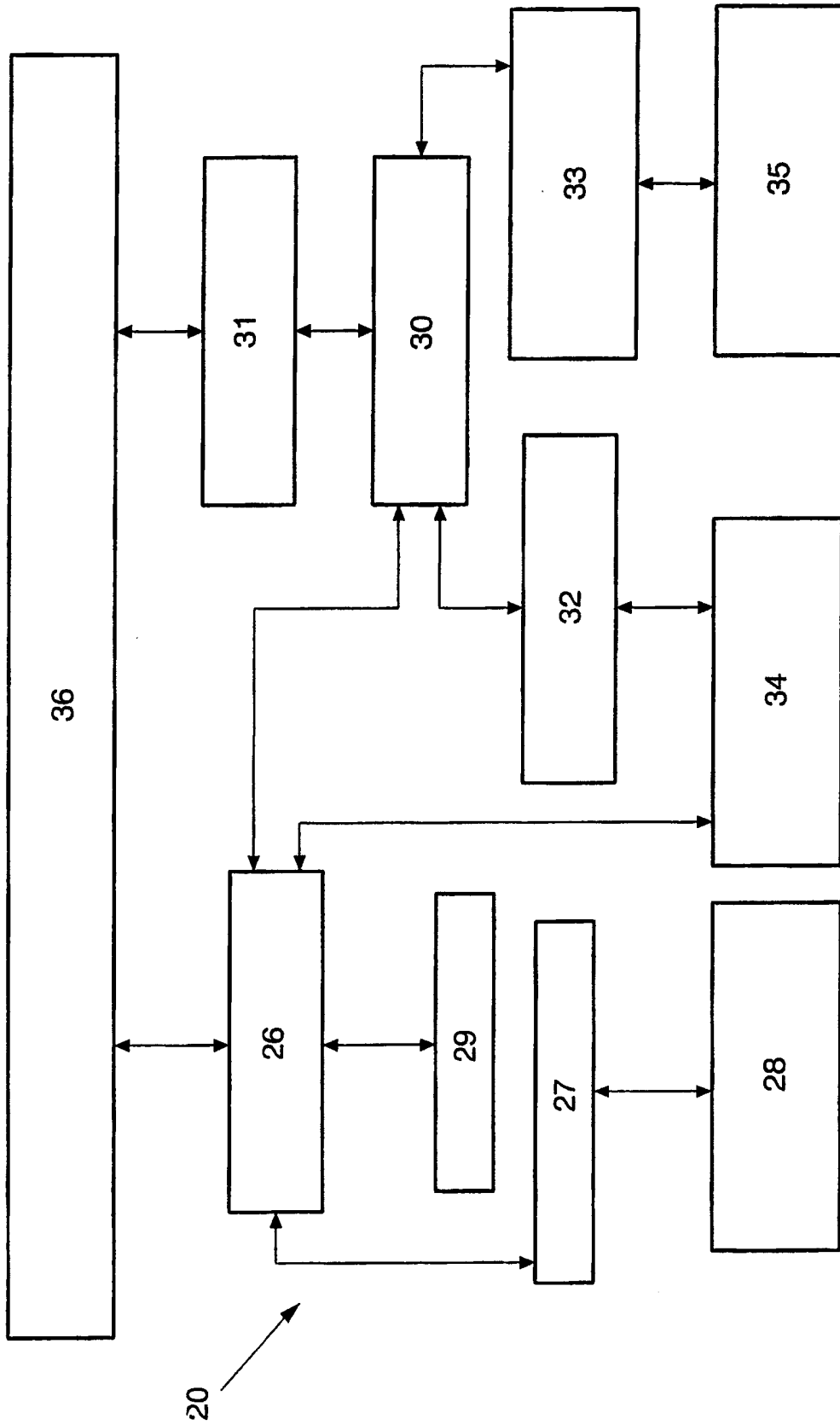


图 2

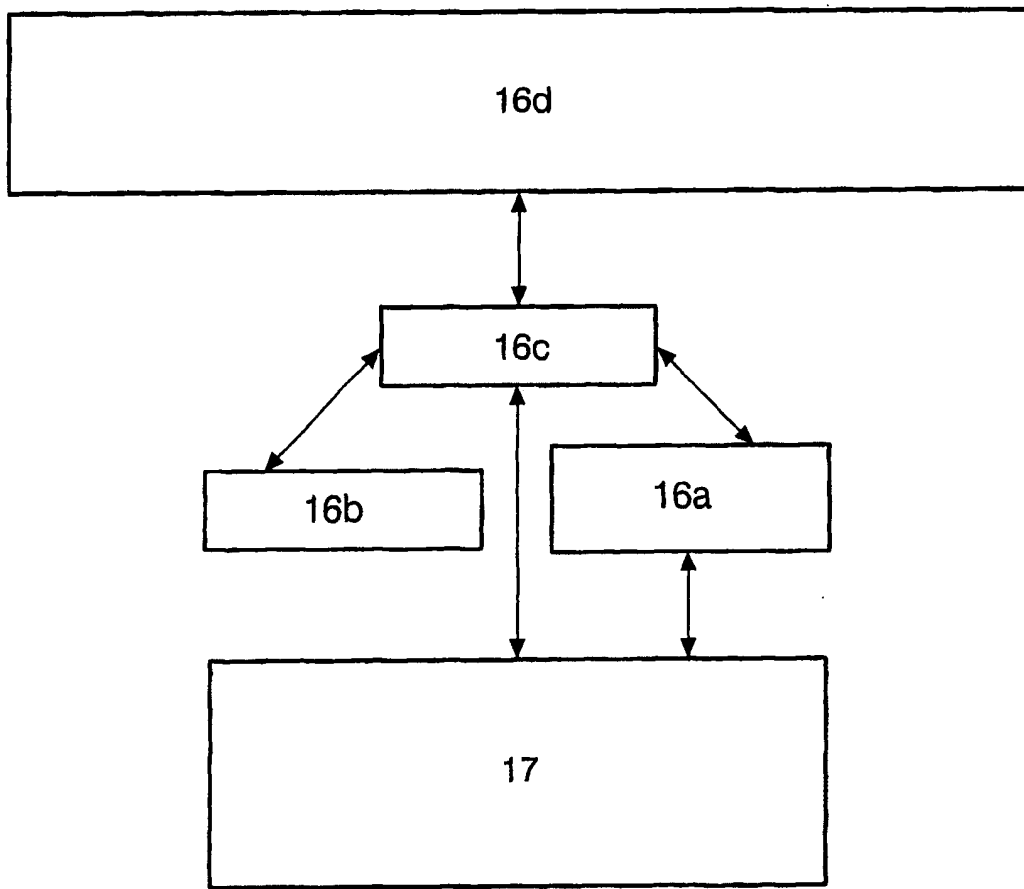


图 3

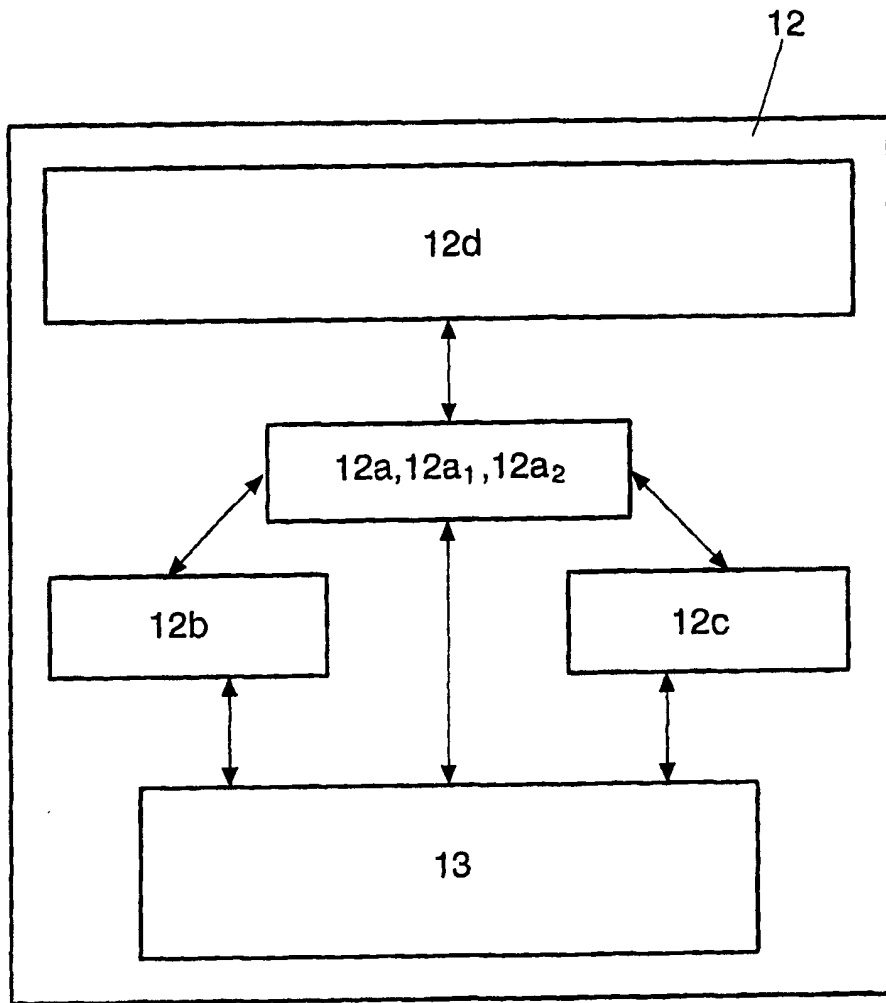


图 4

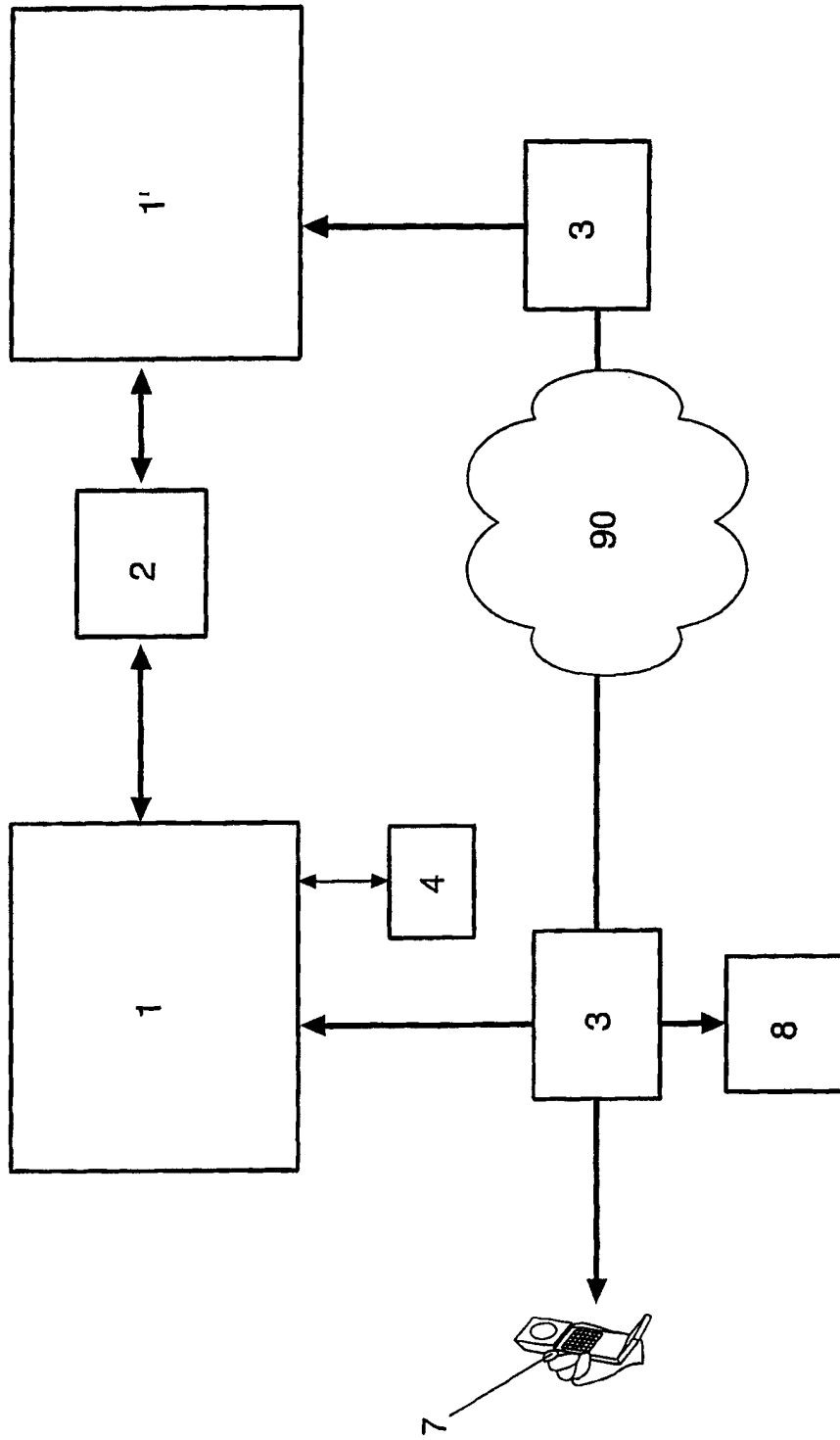


图 5

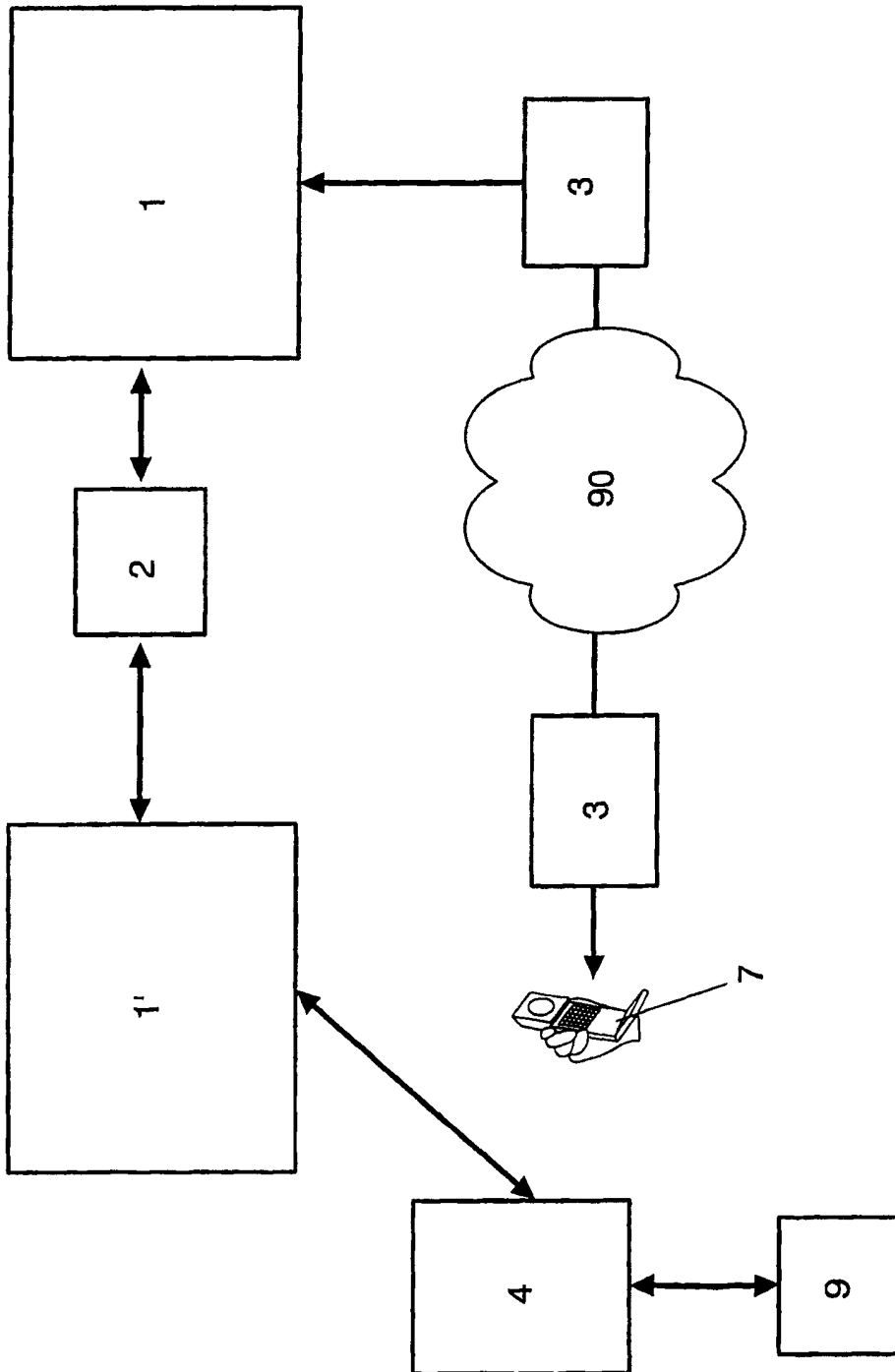


图 6

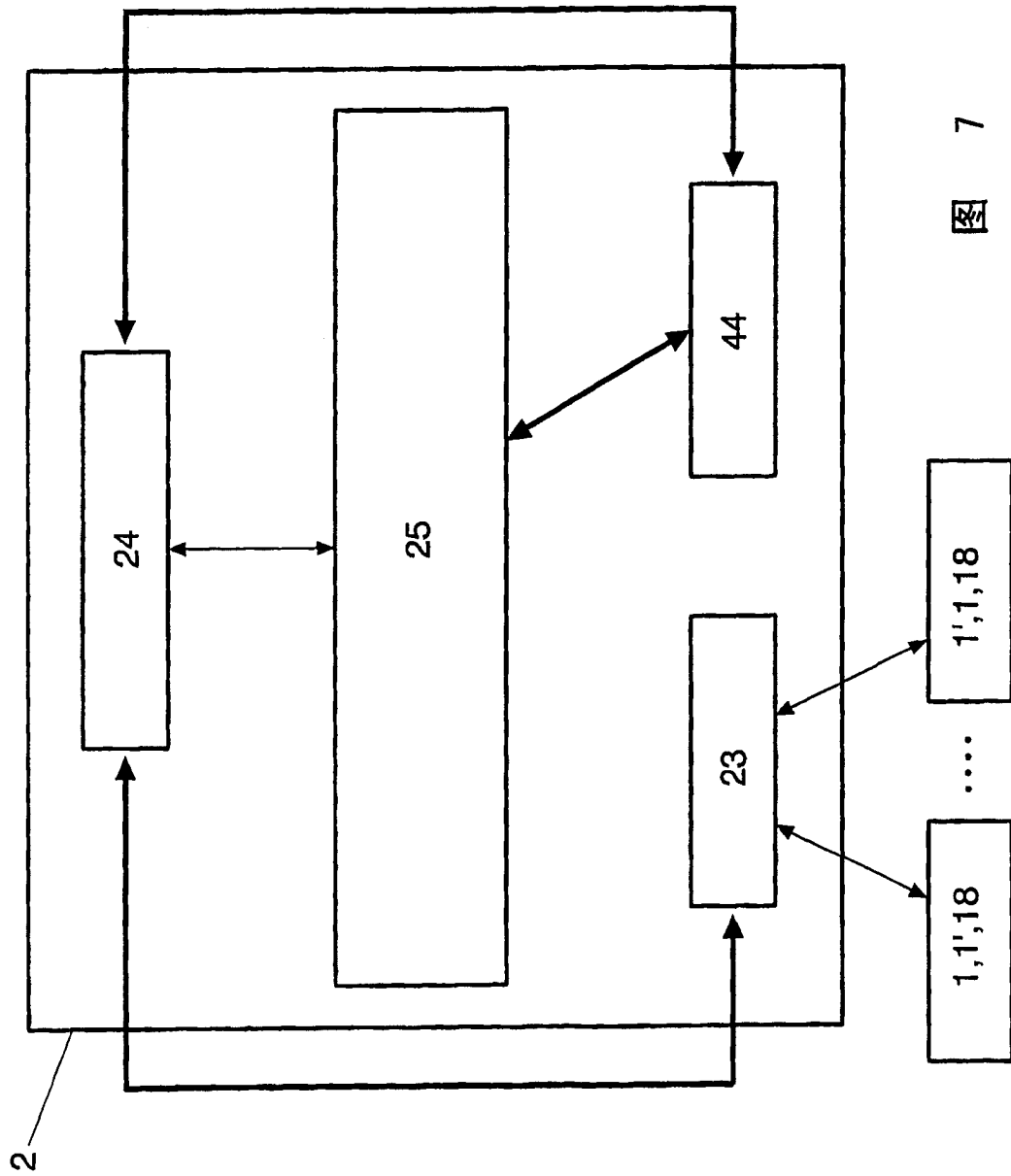


图 7

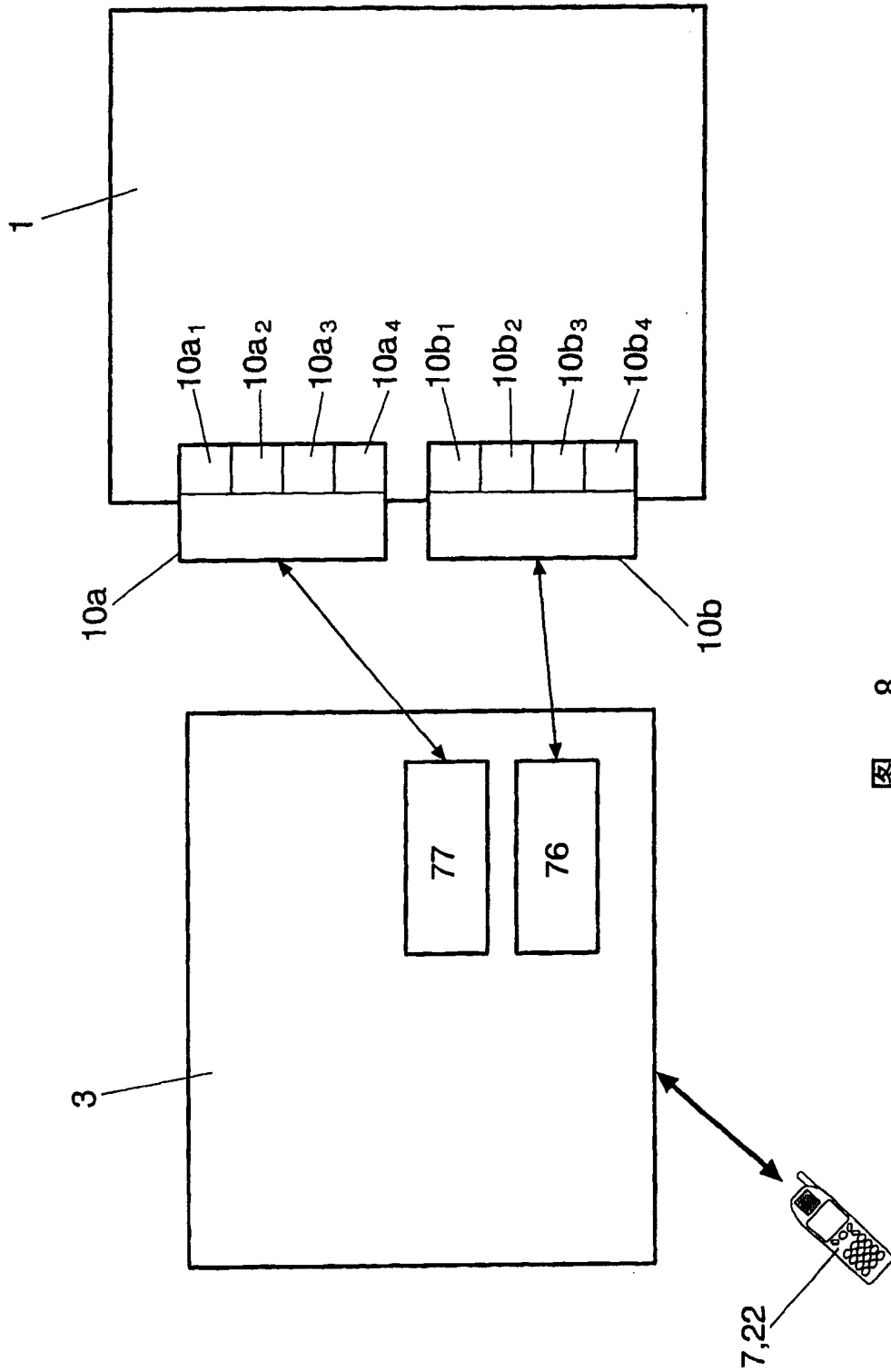


图 8

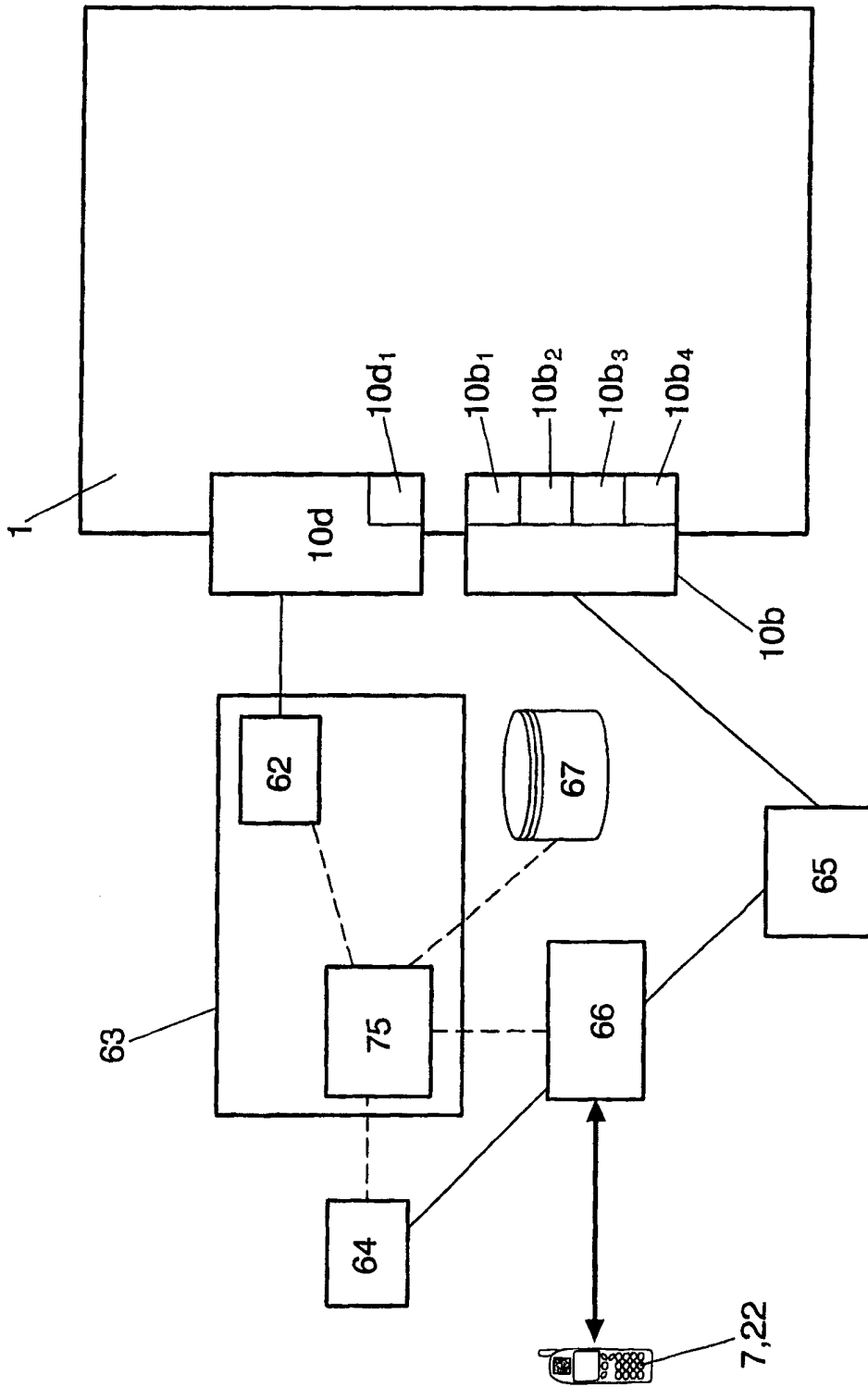


图 9

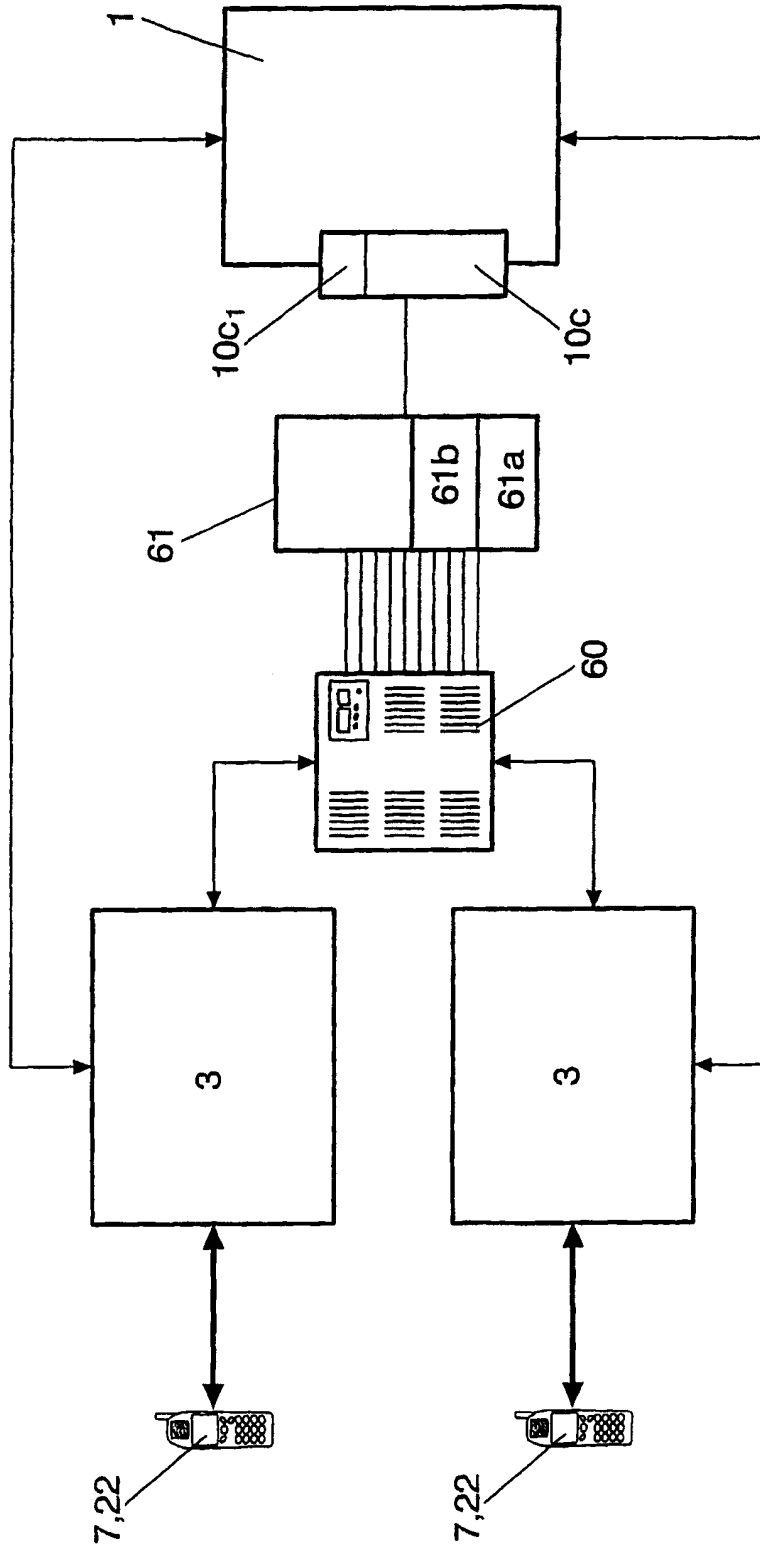


图 10

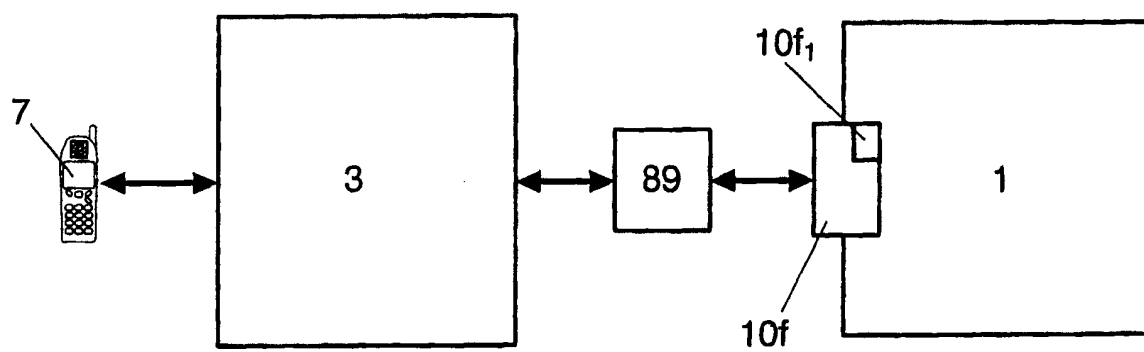


图 11

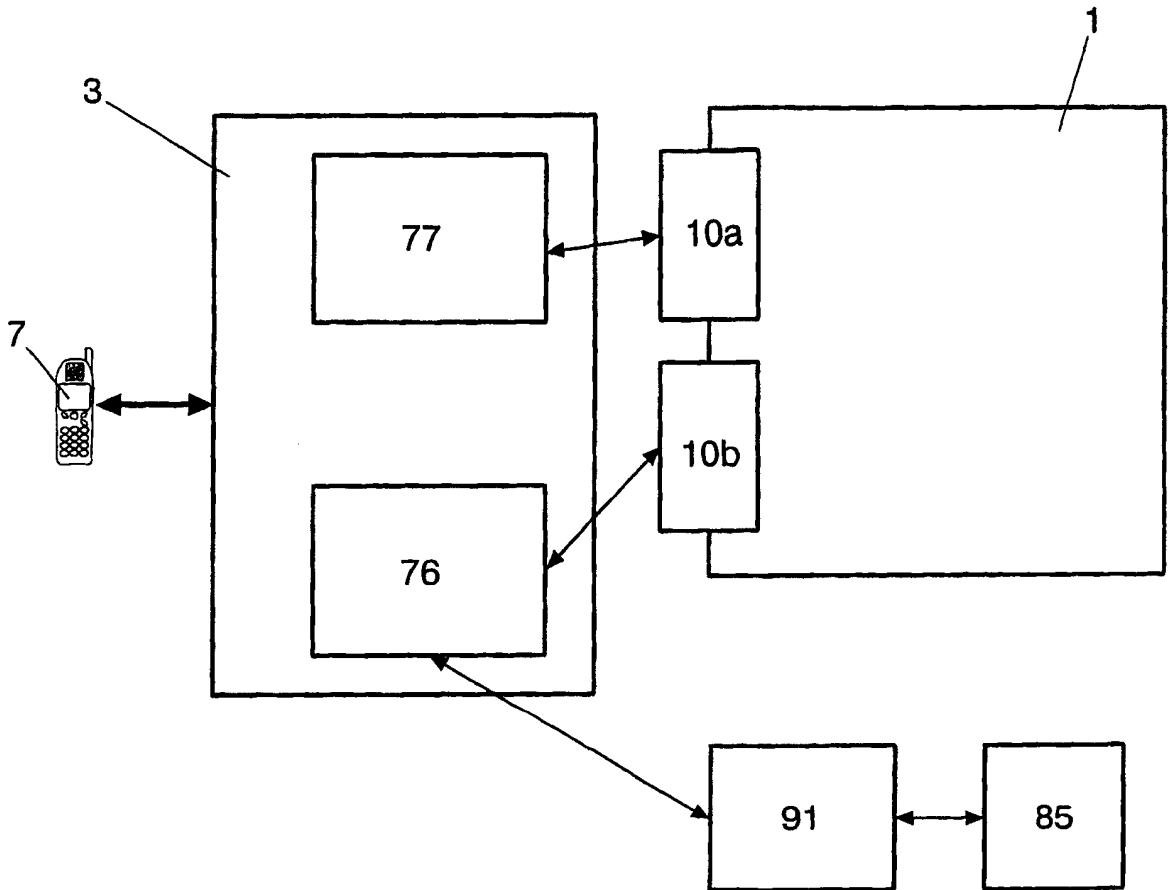


图 12

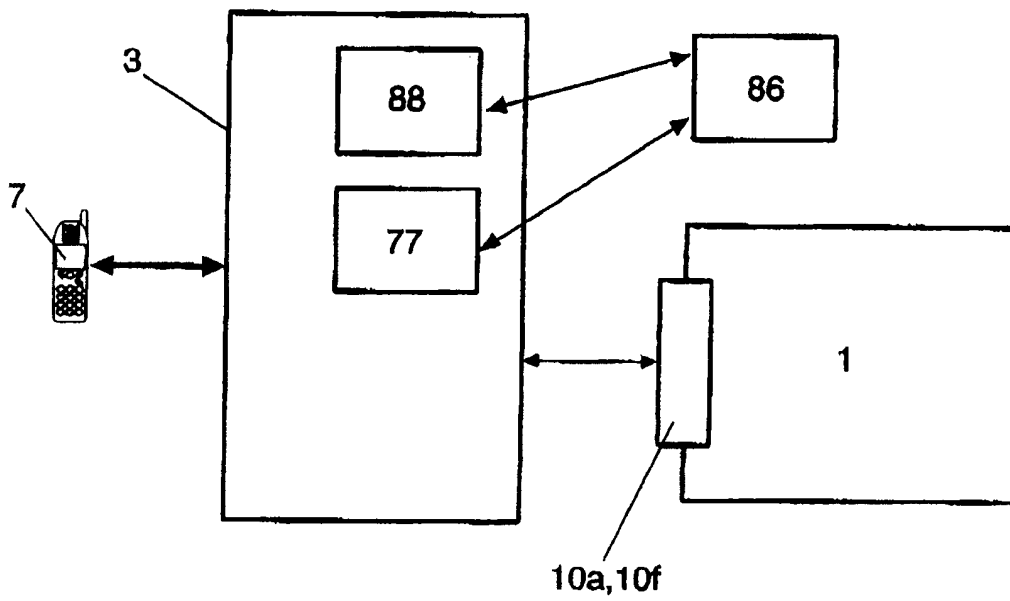


图 13

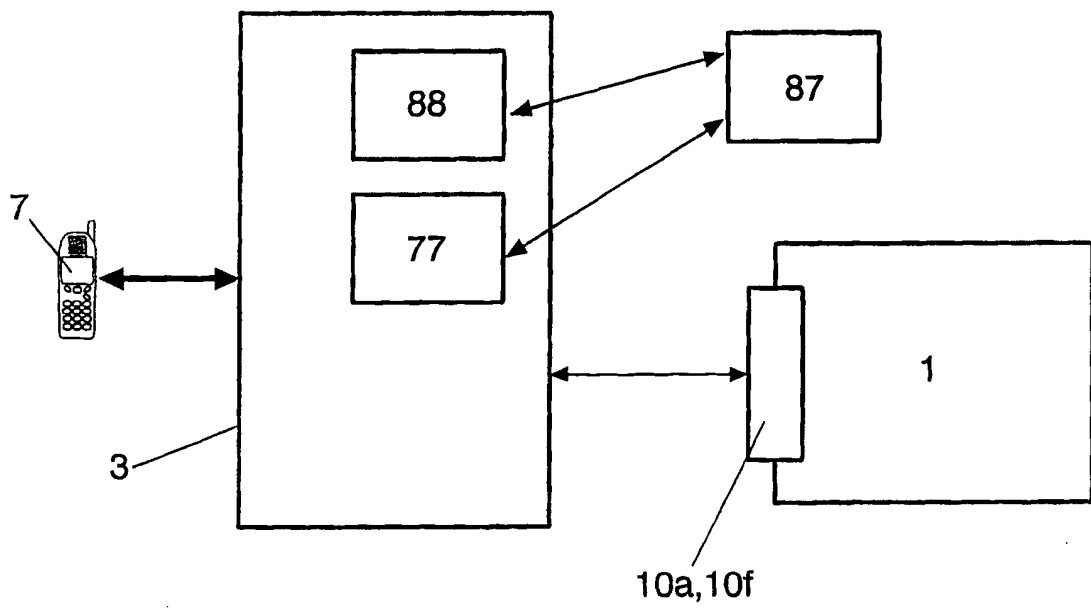


图 14

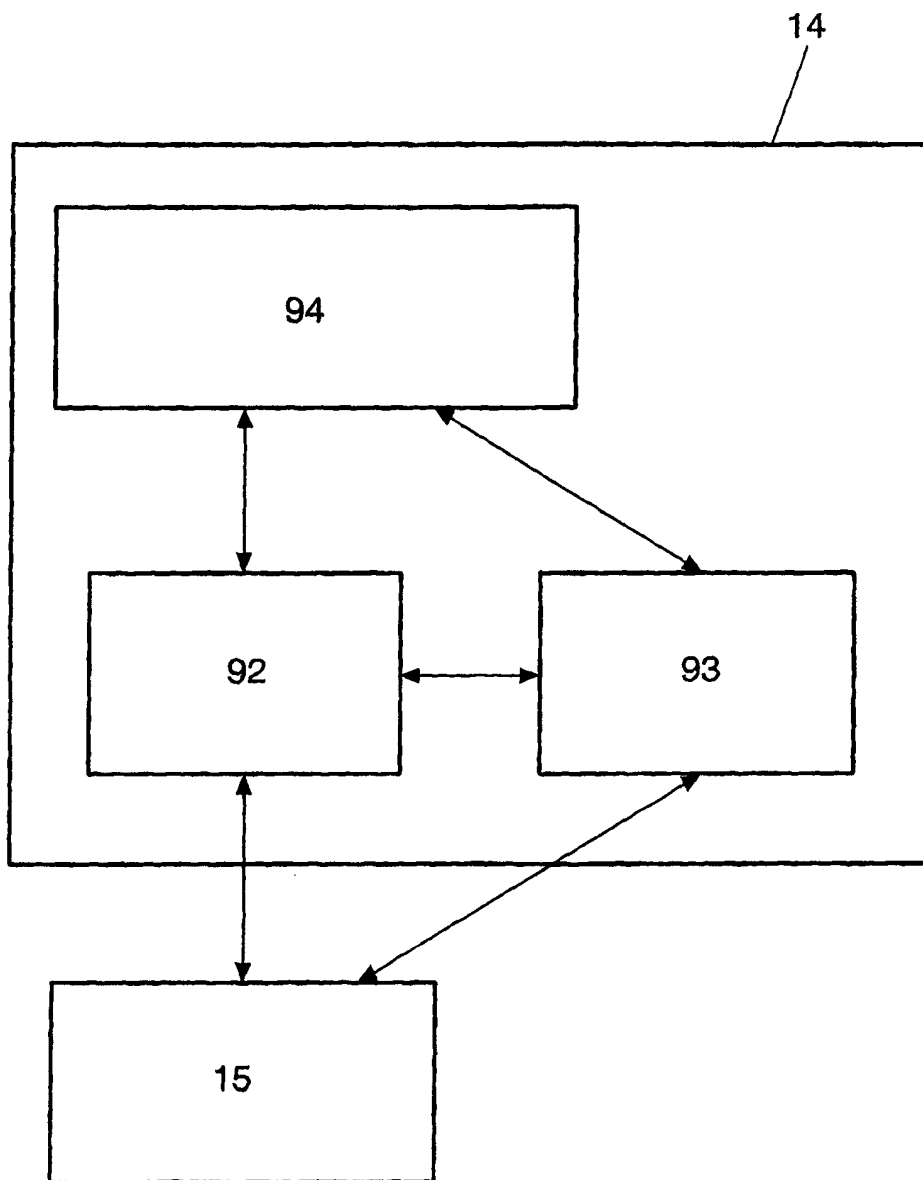


图 15