[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07F 19/00
G07F 7/08 G07F 7/10

[12] 发明专利申请公开说明书

[21] 申请号 02817732.0

[43] 公开日 2004 年 12 月 8 日

[11] 公开号 CN 1554079A

[22] 申请日 2002.7.22 [21] 申请号 02817732.0
[30] 优先权
[32] 2001. 7.26 [33] DE [31] 10136414.8
[86] 国际申请 PCT/EP2002/008163 2002.7.22
[87] 国际公布 WO2003/012701 德 2003.2.13
[85] 进入国家阶段日期 2004.3.10
[71] 申请人 德国捷德有限公司
地址 德国慕尼黑
[72] 发明人 达克·T·武 克里斯琴·福达克
查恩吉兹·谢巴尼

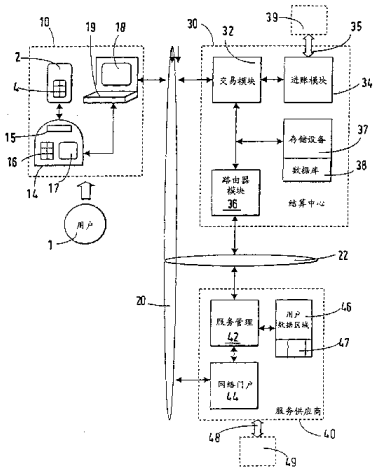
[74] 专利代理机构 北京市柳沈律师事务所
代理人 郭定辉 黄小临

权利要求书 3 页 说明书 16 页 附图 7 页

[54] 发明名称 为借助于数据网络提供的服务付费的方法

[57] 摘要

本发明提出了一种方法，用来针对交易介质(2)的呈现而获取通过数据网络(20)销售的服务。该服务通过用户端系统(10)从服务供应商(40)订购。 该服务供应商呼叫结算中心(30)，该结算中心进入与该交易介质(2)的数据交换，以从该数据介质请求一定数据形式的、获取该服务所要求的必须的进账。 订购过程以及用于请求进账的与交易介质(2)的数据交换通过与该交易介质相关联的标识符(KM)相联系，所述标识符由用户端系统(19)所确定，并且该标识符被用来保护该订购过程与对进账的请求。



ISSN1008-4274

1. 一种针对交易介质的呈现而通过数据网络获取服务供应商所提供的服务的方法，该服务通过用户端系统从该服务供应商订购，该服务供应商就此呼叫结算中心，该结算中心随后进入与该交易介质的数据交换，以从该数据介质请求一定数据形式的、获取该服务所要求的必须的进账，该方法的特征在于：用户端系统（10）在进入用于请求进账的所述数据交换之前，确定与该交易介质（2）相关联的标识符（KM），将该标识符送往该结算中心（30），并且从其接收回该标识符以确认。

2. 如权利要求 1 所述的方法，其特征在于：所使用的该标识符（KM）为也被应用到用于请求进账的随后的数据交换的信息。

3. 如权利要求 1 所述的方法，其特征在于：从该交易介质（2）所请求的进账包括转移待支付的金额。

4. 如权利要求 1 所述的方法，其特征在于：该结算中心（30）在接到该标识符（KM）之后，确定预授权标识符（KV）并且将该预授权标识符（KV）与所述标识符（KM）一起发送给用户端系统（10）。

5. 如权利要求 4 所述的方法，其特征在于：在每个获取过程中单独地形成预授权标识符（KV）。

6. 如权利要求 1 所述的方法，其特征在于：该结算中心（30）监视从接到交易介质（2）的标识符（KM）直到接到用于所述用于请求进账的数据交换的使能信号（B5）的时间。

7. 如权利要求 1 所述的方法，其特征在于：该安全终端（14）监视从发出交易介质（2）的标识符（KM）直到开始所述用于请求进账的数据交换的时间。

8. 如权利要求 1 所述的方法，其特征在于：交易介质（2）的该标识符（KM）被存储在用户端系统（10）。

9. 如权利要求 1 所述的方法，其特征在于：只有当结算中心（30）已经从交易介质（2）收到对服务的请求时，服务供应商（40）才供应一个所请求的服务。

10. 如权利要求 1 所述的方法，其特征在于：在成功实现了用户从交易介质（2）请求进账的数据交换之后发生错误时，从结算中心（30）向用户端

系统（10）传送暂时注入确认（B10），该暂时注入确认包含允许该用户端系统以后对该错误投诉的信息。

11. 如权利要求 1 所述的方法，其特征在于：通过从用户端系统（10）向结算中心（30）所传送的参考信息（RI），来产生所请求的服务与用户（1）的关联。

12. 如权利要求 11 所述的方法，其特征在于：该参考信息（RI）与交易介质（2）的标识符（KM）一起被送回向用户端系统（10）以确认。

13. 如权利要求 1 所述的方法，其特征在于：首先只根据类型产生对来自服务供应商（40）的服务的请求，并且与用户（1）的关联只对于结算中心（30）进行。

14. 如权利要求 1 所述的方法，其特征在于：在获取在程度上可扩展的服务之后，只根据类型从该服务供应商（40）请求所述服务，并且该程度只被传送给该结算中心（30）。

15. 一种结算中心，具有：交易模块，用来进行与用户端系统的数据交换；路由器模块，用来建立与服务供应商的数据链路；以及进账模块，该结算中心的特征在于：在该方法的第一阶段，交易模块（32）取得用户端系统（10）的标识符（KM），并且将该标识符与通过用户端系统（10）所请求的服务供应商（40）的服务相联系，然后在该方法的第二阶段，进账模块（34）使用同一标识符（KM），从用户端系统（10）请求获取该服务所需的交易介质（2）的进账。

16. 如权利要求 15 所述操作结算中心的方法，其特征在于：在从用户端系统（10）收到所请求的进账之后，交易模块（32）请求服务供应商（40）提供所请求的服务。

17. 一种在用于获取通过包括对支付介质的访问的数据网络来销售的服务的方法中、被设计来通过所述数据网络进行防篡改数据交换的安全终端的使用方法，其特征在于：在预协商阶段使用该安全终端以确定交易介质（2）的标识符（KM），并且用该标识符来保护用于订购该服务的过程，同一标识符（KM）被用于随后的交易阶段以保护由交易介质（2）对获取该服务所需的一定数据形式的必须的进账的供给。

18. 一种用来实施权利要求 1 所述方法的联合装置，具有用户端系统、数据网络、结算中心以及服务供应商，该构造的特征在于：结算中心（30）

包含交易模块（32），用来进行服务的订购，以及进账模块（34），用来请求交易介质（2）进行进账。

19. 如权利要求 18 所述的联合装置，其特征在于：用户端系统（10）包括允许对位于交易介质（2）上的标识符（KM）进行确定的安全终端（14）。

20. 如权利要求 18 所述的联合装置，其特征在于：安全终端（14）具有用来存储从交易介质（2）读取的标识符（KM）存储装置。

21. 如权利要求 18 所述的联合装置，其特征在于：结算中心具有用来执行订购过程的功能，以及用来进行用于请求在分离的模块（32，34）中设置的进账的数据交换的功能。

22. 一种安全终端，用于如权利要求 1 所述的方法中，该安全终端具有用来访问交易介质的访问设备，并且通过用户网络接口可被连接到数据网络，该安全终端的特征在于：它具有存储设备，在该存储设备中，该安全终端保存关于将由交易介质(2)进行的进账的信息，以及该交易介质的标识符(KM)。

为借助于数据网络提供的服务付费的方法

本发明开始于根据独立权利要求的方法。此种方法在例如本申请人在2000年出版的小册子“Geldkarte im Netz”中公开。其描述了通过现金卡的方法支付通过因特网订购的服务。在该小册子的第4页显示了支付过程的简化步骤。由此，使用家用计算机来通过因特网从服务供应商（例如信息服务或者在线商店）订购服务。然后，该服务供应商转到支付中心，在那里启动执行支付过程。现在该支付中心通过因特网建立与该现金卡，家用计算机以及与其连接的读卡器的连接，并且向所述卡支取待支付的所需金额。然后，支付中心向该服务供应商确认支付成功，该供应商最终提供所请求的服务。

对于涉及从现金卡到支付中心转移待支付的金额，即从交易介质到结算中心转移取得服务所需的进账（contribution）的实际交易阶段，该公知的方法是安全的。然而，该方法不能保护在交易阶段之前的订购过程。由服务供应商提供的服务确实是用户所订购的，以及随后所转移的金额符合先前所同意的金额，必须在用户与服务供应商之间分别确定。如果不采取保护措施，对订购/供应过程的攻击可以包括（例如）服务供应商所提供的服务使攻击者而不是原先的顾客受益。

保护订购过程的技术基本是公知的。一个已被试用的方法是（例如）对数据交换的加密。然而，公知的技术全是独立孤岛解决方案（independent island solution），尤其使得服务供应商必须对可在用户侧采用的每一孤岛解决方案保持互补的对等物可用。

因此本发明的问题是制定一种方法，用来获取在数据网络上销售的服务，其中已经保护了订购过程，而对所使用的系统组件没有任何附加的需求。

该问题由具有独立权利要求的技术特征的方法所克服。该创新方法具有以下优点：只使用为进行交易阶段而必须已经具有的系统组件，就可以实现该方法。因为订购过程通过使用从随后的交易阶段所抽取的、并且与所使用的交易介质密切相关的标识符而受到了保护，所以订购过程与随后的进账过程被平滑地联系起来。如果需要的话，可以以后使用该标识符，以唯一地证明订购过程与交易阶段的关系。用户端系统的设计允许按需要来调整安全级

别。使用集成到整个系统中的、并且不是以独立单元实现的交易介质允许调整中等安全级别。如果安全终端的功能被进一步被集成到用户网络接口中，则所产生的实施例具有低一些的安全级别，但性价比很高，并且可以由（例如）常规 PC 所实现。不管在用户端系统中实现的安全级别为何，结算中心可以总是具有同样的结构。整个方法可以以匿名方式实施。本创新方法尤其适用于向服务供应商处的专用账户注入资金，例如用来注入电话公司处的预付费账户。在订购与进账过程中使用唯一指定交易介质的标识符使之可能在出错的情况下不用立即撤消交易，而是提供使用交易介质的标识符、对方法实施的随后的改正措施。将获取过程和与交易介质紧密相关的标识符进行耦合给服务供应商提供了在反复获取服务的情况下识别交易介质的可能性。

在从属权利要求中陈述的措施指出了本创新方法的优选实施例与适宜的改进。

优选地，结算中心在收到交易介质的标识符后，进而生成允许整个获取过程以后被唯一地关联到交易介质与结算中心的标识符。

为进一步提高订购过程的安全，优选地，对各个方法步骤之间的时间进行监视，如果超过了预定的最大时间，则终止订购过程。这样的超时监视还尤其防止了攻击者切入订购过程。

在本创新方法的适宜的改进中，交易介质的标识符与结算中心的标识符被记录在用户系统与结算中心自身之中。

在本创新方法的非常优选的实现中，用户首先根据类型，从服务供应商请求所需的服务，例如向电话公司处的特定的预付费账户注入资金。然后，该用户只向结算中心指定所需服务的接受方与程度。该结构允许用户总是与服务供应商联系，而服务供应商自己不需要采取任何进一步保护订购过程的措施。

适宜地，通过在用户端系统上输入参考信息（reference information）并传送到结算中心，所需的服务被与客户相关联。

下问将参照附图，更详细的描述本发明的实施例，其中

图 1 显示适合于执行所提方法的系统的结构。

图 2 到 7 显示在这样一个系统上所提方法的执行的流程图。

图 1 描绘了用来通过数据网络获取服务的系统的结构。该系统包括用户端系统 10，其通过第一数据网络 20 与结算中心 30 和服务供应商 40 连接。

另外，结算中心 30 与服务供应商 40 通过第二数据网络 22 互连。第二数据网络 22 可以被形成为分离的数据网络，或者就在第一数据网络 20 之内。为清楚起见，网络用户 10、30 与 40 每个都画出一个，然而在实践中它们每一个都可以出现多次。一般地，数据网络 20 已经连接到多个用户端系统 10 与多个服务供应商 40。另外，数据网络 20 一般已经连接到多个结算中心 30。多个结算中心 30 的每一个都可以通过一个或更多个第二数据网络 22 与多个服务供应商连接。

通过提供一定的数据（为了获取服务假定拥有该数据），用户端系统 10 允许用户 1 确定、订购并且进账待通过数据网络 20 订购的服务。在内部，其结构包括交易介质 2，被构成以与交易介质 2 通信的安全终端 14，以及用户网络接口 19，该网络接口首先与安全终端 14 连接，其次与数据网络 20 连接。结构组件 2、14、19 的物理分离取决于所选取的安全级别。对于最高安全，组件 2、14、19 每一个都形成为独立的单元，而在中等安全级别，用户网络接口 19 与安全终端 14 实现为独立的单元，而交易介质 2 只以虚拟的形式存在，即作为软件解决方案。在低安全要求的情况下，所有组件 2、14、19 也可以在一个公共单元中实现。

交易介质 2 使用户 1 能够从服务供应商 40 获取通过数据网络 20 销售的服务，该供应商假定由交易介质 2 提供进账。这允许实行交易，对此假定拥有一定的数据，其中在安全终端 14 与另一网络用户 30、40 之间交换敏感数据与信息。例如，这允许通过以下方式将待支付的金额转移到受款人的现金账户：从交易介质 2 直接移除以电子形式存在的金钱，或者不可撤回地，间接使待支付的金额从与交易介质 2 相关联的现金账户中转移。交易介质 2 的安全效果基于其在特殊设计的介质上安全地保有敏感数据，该介质最好是独立的单元。

交易介质 2 具有存储数据的防篡改存储设备 4，为了获取服务假定具有该数据。这样的数据可以是（例如）电子形式的金钱或者允许直接访问在外部设备中保存的现金账户的数据。另外，存储设备 4 可以保存其重要性只在于其所表示的信息的数据，例如加密密钥或者访问代码。该同一交易介质 2 也可以在其中并列设置支付与获取信息方法。交易介质 2 还与各自的标识符 KM 相关联，该标识符适宜于在存储设备 4 中保存在交易介质 2 上。另外，标识符 KM 也可以存储在用户端系统 10 或者通过数据网络 20 连接的网络用

户的另一存储设备中。所使用的标识符 KM 为在通过交易介质 2 的预协商阶段的实现之后在进账阶段的实现的过程中所使用的信息。

为了确保最高的安全，交易介质 2 最好实现为独立的单元。在适宜的实现中，交易介质 2 采用的形式为信用卡形式的便携式数据载体；具体地说，交易介质 2 可以是芯片卡。在后一种实现中，存储设备 4 在该卡的芯片中实现，并且表示（例如）电子金钱或者访问代码的为获取服务而呈现的数据，以及标识符 KM 位于该芯片卡内。

如果安全需求不是很高，可以不采用作为独立单元的实现，而只以虚拟的形式实现交易介质，例如作为安全终端 14 中、在用户网络接口 19 中和/或在通过数据网络 20 连接的网络用户中的软件解决方案。然后，（例如）在访问代码（例如由用户 1 输入的 PIN 或者 TAN（交易号））的帮助下调用它。交易介质 2 也可以通过多个由标识符 KM 互连的独立的分布组件的交互来形成。例如，它可以包括其上保存了标识符 KM 的便携式数据载体以及附属用户设备 4，其实现为用户端系统 10 中或者通过数据网络 20 连接的网络用户中的软件解决方案。

安全终端 14 首先响应交易介质 2，并且允许对存储在存储设备 4 内的数据的访问。其次，安全终端 14 形成安全端到端连接的用户系统端。在此功能中，安全终端 2 检查并保护在通过数据网络 20 获取服务的方法的过程中的所有数据交换，并且包含了所需的装置。具体地说，它保护预协商阶段，提供确认或者错误消息，并且记录所进行的具体的数据交换。

安全终端 14 的核心构件为处理器装置，其被设计来建立在交易介质 2 与结算中心 30 之间安全的端到端连接，即该连接的安全性只由交易中所涉及的终端来实现，并且使用所述安全连接来进行在包括用户 1 时在交易介质 2 与结算中心 30 之间的数据移动。为此目的，安全终端 14 具有访问设备 15，该设备允许安全终端 14 访问存储在交易介质 2 上的数据与标识符 KM。优选地，访问设备 15 对于位于交易介质 2 上的数据允许写与读访问，即既从交易介质 2 上移除数据所表示的内容，也相反地向交易介质施加数据所表示的内容。安全终端 14 还具有输入装置 16，最好为键盘的形式，以由用户 1 向安全终端 14 传送信息，以及输出装置 17，适宜为显示器形式，以由安全终端 14 向用户传送信息。

安全终端 14 为防篡改设计，以防止未授权的交易介质 2 的数据（例如表

示金钱值）的数据移除，或者用户 1 生成的这样的数据。为此目的，访问设备 15、输入装置 16 以及输出装置 17 每个都是防篡改设计，并且与处理器装置连接以形成单元，从而对组件 15、16、17 之一的硬件或软件攻击只有通过毁坏它才有可能，或者至少只能以立即可见的方式才能实现。为了确保在交易中传送的数据的安全，处理器设备包括用来加密外出数据和解密进入数据的装置，以及用来验证从交易方收到的证书的装置。

如果交易介质 2 实现为芯片卡，则安全终端 14 适宜为所谓的 3 类芯片卡阅读器，即具有芯片卡阅读器形式的访问设备 15，独立的防篡改键盘，用来在传送到芯片卡之前显示安全相关数据的防篡改字母数字显示器，以及加密软件的设备。

如果用户端数据 10 的所需安全使之不必以防篡改的方式将输入与输出装置链接到处理器装置，则安全终端 14 也可以实现为用户网络接口 19 的有机部件。在这种情况下，其不具有任何独立的输入与输出装置，但使用由用户网络接口 19 所提供的输入与输出装置。此处，安全终端 14 的功能可以实现为具有独立的处理器装置的硬件滑入型模块（slide-in module），或者使用用户网络接口 19 的处理器装置的纯软件解决方案的形式。

用户网络接口 19 为允许用户 1 通过数据网络 20 与结算中心 30 或服务供应商 40 交互地进行联系的设备。用户网络接口 19 的基础为具备所有一般结构特征的计算机。具体地说，用户网络接口 19 具有输入输出设备 18，其含显示装置，例如以图像显示器的形式，用来显示传送到用户网络接口 19 的信息，以及输入装置，例如以小键盘的形式，其允许用户 1 传送信息给连接到数据网络 20 的网络用户 30、40。另外，用户网络接口 19 包括数据网络 20 的双向接口。用户网络接口 19 的处理器装置被准备用来通过数据网络 20 获得信息与程序构件，并且应用或执行它们。用户网络接口 19 的典型实施例为家用计算机。然而，用户网络接口 19 也可以由如在网吧中所使用的公开访问的网络终端来实现，或者由相应配置的手机来实现。

数据网络 20 最好为因特网。在这种情况下，网络用户 10、30、40 被相应地组织为因特网用户，并且具有适合于以本领域公知的方法应用到所述网络的技术规范的结构。然而，数据网络 20 也可以由适合于构造在多个网络用户 10、30、40 之间的数据或通信链接的任何其他网络结构来实现。数据网络 20 可以包括物理上不同的形式的多个网络的互连。例如，用户端系统 10 可

以借助移动无线网络运营商通过移动无线网络与固定网络进行链接。

结算中心 30 一般的形式为大型计算机，具有很强的计算能力，在其上以软件模块的形式实现用于执行涉及敏感数据交换的交易的功能。结算中心 30 一般位于服务供应商一侧，其专用于处理通过数据网络进行的交易，并且只可被有限的经特殊授权的人群所访问。在实际的实施例中，结算中心 30 为支付中心，并且用来处理通过数据网络 20（尤其是因特网）的支付过程。

结算中心 30 的必要构件为交易模块 32，与其相连的进账模块 34，以及与所述两个模块连接的路由器模块 36。结算中心 30 的重要的硬件构件为存储设备 37。

交易模块 32 包括用来控制通过数据网络 20 与用户端系统 10 以及通过第二数据网络 22 与结算中心 40 的数据交换的装置，用来执行并保护订购过程的装置，以及用来引起服务供应的装置。

进账模块 34 用来协调并处理安全数据交换，以通过与交易介质 2 借助附属安全终端 14 的交互，请求从交易介质 2 所需要的进账，例如用来执行支付处理，并且具有为此所需的所有程序与硬件装置。其进一步协调不同的并行获取过程的处理。进账模块 34 还具有到后台系统 39 的接口 35，在该后台系统上执行与施行服务获取方法有关的、而其不可能或不方便由结算中心 30 施行的必须的后台处理。这种后台处理例如为对现金账户的保存，以及对不同现金账户之间的交易的处理。典型的后台系统 39 相应地为保存与交易介质 2 以及与结算中心 30 相关联的现金账户的银行或者银行联合体，或者结算中心。

路由器模块 36 管理在交易模块 32 与结算中心 40 之间通过第二数据网络 22 的数据交换。

存储设备 37 包括数据库 38，用来接收支付介质 2 的标识符 KM 以及在获取处理过程中与标识符 KM 相关使用的会话密钥 RS，SS。存储设备 37 还在其中存储了结算中心 30 的公开密钥 OS，以及相应的私有密钥 GS，用来执行通过数据网络 20 的安全通信。

服务供应商 40 对于数据网络 20 为网络用户，就像用户端系统 10 或者结算中心 30 一样。一般它的形式为高能计算机，在运营商的控制下，其上的服务以软件的形式可用，用户 1 可以通过数据网络 20 访问这些服务。在技术上，服务供应商 40 可以由联网的计算机群来实现，该机群只是在逻辑上表现得与

一个网络用户一样。

服务供应商 40 所提供的服务基本上可以是可以通过数据网络 20 销售的任意种类的商品或服务，例如款到送货的诸如软件程序的数字商品，款到送货的物理上存在的消费品，或者见到作为接收方证明的证据例如 PIN（个人标识号码）才送货的数字商品。所提出的方法尤其适用于服务供应商 40 所提供的服务，其中用户 1 不用能够直接检查提供。因此，该方法适合于（例如）基于预付费的信用，对移动无线供应商的移动无线网络的使用。除了实际供应服务，所提出的方法还支持在服务供应商与用户 1 之间长期的联系，这是因为它诱导户 1 转向服务供应商 40。

对于此处所描述的方法来说，服务供应商 40 的必要结构构件为服务管理设备 42，用户数据区域 46 以及网络门户 44。

对于传送给用户 1 的、根据其可以从服务供应商 40 订购服务的每一条参考信息 RI，服务管理设备 42 在用户数据区域 46 中保存参考文件 47。参考文件 47 最好是专用的，并且只允许对于一个或者一组所规定的服务的交易。在实践中，它们可以用来（例如）保存有关还未被服务供应商所提供的服务的信用。与还未提供的款到送货的服务相关，参考文件 47 具有存款账户的功能。在这种情况下，适宜规定只有在用于其付款的存款账户 47 具有足够的资金时，才提供服务。

网络门户 44 被用来建立服务供应商 40 与用户端信息 10 之间的首次联系。其通知用户 1 有关服务供应商 40 以及服务供应商 40 所提供的服务的情况，并且给出用于对所需服务进行支付的指令。为此目的，其包括软件形式的数据包，该数据包当被调用时通过数据网络 20 传送给用户端系统 10，并且被显示给那里的用户 1。如果数据网络 20 为因特网，则网络门户 44 具有因特网存在物的通常的形式，并且如同这样的存在物一样可被用户 1 访问。

网络门户 44 还使具有信息与程序构件的数据包可用于执行获取过程。此后被称为注入小应用程序 LA 的所述数据包可以存储于服务供应商 40 自身或者存储于与其相连的网络用户，具体地是在结算中心 30 中。在后一种情况下，网络门户 44 保存并且传送指向存储器的特定位置的参考（reference）。注入小应用程序 LA 指定结算中心 30，通过该结算中心可以获取所选的服务。另外，每个注入小应用程序 LA 都包含程序构件，这些程序构件使用户端系统 10 能够通过结算中心 30 执行订购以及相关的支付过程。注入小应用程序 LA

可以通过数据网络 20 传送给用户端系统 10。

服务供应商 40 还具有借助接口 48 的到后台系统 49 的连接，在该后台系统上执行与施行服务获取方法有关的、而其不可能或不方便由服务供应商 40 施行的必须的后台处理。这种后台处理具体地包括对现金账户的保存，以及进行不同现金账户之间的金钱转移。相应地，后台系统 49 由（例如）保存与服务供应商 40 相关联的现金账户的银行、银行联合体、或者结算中心所形成。后台系统 49 与后台系统 39 相连，并且也可以完全相同。

结算中心 30 与服务供应商 40 可以进一步重叠，并且以一个网络用户的形式实现。类似地，后台系统 39、49 可以是结算中心 30 或者服务供应商 40 的集成部件。具有结算中心 30、服务供应商 40 以及后台系统 39、49 的功能的网络用户的例子为银行。

下面将参照图 2 至 7，描述使用上述系统通过网络获取服务。

所使用的方法大体分为预协商阶段与交易阶段，后者进而分为进账阶段与供应阶段。预协商阶段与进账阶段进行于用户端系统 10、具体为安全终端 14 与交易介质 2，与结算中心 30 之间；供应阶段的进行包括服务供应商 40。在预协商阶段，使用标识符 KM 订购服务，在进账阶段，作为供应服务的条件，使用标识符 KM，请求由支付介质 2 进行进账，并且在供应阶段，使该服务可用于向用户 1 供应。

为了将该方法描述的更加清楚，此后将大致规定服务供应商 40 为移动网络运营商，并且用户 1 希望通过现金卡借助用户端系统 10 来对移动无线网络运营商 40 所保存的网络时间信用账户（network time credit account）注入（load）资金，以继续能够使用手机。在这中方案中，参考文件 47 作为网络时间信用账户，服务管理设备 42 作为账户管理单元出现，交易介质 2 作为现金卡；由服务供应商 40 所提供的服务是使其网络可以在限定的时间内可用。交易介质 2 为了获取该服务而必须作出的进账通过以下方式进行：从现金卡 2 向与移动无线网络运营商相关联的现金账户转移电子金钱。

该方法并不局限于上述的示范性应用。只要对通过数据网络 20 销售的服务的获取是通过以下方式实现的，都可以使用该方法：使用与交易介质 2 相关联的标识符 KM，连续地执行开始的订购过程以及随后的交易过程。此种类型的另一应用为（例如）对信息的获取，该信息基本免费但却必须安全，例如 PIN，其随后允许访问其他情况下被阻塞的服务供应商 30 所提供的服务。

该方法的使用开始于用户 1 借助用户端系统 10 通过网络连接到服务供应商 40 的网络门户 44，以浏览网络门户 44 在其上提供的信息服务，并且从信息服务中选择选项“预付费账户注资”(步骤 200)。跟着该选择，服务供应商 40 的网络门户 44 向用户端系统 10 发送开始数据块，该数据块包含有关待选择的结算中心、所支持的支付模式、可能需要用来处理投诉的联系地址 AD 以及注入小应用程序（load applet）LA 或者指向其在存储器中的位置的参考的数据，这使安全终端 14 将被包含在获取过程中，并使所需的信息将被用户 1 输入(步骤 202)。步骤 202 最后以安全模式进行，该模式可以直接由数据交换所涉及的双方直接使用，例如通过根据 SSL 协议的加密。

当已经收到注入小应用程序 LA，并且已经将其安装到用户网络接口 19 中时，它通过数据网络 20 建立与在开始数据块中所指定的结算中心 30 的连接。

如果服务供应商 40 所提供的服务是提供个人信息，则在该连接建立后，注入小应用程序适宜于首先促成在用户 1 与结算中心 30 之间的相互认证(步骤 203)。用户 1 与结算中心由此通过检查对方对预定秘密的知识而相互证明其真实性。在用户一侧，该秘密可以是（例如）待输入的 PIN，或者它可以存储在签名卡上，该签名卡适宜于通过安全终端 14 可读，并且从该签名卡读取该秘密。

当已经建立了与结算中心 30 的连接并且证明了真实性时，如果需要此步骤，则注入小应用程序开始预协商阶段。为此目的，它在输入输出设备 18 上生成显示，步骤 204 要求用户 1 指定支付模式与所需的注入金额 LE。用户 1 使用输入输出设备 18 的输入装置提供所需的数据。当该输入完成时，注入小应用程序 LA 生成注入消息 B1，该消息包含所选择的支付模式，所指定的注入金额 LS，以及投诉联系地址(步骤 206)。

如果支付介质 2 未实现为物理上独立的单元，则注入小应用程序还生成用于支付介质 2 的单独的标识符 KM。

注入消息 B1 由注入小应用程序 LA 发送给安全终端 14(步骤 208)。

在安全终端 14 接收到注入消息 B1 之后，前者检查交易介质 2 对访问设备 15 是否可访问。如果不可访问，则安全终端 14 向用户网络接口 19 发送确认，使其在输入输出设备 18 的显示装置上显示请求，请求用户 1 向访问设备 15 提供交易介质 2。如果交易介质 2 只是被虚拟地实现，则用户 1 通过输入

输出设备 18 得到请求，请求使其可被相应的输入访问。

当提供了交易介质 2 并且对其的访问也是可能的时，安全终端 14 通过访问设备 15 从交易介质 2 请求其各自的标识符 KM(步骤 210)。此时交易介质 2 将其各自的标识符 KM 发送给安全终端 14(步骤 212)。

如果施行此方法而交易介质 2 在物理上不存在，则安全终端 14 通过注入小应用程序 LA 取得在步骤 208 发送的消息中的标识符 KM。此处，注入小应用程序 LA 可以直接构成标识符 KM。其也可以仅作为中间方，并且在独立的数据交互中通过数据网络 20，例如从结算中心 30 取得标识符 KM。还可以规定标识符 KM 在安全终端 14 的输出装置上向用户显示，并且必须被用户确认。

标识符 KM 与用户 1 所指定的注入金额 LS 由安全终端 14 存储，以在该方法的随后过程中进一步使用(步骤 214)。另外，安全终端 14 生成会话密钥 SK(步骤 216)。会话密钥 SK 由常规方法生成，一般为基于随机数生成的方法。交易介质 2（例如）也可以被包括在其中，并且提供随机数。类似于标识符 KM 的存储，会话密钥 SK 由安全终端 14 存储，以备进一步方法使用(步骤 218)。

然后，通过输出装置 17 上的相应的显示，安全终端 14 请求用户 1 输入参考信息 RI，该信息指定了用户 1 对服务提供商的承诺(步骤 300)。在假设的向移动无线网络运营商处的预付费的网络时间账户注入资金的方案中，参考信息 RI 包括（例如）相关联的手机的电话号码。为了取得最高的安全性，适宜于规定用户 1 通过重复该输入来确认参考信息 RI。

当这时用户 1 所输入的参考信息 RI 可用时，安全终端 14 生成第一预协商消息 B2。为此目的，其构成包含以下内容的信息块：参考信息 RI、会话密钥 SK、标识符 KM 以及注入金额 LS，并且用结算中心 30 的公开密钥 OS 将此信息块加密(步骤 302)。结算中心 30 的公开密钥 OS 可以是已经在开始数据块内传送来的，该数据块在开始联系时从网络门户 44 取得。可替换地，可以提供分离的方法步骤，通过该步骤安全终端 14 从结算中心 30 请求后者的公开密钥 OS。

此时存在并且由加密保护的预协商消息 B2 通过数据网络 20 传送给注入小应用程序 LA 所指定的结算中心 30(步骤 304)。一旦接到消息 B2，安全终端 14 同时启动时间监视(步骤 305)。由此规定一个或更多个时间段，在这些时间段内一或更多条预定的消息必定已经由结算中心接收。如果时间段过期

而所期望的消息没有收到，则中止该方法。监视涉及（例如）直到第二预协商消息 B5 的接收和/或直到支付过程的开始的时间段。

在收到它之后，结算中心 30 用对应于用于加密的公开密钥 OS 的私有密钥 GS 解密安全的预协商消息 B2，并且确定交易介质的标识符 KM 以及会话密钥 SK(步骤 306)。同时，结算中心 30 进而类似地开始时间监视(步骤 307)。它监视（例如）直到使能信号 B6 的接收的时间段。

现在步骤 308，结算中心 30 检查标识符 KM 是否已经被存储在其数据库 38 中(步骤 308)。如果如此，则结算中心 30 检查与同一标识符 KM 相关地最后一次存储的会话密钥 RS 是否仍然有效(步骤 310)。每一个会话密钥 SS 都有与其相关联的预定的有效期。如果该期限没有过期，则结算中心 30 借助查询 B3 通过数据网络 20 从安全终端 14 请求存储在那里的最后一次的有效会话密钥 PS(步骤 402)。查询 B3 用所传送的会话密钥 SK 加密保护。

另外，结算中心 30 将所传送的参考信息 RI、所传送的注入金额以及标识符拿来给存储设备 37(步骤 316)。

如果在步骤 308 的检查发现所传送的标识符 KM 还没有被包含其中，则结算中心 30 将其拿来作为新的项输入数据库 38(步骤 309)。

如果在步骤 310 的检查发现因为有效期已过，与同一标识符 KM 相关地最后一次存储的会话密钥 RS 不再有效，则结算中心 30 将所传送的会话密钥 SK 作为新的有效会话密钥 SS，并且将其拿来输入其存储设备 37(步骤 314)。

安全终端 14 接收查询 B3，并且将其用会话密钥 SK 解密（步骤 403）。然后其进而构成安全的响应 B4，该响应包含交易介质 2 的标识符 KM，以及在先前最后一次支付过程中所使用的会话密钥 PS（步骤 406）。通过用结算中心 30 的公开密钥 OS 加密进行保护。这样保护的响应 B4 由安全终端 14 传送给结算中心 30（步骤 408）。

后者在接收后用对应于在加密时所使用的公开密钥 OS 的其私有密钥 GS 解密安全的响应 B4。得自解密的先前的会话密钥 PS 进而由结算中心 30 与所存储的会话密钥 RS 进行比较（步骤 412）。

如果二者不匹配，则结算中心 30 向安全终端 14 传送错误信息，并且中止与安全终端 14 的通信（步骤 413）。也可以规定进行所述中止而没有错误消息。

如果在步骤 412 的检查发现所比较的会话密钥 PS 与 RS 的匹配，则结算

中心 30 规定已经被存储的先前的会话密钥 PS 为新的有效会话密钥 SS（步骤 414）。

在下一步，结算中心 30 生成预授权标识符 KV（步骤 500）。预授权标识符被用做交易的特有标识。其被结算中心所存储，并且以后在预协商与进账阶段结束之后在出现错误时支持有关所述阶段的成功执行的证据。预授权标识符 KV 适宜通过执行以后的可重构算法（reconstructible algorithm）而取得。在非常简单的方法中，该预授权标识符为连续的数字。

然后使用预授权标识符 KV，其可以构成第二预协商消息 B5。为此目的，结算中心 30 连接预授权标识符 KV 与为标识符 KM 的所存储的信息、注入金额以及参考信息 RI，由结算中心 30 的私有密钥 GS 对该信息组签名，并且还用会话密钥 SS 对其加密（步骤 502）。结果的第二预协商消息 B5 由结算中心 30 通过数据网络 20 传送给安全终端 14（步骤 504）。

后者使用会话密钥 SS 解密第二预协商消息 B5（步骤 505），并且使用结算中心 30 的公开密钥 OS 检查签名（步骤 506）。另外，它还通过其时间监视检查预协商消息 B5 是否在许可的时间段内被接收（步骤 507）。然后，解密后出现的参考信息 RI 与注入金额 LS 的表示由安全终端 13 与先前存储的相对应的信息进行比较（步骤 508）。如果该比较发现所比较的信息中有一处或多处不匹配，则安全终端 14 在不用任何进一步确认的情况下，就中止与结算中心 30 的通信（步骤 509）。

如果在步骤 508 中的比较发现所有被比较信息的匹配，则安全终端 14 在输出装置 17 上显示参考信息 RI 与注入金额 LS，并且请求用户 1 通过输入设备 16 确认（步骤 510）。然后，借助安全终端 14 的输入装置 16，用户 1 确认该数据（步骤 512）。

当用户已经作出确认时，安全终端 14 生成使能信息 B6，并将其送往结算中心 30（步骤 514）。

结算中心 30 进一步生成有送往安全终端 14 的所有数据与信息的协议 PA。其将协议 PA 传送给安全终端 14，安全终端 14 检查该协议，并且可选地添加存在于安全终端 14 中的其他信息（步骤 516）。然后，协议 PA 具体地包括预授权标识符 KV 与结算中心 30 的签名。这样被完成后，其由安全终端 14 送往用户网络接口 19，并被存储在那里。协议 PA 允许用户 1 在随后该方法过早终止的情况下进行投诉。这就结束了预协商阶段，并且作为交易阶段的

第一部分，进账阶段随后请求由交易介质 2 为获取服务而作出进账。

在收到使能信号 B6 时，结算中心 30 首先在其时间监视中检查其是否是在许可的时间段内收到的（步骤 517）。如果情况如此，则结算中心 30 通过网络 20 启动本领域公知的支付过程（步骤 518）。安全终端 14 由此首先在其时间监视中检查支付过程是否是在许可的时间段内开始的（步骤 519）。如果情况如此，则随后进行支付过程。

支付过程进行于用户端系统 10 与结算中心 30 中的进账模块 34 之间。如同预协商阶段，其基于对交易介质 2 的标识符 KM 的使用。将标识符 KM 包含于支付过程与预协商阶段就建立了该方法这两个部分之间在内容上的直接连接。以后如果需要，标识符 KM 可以被用来建立关联。

支付过程可以是属于开头所引的出版物“Geldkarte im Netz”中所描述的类型。首先通过交换认证的交易介质 2 与结算中心 30，确保了在结算中心 30 与安全终端 14 之间存在安全的端到端连接。使用交易介质 2 的标识符 KM，确定加密的密钥，在其帮助下导出密钥或者密钥对。因此，标识符 KM 构成了在订购过程与支付构成之间的特有的连接链条。然后使用该密钥或者密钥对，进行数据交换，其中将位于交换介质 2 的存储器 4 中的电子金钱减少待支付的金额，即注入金额 LS，并且将相应的金额贷入结算中心，由此将待支付的金额从交易介质 2 转移到结算中心 30。

支付过程不一定使用预协商阶段所使用的同样的结构装置在用户一侧进行。也可能（例如）使用特殊支付介质，其借助标识符 KM 与交易介质 2 连接，但与交易介质 2 不完全相同和/或不使用安全终端 14。然而，在前一种情况中，标识符 KM 必须或者存储在用户端系统 10 中，或者在通过数据网络 20 连接的网络用户处，或者由用户 1 手工输入。

如果支付过程不成功，则结束整个获取方法（步骤 521）。用户 1 收到作为支付过程一部分而提供的错误消息。

如果支付过程成功，则进账模块 34 通过传送包含标识符 KM 的确认信号，将其向交易模块 32 确认。这就结束了进账阶段。

现在结算中心 30 在交易阶段的过程中启动供应阶段。通过路由器模块 36，其建立与服务供应商 40 通过后台数据网络 22 的连接，并且向其传送注入请求 B7（步骤 600）。所述请求包含预授权标识符 KV，参考信息 RI，标识符 KM 与注入金额 LS。

在由服务供应商 40 接收后，服务管理设备 42 构造对应于注入金额 LS 的网络时间信用（步骤 602）。如果用户所订购的服务（在此例中为在网络运营商的移动无线网络中打电话）的使用是通过减少现有的网络时间信用，则服务供应商 40 将该网络时间信用注入到注入请求 B7 所指定的参考文件 47 中。

与提供该服务相关，可以规定与参考信息 RI 相关联的用户 1 被传送对应于网络时间信用的价值单位，即注入金额 LS。如果是这种情况，则服务供应商 40 在收到注入金额 LS 后，进行价值单位的生成（步骤 604）。该价值单位被传送给用户 1。相应地在参考文件 47 中管理网络时间信用。

如果使用价值单位，则可以在另一方面规定不注入参考文件 47，并且用户 1 被传送完全以价值单位形式的网络时间信用。然后在使用该服务时，用户 1 将该价值单位返回给服务供应商，并由此用完。在这种情况下，参考文件 47 适宜于进行支取管理。

如果成功注入了参考文件 47 和/或生成了价值单位，则服务供应商 40 传送确认信号 B8 给结算中心 30（步骤 606）。如果生成了一些，则服务供应商 40 还与确认信号 B8 一起或者紧跟其后传送价值单位给结算中心（步骤 607）。

收到确认信号 B8 之后，结算中心 30 进而形成注入确认信号 B9，该信号包含参考信息 RI、注入金额 LS、预授权标识符 KV 以及标识符 KM。结算中心 30 用其私有密钥 GS 对该注入确认签名，并且用会话密钥 SS 对其加密（步骤 608）。结算中心将如此形成的注入确认 B9 通过数据网络 20 传送给用户端系统 10（步骤 610）。与此一道或者紧跟其后，结算中心还将可选生成的价值单位传送给用户端系统 10（步骤 611）。

如果在步骤 602 注入用户账户 47 期间发生了错误，或者结算中心 30 在发送了注入请求 B7 之后没有从服务供应商 40 收到确认信号 B8，则结算中心 30 生成暂时注入确认 B10（步骤 612）。暂时注入确认 B10 首先包含与成功注入处理之后的注入确认 B9 所包含的相同的数据。另外，暂时注入确认 B10 还包含不定指示符 FU，该指示符表示可能存在错误并且还包含用户可用来对该错误投诉的联系地址（步骤 614）。类似地，暂时注入确认 B10 用结算中心的私有密钥 GS 进行签名并用会话密钥 SS 加密。

注入确认 B9 或者暂时注入确认 B10 由安全终端 14 使用会话密钥 SS 解密（步骤 616）。然后，安全终端 14 将解密的结果通过输出装置 17 向用户显

示（步骤 616），该结果即为在收到注入确认 B9 之后对成功执行注入过程的确认或者在收到暂时注入确认 B10 与所发送的投诉联系地址之后对可能的错误的指示。另外，安全终端使所有被传送的价值单位被存储（步骤 619）。这可以在用户端系统 10 的组件之一内完成，在通过数据网络 20 连接的网络用户处完成，或者在外部设备例如手机中完成。

从此处开始，可以规定安全终端 14 形成对价值单位的接收的确认，并且该确认被返回给结算中心 30（步骤 620）。当这些价值单位为其价值在于用户记下它们或者它们随后永久保留在交易介质 2 上以备反复使用的数据（例如 PIN 或者加密密钥）时，该措施尤其方便。

结算中心 30 形成有关所进行的整个数据交换的协议 PB，以延续协议 PA。结算中心 30 将整个协议 PB 或者至少新加至协议 PA 的部分传送给安全终端 14，安全终端 14 对其检查并且添加只在安全终端 14 中存在的信息。因此，协议 PB 包含由结算中心 39 以及由服务供应商 40 通过数据网络 20 与用户端系统 10 交换的所有的必要信息。完整的协议 PB 由安全终端 14 传送给用户网络接口并被存储在那里（步骤 622）。

在保持以下基本原理的前提下，上述方法允许许多实施例：通过使用与所用交易介质相关联的标识符 KM，并且通过借助标识符 KM 将预协商阶段与随后的进账和供应阶段相联系，以保护添加到执行服务订购的服务获取过程中的预协商阶段。因此上述的方法并不局限于其中在传送了待支付金额或者等价物时才提供服务的应用。待支付金额的传送可以在交易阶段由包括访问交易介质上敏感数据的任意其他操作所替换。例如，该方法可以用来从结算中心 30 向用户端系统 10 传送 PIN 或者访问代码。在进账阶段的支付过程中，不传送待支付的金额，而是交换或者只出示秘密记录。

另外，进账阶段不一定涉及在交易介质 2 上的数据改动。而是可以规定只出示并检查获取服务所需的一定数据。

在只需要低安全级别的情况下，预协商阶段、进账阶段、与供应阶段之间的耦合可以以弱化形式进行。例如，交易介质 2 的标识符 KM 可以在结算中心被转换为简单的标准值，该值只确认标识符 KM 的存在。

时间监视例程的设计是可变的。除所描述的那些外，可以监视其他的或者不同的时间段。监视也可以包括不同时间段之间的相关。另外，网络用户 10、30 与 40 有各种设计。具体地说，组件既可以组合在一起，也可以分布

在多个进一步的组件上。

所用的加密技术可以在很宽的限制内被进一步设计。可以使用不同的原理与其他加密。

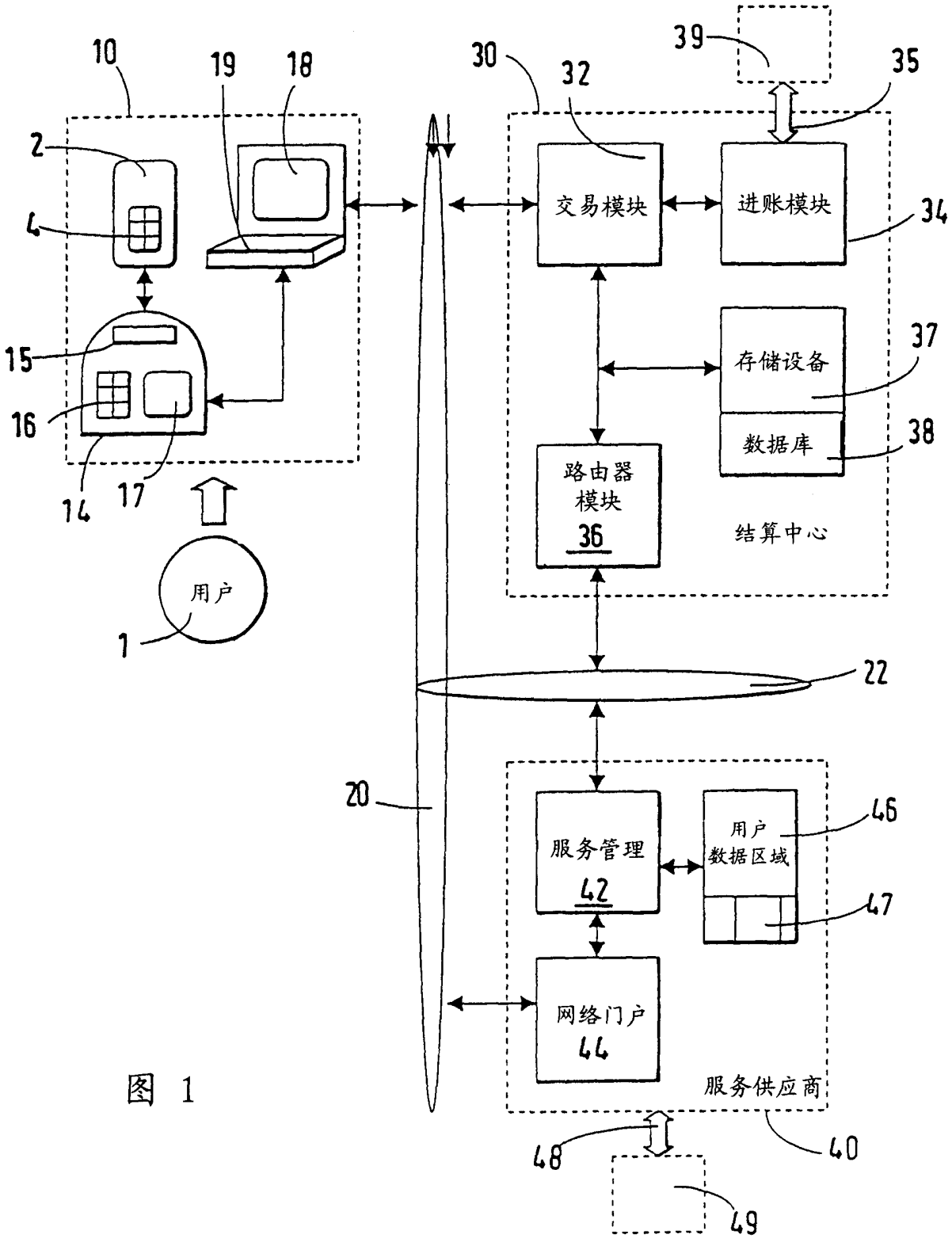

10
19
18
30
32
39
35
2
4
交易模块
进账模块
34
15
存储设备
37
16
数据库
38
14
17
路由器
模块
36
结算中心
用户
1
22
20
服务管理
42
用户
数据区域
46
47
网络门户
44
服务供应商
48
40
49

图 1

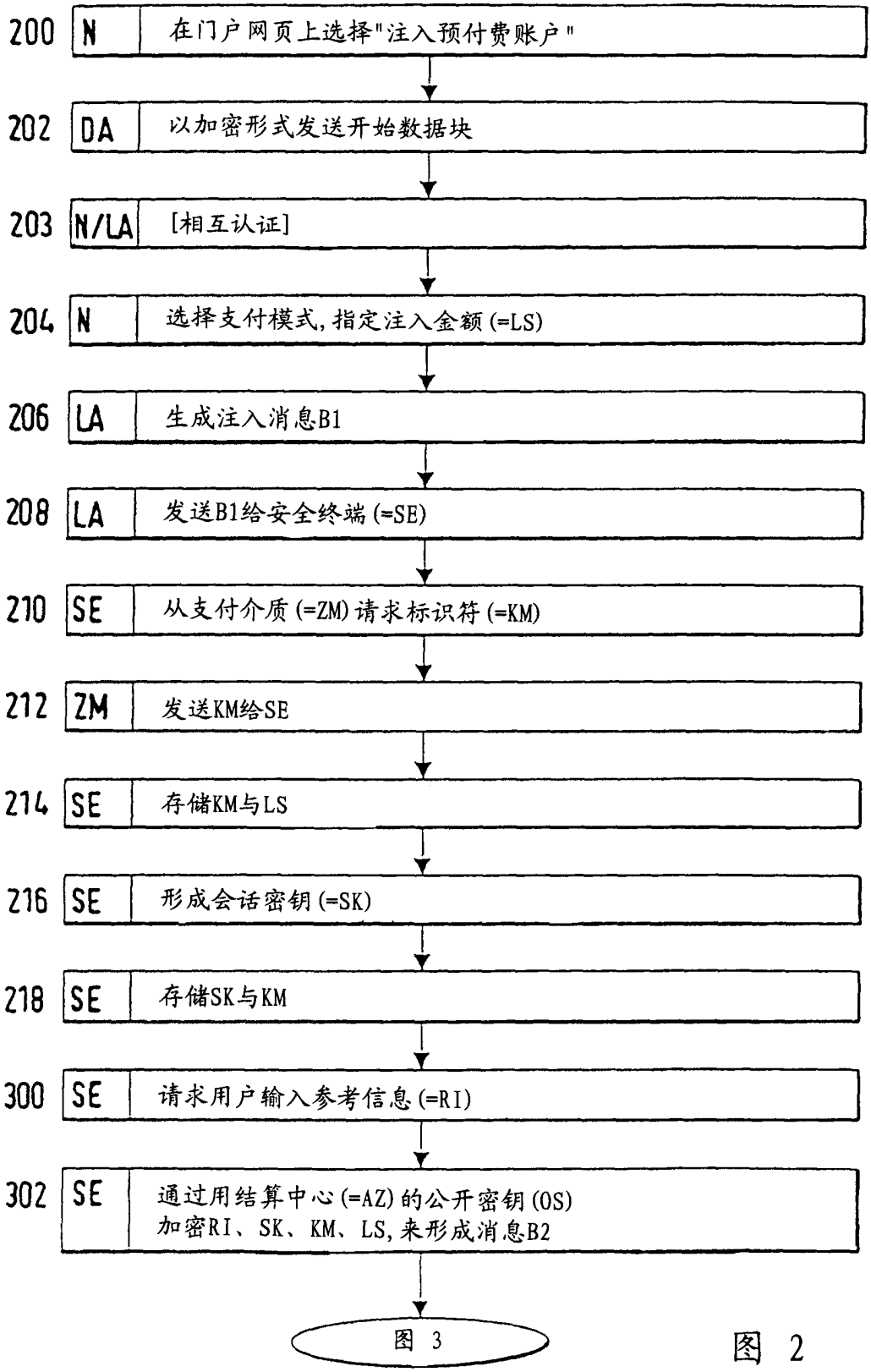

200 N 在门户网页上选择"注入预付费账户"
202 DA 以加密形式发送开始数据块
203 N/LA [相互认证]
204 N 选择支付模式,指定注入金额(=LS)
206 LA 生成注入消息B1
208 LA 发送B1给安全终端(=SE)
210 SE 从支付介质(=ZM)请求标识符(=KM)
212 ZM 发送KM给SE
214 SE 存储KM与LS
216 SE 形成会话密钥(=SK)
218 SE 存储SK与KM
300 SE 请求用户输入参考信息(=RI)
302 SE 通过用结算中心(=AZ)的公开密钥(OS)
加密RI、SK、KM、LS,来形成消息B2
图 3

图 2

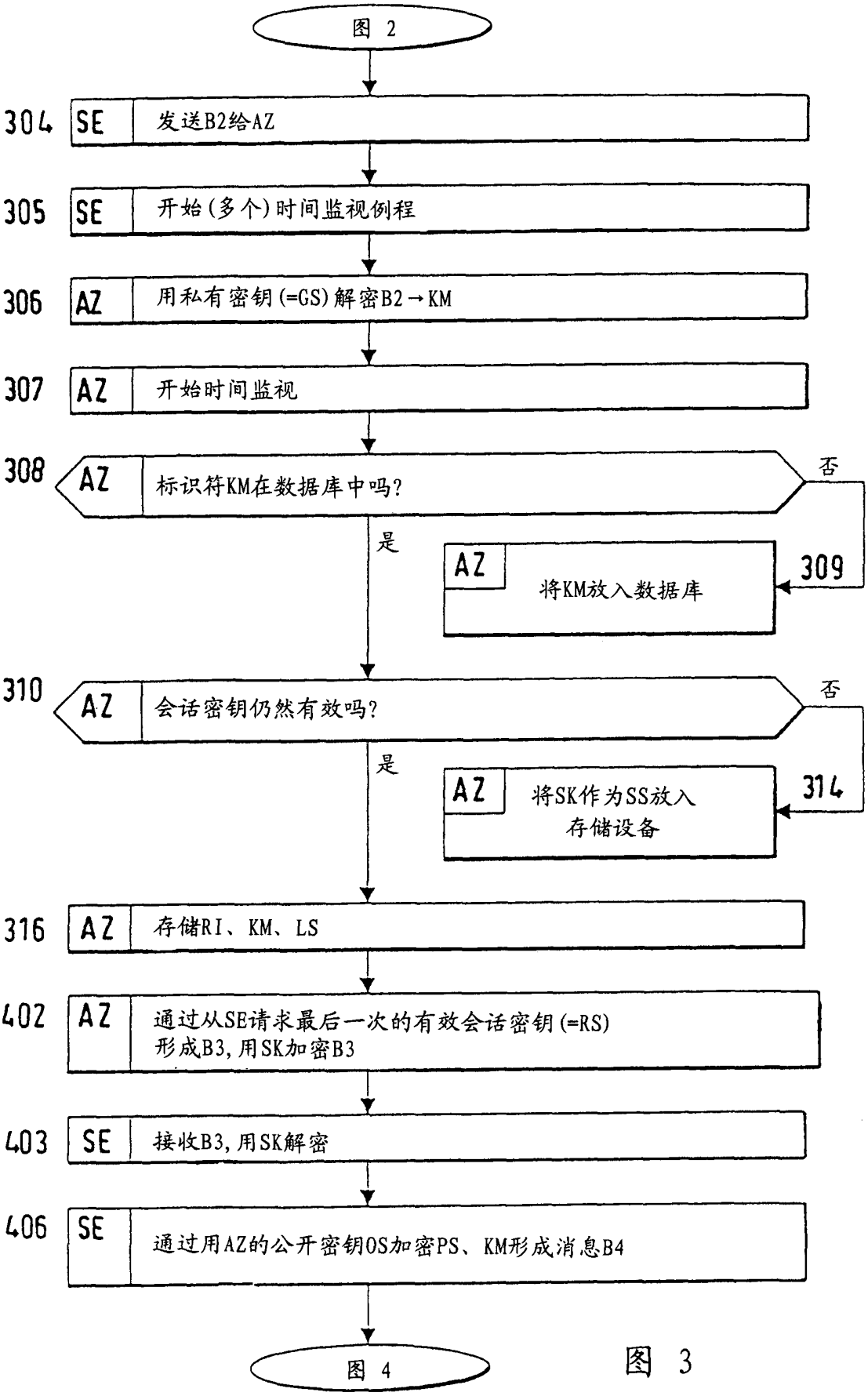


图 2
304
SE
发送B2给AZ
305
SE
开始(多个)时间监视例程
306
AZ
用私有密钥(=GS)解密B2→KM
307
AZ
开始时间监视
308
AZ
标识符KM在数据库中吗?
否
是
AZ
将KM放入数据库
309
310
AZ
会话密钥仍然有效吗?
否
是
AZ
将SK作为SS放入
存储设备
314
316
AZ
存储RI、KM、LS
402
AZ
通过从SE请求最后一次的有效会话密钥(=RS)
形成B3,用SK加密B3
403
SE
接收B3,用SK解密
406
SE
通过用AZ的公开密钥OS加密PS、KM形成消息B4
图 4

图 3

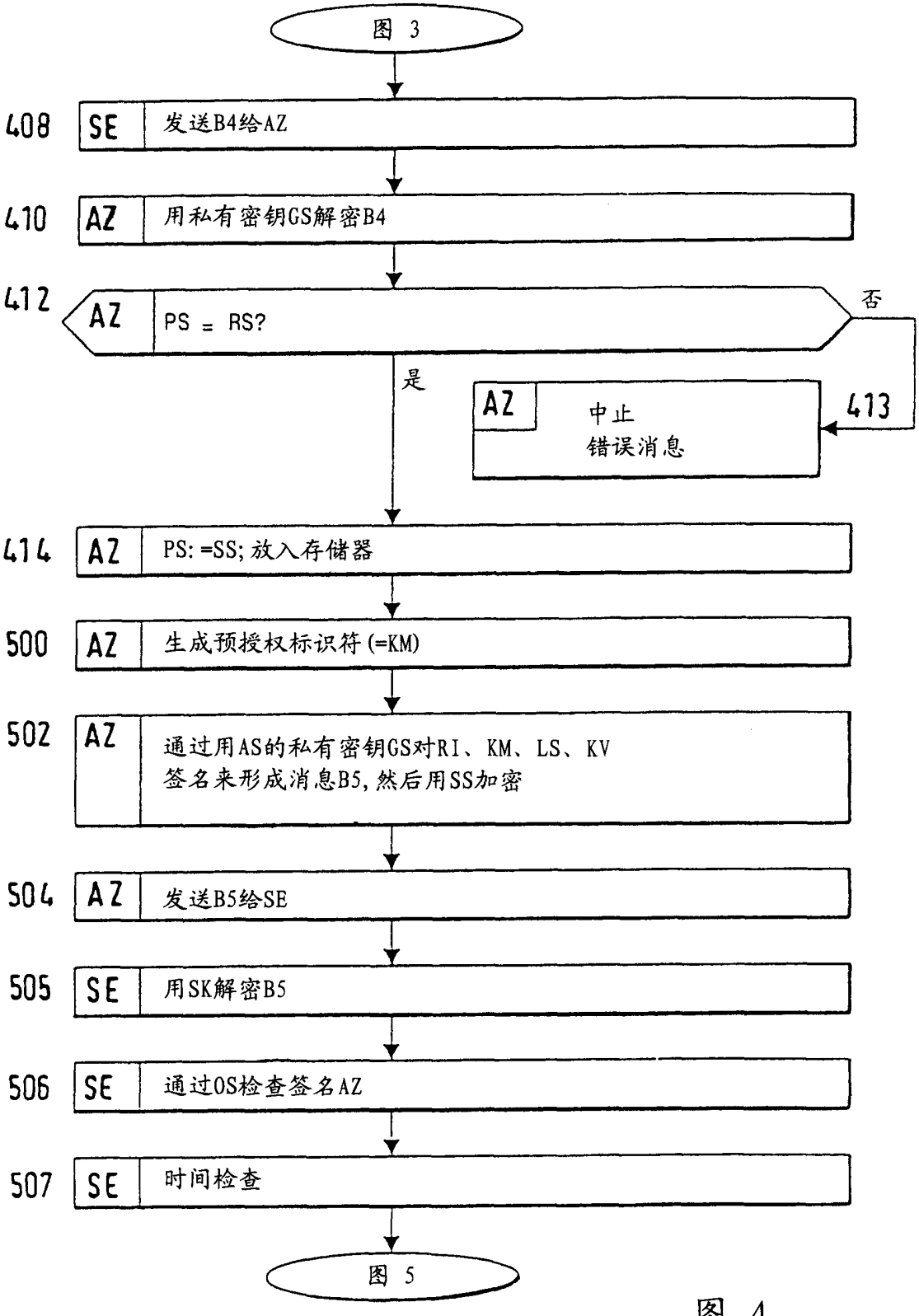


图 3
408
SE
发送B4给AZ
410
AZ
用私有密钥GS解密B4
412
AZ
PS = RS?
否
是
AZ
中止
错误消息
413
414
AZ
PS: =SS; 放入存储器
500
AZ
生成预授权标识符 (=KM)
502
AZ
通过用AS的私有密钥GS对RI、KM、LS、KV
签名来形成消息B5, 然后用SS加密
504
AZ
发送B5给SE
505
SE
用SK解密B5
506
SE
通过OS检查签名AZ
507
SE
时间检查
图 5

图 4

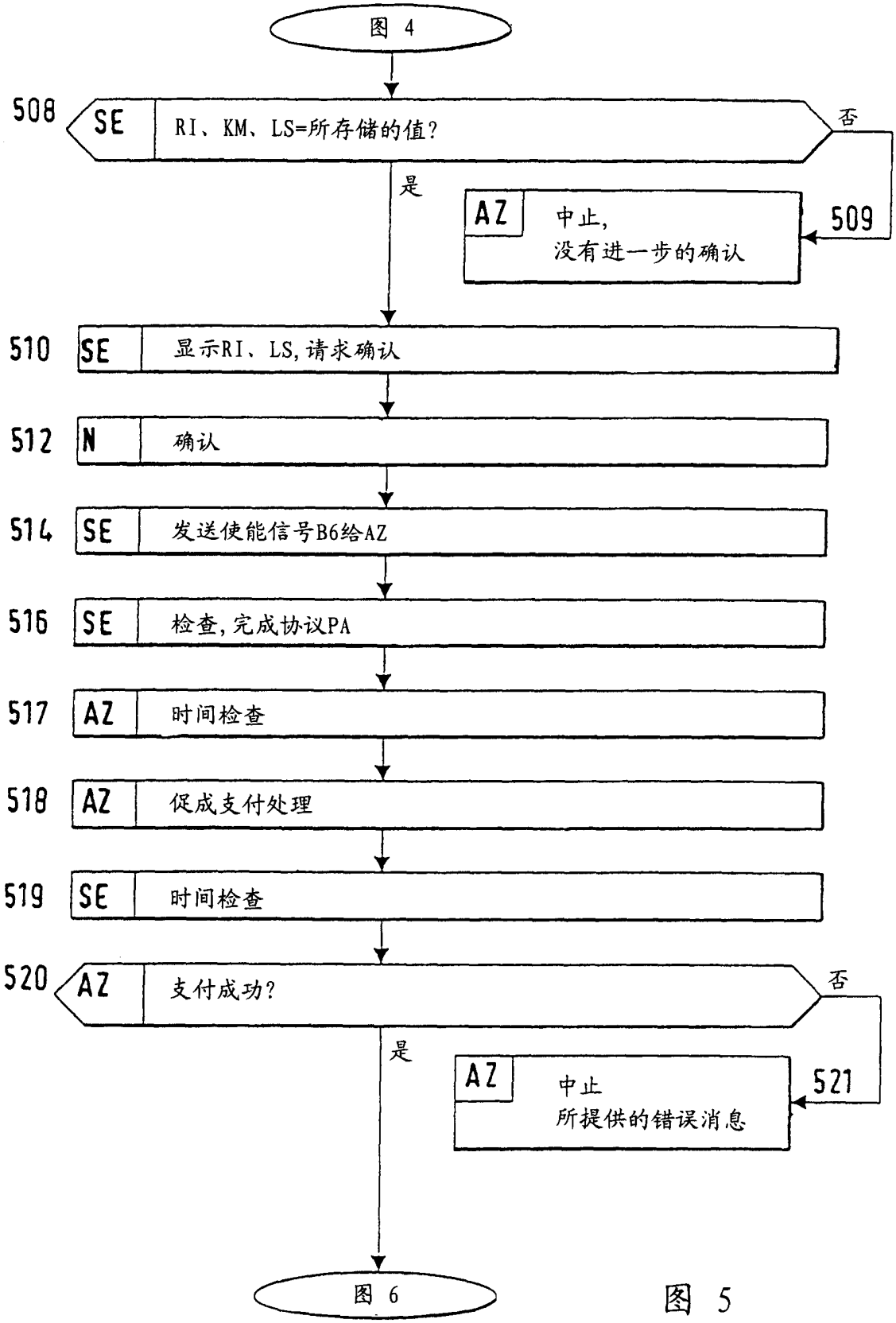


图 4
508
SE
RI、KM、LS=所存储的值?
否
是
AZ
中止,
没有进一步的确认
509
510
SE
显示RI、LS,请求确认
512
N
确认
514
SE
发送使能信号B6给AZ
516
SE
检查,完成协议PA
517
AZ
时间检查
518
AZ
促成支付处理
519
SE
时间检查
520
AZ
支付成功?
否
是
AZ
中止
所提供的错误消息
521
图 6

图 5

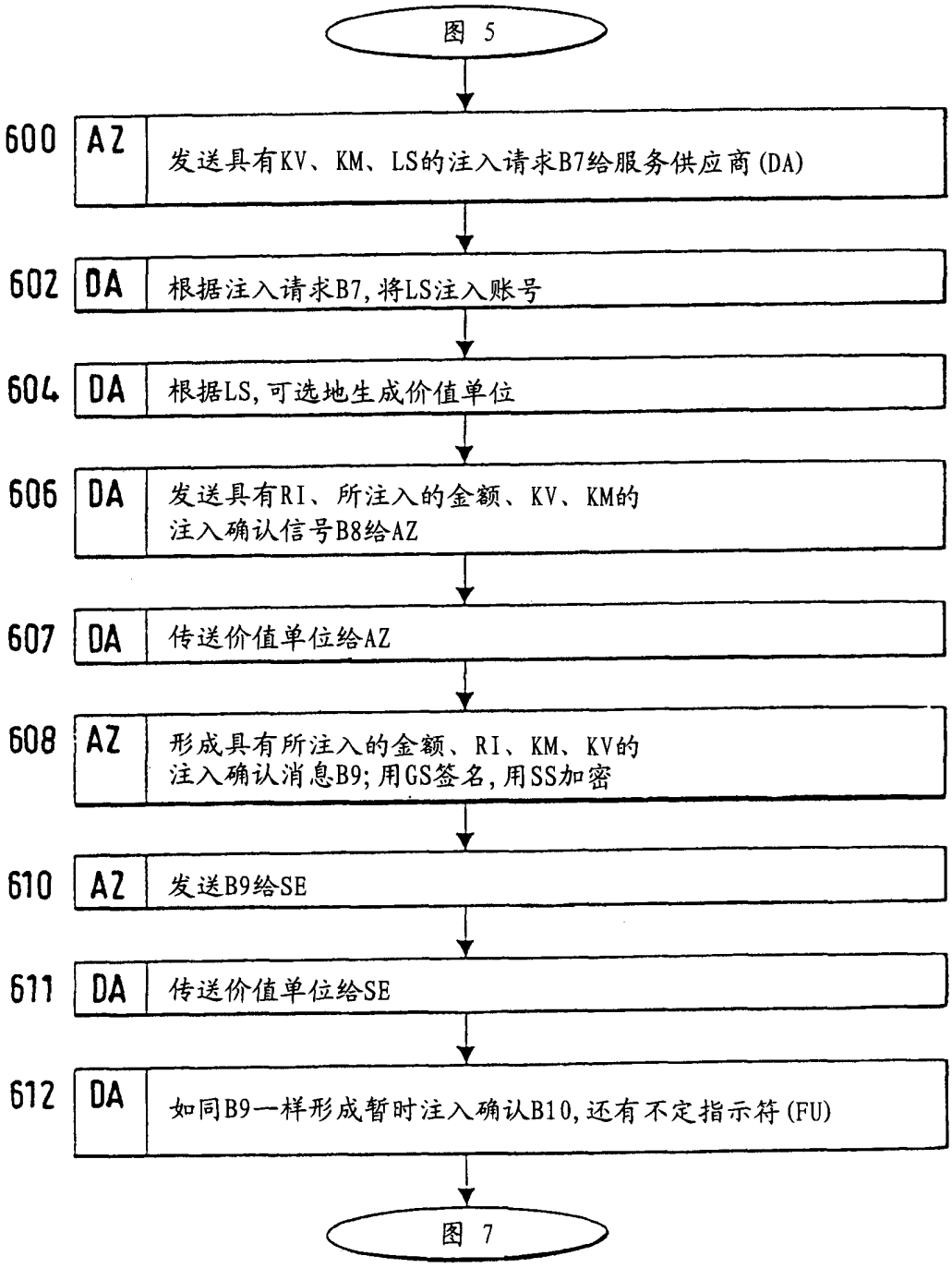


图 5
600
AZ
发送具有KV、KM、LS的注入请求B7给服务供应商(DA)
602
DA
根据注入请求B7,将LS注入账号
604
DA
根据LS,可选地生成价值单位
606
DA
发送具有RI、所注入的金额、KV、KM的
注入确认信号B8给AZ
607
DA
传送价值单位给AZ
608
AZ
形成具有所注入的金额、RI、KM、KV的
注入确认消息B9;用GS签名,用SS加密
610
AZ
发送B9给SE
611
DA
传送价值单位给SE
612
DA
如同B9一样形成暂时注入确认B10,还有不定指示符(FU)
图 7

图 6

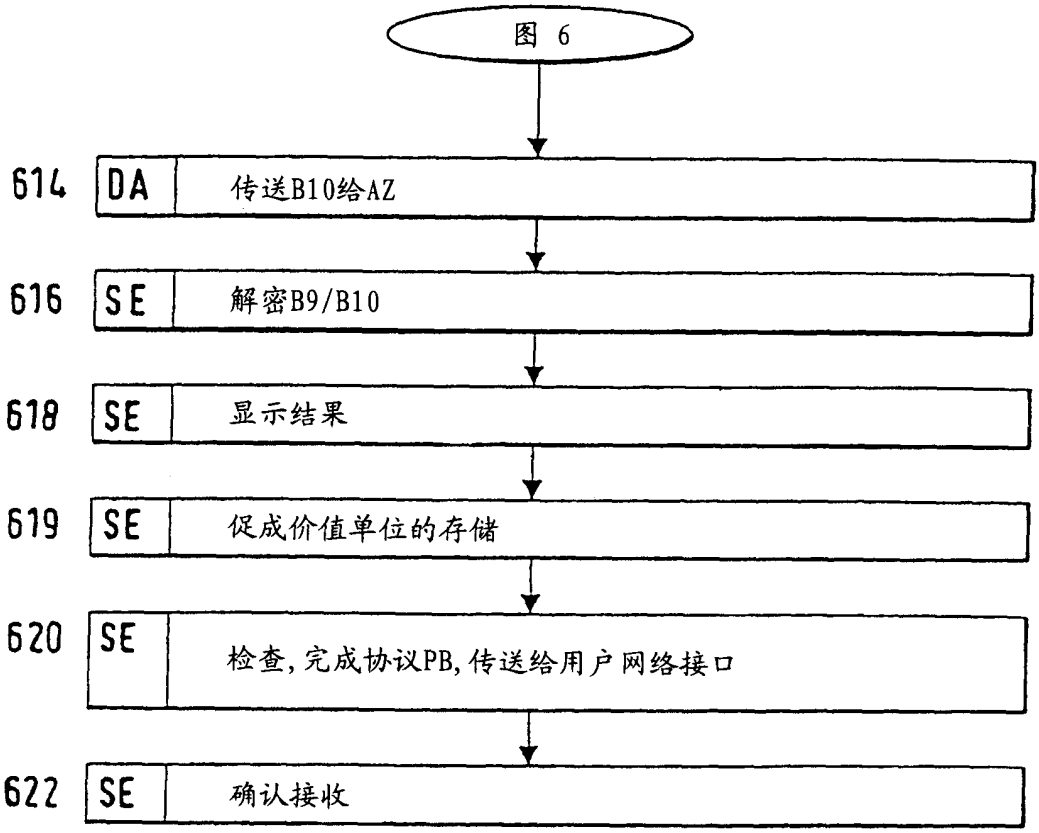


图 6
614
DA
传送B10给AZ
616
SE
解密B9/B10
618
SE
显示结果
619
SE
促成价值单位的存储
620
SE
检查,完成协议PB,传送给用户网络接口
622
SE
确认接收

图 7