

[51] Int. Cl.

G06Q 20/00 (2006.01)

G07F 7/10 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200580005149.8

[43] 公开日 2007 年 2 月 28 日

[11] 公开号 CN 1922623A

[22] 申请日 2005.2.10

[21] 申请号 200580005149.8

[30] 优先权

[32] 2004. 2.17 [33] US [31] 60/544,300

[32] 2004. 3. 3 [33] US [31] 60/549,148

[32] 2004. 6. 2 [33] US [31] 60/575,835

[32] 2005. 1.31 [33] US [31] 11/045,484

[86] 国际申请 PCT/US2005/004049 2005.2.10

[87] 国际公布 WO2005/079254 英 2005.9.1

[85] 进入国家阶段日期 2006.8.17

[71] 申请人 富士通株式会社

地址 日本国神奈川县

[72] 发明人 扬尼斯·拉布劳 季稻胜

乔纳森·罗素·阿格雷

赫苏斯·莫利纳·特里萨 陈玮伦

[74] 专利代理机构 隆天国际知识产权代理有限公司

代理人 张龙哺

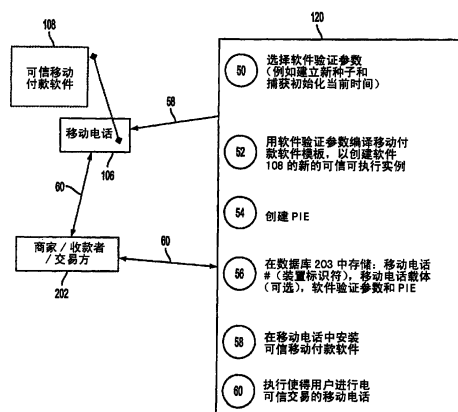
权利要求书 6 页 说明书 35 页 附图 15 页

[54] 发明名称

无线钱包

[57] 摘要

一种移动电话系统和方法，包括：在安全交易服务器(STS)用软件验证参数来初始化移动付款软件，以作为可信移动付款软件；提供个人标识项(PIE)与可信移动付款软件之间的 STS 相关；在移动电话中安装可信移动付款软件；以及由用户将 PIE 输入到所安装的可信移动付款软件，并将所述可信移动付款软件作为移动电话用户的移动电话无线钱包，以根据 PIE 和软件验证参数，在移动电话网上产生经过变换的安全可信移动电话无现金货币交易。 根据协定视图协议来进行移动电话可信无现金货币交易。



1、一种方法，包括：

在安全交易服务器 STS 用软件验证参数来初始化移动付款软件，以作为可信移动付款软件；

提供在个人标识项 PIE 与可信移动付款软件之间的 STS 相关；

在移动电话中安装可信移动付款软件；以及

由用户将所述 PIE 输入到安装的可信移动付款软件，并将所述可信移动付款软件作为移动电话用户的移动电话无线钱包，以根据所述 PIE 和软件验证参数在移动电话网络上产生经过变换的安全可信移动电话无现金货币交易。

2、根据权利要求 1 所述的方法，还包括，根据移动电话的应用平台实施可信移动付款软件。

3、根据权利要求 1 所述的方法，还包括，根据 Java 2 平台微版本 J2ME 和/或无线二进制运行环境 BREW 实施可信移动付款软件。

4、根据权利要求 1 所述的方法，还包括：

向移动电话提供对可信移动付款软件的下载链路；以及

经由所述下载链路将可信移动付款软件下载到移动电话，从而进行可信移动付款软件的安装。

5、根据权利要求 4 所述的方法，其中使用短消息业务/多媒体消息业务向移动电话传送可信移动付款软件下载的链路。

6、根据权利要求 1 所述的方法，其中根据通用交易构架安全协定提交 UPTF SAS 协议来进行移动电话可信无现金货币交易。

7、根据权利要求 1 所述的方法，其中根据通用交易构架安全协定提交 UPTF SAS 协议来进行可信移动电话无现金货币交易，

其中初始化可信移动付款软件的步骤包括：

在计算装置向用户提供移动电话无现金货币交易激活链路；

经由所述激活链路注册用户移动电话的电话号码；

向 STS 传送移动电话的已注册电话号码；

由 STS 产生包括初始化参数的可执行移动付款软件，以作为可信移动付款软件；以及

由 STS 产生在 STS 中与可信移动付款软件相关的 PIE；以及
其中安装可信移动付款软件下载链路的步骤包括：

由 STS 使用已注册移动电话号码经由短消息业务/多媒体消息业务向用户的移动电话传送对可信移动付款软件的下载链路；

经由下载链路将可信移动付款软件下载到移动电话，由此执行可信移动付款软件的安装；以及

由 STS 向用户提供 PIE。

8、根据权利要求 6 所述的方法，还包括：

在 STS，将用户的提取的已注册财务实体信息与可信移动付款软件相关；
将可信移动付款软件与交易方的交易信息进行捆绑；

在移动电话，由 STS 呈现提取的标识符的可选列表，所述标识符对应于与可信移动付款软件相关的用户的已注册财务实体；以及

使用 PIE 和软件验证参数并根据 UPTF 交易消息，执行与交易方的移动电话无现金货币交易，所述 UPTF 交易消息包括移动电话的标识符、交易方标识符和交易标识符，其中基于在移动电话的可信移动付款软件和 STS 相关的组合，以及在用户、交易方和 STS 之间的 UPTF 交易消息的交换提供移动电话无线钱包，所述 STS 相关为可信移动付款软件与 PIE、软件验证参数、和用户的财务实体的 STS 相关。

9、根据权利要求 6 所述的方法，其中 UPTE SAS 包括

由移动电话产生移动电话无现金货币交易的第一视图，并根据 SAS 向 STS 传送所述交易的第一视图；

由指向交易的一方独立产生交易的第二视图，并根据 SAS 向 STS 传送交易的第二视图；以及

由 STS 检验第一和第二视图，以验证交易，以及

由 STS 基于所述检验步骤促使交易执行。

10、根据权利要求 9 所述的方法，其中第一和第二视图是对称的，SAS 包括产生未加密可认知部分和加密部分作为交易的每个独立视图，所述未加密可认知部分包括用于第一视图的第一移动电话的标识和当前时间戳，所述加密部分通过在交易消息上基于 PIE 来执行时间和可信移动付款软件的变换组合而获得，所述交易消息包括交易数据、第一移动电话的标识以及用于第二视图

的第二装置的标识。

11、根据权利要求 9 所述的方法，

其中软件验证参数包括初始化时间戳和初始化随机种子数的多个参数；以及

其中第一和第二视图是对称的并且 SAS 包括：

产生未加密可认知部分和加密部分作为交易的每个独立视图，所述未加密可认知部分包括用于第一视图的第一移动电话的标识符和当前时间戳，所述加密部分通过在交易消息上由 STS 在初始化中基于 PIE 和包括在可信付款软件中的软件验证参数来执行变换组合而获得，所述交易消息包括交易数据、第一移动电话的标识以及用于第二视图的第二装置的标识。

12、根据权利要求 11 所述的方法，其中用于加密的变换组合包括：

基于可信付款软件中的软件验证参数来产生交易随机序号；以及

基于交易随机序号和 PIE 来产生加密密钥。

13、根据权利要求 12 所述的方法，其中产生加密密钥的步骤还包括：

产生当前时间戳；

将当前时间戳转换为字符串；

使用一种方式函数将当前时间戳字符串转换为当前时间戳值；

确定在当前时间戳与初始化时间戳之间的时间差值；

基于初始化随机种子数和所述时间差值来计算用于消息验证的键入散列 HMAC 结果，以产生交易随机序号；

从 HMAC 结果选择比特数作为交易随机序号，并将所选数量的比特与 PIE 组合；

计算组合的散列值；以及

选择散列值的比特数，以产生加密密钥。

14、根据权利要求 13 的方法，其中比特数约为 128。

15、根据权利要求 4 所述的方法，其中联机付款系统向作为用户的联机付款系统成员提供移动电话无现金货币交易激活链路，从而使用用户的移动电话无线钱包来提供人对人移动电话可信无现金货币交易。

16、根据权利要求 15 所述的方法，还包括：

在用户的移动电话上显示呈现可选菜单项的图形用户界面，其中所述可选

菜单项包括人对人付款、人对人交易、他人的等待付款请求、设置或其任何组合；

在选择人对人付款或者等待付款请求菜单项时，显示接受输入的图形用户界面，所述输入包括交易方的移动电话号码、电子邮件地址或者其任何组合；以及

在输入交易方的移动电话号码和/或电子邮件地址以及 PIE 时，使用移动电话用户的移动电话无线钱包执行与交易方的移动电话无现金货币交易。

17、根据权利要求 16 所述的方法，其中接受输入步骤还包括接受移动电话用户的提取的先前注册的财务账户参考标识符，以执行交易。

18、根据权利要求 1 所述的方法，

其中根据通用交易构架安全协定提交 UPTF SAS 协议来进行移动电话可信无现金货币交易，并且该方法还包括：

在 STS 将用户的已提取的财务实体信息与可信移动支付软件相关；以及

使用用户移动电话无线钱包提供人对人移动电话 UPTE 可信无现金货币交易。

19、根据权利要求 1 所述的方法，其中 PIE 是具有小于或等于 5 个字符的字母数字字符串。

20、根据权利要求 6 所述的方法，还包括根据超文本传输协议 HTTP、基于网络通信接口的通信和/或 web 服务呼叫，在移动电话通信网络上传送移动电话可信无现金交易消息。

21、根据权利要求 8 所述的方法，其中移动电话无现金货币交易的执行步骤还包括：

接收移动电话显示屏幕可显示的条形码图像作为已执行的移动电话无现金货币交易和/或其它交易的收据、与收据有关的信息；

在移动电话的显示屏幕上显示条形码图像；以及

由交易方在交易方的物理服务点读取用于交易管理的已显示的条形码图像。

22、根据权利要求 18 所述的方法，其中人对人移动电话 UPTF 可信无现金货币交易包括：向个人发送付款，向他人请求付款，检验来自他人的付款的

等待请求，存储并检索交易的记录，或者其任何组合。

23、根据权利要求 1 所述的方法，其中在移动电话中安装可信移动付款软件的步骤包括：将可信移动付款软件下载到移动电话，在移动电话可安装计算机可读介质上存储所述可信移动付款软件，将可信移动付款软件存储在移动电话嵌入式计算机可读介质中，或者其任何组合。

24、根据权利要求 7 所述的方法，其中向用户提供 PIE 的步骤包括通过第三方向用户传递作为图像的 PIE。

25、根据权利要求 21 所述的方法，还包括在移动电话中存储条形码图像交易收据。

26、根据权利要求 1 所述的方法，还包括用移动电话内容的自动下载奖励移动电话无线钱包交易，所述移动电话内容包括铃声、游戏、数字/媒体内容、软件或者其任何组合，和/或用于其任何一个的积分。

27、根据权利要求 22 所述的方法，还包括使用短消息业务/多媒体消息业务、电子邮件和/或语音消息，在移动电话向用户通知移动电话 UPTF 可信无现金货币交易的状态。

28、根据权利要求 21 所述的方法，还包括使用包含交易收据信息的短消息业务/多媒体消息业务、电子邮件和/或语音消息，在移动电话向用户通知移动电话 UPTF 可信无现金货币交易的状态。

29、根据权利要求 18 所述的方法，其中所述 PIE 是具有小于或等于 5 个字符的字母数字字符串。

30、一种移动电话，包括：

计算机可读介质，存储移动付款软件，该移动付款软件在安全交易服务器 STS 用软件验证参数初始化，并且将该移动付款软件与个人标识项 PIE 相关，以作为可信移动付款软件；

程序控制计算机处理器，通过根据以下处理来控制移动电话执行可信移动付款软件，该处理包括：

提示用户输入 PIE；以及

将该移动付款软件作为移动电话用户的移动电话无线钱包，根据 PIE 和软件验证参数，在移动电话网络上产生经过变换的安全可信移动电话无现金货币交易。

31、一种计算机系统，包括：

计算机服务器，包括根据以下处理来控制服务器的程序控制计算机，所述处理包括：

用软件验证参数来初始化移动付款软件，以作为可信移动付款软件，产生安全的个人标识项 PIE；

提供在 PIE 与可信移动付款软件之间的安全相关；和

提供联机购买界面；以及

在移动电话网络中与服务器通信的移动电话包括：

计算机可读介质，存储可信移动付款软件；和

计算机处理器，根据以下处理来控制移动电话执行可信移动付款软件，所述处理包括：

连接联机购买界面，以产生虚拟购物车，

提示用户输入 PIE，

基于虚拟购物车，根据 PIE 和软件验证参数产生经过变换的安全可信移动电话无现金货币交易，以及

在移动电话网络上向计算机服务器传送已变换的安全可信移动电话无现金货币交易，以执行交易。

无线钱包

相关申请的交叉参考

本申请涉及并且是 2003 年 6 月 11 日提交的美国专利申请 No.10/458205 的部分继续申请、2003 年 7 月 29 日提交的美国专利申请 No.10/628584 的部分继续申请、2003 年 7 月 29 日提交的美国专利申请 No.10/628569 的部分继续申请以及 2003 年 7 月 29 日提交的美国专利申请 No.10/628583 的部分继续申请，其中上述美国专利申请 No.10/458205 要求 2002 年 8 月 8 日提交的美国临时专利申请 No.60/401807 的优先权；上述美国专利申请 No.10/628584 要求 2002 年 8 月 8 日提交的美国临时专利申请 No.60/401807 的优先权；上述美国专利申请 No.10/628569 要求 2002 年 8 月 8 日提交的美国临时专利申请 No.60/401807 的优先权；以及上述美国专利申请 No.10/628583 要求 2002 年 8 月 8 日提交的美国临时专利申请 No.60/401807 的优先权。

本申请还涉及并要求美国临时专利申请 60/544300（律师备审案件目录表 No.1634.1002P2）的优先权，该临时专利申请是 Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen 于 2004 年 2 月 17 日向美国专利商标局提交的，其名称为 A UNIVERSAL PERVASIVE TRANSACTION FRAMEWORK APPLICATION: WIRELESS WALLET ON MOBILE PHONE（通用交易构架应用：移动电话的无线钱包），该申请的内容在此作为参考引用。

本申请还涉及并要求美国临时专利申请 No.60/549148（律师备审案件目录表 No.1634.1002P3）的优先权，该临时专利申请是 Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen 于 2004 年 3 月 3 日向美国专利商标局提交的，其名称为 WIRELESS WALLET（无线钱包），该申请的内容在此作为参考引用。

本申请还涉及并要求美国临时专利申请 No.60/575835（律师备审案件目录表 No.1634.1002P4）的优先权，该临时专利申请是 Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen 于 2004 年 6 月 2 日向美国

专利商标局提交的，其名称为 A WIRELESS WALLET FOR PERSON-TO-PERSON TRANSACTIONS（用于人对人交易的无线钱包），该申请的内容在此作为参考引用。

本申请还涉及 2002 年 8 月 8 日向美国专利商标局提交的美国临时专利申请 No.60/401807（律师备审案件目录表 No.1634.1002P），该申请的内容在此作为参考引用。

本申请涉及美国专利申请 No.10/458205（律师备审案件目录表 No.1634.1003），该专利申请是 Yannis Labrou, Lusheng Ji 和 Jonathan Agre 于 2003 年 6 月 11 日向美国专利商标局提交的，其名称为 SECURITY FRAMEWORK AND PROTOCOL FOR UNIVERSAL PERVASIVE TRANSACTIONS（用于通用交易的安全构架和协议），该申请的内容在此作为参考引用。

本申请涉及美国专利申请 No.10/628584（律师备审案件目录表 No.1634.1002），该专利申请是 Yannis Labrou, Lusheng Ji 和 Jonathan Agre 于 2003 年 7 月 29 日向美国专利商标局提交的，其名称为 METHODS FOR PURCHASING OF GOODS AND SERVICES（购买商品和服务的方法），该申请的内容在此作为参考引用。

本申请涉及美国专利申请 No.10/628569（律师备审案件目录表 No.1634.1004），该专利申请是 Yannis Labrou, Lusheng Ji 和 Jonathan Agre 于 2003 年 7 月 29 日向美国专利商标局提交的，其名称为 APPARATUSES FOR PURCHASING OF GOODS AND SERVICES（购买商品和服务的设备），该申请的内容在此作为参考引用。

本申请涉及美国专利申请 No.10/628583（律师备审案件目录表 No.1634.1005），该专利申请是 Yannis Labrou, Lusheng Ji 和 Jonathan Agre 于 2003 年 7 月 29 日向美国专利商标局提交的，其名称为 FRAMEWORK AND SYSTEM FOR PURCHASING OF GOODS AND SERVICES（购买商品和服务的构架和系统），该申请的内容在此作为参考引用。

技术领域

本发明涉及一种能够进行可信交易，例如可信的无现金货币交易的无线计

算装置。例如一种移动电话无线钱包。

背景技术

未来普遍存在的计算环境将由具有信息计算设备（移动装置）的移动用户组成，所述的信息计算设备例如为蜂窝电话或者个人数字助理（PDA），其将与在任何特定时刻和地方碰到的各种服务和装置进行无线通信和交互。从研究团体和企业界已经提出可在这种环境下运行的许多应用，但是对于任一特定的应用都不具有强大的市场。显然，普遍的计算技术出现在市场中的关键因素是在这种环境形式下使用移动装置安全地进行财务交易的能力。

然而，移动装置，特别是移动电话，可能呈现某些特征，比如：有限能力（计算能力，通信带宽，电池容量，小显示屏，有限键盘等）；技术上不了解并且不能过度担负与其它方执行交易的复杂应用的典型用户；以及被认为在网络层不安全的无线传输网。

对于移动商务（m-commerce）问题，人们已经建议了许多方法和解决方案。少量制造商已经提供了支持无线局域网（WLAN）移动电话，并且摩托罗拉（MOTOROLA）和诺基亚（NOKIA）已经发布了在 2004 年提供这种电话的公告。

目前的移动商务实践包括 Web 铺面付款（Web Store-Front Payment），其中消费者对以互联网存在的零售商提供的商品或者服务付款。对于为移动装置专门制备的 web 页面，比如支持 WAP 的网页，人们可以使用移动装置进行购买，如同通常使用个人计算机上的 web 浏览器进行电子商务交易。但是，由于付款典型地需要登录并键入用户名和口令，所以在移动装置上这种方法不切实际并且效率很低，即使该交易使用无线应用协议（WAP）并且经由链路诸如 HTTP 或安全网络通信接口层（SSL）的安全网络链路进行，也是如此。在许多当前的 web 浏览应用中，消费者可以向商家预先注册一个或多个财务账户，以便节省时间并避免重复输入其财务信息，但是这种方法需要消费者向多个商家注册多个用户账户信息。此外，在物理销售点（POS）情况下，因为常常涉及与末端商店系统的整合以及在付款者与已购买的实际商品之间的某种形式的捆绑，所以根据商业观点进行部署是过于复杂的。

从数据安全的观点来看，现有的移动商务数据安全方案依赖于公共密钥基

基础结构（PKI）技术。然而，PKI 方案受到移动装置环境下的低计算性能以及用户经验的复杂性的影响。存在可将 PKI 用于移动付款的许多不同方式。由 MET 有限公司提出一种用于移动付款的基于 PKI 的方案，在[2005 年 1 月 5 日获取的 www.mobiletransaction.org]论述了该方案。在现有的移动商务安全方案下，用户使用验证用户身份的证书账户来签定交易（订购单）（并且不清楚每个用户具有一个还是多个这样的证书，每个证书用于各个合法的账户）。例如，来自许多卖主的多个安全证书的处理最有可能引起混乱，并且如果将证书留给用户，则可能是危险的。由于这些证书被存储在移动装置中，因此每次使用时需要保护和解锁证书存储。如果证书存储用软件实现，则用来解锁存储的密钥应当足够长以保护该存储，或者，可以改用硬件实现证书存储，在移动电话的情况下，将需要为此目的设计的电话。这种方法需要用于证书分发（包括撤销）的基础结构、可专用的移动电话以及由用户可对证书和他们的使用有一些基本的了解。

发明内容

这里描述的实施例涉及能够使用户进行电子可信交易的无线移动计算装置，例如能够使用户进行可信无现金货币交易的移动电话。例如，用户移动电话无线钱包。

一种移动电话系统和方法包括：在安全交易服务器（STS）用软件验证参数来初始化移动付款软件，以作为可信移动付款软件；提供个人标识项（PIE）与可信移动付款软件之间的 STS 相关；在移动电话中安装可信移动付款软件；以及由用户将 PIE 输入到所安装的可信移动付款软件，将所述可信移动付款软件作为移动电话用户的移动电话无线钱包，以根据 PIE 和软件验证参数，在移动电话网络上产生经过变换的安全可信移动电话无现金货币交易。移动电话可信无现金货币交易是根据协定视图协议（agreement view protocol）执行的。

本发明的上述以及其它方案和优点部分在以下说明书中说明，部分可以从说明书中清楚理解，或者可以通过所述实施例的实践获知。

附图说明

随后可清楚理解本发明的上述以及其它方案和优点，这可归应于下面参照

构成本发明一部分的附图、更加充分描述和请求保护的结构和操作的细节，其中在所有附图中相同的标记表示相同的部件。

图 1A 是根据本发明实施例的激活移动电话无现金财务交易能力的流程图；

图 1B 是根据本发明另一个实施例的激活移动电话无现金财务交易功能的流程图；

图 1C 是根据本发明实施例的激活移动电话无现金财务交易的移动电话显示屏幕用户界面图像的示意图；

图 2 是根据本发明实施例的执行移动装置无现金财务交易的、通用交易构架安全协定提交（Universal Pervasive Transaction Framework Secure Agreement Submission）（UPTF SAS）系统结构的功能方框图；

图 3 是根据本发明实施例的执行与实际销售点（POS）的移动电话无现金财务交易的、基于 UPTF 的系统结构的功能方框图；

图 4 是根据本发明实施例的执行移动电话无现金财务交易的、基于安全协定提交（SAS）协议的 UPTF 无现金财务交易消息的示意图；

图 5 是根据本发明实施例的与商家的基于 UPTF 的移动电话无现金财务交易的流程图；

图 6 是根据本发明实施例的购买电影票的基于 UPTF 的移动电话无现金财务交易的流程图；

图 7A-B 是根据本发明实施例的执行购买电影票的移动电话无现金货币交易以及获得、存储和检索交易收据无现金货币交易的移动电话显示屏幕用户界面；

图 8 是根据本发明实施例的基于移动电话显示屏幕用户界面图像以及在请求者装置、安全交易服务器（STS）和被请求者之间用于执行人对人移动电话无现金付款交易的消息流的流程图。

图 9 是根据本发明实施例的基于移动电话显示屏幕用户界面图像以及在请求者装置、安全交易服务器（STS）与被请求者之间用于执行人对人移动电话无现金付款请求交易的消息流的流程图。

图 10 是根据本发明实施例的整个移动电话显示屏幕用户界面图像以及对于在移动电话上执行人对人无现金货币交易的无线钱包的运营商可用的可能

的工作流程。

图 11-12 是根据本发明的执行各种移动电话无现金货币交易的移动电话人对人无现金货币交易消息格式的示意图。

具体实施方式

下面详细描述本发明的当前实施例，在附图中示出所述实施例的实例。在下文中，将参照附图来说明这些实施例，以解释本发明。

一般来说，有如下三类移动商务交易：

1.人对人付款：消费者可以使用他们的移动装置直接做出关于向另一消费者付款的协定。

2.Web 铺面付款：消费者对以互联网存在的零售商提供的商品或者服务付款。用户使用移动装置浏览零售商的 web 页面，以识别要购买的商品或者服务，然后付款。这种情况的实例是通过 web 服务来对书付款或者购买电影票。

3.物理销售点（POS）购买：比如当消费者在“实体店面”商店或饭店进行付款时，可使用移动装置在结帐台向零售商付款。

这些分类之间的边界是可延展的，并且可使用交易协定的观点来开发它们的公共特性。这里所述的实施例适合于这些和/或其它移动商务交易。

在这里所述的实施例中，移动装置是任何无线手持或像手大小的、电子计算装置，包括但不限于移动电话。这里所述的实施例涉及基于通用交易构架安全协定提交（UPTF ASA）协议的使得用户进行电子可信交易的无线移动计算装置，比如（不限于）可以或不可以进行财务结算的使得用户进行可信交易的移动电话，和/或使得用户进行可信无现金财务/货币交易的移动电话，例如，用户可信移动电话无线钱包。更具体地说，根据这里所述的实施例的一个方面，无线移动计算装置依据时间和基于安全（例如加密）、匹配（在彼此之间的检验）的软件，以及匿名的交易方、一方或多方的交易视图（即，在一个典型实施例中，是成对和/或两个以上的交易视图）来提供用户电子可信交易。

图 1A 是根据本发明实施例的激活移动电话无现金货币交易功能的流程图。用于使得用户进行电子可信交易（即，用户和/或用户交易的电子验证）的无线移动计算装置的计算机系统和方法包括：在操作 50 和 52，在安全交易服务器（STS）120，用软件验证参数来初始化移动付款软件模板，以作为可

信移动支付软件 108。在操作 54 和 56，在 STS 120 上将个人标识项 (PIE) 和移动电话 106 的标识符与可信移动电话付款软件 108 相关联。在操作 58，在移动电话 106 中安装可信移动支付软件 108。在操作 60，在移动电话 106 上，使用 PIE 运行已安装的可信移动支付软件 108，将所述可信移动支付软件 108 作为移动电话 106 用户的移动电话无线钱包，以进行移动电话可信无现金货币交易。更具体地说，在操作 60，用户将 PIE 输入到已安装的可信移动电话付款软件，以根据该 PIE 和软件验证参数产生经过变换的安全可信移动电话无现金货币交易。根据这里所述实施例的一个方面，在操作 50，选择一个或多个软件验证参数，它可以是（不限于）新种子 (seed) 的创建，比如新的随机种子数，和初始化时间。在操作 56，STS 120 在数据库 203 中存储用于移动电话 106 的唯一标识符（称之为设备 ID，或者 DID），该标识符例如可以是移动电话 106 的移动电话号码，或者某些随机产生的全球唯一标识符 (GUID)、移动电话电信公司（视情况而定）、在操作 50 上选择的软件验证参数、以及产生的 PIE。根据所述实施例的一个方面，移动电话号码还可以用作移动电话 106 的装置标识符。STS 120 使用移动电话 106 的唯一标识符 (装置 ID (DID)) 将交易消息与可信移动电话付款软件 108 相关联；将 DID 与软件验证参数和在 STS 120 存储的 PIE 相关联，从而 STS 120 可以产生与具有 DID 的装置 106 对应的密钥。移动电话号码可以用来与移动电话 106 通信（例如，通知等）（例如，短消息业务 (SMS) 和/或多媒体消息业务 (MMS)）。根据已知技术，移动电话 106 可以是支持互联网的移动电话。下面进一步详细描述 PIE。移动电话可信无现金货币交易是根据称之为通用交易构架 (UPTF)（以下更详细说明）的协定视图协议来进行，并且根据称之为安全协定提交 (SAS)（以下更详细说明）的协议来保护（例如加密）。根据这里所述实施例的一个方面，将交易消息捆绑到用户和装置（例如，移动电话无线钱包 106）的唯一组合上，对用户的捆绑是经由 PIE 而进行的，并且对设备 106 的捆绑是经由可信移动支付软件 108 的软件验证参数而进行的。特别地，交易是基于 SAS 的加密消息，并且该加密消息可以通过 PIE 和可信移动支付软件 108 的软件验证参数被追溯到用户和装置 106 的组合。

图 1B 是根据本发明另一实施例的激活移动电话无现金货币交易功能的流程图。在图 1B 中，计算机系统和/或方法包括：在操作 100，在计算装置 102 向

用户提供移动电话无现金货币交易激活链路（签约应用 102）；在操作 104，经由激活链路来注册用户的移动电话 106 的电话号码；在操作 105，使移动支付软件 108 与软件验证参数相关联，以作为可信移动支付软件 108；并且在操作 110，在 STS 120 提供在个人标识项（PIE）和可信移动支付软件 108 之间的关联。在操作 112，使用移动电话 106 的已注册的电话号码，向移动电话 106 传送对移动支付软件 108 的移动电话下载链路。在操作 114，移动支付软件 108 经由下载链路被下载到移动电话 108。在操作 116，用户可以使用可选的激活码来激活下载的移动付款软件 108。在可信移动支付软件 108 的安装之后，作为移动电话用户的用户移动电话无线钱包 106（即，移动电话无线钱包应用 108），用户可以使用用户移动电话无线钱包 106 来执行移动电话用户电子可信无现金交易。

移动支付软件 108 是根据移动电话 106 的应用平台来实现的。例如，可以根据 Java 2 平台微版本（J2ME）来实现移动支付软件 108。根据这里所述实施例的一个方面，在操作 112，使用短消息业务（SMS）和/或多媒体消息业务（MMS）向移动电话 106 传送移动支付软件下载链路。

在图 1B 中，在操作 116 之后，可以根据通用交易构架安全协定提交（UPTF SAS）协议来执行移动电话无现金货币交易。以下相关的普通转让待审美国专利申请中讨论了 UPTF SAS 协议：2003 年 6 月 11 日提交的第 10/458,205 号专利申请；2003 年 7 月 29 日提交的第 10/628,584 号专利申请；2003 年 7 月 29 日提交的第 10/628,569 号专利申请；和 2003 年 7 月 29 日提交的第 10/628,583 号专利申请，该专利申请由本申请的受让人 FUJISU 有限公司所拥有，以上所有申请全部公开于此以资参考。

在图 1B 中，在操作 105，移动支付软件 108 与软件可信参数的关联包括：由移动电话无现金货币交易活动的提供商 122 产生 UPTF 随机号标识符，从而 UPTF 随机号可以与用户相关联；以及向安全交易服务器（STS）120 传送 UPTF 随机号标识符和移动电话 106 的已注册的电话号码。例如在操作 105，在提供商 122 是交易方（用户）注册财务账户信息的付款业务 122 的情况下，付款业务 122 可以在与 STS 120 通信时指定标识用户的 UPTF 随机号标识符（提取的标识符）123。因此，STS 120 可以基于提供商 122 UPTF 随机号并且在不知道实际交易方账户信息的情况下与提供商 122 通信，以执行基于 UPTF 的交易。

此外,操作 110 包括:由 STS 120 产生包括初始化参数的可执行移动支付软件作为可信移动支付软件;以及产生在 STS 中与可信移动支付软件 108 相关的 PIE。在操作 112,移动支付软件下载链路的传送包括由 STS 120 经由短消息业务(SMS)向用户的移动电话 106 传送移动支付软件 108 的下载链路;以及由 STS 120 向用户提供 PIE。所述的实施例不限于上述的可信移动支付软件 108 的产生、激活和安装,并且,在操作 58,可以经由移动电话可拆卸/可安装(例如,智能卡)和/或嵌入式计算机可读介质来为移动电话 106 安装或提供可信移动支付软件 108,其中经由电子邮件下载链路、电子邮件附件链路等等,将所述介质嵌入在移动电话计算处理器中。

图 1C 是根据本发明实施例的激活移动电话无现金货币交易的移动电话显示屏幕用户界面图像的示意图。当移动电话 106 从代表提供商 122 的 STS 120 接收到 SMS 消息时,在操作 112 显示用户界面屏幕图像 150。用户界面屏幕图像 152 显示已接收的 SMS 消息,所述 SMS 消息用于指导移动电话用户访问互联网地址,以下载可信无线钱包软件 108。当完成将可信无线钱包软件 108 下载到移动电话 106 时,在操作 114 之后显示用户界面屏幕图像 154。当安装可信无线钱包软件 108 时,显示用户界面屏幕图像 156。当已经提供可信无线钱包软件 108 的可选激活码以在移动电话 106 输入时,在操作 116 显示用户界面屏幕图像 158。在经由用户界面屏幕图像 158 输入激活码之后,显示用户界面屏幕图像 160,所述图像向用户确认已经激活可信无线钱包软件 108,并且准备执行移动电话用户电子可信的无现金货币交易。

根据这里所述实施例的一个方面,在操作 100,诸如联机付款系统/业务、商家/业务提供商、金融机构等的提供商 122 向作为用户的提供商 122 的成员提供移动电话无现金货币交易激活链路。在联机付款系统 122 的情况下,所述实施例使用用户移动电话无线钱包 108 来提供成员对成员的移动电话无现金货币交易。

根据这里所述的实施例的一个方面,在操作 110,STS 120 向提供商 122 发送 PIE,并且在操作 111,提供商 122 接收到 PIE,并且向在计算机 102 的用户显示 PIE。在操作 111,为了增加安全性,PIE 可以仅仅是图像,使提供商 122 不知道该 PIE,因而允许交易方匿名。可以根据其它安全方式,比如邮件、电子邮件、客户业务代表等方式来传递 PIE。

因此参照图 1A 和图 1B, 在不受限制的实例中, 无线钱包应用 108 作为 J2ME 应用来实施, 该应用可以下载到移动电话 106 上并在其上运行, 并且能够使用户操纵通用交易构架 (UPTF) 来进行购买和付款。目前由美国电信公司提供的许多移动电话是支持 J2ME 和支持 web 的, 从而在移动电话上的 J2ME 的普遍可用性能够启用把内容和业务传递给移动用户的新的商务模型。使用 J2ME, 任何人都可以针对定制内容或向移动电话的业务递送来开发可下载的 J2ME 应用程序。这是无线钱包应用 108 的情况, 该应用允许使用移动电话 106 来提供安全付款业务。

J2ME 无线钱包应用是相对小的应用 (根据本发明, 通常小于 90K 字节), 它组合 web 浏览器 (例如, cHTML web 浏览器) 的功能以及实施 UPTF SAS 构架和安全协议的购买应用的功能。它允许移动用户启用和停用付款功能性, 并存储购买的收据。任何零售商或者付款业务都可以提供无线钱包方法, 以便客户用他们的移动电话进行付款。这是使用移动装置解决安全付款问题的纯软件方案。如果无线钱包的提供商是 web 铺面零售商如电影票提供商, 则无线钱包应用 108 可以用来对向该零售商注册的任何账户进行付款。如果提供商是联机付款业务, 则无线钱包软件 108 可以用来对其它联机付款业务用户 (人对人) 或者向使用可呈现多个付款服务界面的这种付款服务或者中间服务/系统来接受付款的“实体店面”零售商进行付款。在后者情况中, 商家可以使用无线钱包客户 108 的商家版本来指定交易信息, 如付款金额。通过客户在使用与商家零售应用软件连接的无线钱包应用 108 上键入收据号 (例如, 在为用餐付款的饭店的收据中打印的收据号) 和/或商家标识符 (例如, 商家的电话号码, 包括商家 POS 标识符等) 这样的方式可以处理识别客户经由移动电话 106 要对什么付款的问题; 其目的是将虚拟购物车与特定消费者捆绑。

更详细的移动付款软件 108 下载和激活如下所述:

1. 在用户使用计算机装置如个人计算机 102 登录提供商 122 的 web 站点后, 呈现使用用户的移动电话付款的选项, 并且把用户重新引到向用户询问用于移动电话无现金付款的移动电话的电话号码的网页上。

2. 提供商 122 对于已经捕获的用户名和口令 (操作 105) 产生 UPTF_ID (随机数), 并且向 STS 120 发送 UPTF_ID 和移动电话号码。因此, 在该实例中, 提供商 122 不必与 STS 120 的运营商分享用户的真实账户信息, 而是提供商

122 和 STS 120 基于由提供商 122 产生的随机标识符将交易与用户相联系。

3.STS 120 随后创建新的可执行无线钱包 108（每个 UPTF 需求，具有“刷新”初始化参数）、下载该可执行无线钱包的链路、可选激活码以及个人标识项(PIE)，在 STS 120 对所有这些进行相关并通过 STS 120 来维护（操作 50-56 和 110）。STS 120 可以向提供商 122 发送 PIE。

4.如果 STS 120 向提供商 122 发送 PIE，则由提供商 122 接收该 PIE，并将该 PIE 显示给用户（操作 111）。任选地，STS 120 可以经由 SMS（例如，操作 116）或者经由提供商 122（例如，操作 111）向用户提供激活码。作为选择，可以通过除了提供商 122 或者 SMS 之外的渠道，例如经由邮件、电子邮件等，将 PIE 和激活码（视情况而定）传递给用户。通常在本发明中，激活码是数字（便于用户输入），并且用作一个时间口令，它加密已下载软件 108 的关于 UPTF 的初始化参数，所以如果在传输时第三方攻击者拦截该软件，则该攻击者不能访问装置特有的初始化参数。

5.STS 利用下载链路向预先输入的移动电话号码传送短消息业务（SMS）消息（操作 112）。

6.移动用户下载无线钱包软件 108（例如在操作 114，可以容易地从 SMS 文本本身直接访问链路），随后使用无线钱包软件 108（操作 116）。初始激活可以包括使用激活码。反之，在操作 116，用户通过仅仅使用 PIE 可以随后使用无线钱包软件 108 以执行移动电话无现金货币交易。

在操作 114 后（在把无线钱包应用 108 下载到移动电话 106 之后），无线钱包 108 准备使用；可以使用向无线钱包提供商 122 注册的任何账户来付款购买和/或财务交易。分发软件的此方案保证在请求时软件的安全发布和 PIE 的安全分发。移动电话无线钱包软件 108 的发布模型被实施，以在移动电话 106 上下载和安装可执行 J2ME。软件 108 的操作非常容易，并且交易时间主要依赖于移动电话电信公司网络的速度。基于测试，移动电话无现金货币交易时间可以在 30 和 45 秒之间变化，该差值归应于移动电信公司的关于网络的延迟。对于每次交易，由移动付款软件应用 108 产生的通信量（在确定要购买什么之后）小于 1K 字节（发送/接收），因为每个移动电话无现金货币交易消息可以小于 256 字节。在无限实例中，付款期间在移动电话 106 与 STS 120 之间的通信或者通过提供商 122 来路由或者直接路由到 STS 120（依赖于财务交易的

类型，下面将详细说明），并且经由移动电话通信网络上的互联网超文本传输协议（HTTP）传播。更具体地说，由于 UPTF SAS 安全是基于消息视图（如下文的更详细说明）加密（即，不基于通信对话安全性），比如安全网络通信接口层（SSL）的无对话，因此充分提高通过移动电话 106 进行的安全交易处理效率。

图 2 是根据本发明实施例的执行移动装置无现金货币交易的通用交易构架安全协定提交（UPTF SAS）系统结构的方框图。在图 2 中，颜色用来加亮这里所述的特征/概念。通用交易构架（UPTF）基于独立和匿名交易协定视图和用于传送该视图的称作安全协定提交（SAS）协议的通信安全协议来定义系统结构。UPTF 实际上提供导管（vessel），该导管能够使用通信网络将交易协定的各自视图从交易中涉及的每一方传送到用于验证的受信赖的第三方，其中所述通信网络可以包括诸如无线 LAN 或者蜂窝链路的不安全部分。当用于诸如电子无线钱包的财务应用时，交易方是付款者 200 和收款者 202，例如客户付款者 200 和商家收款者 202，并且“协定”的典型实例可以读出：“A 方向将向 B 方为项目 Y 付款 X 美元”。

UPTF SAS 协议使用对称密钥方案加密/解密交易消息，其中密钥仅仅可由各方装置 106 和受信赖的第三方（例如被实施为 STS 120）产生，并且不在各方中传输密钥。换言之，UPTF SAS 提供隐含的用户验证，因为由受信赖的第三方如 STS 120 对发送方加密的消息进行解密来验证发送方。SAS 确保各方的真实性被验证，并且在传递期间，即使当各方彼此不信任并且来自一方的消息由另一方转发给第三方验证时，也能保护信息的私密性（交易方匿名）。UPTF 还提供受信赖的第三方以检验协定的独立视图彼此一致的机制。

在从各方接收的交易视图提取协定数据并且由受信赖的第三方检验数据之后，还需要采取实际执行协定的行为。这由与金融机构交互的受信赖的第三方实现，这些金融机构与付款者 200 和收款者 202 相关联，以便在客户付款者 200 与商家收款者 202 之间建立指定资金的转帐。

在图 2 中显示无线钱包 UPTF 系统结构，该结构包括：操作 UPTF 装置（称作 UPTD）如加载了移动电话无线钱包 108 的移动电话 106 的付款者 200；操作另一个 UPTF 装置的收款者 202；安全交易服务器（STS）120；多个金融机构 204；以及它们之中的若干通信通道。例如，付款者 200 操作与收款者 202

交互的移动电话无线钱包 106，以确定购买交易的细节，并执行 UPTF 协议和它的相应的安全操作 SAS。移动电话无线钱包 106 可以支持经由收款者 202 的服务点（连接移动电话无线钱包 106 的信号存在的地点）发现/连接收款者 202 所需的无线通信能力。与服务点付款者 202 和/或 STS 120 通信的移动电话无线钱包 106 的无线通信能力可以是无线局域网（WLAN）和/或移动电话通信（蜂窝）网络。移动电话无线钱包 106 还可以具有用户界面，用于通过某些通用应用程序与付款者 202 交互，并在需要时连接 STS 120。收款者 202 也可以操作 UPTD，比如实施零售应用程序的商家交易服务器（MTS）302，该服务器 302 负责与付款者 200 交互，执行 UPTF 协议和它的相应安全操作并且与 STS 120 交互。在图 1B 中，在提供商 122 是联机付款系统的情况下，提供商 122 将对应于图 2 的金融机构 204，从而允许经由作为逻辑通信通道的通道 A、B 和 C 进行任何类型的 UPTD 人对人无现金货币交易。当然，STS 120 和金融机构 204 可以由单个实体或者分离实体（视情况而定）实现。

根据这里所述实施例的一个方面，STS 120 是付款者 200 和收款者 202 已经在其上注册的后端验证服务器，该服务器提供在安全 STS 数据库 203 中维护的识别账户信息。用来加密到达/来自每个付款者 200 和收款者 202 的消息的秘密信息也存储在该 DB 203 中。STS 120 从付款者 200 和收款者 202 接收关于在他们之间执行的财务交易的独立产生的 UPTF SAS 交易视图（以下将更详细描述）。STS 120 能够使用来自 UPTF SAS 无现金货币交易消息的信息和存储在 STS 120 数据库 203 中的信息来解码两种视图。在成功解码之后，STS 120 验证该视图消息是原始的、真实的，包含预期付款者 200 和收款者 202，以及验证协定视图中的信息字段彼此一致。STS 120 将维持用于认可目的的消息通知活动的登录。

在图 2 中，明确指示了通信通道的一般设置。所示通信通道反映了根据 UPTF 的交易方通信的匿名（匿名交易方通信通道）。通道 A（Ch A）逻辑上表示付款者 200 与收款者 202 之间的链路。该链路用来协商无现金付款交易的细节。这方面是基于应用程序的并且不认为是 UPTF 构架的部分。Ch A 可能存在或可能不存在，如果存在，则例如在支持 WLAN 的移动电话 106 的情况下，它可能是无线信道，并且/或者在销售金融交易点中使用非 WLAN 移动电话 106 的情况下，通道 A 可以是付款者 200 与收款者 202 之间的口头通信。

通道 B 和 C 是付款者 200、收款者 202 和 STS120 之间的实例逻辑链路。在移动电话无线钱包 106 的情况下，通道 B 和 C 是可以承载互联网通信的移动电话通信网络。在大多数情况下，这些通道不是直接链路，而是包含通过移动通信网络和/或互联网的通信。一般来说，这些通道是不安全通道。从 STS 120 到金融机构 204 的通道 D 是不同类型的通道，它被假设是高度安全通信路径。此外，STS 120 本身被假设安装在受保护的设施中，所以它的数据库 203 在物理上是安全的并且不能从网络访问。

下面参照图 2 描述包含在实例交易中的移动电话无线钱包 106 的操作。付款者（运营商）200 通过明确动作启动 SAS 协议，输入由 STS 120 在操作 110 产生的 PIE。这允许付款者 200 产生交易的视图，并基于 PIE 和软件验证参数用它的私钥加密该视图，然后将加密的视图作为消息发送给 STS 120。类似地，收款者（运营商）202 输入也是由 STS 120 在操作 110 产生的自身 PIE，并产生它自己的交易视图，基于 PIE 和软件验证参数用它的私钥加密视图，然后将该视图发送给 STS 120。STS 120 接收已加密的视图并通过成功的视图解密（即，成功的视图解密来验证用户）和两个或更多个视图（视情况而定）的成功比较（即，交易方视图的成功比较来验证交易）来检验视图。STS 120 随后使用安全反向通道 D 与用来转移资金的付款者 200 和收款者 202 的金融机构 204 交互。STS 120 把收据（或者失败通知）送回给付款者 200 和收款者 202，以完成交易。对于每个预期目的地，也是由 STS 120 来对应答消息加密。

这里所述的其它实例是图 2 的 UPTF 系统结构的特定实例。特别是，物理 POS 配置表示该方案的普通变型。对于该情形，付款者 200 是客户装置，如执行无线钱包应用 108 的移动电话 106；收款者 202 是商家操作的装置。商家操作的装置位于固定的站点，并且可以是更强大的计算机并且提供附加网络服务，比如互联网连接。不使用付款者 120 到 STS 120 的直接通道 ch B，而是通过商家 202 向 STS 120 转发付款者 200 的 UPTF 无现金货币交易消息。在此情况下，通道 A 和 B 将是付款者 200 与商家服务器 302 之间的移动通信通道，以将移动电话用户与商家的交易信息（比如购买可得到的商家产品/服务）捆绑起来，以及由商家服务器 302 将付款者 200 的 UPTF 交易消息转发给 STS 120（参见图 3、5 和 6）。协议的属性防止商家从客户 200 收集个人信息。下面进一步描述作为 SAS 的部分的加密过程的其它细节。

因此,移动电话 106 的无线钱包应用 108 基于称作通用交易构架(UPTF)的普通构架、普通结构和新安全协议,该新安全协议使用无线传输网络上的移动装置进行安全多方协定。该构架被设计成处理专用于预想的普遍环境的几个关键方面。

图3是根据本发明实施例的执行移动电话无现金货币交易的基于UPTF的系统结构的功能框图。通用交易装置(UPTD)是无线移动计算装置,比如移动电话 106a-n,通过在移动电话 106a-n 中安装相应的可信移动付款软件 108a-n 基于 UPTF SAS 来实现无线钱包。一种计算机系统和方法包括:将移动付款软件 108a 与交易方(例如商家联机零售应用 302)的交易信息进行捆绑;由用户在用户移动电话 106a 上输入 PIE;由 STS 在移动电话 106a 执行可信移动付款软件 108a 并呈现提取关系标识符(是从实际标识符移除的级别的标识符)的可选列表,这些标识符对应于与可信移动付款软件 108a 相关的用户已注册财务实体;以及使用 PIE 和软件验证参数,根据 UPTF 交易消息执行与交易方 302 的移动电话无现金货币交易,所述 UPTF 交易消息包括移动电话 106a 的标识符、交易方 302 的标识符以及交易的标识符,其中基于在移动电话 106a 的可信移动付款软件 108a 和 STS 120 相关的组合(所述 STS 相关是可信移动付款软件 108a 与 PIE、软件验证参数、和用户财务实体的相关),和在用户、交易方与 STS 之间的 UPTF 交易消息的独立、匿名的交换来提供移动电话无线钱包。如下面将要更详细说明的那样,可信移动付款软件 108 和 STS 120 相关导致用来保护(例如加密)消息的安全工具(例如,加密密钥)的产生,并因此通过对每个消息进行成功解密来验证发送者,并且在 UPTF 交易消息情况下,通过解密和匹配一个或多个交易方的 UPTF 交易视图来验证该交易。

UPTD 无线钱包可以是支持 WLAN 的钱包大小的计算装置,包括支持 WLAN 的移动电话,它能够检测支持 UPTF 的物理销售点(POS)、使用无线局域网/短距离无线技术(例如,802.11,蓝牙,红外线等)无线连接到 POS、并且允许他们的拥有者用 UPTD 无线钱包进行购买和/或付款。UPTD 无线钱包还可以是没有 WLAN 能力的移动电话。例如通过参照在此引用以资参考的美国待审专利申请 10/628,583(代理案卷号 1634.1022)可以得到清楚的理解,其中描述了使用 UPTD(作为支持 WLAN 的移动电话)的 UPTF 可信交易,该专利申请于 2003 年 7 月 29 日提出,并且由本专利申请的受让人 FUJITSU

有限公司拥有。在这里讨论的典型实施例中，UPTD 无线钱包是互联网和/或能够支持 web 的移动电话 106（以下称作移动电话 106 或者移动电话无线钱包 106）。例如，移动电话无线钱包 106 可以用来在餐馆点菜，然后付款，方式如下：（1）用户消费者 200 通过根据图 1A 的处理激活 UPTD 移动电话无线钱包软件 108 功能，在移动电话通信网络 317 上连接服务点商家 202（例如，所述服务点商家 202 可以是用于电影院票，加油站等的互联网 310 上的零售应用服务器 302，在商家 202 的物理位置上的销售点 315）-零售应用 302 实现虚拟铺面（用来定购物品或者检索付款金额，并可以经由 web 服务器访问），并且实现用来启动移动电话无现金购买的有关 UPTF 的功能；（2）移动电话无线钱包 106 显示提供服务的有效商家 202 的列表（经由图 2 和图 3 中的移动电话无线钱包 106 与零售应用 302 之间的通道 A）；（3）消费者 200 在移动电话无线钱包 106 用简单键盘输入来选择服务（例如点菜或者在结帐柜台付款）；（4）一旦确定购买量，消费者 200 就按压在移动电话无线钱包上的指定付款按钮，由此开始付款阶段并导致从商家 202 检索购买订单（即，协定）；在消费者 200 的目视检查之后，请求消费者 200 输入消费者的安全 PIE（还任意地选择用来付款的那个财务实体账户）；（5）如果交易成功，消费者 200 在移动电话无线钱包 106 上接收确认和收据（服务点商家 202 也接收成功交易的通知）。

重要的是，由消费者 200 明确启动付款阶段（5），从而不能欺骗消费者将 PIN 键入服务于攻击者的网页上。在这里所述实施例的典型实施中，按压付款按钮导致在移动电话 106 执行的浏览应用程序的终止（例如执行线程），以及对用户项目（尽管透明于用户）的新应用程序（例如，另一个执行线程）的启动。只要用户不在没有首先按压付款按钮的情况下输入 PIE，可防止 PIE 的劫持。

零售应用 302 实现虚拟铺面（用来定购商品或检索付款金额，并且可通过 web 服务器访问）和用来进行购买的有关 UPTF 的功能。

移动电话无线钱包 106 可以发布用户体验，以快速和直觉方式执行基于 UPTF SAS 的无现金货币交易。移动电话无线钱包软件 108 通过允许在任何位置（位置独立）与商家 202 连接来发布隐含定位。速度和其简单与统一的界面是有效的，并且通过某些实践，进行交易可以在几秒中完成（例如 30 秒，或

者在 WLAN 移动电话无线钱包 106 的情况下小于 12 秒)；其用时可以小于包括找钱或者物理的纸收据的典型现金或卡交易。消费者 200 可以购买(或者被提供)移动电话无线钱包 106，例如经由签约应用计算机 102 联机。换言之，消费者 200 将获得 PIE 以及获得(下载)无线钱包软件 108，用来使移动电话执行基于移动电话 UPTF SAS 的交易。商家 202 将提供零售 UPTF SAS 功能和购买应用 302、315。

图 4 是根据本发明实施例的基于执行移动电话无现金货币交易的安全协定提交(SAS)协议的 UPTF 无现金货币交易消息的示意图。在图 4 中，用颜色来加亮这里所述的特征/概念。SAS 协议用来加密和提交基于期望的 UPTF 的无现金财务交易的视图。SAS 的消息结构和加密机制被设计成在预想用于无线购买的不安全的普遍通信环境中提供许多期望的安全属性，比如：

- o 验证：由于协定组的完整性，因此协定方和验证方被相互验证；
- o 匿名：协定方可以彼此保持匿名，并且与个人和/或账户有关的信息不披露给其他方；
- o 协定内容的保护：保持协定秘密，它是抗篡改的，不可重播的，并提供了强认可特性。特别是，将连续改变、时间依赖、装置专用密钥用来加密视图。

基本的 SAS 算法非常适合于使用已经限制计算资源的低成本用户装置的系统，同时最小化用户使用的复杂性。此外，使用 SAS 所需的某些信息，特别是 PIE，不永久地存储在 UPTD 106 上，并且不包含在任何数据交易中，所以如果 UPTD 106 丢失或者被盗，则 UPTD 106 不能使用。下面参考图 4 提供 SAS 和加密机制的附加细节。

图 4 显示了视图消息 402、404 (即，UPTF SAS 无现金货币交易消息)的内部结构和产生处理。基于 UPTF SAS 的视图 402、404 作为在 UPTD 106 (比如移动电话 106)中执行的电子无线钱包软件应用 108 以软件和/或计算硬件来实现。由于来自付款者和收款者的视图 402、404 是对称的，因此仅仅描述付款者 200 的视图 402。图 4 中使用的符号被解释如下：

- o DIDc：装置 ID，付款者的 UPTD 装置 106 (消费者(c)或者源交易方)的唯一标识符。
- o DIDm：装置 ID，收款者装置 (商家(m)或目的地交易方)的唯一标

识符。

- RSN: 随机序号。

- TS: 本地当前时间戳。

- TID: 交易 ID, 分配给协定的唯一标识号, 它由 STS 120 维护, 以标识相应的 UPTF 协定视图 402、404。

- MD: 消息摘要

- PIE: 个人标识项, 用户和 STS 120 维护的输入秘密项, 比如字母数字字符串。在这里所述典型实施例中, PIE 仅仅由用户和 STS 120 维护, 交易的另一方和/或金融机构 122、204 不知道和/或不维护该 PIE, 并且该 PIE 被临时称作用于加密付款者视图 402 的付款者 200 的移动电话 106 的中间参数。更具体地说, PIE 不包括在交易消息(例如, UPTF SAS 消息和/或基于 SAS 的信息消息)中, 因而无线钱包软件 108 不传送 PIE。PIE 在为相当短的字母数字字符串, 比如 4 位数字的情况下是安全的。只要用户试图交易, 用户就键入 PIE。最好在用户注册了客户设备 106 所使用的应用 108 之后, 将 PIE 发给用户。在这种时候, 用户也可以选择 PIE。PIE 是字母数字字符串。为了加速用户输入, 使用户更容易记住它, PIE 可以是诸如 4 位或者 5 位 PIN 的数。然而, 在 UPTF 协议执行期间从不传送 PIE 的意义上, PIE 是一条高度安全的信息, 它仅仅为用户和 STS 120 所知, 因此它的秘密将被很好地保护。假设用户可以在移动电话 106 上以安全方式输入 PIE, 或者可以使用诸如指纹传感器的生物统计装置确定地产生该 PIE。例如, 应用于从指纹传感器接收的指纹数据的计算可以用来产生由用户最初向 STS 120 传送的 PIE。只要用户试图交易, 用户就把她的手指贴在指纹传感器上, 由此产生 PIE。该 PIE 不保存在移动电话 106 的永久性存储器中, 而是用作产生交易的加密密钥所需的中间参数, 并且设备 106 不应当保留它大于交易执行时间的期间。如果本发明的特定实施使用不便于用户为每个协定交易输入的 PIE 的格式, 并且装置需要存储它的用户 PIN, 则存储器必须是安全和抗篡改的。

如图 4 所示, 视图 402 包括密文部分(或已加密部分) 406 和可认知(例如, 明文)部分 408。明文部分 408 包括 TID、产生视图 402 的付款者 200 的 DIDc、以及装置 106 的本地当前时间戳(TS)。在这里所述其它功能之中, TS 还用来防止交易重放(replay)。加密部分 406 包括两个关键字段: 包含在

协定中的协定数据和付款者 202 的装置 106 的 DIDm。DIDm 是最小需要参考字段，以便提供 UPTF 协议的期望验证属性。因此，用户可以根据 PIE 和无线钱包软件 108 验证参数 RSN 和交易消息，与一个交易方执行 UPTD 106 无现金货币交易，所述交易消息包括移动电话标识符、交易方的标识符和交易的标识符（例如，标识符和/或有关其它交易的数据，如付款金额等），其中基于在 UPTD 的移动付款软件和 STS 关联（该关联是 PIE 及软件验证参数与用户财务实体的关联）的组合，以及在用户、交易方与 STS 120 之间的交易消息的交换，从而提供 UPTD 无线钱包。

首先，由设备 106 的伪随机数据产生器利用从 UPTD 的本地时钟获得的 DIDc 和 TS（和/或如协定数据的一部分提供的）来产生依赖时间的 RSN。因此，产生器的参数对每个设备 106 都是特定的。随后根据 RSN 和用户输入 PIE（在图 4 中用绿颜色显示）产生加密密钥 K，其中由图 1A 所示的 STS 120 产生 PIE。首先，使用函数 F 来组合 RSN 和 PIE，然后把散列函数 H 应用于结果（通常是字符串），以产生加密密钥。

$$K = H(F(\text{PIE}, \text{RSN}))$$

可以将消息摘要功能应用于协定数据、DIDm 和 DIDc，以产生视图的 MD。MD 可以通过确保其他方不以任何方式篡改或者修改视图 402 的内容来加强安全。随后将具有加密密钥 K 的加密算法应用于 MD、协定数据、DIDc 和 DIDm，以产生视图 402 的密文部分，如图 4 中黄颜色所示。为了进一步保护，SAS 协议使用随机消息填充，以便进一步防止“已知文本”攻击。根据这里所述实施例的一个方面，该实施例使用了用于加密的高级加密标准（AES）、用于随机数生成的基于消息验证的键入散列（HMAC）方案，以及用于散列函数的 SHA1 安全散列算法。

STS 120 具有在加密处理中由每个设备 106 使用的函数和特定参数的足够现有知识，从而当与消息 402、404 的明文部分进行组合时，通过颠倒上述处理能够解密消息 402、404。例如，STS 120 根据视图 402 的明文 408 来恢复 DIDc 和 TS，所述 DIDc 和 TS 用于查找可以存储在 STS 数据库 203 中的客户 200 的 PIE 和 RSN 产生器的其它参数。所述这些用来计算 RSN。随后使用与客户 UPTD 106 生成加密密钥相同的方法来计算加密密钥 K。然后解码视图消息 402 的密文部分 406。

在获得付款者 200 视图 402 的所有可应用字段之后，STS 120 使用包含在先前解码的付款者 200 视图 402 中的 DIDm 和 TID 来定位对于相同交易的付款者 202 视图 404。在经过类似解密处理之后，将付款者 202 视图 404 的协定数据的解码字段与根据付款者 200 视图 402 的相应字段进行比较。如果所有可应用的相应字段匹配（根据应用设计对应），则认为已接收的视图 402、404 被验证。然后执行进一步处理并根据需要触发外部运行。

使用相同加密方法和使用目标设备 106、302 的参数以及原始交易的 TS，由 STS 120 来加密从 STS 120 到付款者 200 或者收款者 202 的任何应答。只有预期的收据才可以解密应答消息，从而确保 STS 的私密保护和验证。

这里描述用于 UPTF SAS 的另一个实例加密密钥产生。在图 4 中，使用视图 402，密钥 KEYc 是 RSNc 和 PIEc 的散列；详细密钥产生过程如下：

当由 STS 创建新的 UPTD 账户时（例如，当由 STS 120 在图 1A 中的操作 110 创建可执行代码 108 时），创建用于 RSNc 的初始化数据，具体地：

1. 使用软件服务函数生成随机的 128 比特种子。

2. 使用软件服务函数在新的 UPTD 账户建立时间还创建随机的 160 比特初始化时间戳。因此在图 1A 中，在操作 110，STS 120 产生装置 106 特有的随机数初始化参数以及初始化时间戳，在操作 114，经由无线钱包应用 108 向 UPTD 装置 106（例如移动电话 106）传送所述初始化参数和初始化时间戳两者。

在图 1A 中，在操作 110，当在 STS 120 创建新账户时，由 STS 120 创建 PIE，具体如下：使用软件服务函数创建 32 字节随机值，将每个字节转换为十进制值字符串，并且将它们全部进行连接以产生长字符串。随机地分割来自该字符串的 4 位数字以创建 PIE。

当需要创建密钥以便加密交易消息时，发生以下步骤：

1. 产生 160 比特当前时间戳，具体如下：

- a. 将当前时间转换为字符串，例如将当前时间转换为 16 个字符串，例如把 2004 年 1 月 26 日 5: 04pm 写为“0000170401262004”。

- b. 获取输出另一个值的字符串和一个方式函数，例如通过利用 SHA1 算法对当前时间字符串进行散列计算，以产生 160 比特输出。

2. 异或（XOR）初始时间戳和当前时间戳，以产生 160 比特输出。该操

作基本上是确定地计算两个时间值之差的一种形式（即，两个值之间的确定变换）。

3. 将 128 比特种子软件验证参数用作数据，并且把两个时间戳的经过异或计算的值用作密钥，计算 HMAC 结果（160 比特值）。HMAC 的结果是 RSNc。HMAC 的使用提供在 RSNc 产生中的不可预测性。

4. 分割 HMAC 结果的第一 128 比特，与用于 160 比特值的 32 比特 PIE（从 4 位数字字符串变换）进行组合（例如，连接）。

5. 计算在操作（4）中的 160 比特流的散列（SHA1）值，并将第一 128 比特进行分割为最终密钥。

在消息的已加密部分中，使用 SHA1（作为选择，可以利用 CRC）的消息（具有填充）的交易部分的散列被使用。

在上述实施例中，作为不受限制实例，提供若干比特的值，并且本发明不限于特定数量的比特值。因此，如参考图 1、2、3 和 4 所示的那样，基于 UPTF SAS 的交易需要装置 106 和设备运营商，装置 106 提供装置特定参数，其中这些参数确定装置特定和时间特定密钥；而设备运营商提供仅仅为 STS 120 和运营商所知的固定 PIE。这两者的组合对于可以被 STS 120 验证的已加密交易请求是需要的。截取一个（或多个）交易消息和成功解密它将不足以推断 PIE 或密钥生成处理中采用的装置特定参数。此外，单一、时间依赖密钥是不可重用的，因为由 STS 120 处理成对的交易协定通知。

因此一种系统和方法包括：由移动电话产生移动电话无现金货币交易的第一视图，根据 SAS 向 STS 传送交易的第一视图；由交易的一方独立产生交易的第二视图，并根据 SAS 向 STS 传送交易的第二视图；以及由 STS 检验第一和第二视图以验证交易，并且由 STS 基于检验促使交易执行。第一和第二视图是对称的，并且 SAS 包括：产生未加密的可认知部分和已加密部分作为交易的每个独立视图，所述可认知部分包括用于第一视图的第一移动电话的标识和当前时间戳，所述已加密部分通过在交易消息上基于 PIE 来执行时间和可信移动支付软件的变换组合来获得，所述交易消息包括交易数据、第一移动电话的标识以及用于第二视图的第二移动电话的标识。

产生 UPTF SAS 视图的可信移动电话无线钱包软件 108 包括：其中的初始化时间戳和初始化随机种子数的软件验证参数，以及其中第一和第二视图是对

称的, SAS 包括: 产生未加密的可认知部分和已加密部分作为交易的每个独立视图, 所述可认知部分包括用于第一视图的第一移动电话的标识和当前时间戳, 所述已加密部分通过在交易消息上基于 PIE 和包含在来自 STS 的可信付款软件中的软件验证参数执行变换组合来获得, 的所述交易消息包括交易日期、第一移动电话的标识以及用于第二视图的第二移动电话的标识。加密的变换组合包括: 基于可信付款软件中的软件验证参数来产生交易随机序号; 和基于交易随机序号及 PIE 产生加密密钥。

加密密钥的产生还包括: 生成当前时间戳; 将当前时间戳转换为字符串; 使用一个方式函数如散列函数以将当前时间戳字符串转换为当前时间戳值; 确定在当前时间戳与初始化时间戳之间的时间差值; 基于初始化随机种子数和所述时间差值来计算用于消息验证的键入散列 (HMAC) 结果, 以产生交易随机序号; 从 HMAC 结果选择比特数作为交易随机序号, 并将所选数量的比特与 PIE 组合; 计算组合的散列值; 以及选择散列值的比特数, 以产生加密密钥。比特数约为 128。

图 5 是根据本发明实施例的与商家进行基于 UPTF 的移动电话无现金货币交易的流程图。计算机系统被描述为包括: 联机付款服务 (122, 204), 安全交易服务器 (STS) 120, 以及移动电话无线钱包应用 108, 其包括移动电话特定的电子财务交易初始化参数, 该参数可下载到消费者的移动电话 106, 以执行与商家的移动电话无现金货币交易, 使用他们的移动电话将货币传送给其它消费者, 或者使用他们的移动电话向其它消费者请求货币。当使用移动电话付款时, 消费者可以选择向联机付款服务 122、204 注册的任何一个账户, 以利用该账户付款。

联机付款服务 (OPS) 122、204 是 web 可访问服务, 这种服务能够使消费者向其他消费者或者商家付款, 或者使消费者或商家向其它客户请求付款。在当前联机付款服务 122、204 中, 消费者 200 通过已经由 OPS 122、204 检验的电子邮件地址 (或者某些其它用户标识符, 比如用户名等) 来识别商家 202 或者另一个消费者 200。OPS 122、204 的用户 200、202 向联机付款服务 122、204 提供他们的个人账户 (信用卡, 银行账户等) 信息, 所以当进行无线设备无现金付款时, 可以使用这些账户的任何一个。安全交易服务器 (STS) 120 是基于通用交易构架 (UPTF) 的系统, 该系统检验查看 UPTF 的交易请

求。

如上述参照图 1B 所述，当用户经由 web 登录 OPS 122、204 时，用户可以看见使他们能够付款或者从移动电话 106 请求付款的选项。在访问与该选项关联的链路时，将向用户询问她想用于这种交易的移动电话 106 的电话号码和对于该电话号码的可能的移动通信公司。在提交该信息时，将向用户显示用来进行付款和从移动电话 106 请求货币的 PIE，并且她还将在指定的移动电话上使用链路来接收 SMS（短消息服务）消息，其中如果访问该链路则能够使她把移动电话无线钱包软件 108 下载到移动电话 106，该软件 108 能够使她利用她的移动电话 106 来付款和请求货币。该链路指向在 STS 120 的与此用户关联的唯一可下载可执行的经由 STS 120 维护的软件验证参数和 PIE。如果用户已经从移动电话 106 访问 web，则她能够访问该链路，并把软件 108 下载到移动电话 106。在完成移动电话无线钱包应用 108 的下载时，要求用户将应用程序保存在移动电话 106 上。从此刻起，应用 108 已准备好使用。所述下载的应用程序可称为移动电话电子无线钱包 108。还称为 OPS 122、204 用户并且将移动电话无线钱包 108 下载到她的移动电话的消费者 200 将称为移动 OPS 用户（与 OPS 用户相对）。所有移动 OPS 用户也是 OPS 用户，所以当使用术语 OPS 用户时，它涉及 OPS 用户和移动 OPS 用户。

正如以上参照图 1A 所讨论的那样，移动电话无线钱包软件 108 是以可在移动电话 106 上安装和运行的语言写入的可执行软件，比如 Java 2 平台微版本（J2ME），无线的二进制运行环境（BREW），可以安装在移动电话 106 上的任何其它语言（从而以该语言写入的应用可以在移动电话 106 上运行），或者其任何组合。由于 STS 120 需要创建、存储和检索用于识别可执行软件 108 和对于每一未来的交易与其相关的用户的数据，所以此可执行软件 108 完全地、或者至少部分地由 STS 120 创建。STS 120 还创建和存储用于这种交易的 PIE。PIE 不存储在可执行软件 108 上，或者不存储在该可执行软件 108 将最终下载到的移动电话 106 上。移动电话无线钱包软件 108 中只包含软件验证参数（操作 50、52）。

此外，OPS 用户可以通过使用移动 OPS 用户移动电话号码从 web 可访问 OPS 122、204 向移动 OPS 用户进行付款，其中所述的移动电话号码用于识别将接收付款的消费者。通常，OPS 用户用电子邮件地址识别其它 OPS 用户。

如果 OPS 用户知道移动 OPS 用户的移动电话号码，则她可以通过移动电话号码识别该用户，并向该用户付款。同样地，如果 OPS 用户期望向移动 OPS 用户请求金钱，则她将必须通过移动电话号码识别该用户。在后者情况中，移动 OPS 用户可以在她的移动电话上接收到告知她某人已经向她请求金钱的 SMS 通知。被请求人可以使用她的移动电话 106 向 OPS 用户付款。

此外，移动 OPS 用户可以使用她的移动电话向其它 OPS 用户付款。如果收款者也是移动 OPS 用户，则付款者可以用移动电话号码识别收款者，尽管如果她这样选择的话她也可以用电子邮件地址标识该收款者。在移动电话中输入电话号码比键入电子邮件地址容易和快速。如果用电话号码识别收款者，则收款者将接收关于该付款的 SMS 通知。如果付款成功，则付款者也将接收通知 SMS。付款者可以选择由此付款的任何 OPS 注册账户。

通过类似地由电子邮件或者移动电话号码（如果用户知道的话）指定 OPS 用户，移动 OPS 用户还可以使用她的移动电话请求 POS 用户付款。请求人和被请求人将接收通知他们成功请求的 SMS 消息。移动 OPS 用户还可以在包含他们的移动无线钱包软件 108 的他们的移动电话中从应用 108 的有关菜单查看交易列表。该列表可以包括涉及移动电话 106 的所有交易，以便实现交易。特别是，这包括从移动电话 106 作出的付款（包括响应付款请求而进行的付款）以及向其它 OPS 用户请求付款。不论所述交易是从 web 可访问 OPS 进行还是从他们的移动电话 106 进行的情况下，OPS 用户可以在 web 可访问 OPS 中查看他们已经进行的所有交易的列表。

从使用移动电话无线钱包软件 108 的移动电话 106 付款和付款请求导致根据 UPTF 加密的 UPTF 消息（例如，402，404），该消息由移动电话 106 的无线钱包 108 传送给 STS 120 和/或由 STS 120 生成（即，在人对人移动电话付款的情况下，STS 可以或者不可以依赖于系统配置和/或应用设计和/或交易方参考建立付款交易的第二视图）。例如，在图 5 中，在成员对成员的情况下，作为人对人交易实例，包含一个付款服务 122、204 的无现金付款交易（其中两个成员都具有已注册的账户），商家 202 交易系统 302 和付款服务 122、204 可以是逻辑上（概念上）的一个实体/系统 500，用于处理（经由在 OPS 122、204 与 STS 120 之间的通道 D）达到/来自 STS 120 的 UPTF 视图。通常，在人对人型交易情形中，每个交易方创建它自己的视图。在使用移动电话无线钱包

106 由一人对他人进行付款情况下，因为其他人（收款者）也许不需要（或者被要求）批准向收款者支付款项，所以收款者也许不需要创建接受该付款的视图。因此，在付款交易的情况下，可以省略收款者视图，并且 STS 120 可以简单地仅仅检验来自付款者 200 的第一付款请求视图 402，或者 STS 120 可以创建代表收款者的他人（收款者 202）的第二视图 404。成对视图 402、404 被用在多个联机付款服务 122、204 的情况下，以实现人对人移动支付交易。根据所述实施例的一个方面，系统 500 还可以包括 STS 120。此外，对从 STS 120 到移动电话 106 的消息的响应是根据 UPTF SAS 加密的 UPTF SAS 消息。OPS 122、204 具有对 STS 120 的安全连接（即，信道 D）。

根据这里所述实施例的一方面，在人对人付款交易情况下，来自 web 可访问 OPS 122（即，在从台式计算机向移动电话无线钱包 106 付款的情况下）204 的付款行为可以通过到达 STS 120 的安全通道 D 来实现，并且不需要根据 UPTF SAS 加密。如上所述，来自 web 可访问 OPS 的付款是立即有效的，并且不需要收款者的动作。此外，STS 120 将接收包括交易的付款行为，解密该付款行为（根据 UPTF SAS 用来验证发起付款行为的请求人），并且将确定收款者是否是仍然有效于 STS 120 并且能通知收款者 202 的移动电话无线钱包 106 的有效移动 OPS 用户。

根据这里所述实施例的另一方面，STS 120 通过在 STS 120 与 OPS 122、204 之间的安全通道 D 可以接收向 OPS 用户付款的请求（即，在请求从台式计算机向移动电话无线钱包 106 付款的情况下）。在收到该请求时，STS 120 将向移动 OPS 被请求人的移动电话 106 传送移动电话无线钱包 106。当移动 OPS 用户使用她的移动电话 106 和移动电话无线钱包软件 108 检验等待请求时，她将看见该请求，并且可以决定向请求人付款。在由 STS 120 收到付款消息时，STS 120 将通过请求再次检验等待请求，将根据 UPTF 方法确定完成的交易是有效的，并由此通知请求人和被请求人。

根据这里所述实施例的另一方面，类似地处理使用用于该请求的她的移动电话的移动 OPS 用户的付款请求。如果被请求人被识别为移动 OPS 用户，则被请求人将接收通知 SMS，并且在用无线钱包软件 108 检验等待请求时将查看该请求，以及可以决定完成付款。STS 120 将使用 UPTF 标准比较到达 STS 120 的请求人的消息，并且确定完成的交易的有效性。在完成确定时，STS 120

将通知 OPS 和请求人以及被请求人。

所有上述交易实例仅仅需要移动 OPS 用户使用移动电话 106 和移动电话无线钱包软件 108，并输入用于这些交易的指定 PIE。STS 120 和 OPS 122、204 可以由同一实体操作和/或在同一计算机系统中执行，或者他们可以由不同实体操作。根据这里所述实施例的一方面，用户可以使用短消息/多媒体消息服务、电子邮件和/或语音消息在移动电话无线钱包 106 通知移动电话 UPTF 的可信无现金货币交易的状态（结果、确认、情况、成功/失败、问题/帮助通知等）。

图 6 是根据本发明实施例的购买电影票的基于 UPTF 的移动电话无现金货币交易的流程图。图 7A-B 是根据本发明实施例的用于执行移动电话无现金货币交易以购买电影票和获得、存储及检索交易收据的移动电话显示屏幕用户界面图像。下面参考图 5、图 6 和图 7A-7B 说明与商家的实例性的移动电话无现金货币交易。在图 5 中，在操作 502，移动电话 106 用户/消费者 200 使用已安装的（图 1A、1B 和 1C）移动电话无线钱包 108 从商家 302 收款者请求购买订单。在图 5 和图 6 中，操作 502 包括将消费者 200 与商家 302 交易信息捆绑起来，例如通过浏览用经由移动电话（蜂窝）通信网络来购买电影票的商家售票应用（商家交易服务器（MTS））302（图 2、图 3）来实现。也可以通过在移动电话无线钱包软件 108 输入商家的标识符（例如 POS 135 交易纸收据信息）来执行用户与商家虚拟购物车的捆绑，和/或移动电话无线钱包可以预存商家标识符（例如，互联网通用资源定位符（URL）地址）。在图 7A 中，例如在操作 502，显示移动电话用户界面屏幕图像 702a-h，以浏览商家售票应用 302，所述屏幕图像包括：在 702a 上选择移动电话无线钱包软件 108；在 702b 上选择“购物”；在 702c 上选择“电影院”；在 702d 上选择“下一个电影放映”；在 702e 上从已显示的电影时间信息中选择电影时间；在 702f 上从所选时间的已显示电影中选择电影；以及在 702g 上完成将传送给商家 302 的购买订单表格请求；和在 702h 上将购货订单请求传送给商家 302，这是消费者 200 与商家 302 交易信息的捆绑，该捆绑通过识别将为什么付款（电子购物车）和付款信息来实现。

在操作 504，移动电话无线钱包软件 108 从商家售票应用 302 接收购货订单，例如这可以导致移动电话用户界面屏幕图像 704，该图像显示电子购货车

的概要，包括来自商家 302 的付款信息，以及“请按压 PAY 按钮”选择。根据本发明一个方面，在操作 504，基于从商家 302 的收款者 202 接收的购买订单由移动电话无线钱包 108 可以识别用作商家的装置标识符 (DIDm) (图 4) 的信息。

在操作 506，选择在 704 的“付款”键开始本实施例的 UPTF SAS 功能。特别是，经由移动电话用户界面屏幕图像 706a、706b，移动电话无线钱包软件 108 请求输入 PIE (例如，PIN) 并产生 UPTF SAS 视图 402 (如参照图 4 所述)，当消费者 200 请求交易时，将请求交易传送给商家 302。如图 6 所示，来自移动电话无线钱包软件 108 的基于 USTF SAS 消息 402，在移动通信公司的网络上或者直接传送给 STS 120，或间接通过商家应用 302，如通道 B 所示。在客户 108 与 MTS 302 和/或 STS 120 之间的传输层采用互联网(互联网协议) HTTP 通信。但是，传输层可以是任何已知的传输层，如 HTTP、web 服务呼叫、基于网络通信接口的通信等。根据这里所述实施例的一方面，用 web 界面来实现 MTS 302，以从移动电话客户 106 传送消息和接受来自移动电话客户 106 消息；特别是，在移动电话 106 上运行的移动电话无线钱包软件客户 108，通过将其消息提交给预先指定的、类似 CGI 这样的界面而将其传送给 MTS 302，MTS 302 使用 web 服务呼叫向 STS 120 转发和接收来自该 STS 120 的同样响应。换句话说，UPTF 消息是 HTTP 参数。由于 HTTP 是无国界的，因此 MTS302 在传送和接收消息的期间使用小数据库来指名国家。而且，由于消息是在 HTTP 上传送的，因此当其在 HTTP 上传送时，将基于加密的 UPTF SAS 消息的十六进制编码以消息的加密的形式用于避免具有专用 ASCII 字符的问题。

在操作 508，MTS302 产生 MTS UPTF SAS 视图 404，作为 MTS REQ，并且将 MTS REQ 和客户请求 REQ (即视图 402、404) 传送给 STS 120。根据实施例的一方面，在操作 506，由 MTS 302 从消费者请求视图 402 的未加密部分来获得用作消费者的装置标识符 (DIDc) 的信息，MTS302 基于该信息产生 MTS REQ 视图 404。

在操作 510，STS 120 从付款服务 122、204 获得消费者 200 的提取的账户列表。特别是，如果在 706b，在消费者 200 输入使用财务账户而不是默认账户的请求，消费者视图 402 包括财务账户信息的请求。在操作 510，STS 120

使用客户 200 的账户关联 123，它是从付款服务 122、204 提供（即图 1A 中的操作 105），以用付款服务 122、204 来确认客户请求。在操作 512，STS 120 从付款服务 122、204 接收账户参考列表（非实际账户）。在操作 514、516，STS 120 经由 MTS 302 将 STS 响应转发到包括账户参考列表的客户请求视图 402。在操作 516，移动电话用户界面屏幕图像 708 显示可选择用户账户参考列表。在操作 518，消费者 200 对交易进行授权。在操作 520，MTS 302 传送 MTS 授权和消费者授权到 STS 120。

在操作 522，响应于操作 520 的 MTS 和客户授权请求，STS 120 传送授权交易到付款服务 122、204，并在操作 524，接收付款服务响应。在操作 526，STS 120 向 MTS 302 转发对授权交易的付款服务响应，在操作 528，MTS 302 将对授权交易的 STS 响应转发到客户 200。特别是，在操作 528，移动电话用户界面屏幕图像 710 显示交易成功确认消息。因此，在操作 508 和 520，STS 120 接收和检验基于 UPTF SAS 的商家和消费者视图 402、404（如解密和交叉参考基于 UPTF SAS 的 MTS REQ 和消费者 REQ 消息以及 MTS AUTH 和消费者 AUTH 消息）

根据这里所述的实施例的一个方面，在移动电话 106 上运行的无线钱包应用 108 在每次成功购买之后接收收据相关信息，如显示屏幕图像 712 所示，根据本实施例的一个方面的屏幕图像在计算机显示屏上是以条形码图像的形式，如移动电话显示屏 106 上显示的条形码图像 714 所示，并且在移动电话 106 上存储这些收据以便做进一步引用和再使用（如显示在移动电话无线钱包 106 的显示屏上，和通过条形码读取器 315 读取计算机显示条形码图像，以便取得对在实际商家服务地点如电影院售票点（POS）315 的付款服务的物理访问）。能够将交易收据相关信息进行远程存储和获取。因此，无线钱包应用 108 提供交易收据管理，在图 7B 中，显示了移动电话显示屏用户界面图像 716a-d 的实例，用于获取交易收据信息。根据本实施例的另一方面，提供使用包括交易收据信息的短消息服务/多媒体消息服务、电子邮件和/或声音消息向移动电话的用户通知移动电话 UPTF 可信无现金货币交易状态的系统和方法，其中收据可以转发给他人（如在购买电影票的情况下，可以将传递给移动电话无线钱包 106 的条形码图像电影票收据转发给进入剧院的另一个人）。因此，无线钱包软件 108 包括基于条形码的计算机显示屏图像 714 的通用收据管理机制。在图

6 中，VPN 是虚拟专用网。

在移动电话 106 上运行的无线钱包应用 108 将浏览器和付款应用结合。浏览器（轻量级 web 客户）用于购买，付款应用组件用于执行 UPTF SAS 交易。

图 8 是根据本发明实施例的基于移动电话显示屏幕用户界面图像以及在请求者装置、安全交易服务器（STS）和被请求者之间用于执行人对人移动电话无现金付款交易的消息流的流程图。图 9 是根据本发明实施例的基于移动电话显示屏幕用户界面图像以及在请求者装置、安全交易服务器（STS）与被请求者之间用于执行人对人移动电话无现金付款请求交易的消息流的流程图。图 10 是根据本发明实施例的整个移动电话显示屏幕用户界面图像以及对于在移动电话上执行人对人无现金货币交易的无线钱包的运营商可用的可能的工作流程。图 11-12 是根据本发明的执行各种移动电话无现金货币交易的移动电话人对人无现金货币交易消息格式的示意图。参照图 8、9、10 和 11 说明人对人付款和人对人请求的实例。图 8 是当移动电话付款者 200 通过付款请求或通过从收款者 202 接收到付款请求的应答而进行付款时的人对人付款的流程图。在图 8 中，在操作 802，移动 OPS 付款者 200 启动移动电话无线钱包 108，并选择对应于移动电话用户界面显示屏幕图像 1002 的选项“P2P 付款”（表格 0）。在操作 804，用户选择对应于移动电话用户界面显示屏幕图像 1004 的选项“进行付款”（表格 1）。另外，在操作 806，用户选择对应于移动电话用户界面显示屏幕图像 1004（表格 1）的选项“等待请求”。如果在操作 804，用户选择“进行付款”，则在操作 810，通过移动电话用户界面显示屏幕图像 1006（表格 2）提示用户，以输入电话号码/电子邮件地址。在操作 804 和操作 806 之后（根据具体情况而定），通过移动电话用户界面显示屏幕图像 1010（表格 4）或 1018（表格 7）提示用户输入 PIE，如 PIN。在操作 812，当用户输入 PIN 时，移动电话无线钱包软件 108 使用输入 PIN 以根据 UPTF SAS 消息视图 402 创建加密的收款者 id 请求/等待列表请求（根据具体情况而定），并将消息视图 402 传送到 STS 120。在操作 814，STS 120 接收到消息视图 402 并授权用户付款者 200，识别收款者 202/返回等待请求列表（根据具体情况而定）。

在操作 814，STS 120 根据 UPTF SAS 消息创建和传送对于“付款请求”或“等待付款请求列表”的响应请求。在操作 816，在“付款”交易的情况下，移动电话无线钱包软件 816 从 STS 120 接收收款者 id（如 udid、id、全名），并

通过移动电话用户界面显示屏幕图像 1012、1014（表格 5、6）分别提示用户，以输入付款者 200 想要付款的金额并确认。在操作 818，在“等待付款请求”交易的情况下，移动电话无线钱包软件 108 从 STS 120 接收等待付款请求列表，通过移动电话用户界面显示屏幕图像 1016、1018（表格 8、6）分别提示用户，以从等待的收款者付款请求列表中选择并确认。在操作 814 中，为了进行付款交易，如果不要收款者 202 确认消息视图 404，则 STS120 仅授权给付款者 200 消息视图 402 并识别收款者 202。在操作 814，为了响应于来自他人的付款请求而进行付款交易，STS 120 根据 UPTF SAS 分别检验付款者 200 和收款者 202 的消息视图 402、404。

在操作 816 和 818，移动电话无线钱包软件 108 传送包括付款者、收款者和金额信息的付款消息视图 402，在操作 820，STS 120 接收并处理付款消息视图 402（显示屏幕图像 1020），并返回最终结果到付款者 200。如果付款交易成功，则也能够通知收款者 202。特别是，在操作 822，移动电话无线钱包软件 108 接收付款结果消息视图 402，并通过移动电话用户界面显示屏幕图像 1022b（表格 10）向用户付款者 200 通知付款结果，并询问用户是否想要对收款者标注书签。在操作 820，能够通过 SMS 或电子邮件向收款者 202 传送通知。

图 9 是当移动电话收款者 202 请求从付款者 200 付款时的人对人付款流程图。在图 9 中，在操作 902，移动 OPS 收款者 202 启动移动电话无线钱包 108，并选择对应于移动电话用户界面显示屏幕图像 1002（表格 0）的选项“P2P 付款”。在操作 904，用户选择对应于移动电话用户界面显示屏幕图像 1004（表格 1）的选项“请求付款”。在操作 906，用户通过移动电话用户界面显示屏幕图像 1006（表格 2）提示用户，以输入付款者 200 的电话号码/电子邮件地址。另外，在操作 908，能够通过移动电话用户界面显示屏幕图像 1006 和 1008（表格 2 和 3）分别提示用户从喜欢的列表中选择付款者 200。在操作 906 和操作 908 后（根据具体情况而定），通过移动电话用户界面显示屏幕图像 1010（表格 4）提示用户输入 PIE，如 PIN。在操作 910，当用户输入 PIN 时，移动电话无线钱包软件 108 使用输入 PIN，以根据 UPTF SAS 消息视图 402 创建加密收款者验证请求，并将消息视图 402 传送给 STS 120。在操作 912，STS 120 接收付款者验证请求消息视图 402 并验证用户收款者 202，识别付款者 200 并

确定付款者 200 信息,并将付款者 200 信息返回给移动电话无线钱包软件 108。

在操作 912, STS120 根据 UPTF SAS 消息视图 402 创建并传送响应请求。特别是,在操作 912, STS 120 创建付款者 200 信息(如 udid、id、全名)。在操作 914,移动电话无线钱包软件 108 从 STS 120 接收付款者 200 的信息(如 udid、id、全名),并通过移动电话用户界面显示屏幕图像 1012、1014(表格 5、6)分别提示用户,以输入用户收款者 202 要求从付款者 200 付款的金额并确认。

在操作 914,移动电话无线钱包软件 108 从包括付款者、收款者和金额信息的付款者 200 消息视图 402 传送付款请求,并且在操作 916, STS 120 接收并处理来自付款者 200 消息视图 402(显示屏幕图像 1020)的付款请求。在操作 916, STS 120 通过为付款者 200 创建新付款请求项(付款者可以通过操作 806 请求该新付款请求项)的过程来处理(即根据 SAS 解密和登录)来自移动电话无线钱包软件 108 的接收付款请求。特别是,在操作 916, STS 登陆消息视图 402 的交易标识符,并且参照图 8,在操作 806,付款者 200 能够选择“等待付款请求”,以接收操作 916 的包括交易标识符的已创建付款请求。在图 8 中,通过操作 812、814 和 816,付款者 200 创建包括付款请求的交易标识符的相应协定视图 404,其对应于操作 916 的已创建付款请求,并分别通过解密和验证付款者 200 和收款者 202 的视图 402、404 来根据 UPTF SAS 由 STS 120 处理。在操作 916,如果付款者 200 是移动电话无线钱包软件 108 用户,则能够将 SMS 传送给付款者 200,或者另外将电子邮件通知传送到付款者 200。在操作 916, STS 120 将请求结果返回到收款者 202。特别是,在操作 918,移动电话无线钱包软件 108 接收付款请求结果消息视图 402,并通过移动电话用户界面显示屏幕图像 1022a(表格 10)将付款请求结果通知给用户收款者 202,并询问用户是否想要对付款者作出标签。

更特别地,图 11 是六个实例移动电话人对人无现金货币交易消息视图 402、404 的格式图表,包括非加密部分 408 和加密部分 406,用于执行移动电话人对人付款交易。在图 11 中,根据这里所述的实施例的一方面,消息 A 和 C 是信息的信息视图,实质上是 SAS 消息(根据 SAS 加密,其验证消息和内容的发送者),从 STS 120 到移动电话无线钱包 106(消息 B、D 和 G)的响应也是 SAS 消息(根据 SAS 加密,其验证消息和内容的发送者)(即,所

述消息用对应于装置 106 产生的密钥加密（图 4）），即使消息由 STS 120 传送，因此从设备 106 来看，验证发送者（这种情况是 STS 120）和内容，因为只有具有（通过软件鉴别参数和 STS 120）安装的可信无线钱包软件 108 的相应设备 106 能够成功重新构建用于在特定时间（时间戳）加密消息的密钥。消息 E/F 实质上是协定消息视图（交易消息，包括交易标识符，用于包括或涉及两方或多方的协议），该协议消息视图符合 UPTF，并且根据 SAS 加密也是安全的，因此是 UPTF SAS。因此在这里所述的实施例中，根据 SAS 以及 UPTF SAS 执行移动电话交易。例如，消息 A 是在操作 812 之后向 STS 120 提供的在步骤 806 创建的等待付款请求列表消息视图 402。消息 B 是通过 STS 120 在操作 814 创建的等待付款请求列表应答消息视图 402。消息 C 是由移动电话无线钱包 108 在操作 810 创建的人（如同等的人）识别请求消息视图 402，在操作 812 之后将其提供到 STS 120。消息 D 是由 STS 120 在步骤 814 创建的人（如同等的人）识别应答消息视图 402，在步骤 816 将其传送给移动电话无线钱包软件 108。消息 E/F 是在操作 816 和 818 由移动电话无线钱包软件 108 分别创建的付款请求/请求付款请求消息视图 402，并在操作 820 将其传送到 STS 120 进行处理。消息 G 是在操作 820 由 STS 120 产生的交易结果消息视图 402，在操作 822 将其传送给移动电话无线软件。

图 10 示出和描述了移动电话用户界面显示屏幕图像的三种可能的流程。在图 10 中，流程 I 是移动电话用户界面显示屏幕图像 1002、1004、1006、1008、1010、1012 和 1014。在图 10 中，流程 II 是移动电话用户界面显示屏幕图像 1002、1004、1006、1010、1012 和 1014。在图 10 中，流程 III 是移动电话用户界面显示屏幕图像 1002、1004、1018、1016 和 1014。图 12 是用于等待付款请求列表应答（图 11 中的消息 B）的移动电话无现金货币交易消息视图 402 的实例封包图表。在图 12 中，消息 B 视图 402 是根据 SAS。因为根据 SAS 加密，“消息”部分包含消息的实际内容。图 12 示出了用于等待付款请求列表应答的消息 B（图 11）的实例。消息格式 1202 是为应答消息 A 由 STS 120 传送的等待付款请求列表应答消息 B 的“消息”部分。消息格式 1202 包括一系列等待付款请求和一系列提取的账户标识符以便为付款而进行选择。填充（padding）1 和填充 2 可以是随机数字，以隐藏“消息”部分的位置。Ptr1 和 Ptr2 是表示“消息”部分开始的指针。

提供真正的移动（服务地点独立的）电子匿名可信无线钱包 106，其中用户不携带任何财务账户信息，移动装置不临时性和/或永久性存储任何实际用户财务账户信息，该移动装置不需要被在上面刷卡和/或与销售点（POS）读取器相连接（即用户不必在收款人位置）以执行移动可信无现金货币交易，并且不需要在移动装置和/或者经由移动装置由用户来刷银行卡。移动电话包括：存储移动付款软件的计算机可读媒体，该软件在安全交易服务器（STS）上用软件验证参数初始化，作为可信的移动付款软件；和程序控制计算机处理器，用于通过根据以下处理来控制移动电话执行可信移动付款软件，所述处理包括：提示用户输入个人标识项（PIE），和将可信移动付款软件作为移动电话用户的移动电话无线钱包，根据 PIE 和软件验证参数来产生变换的可信移动电话无现金货币交易，从而适合移动电话的基于 UPTF SAS 的交易。

尽管上述实施例指导了移动电话用户电子可信无现金货币交易，但是这些实施例不限于无现金货币交易，可适合于任何类型的用户电子可信交易。用户移动电话无线钱包 106 提供始终工作、始终可用、始终可访问的“覆盖区（footprint）”用于使用可选择账户进行访问、发布和付款业务。“覆盖区”是根据移动电话应用平台如 J2ME 和在消费者移动电话 106 上运行的可信移动电话无线钱包应用 108。可信移动电话无线钱包应用 108 可以在不需要移动电话通信公司的协作、参与和同意的情况下由“商业”直接分配和管理。由用户安全访问的包括“敏感”数据如付款的服务由用户安全地访问，所述数据具有简单的用户维护（即不永久存储在移动电话 06 上）的标识符，如 4 位 PIN。此外，可以提供用于在付款之上的附加业务的提供商控制的“覆盖区”。

例如，在使用用户移动电话无线钱包 106 的电影票购买服务的情况下，主要服务将会是在任何地点（移动电话）的付款和在电影院中的服务点的退回，以获得进入许可。一些附加服务实例可以是在电影购票之前浏览电影时间表、评估电影以获得将来购买的优惠（打折）、具有直接奖励的喜爱节目，下载预览，并且可以基于客户资料提供电影时间的通知。另外，在开始移动电话无线钱包应用 108 时能够传送可访问的促销/广告的通知（SMS）和/或使用所述无线钱包应用 108 来退回（例如，与对某物付款和应用的促销的付款结合）。

其它移动电话无线钱包应用 108 服务实例包括用于人对人和消费者联机商家的财务相关交易。附加服务可以是联机拍卖相关服务，如为联机拍卖服务

消费者的初始化信息服务,检查受监视的拍卖等,以及对成功出价的另一交易方的付款。另外,可以与移动电话有关提供铃声、游戏、数字/媒体内容、软件、广告、商家优惠券等奖励机制(或铃声、游戏、数字内容/媒体、软件等购买的积分),以使用移动电话无线钱包应用 108 进行移动付款。特别是,根据这里所述实施例的一方面,提供一种系统和方法,其将无线钱包 106(如无线钱包软件 108 付款交易/购买)与交易结合到用于接受/购买移动电话相关项目的奖金系统,所述项目如铃声、游戏、数字/媒体内容、软件等。根据这里所述本发明的另一方面,提供一种移动电话奖金系统和方法,其中奖金在例如完成无线钱包 106 付款、自动铃声下载后通过移动电话通信网络立即传送到移动电话。移动电话无线钱包应用 108 使获取和偿还贷款的处理更加容易。消费者可以是联机付款业务、银行、信用卡公司、联机商家和/或作为销售点(POS)的使用移动电话无线钱包 106 的物理商家。

其它示例性移动电话无线钱包应用 108 业务包括定制和支付医生处方,和在获取授权商家之前进行补充。当准备获取、付奖金、通过从移动电话提供医生标识符和处方号并将医生的确认和处方结合而传递处方时,补充的附加通知服务(SMS)到期。

其它示例性移动电话无线钱包应用 108 业务包括付款、库存,使用具有移动电话无线钱包 106 的商店贵宾卡,以及增加特许项目、传送和访问奖金、优惠券等以及退回的附加服务。

其它示例性移动电话无线钱包应用 108 业务包括各种类型财务交易,如浏览账户、基金、股票、销售、购买、转让使用基金、经纪人账户、银行、信用卡/借记卡的股票/基金/债券。股票达到限价时传送到移动电话无线钱包 106 的附加通知服务,发布和访问建议、报告、分析、趋势、跟踪和语音激活。

本发明的上述处理在软件和/或计算机硬件中实现。这里所述的实施例可以看作是服务器端的钱包,可以通过四位 PIN 控制对其的访问,通过多方协议的 UPTF 概念和交易时间独立密钥产生组合以提供预期安全属性。组合方案不需要在移动装置上存储任何重要数据,它不强加特殊硬件要求并“降低”对 4 位 PIN 的安全要求,这显著方便了用户。这里所述的移动电话无线钱包计算速度快;在移动电话上,在使用 J2ME 为每条消息做 160-比特 AES 加密的快速可用移动电话进行密钥产生和加密(解密)(即, SAS 部分)所花的时间

接近 100 ms（慢速移动电话上接近 500 ms）。因此，安全相关计算时间（用于消息在通信链路上传播的时间）相对于交易时间来说并不显著。

鉴于上述优选实施例，适于实现本发明的计算设备 106 可以是任何电子计算设备（能够存储、搜索和处理数据的可编程电子装置），该电子计算装置允许与其它计算装置进行移动（无线）通信，并具有计算机/计算处理器的一个或多个可传达式连接组成，如中央处理器（CPU）；输入单元/装置（如声音命令/控制等的麦克风、键盘/键区、指点装置（如鼠标、指示器、书写笔）、触摸屏等）；输出单元/装置（如计算机显示屏幕（包括其用户界面，如图形用户界面）、扬声器、打印机等）；计算机网络界面，包括其已知的通信协议（如移动电话（语音/数据（互联网））（蜂窝无线网络、人造卫星等）网络，射频技术、局域网等）；存储电子信息的计算机可读记录介质，例如通过计算机/计算处理器和/或电子电路执行的软件（如操作系统、无线钱包软件 108）和/或电子数据（任何已知计算机可读媒体，如易失和/非易失存储器（随机存取存储器）、硬盘、闪存、磁/光盘等）。

从详细说明可以清楚理解本发明的许多特性和优点，因此附加的权利要求目的在于覆盖落入本发明精神和范围内的本发明的这些特点和优点。此外，由于对于本领域的技术人员来说将很容易地进行大量修改和改变，所以本发明不期望限于所示和所述的精确结构和操作，因此所有合适的修改和等同物将属于落于本发明的范围内。

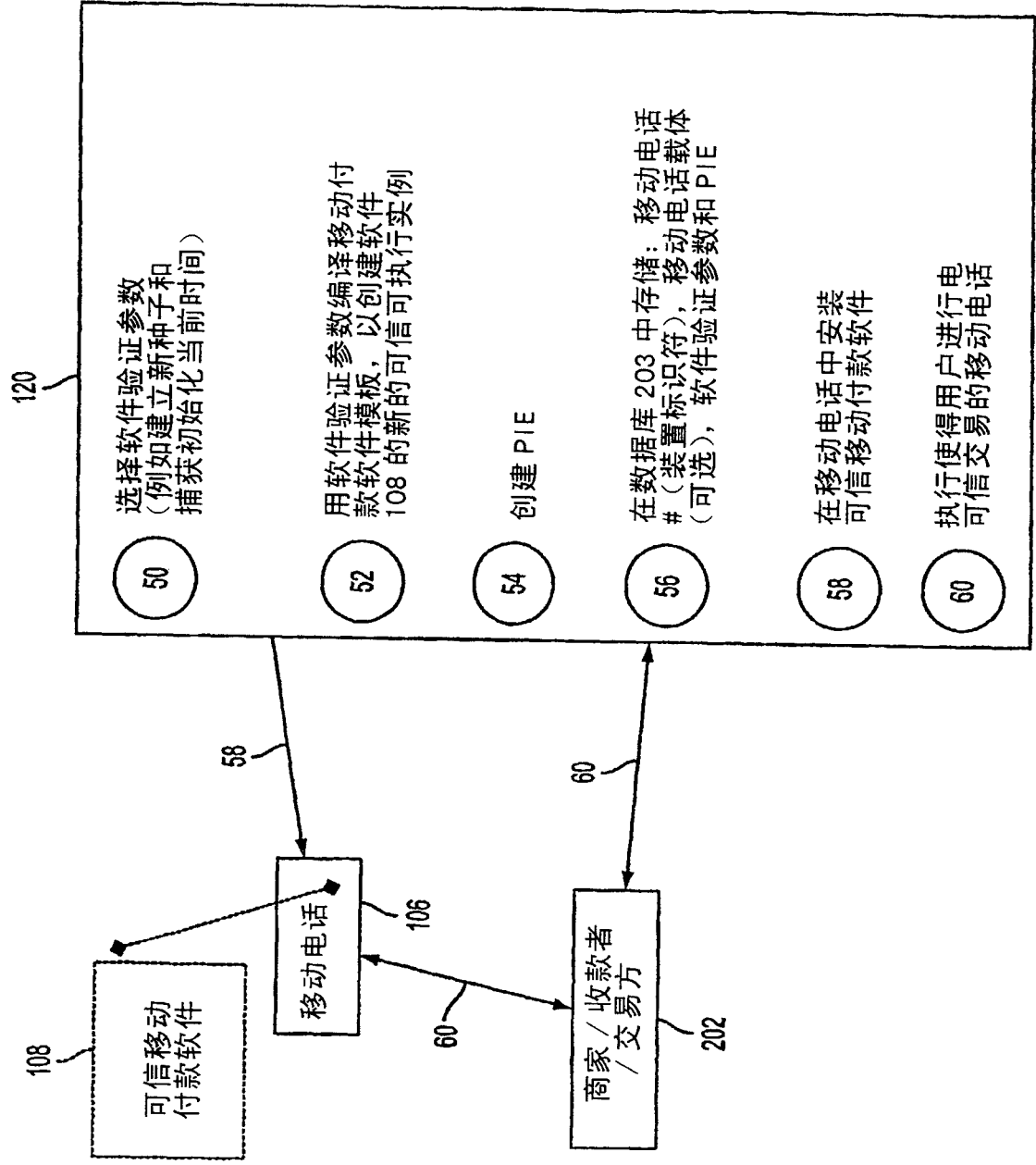
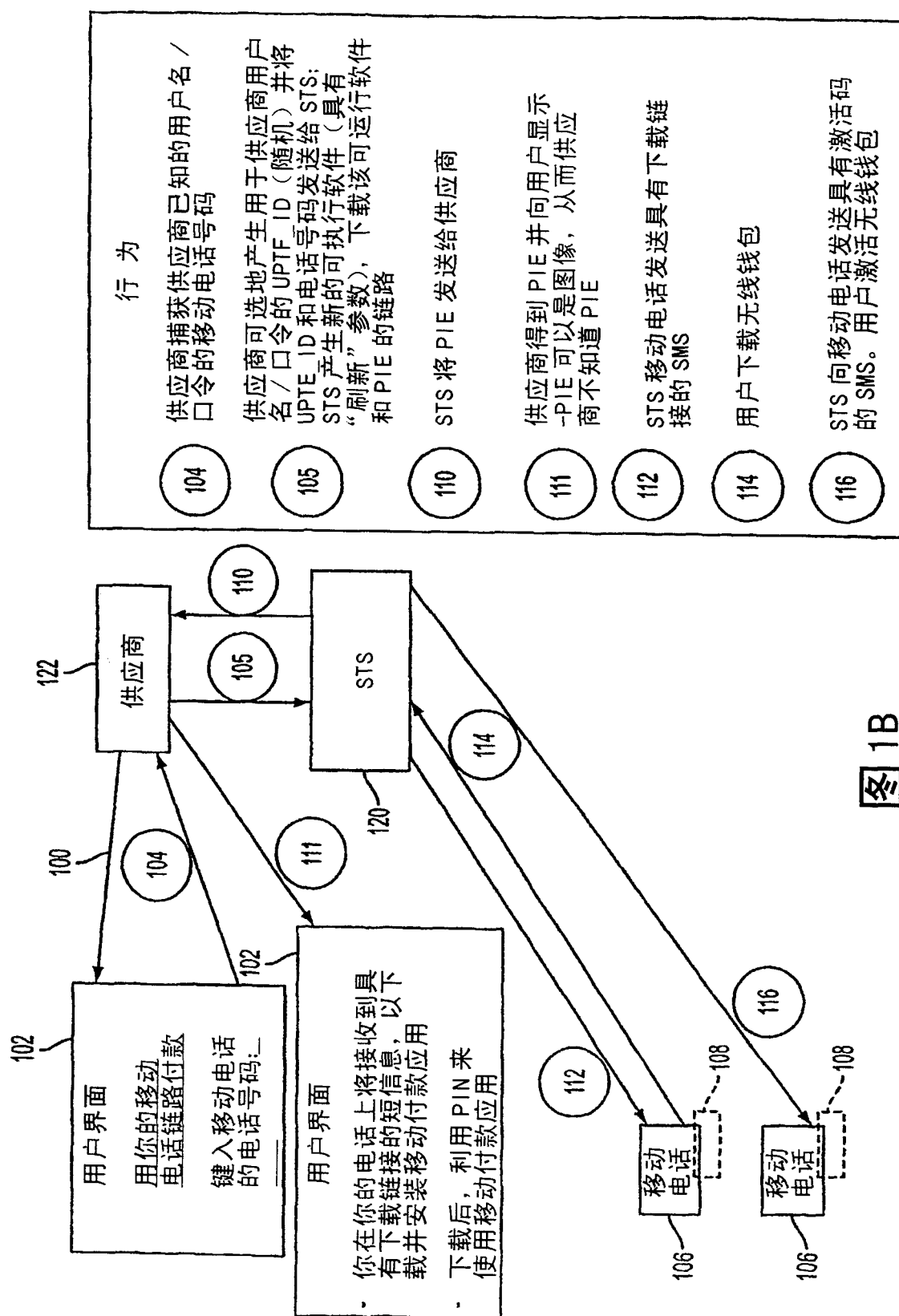


图 1A



18

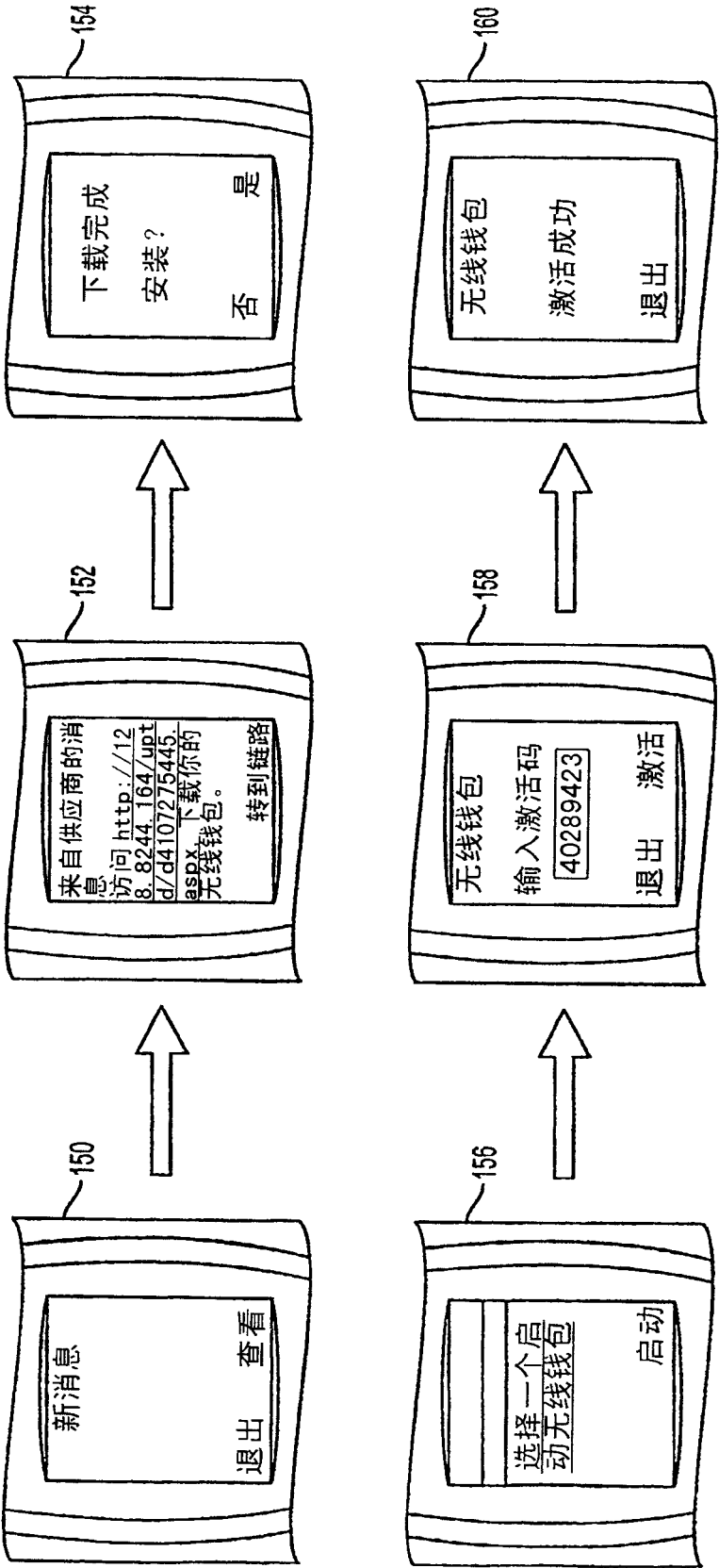
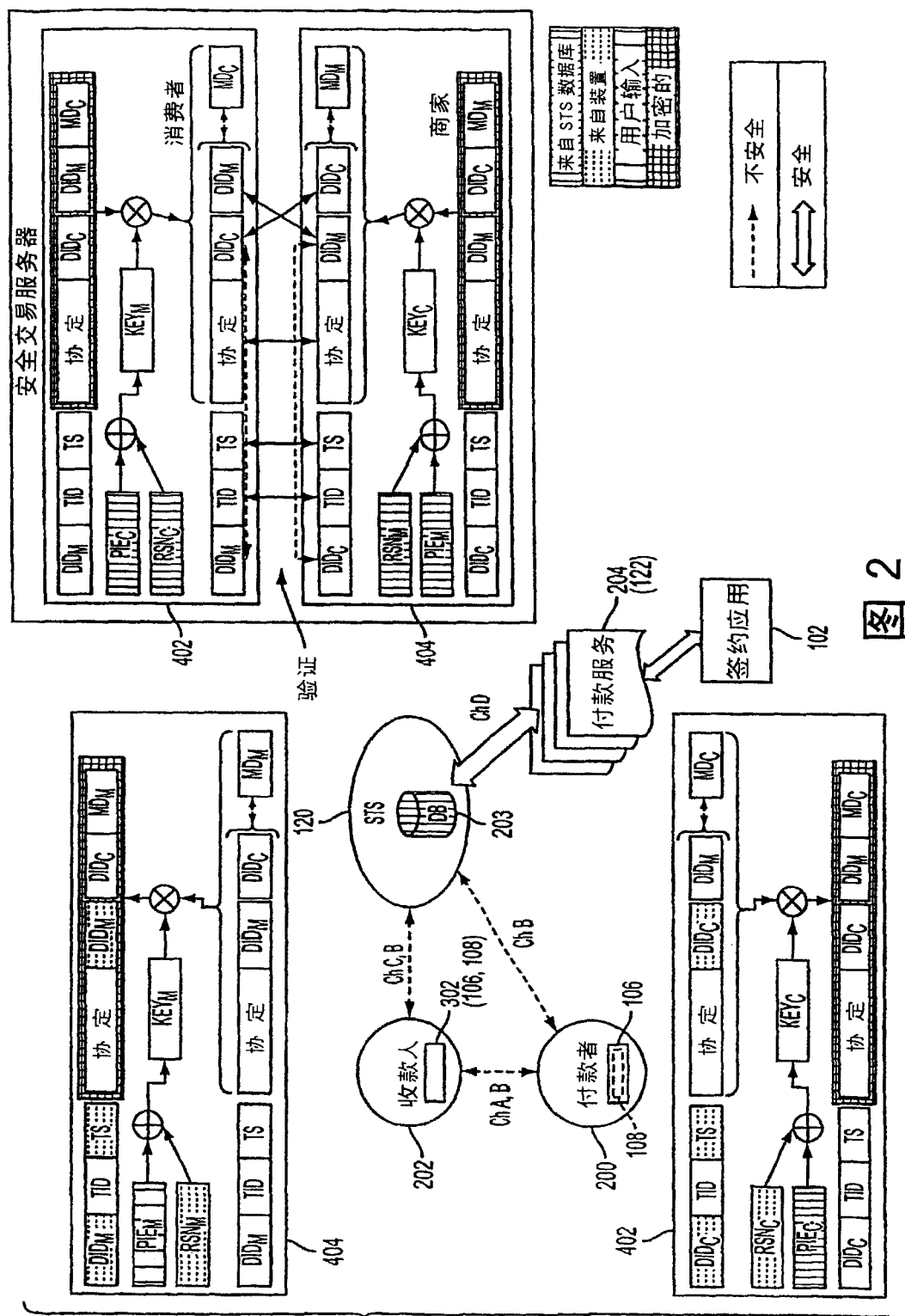


图 1C



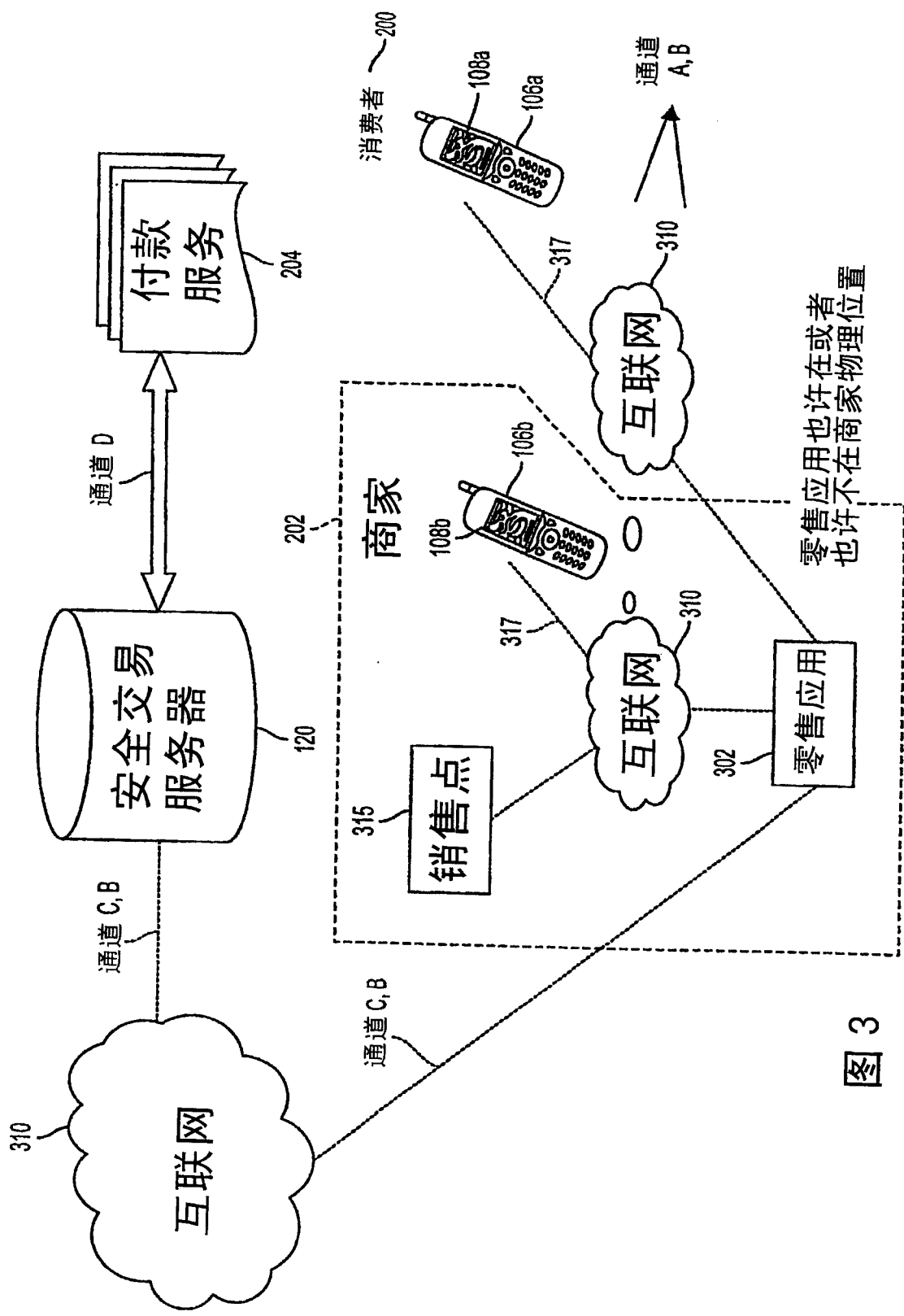
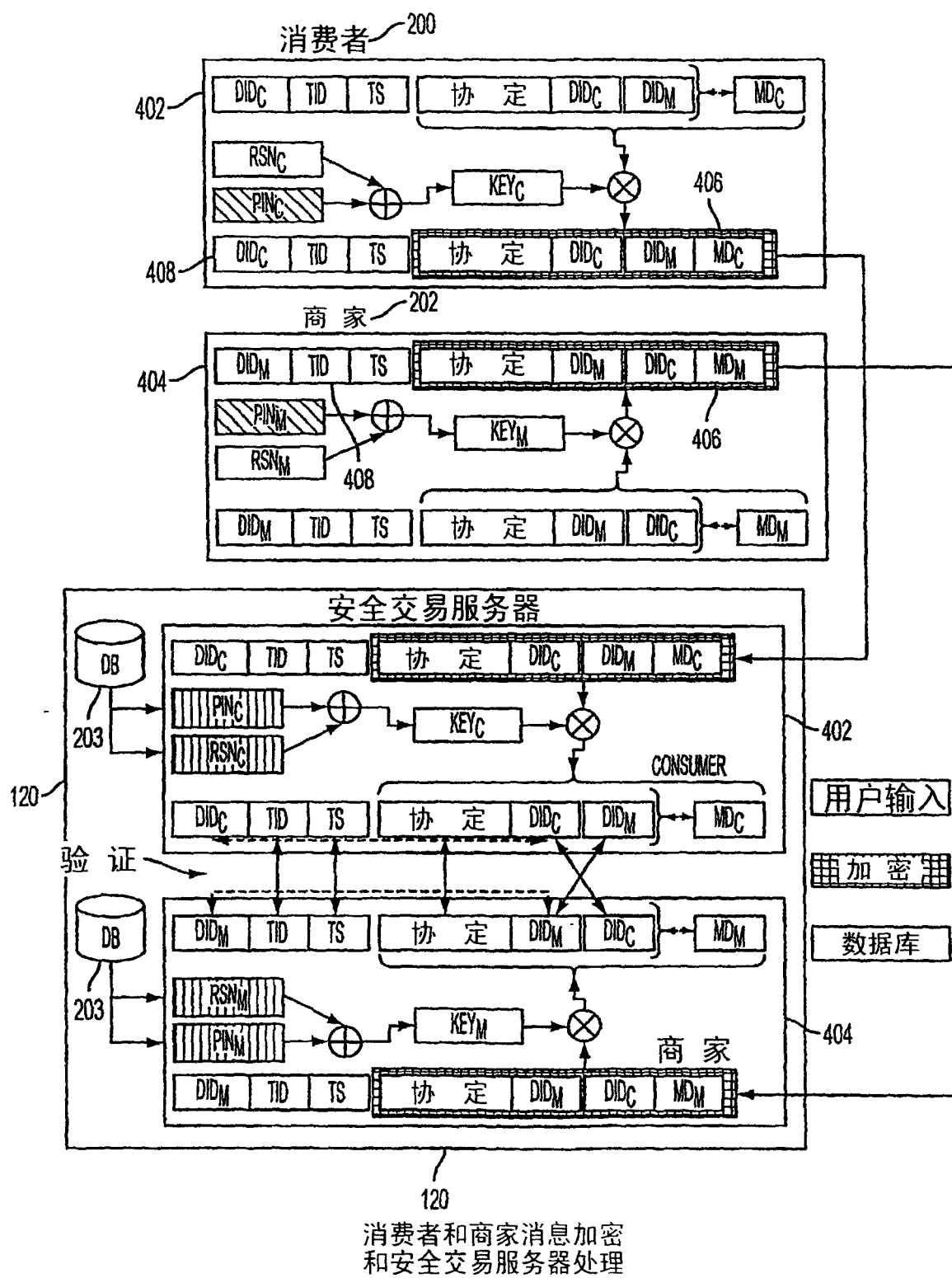
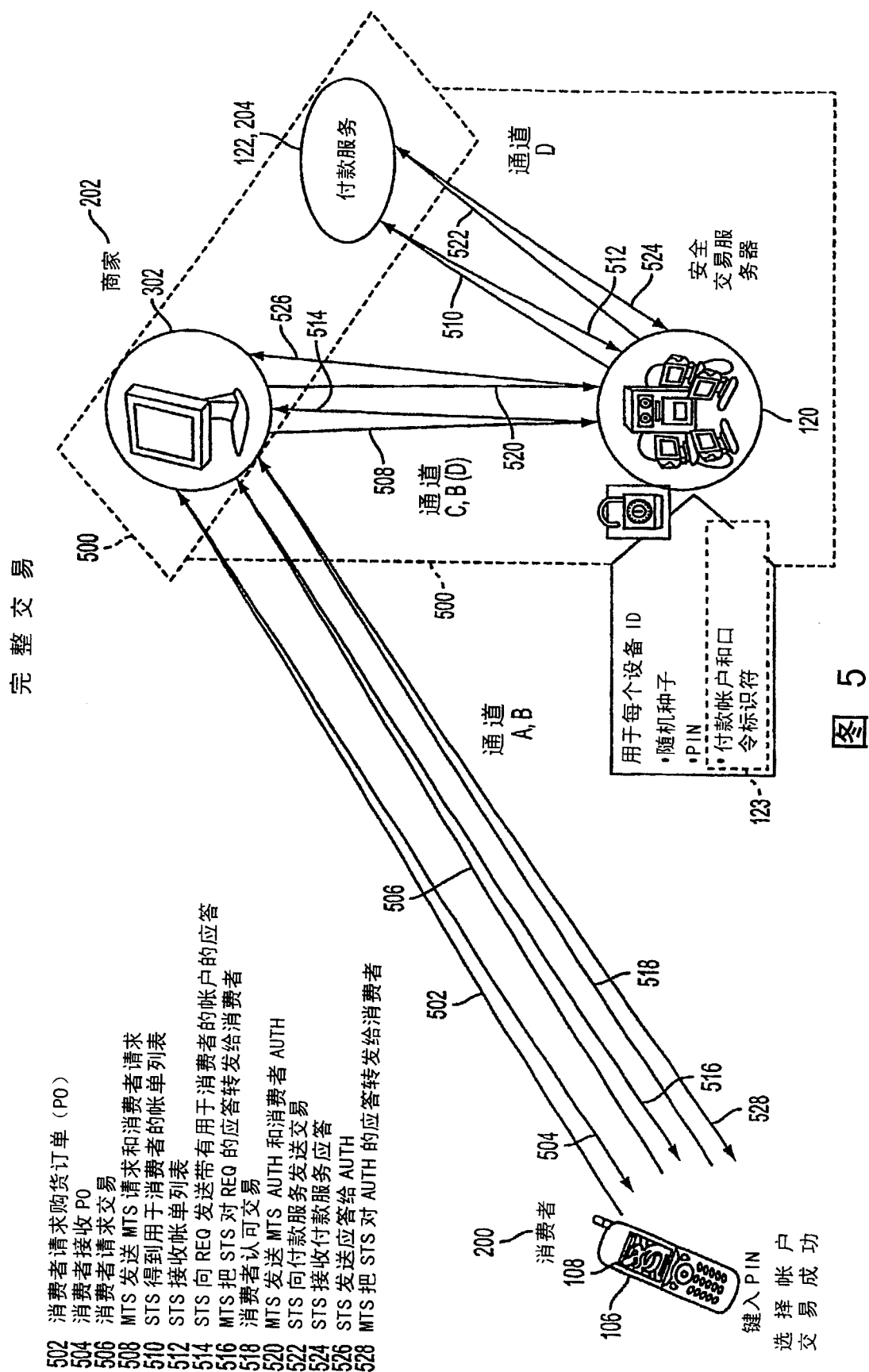
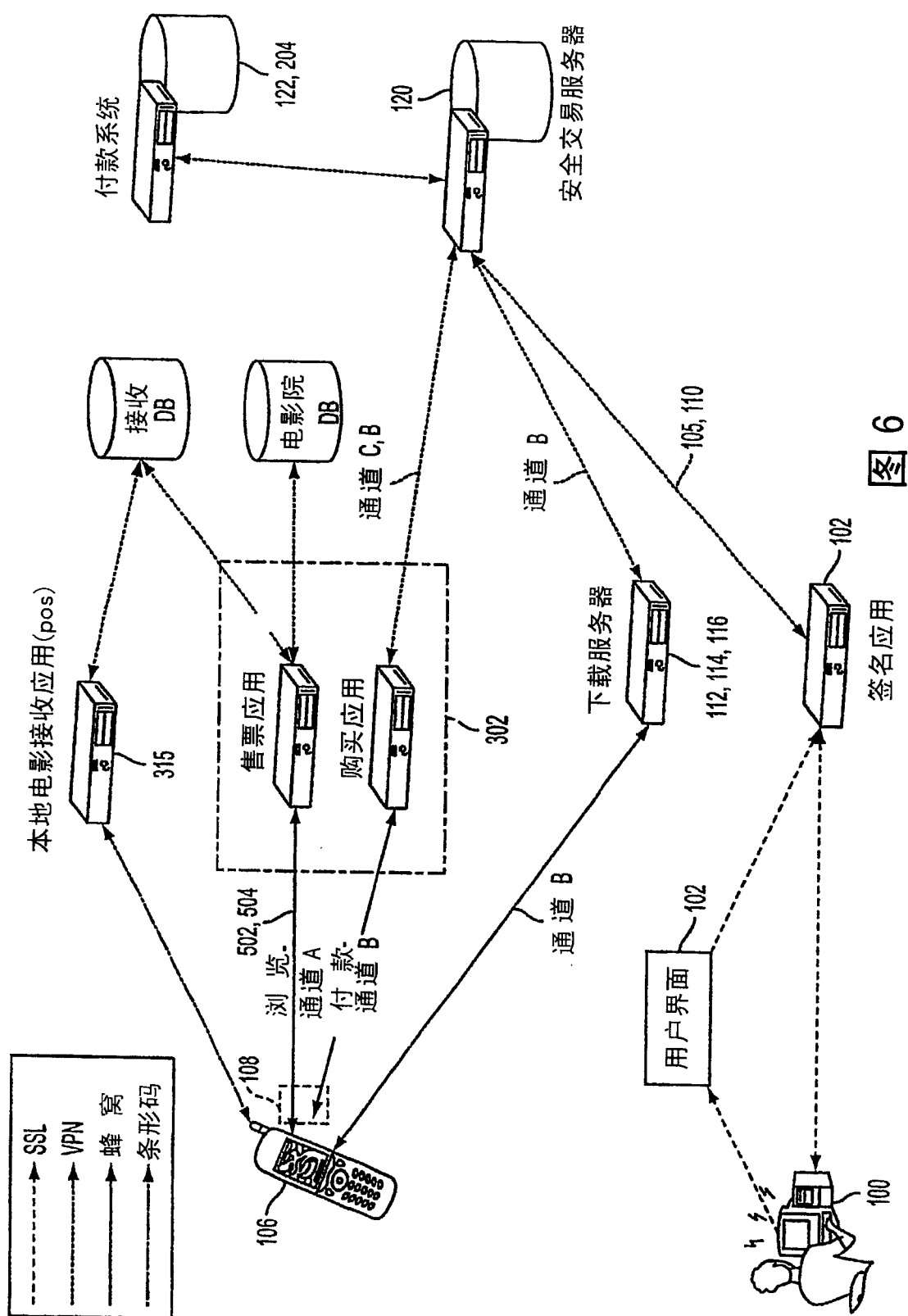


图 3







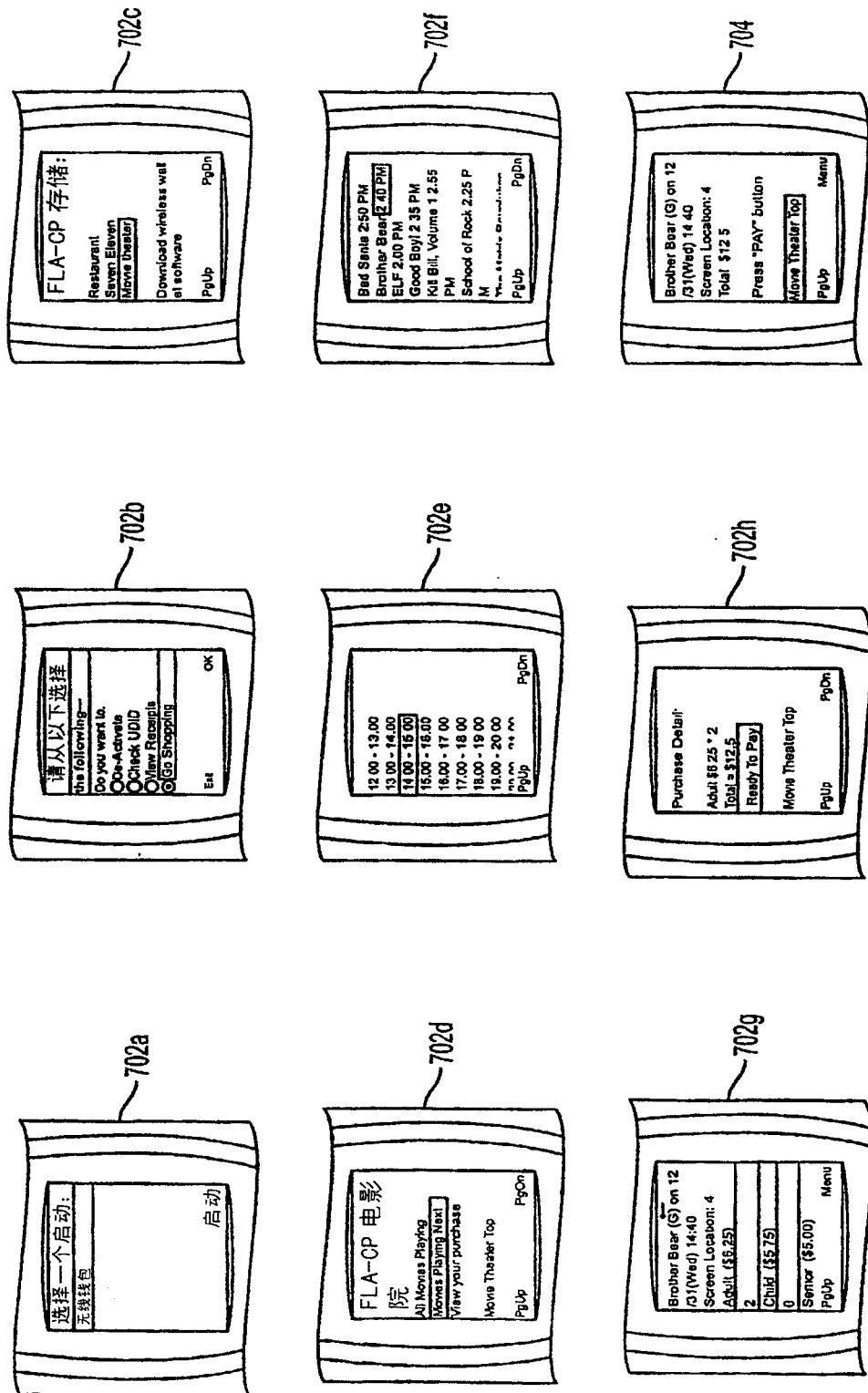


图 7A

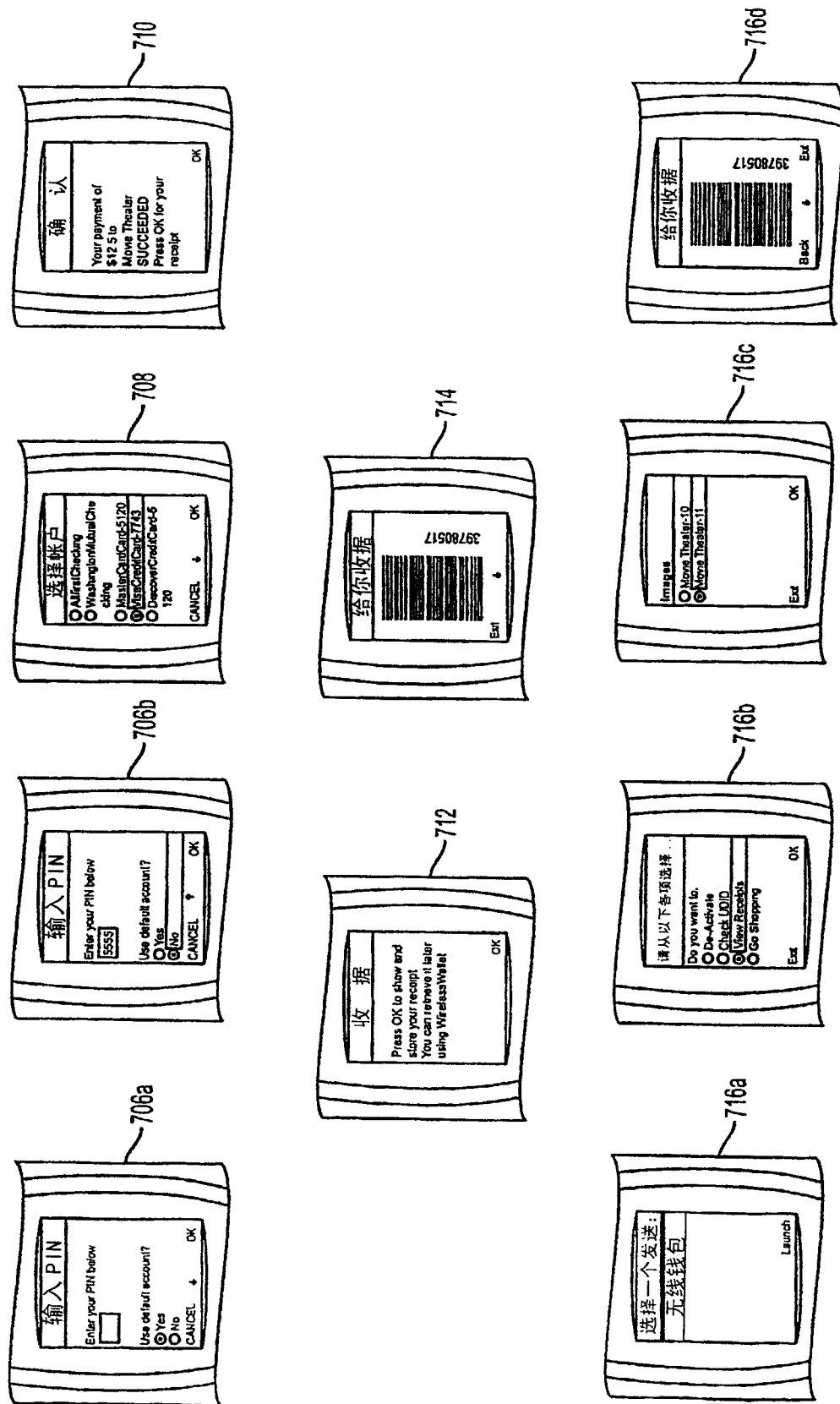


图 7B

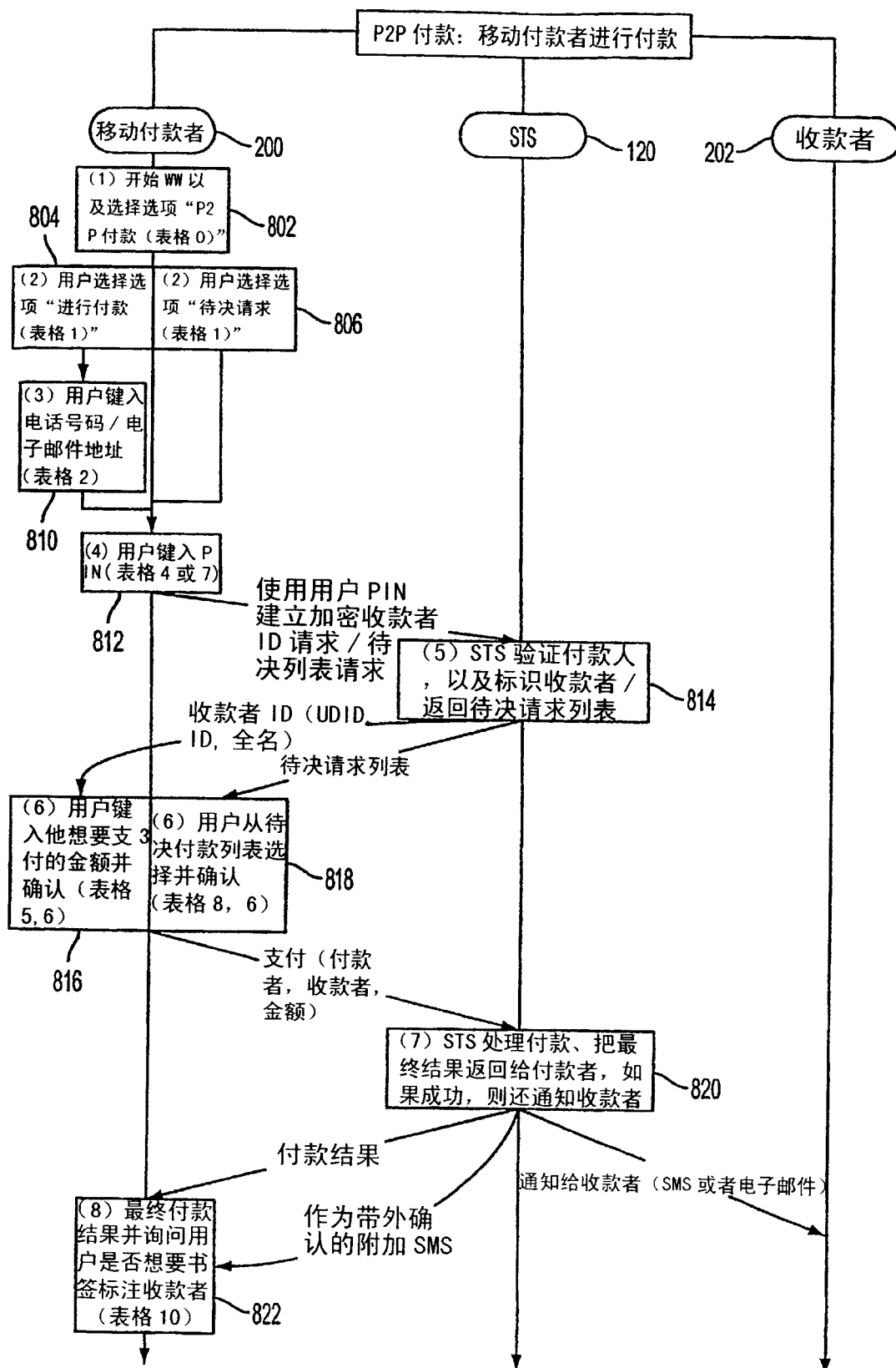


图 8

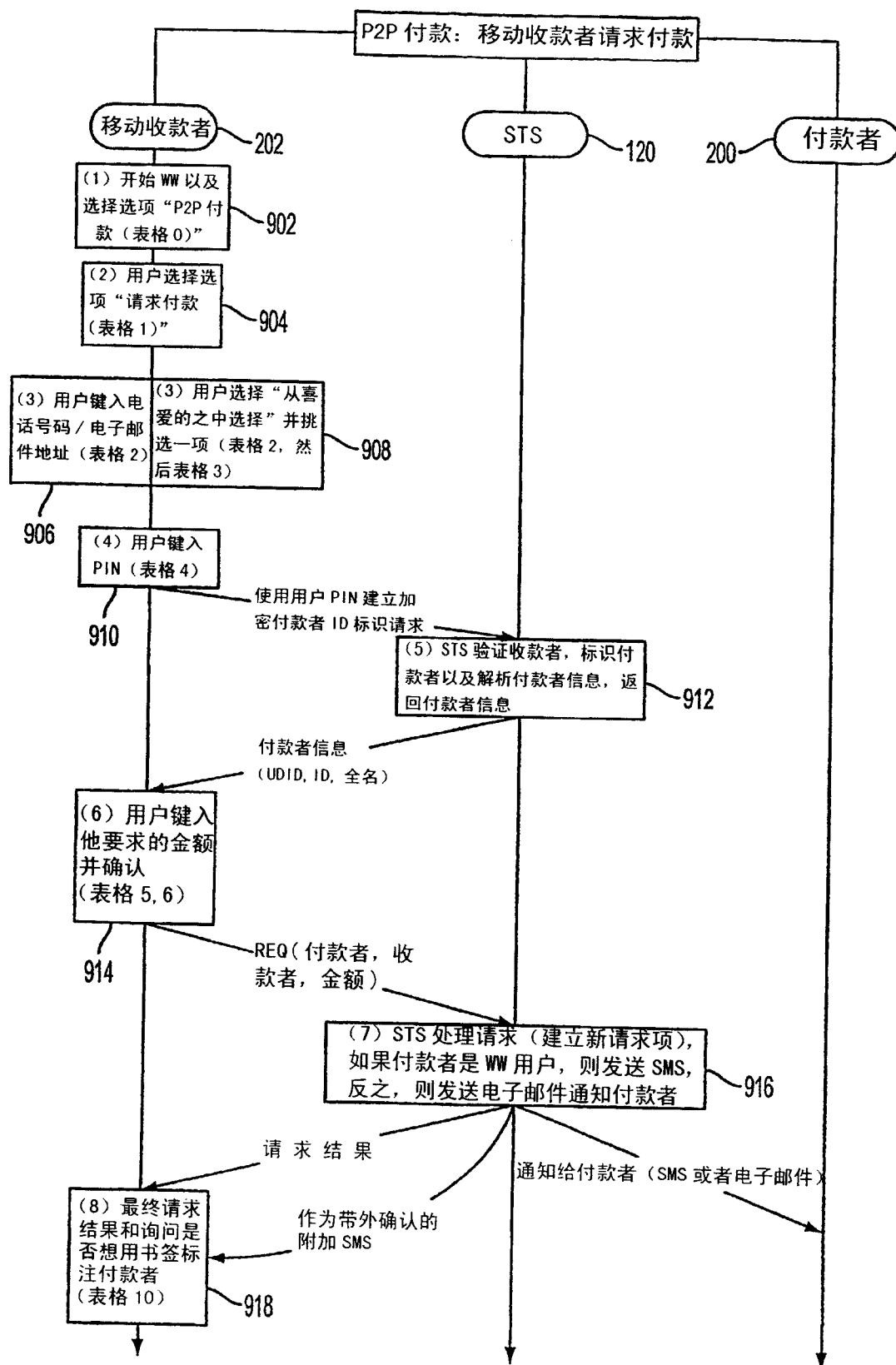


图 9

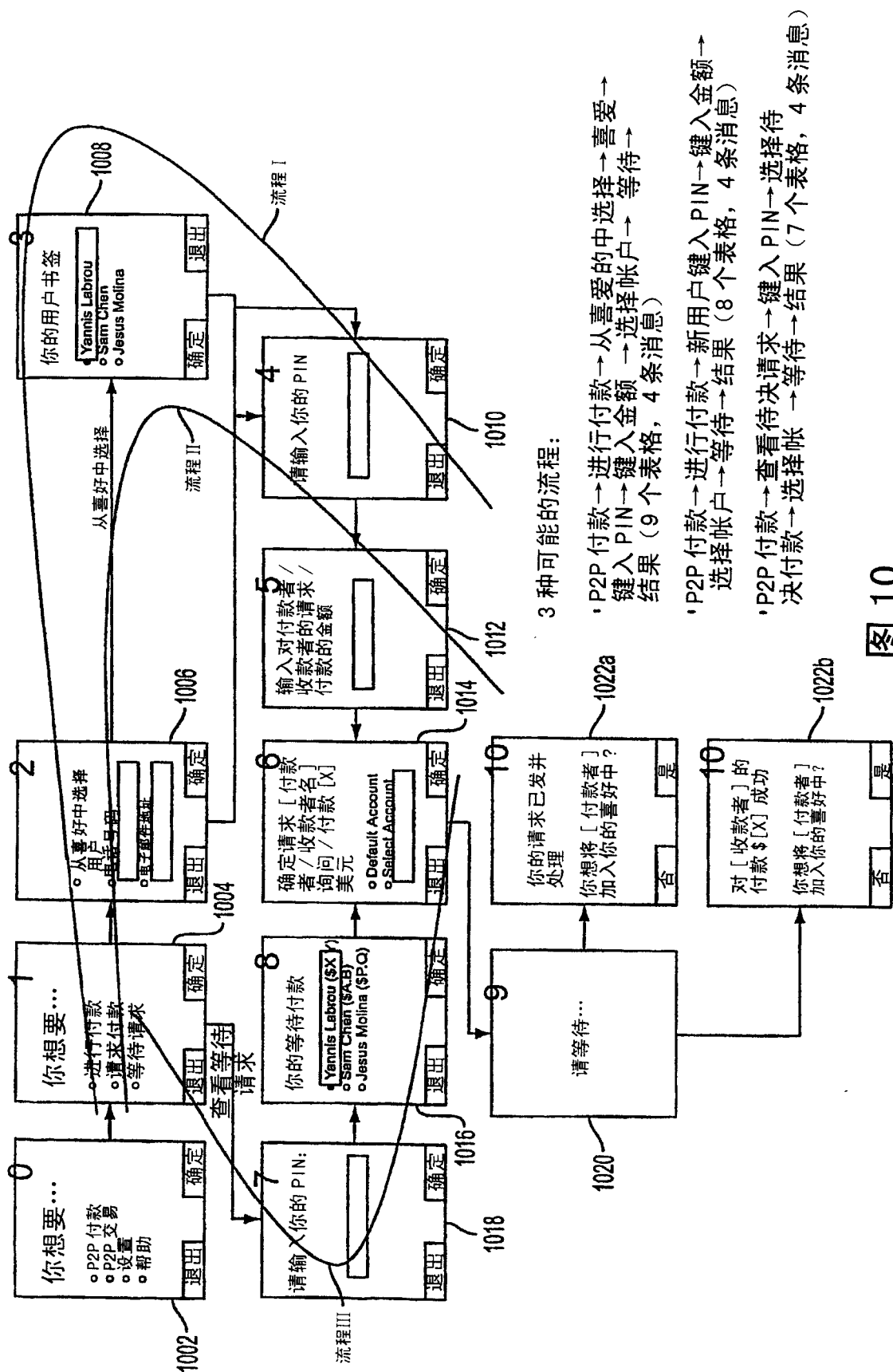


图 10

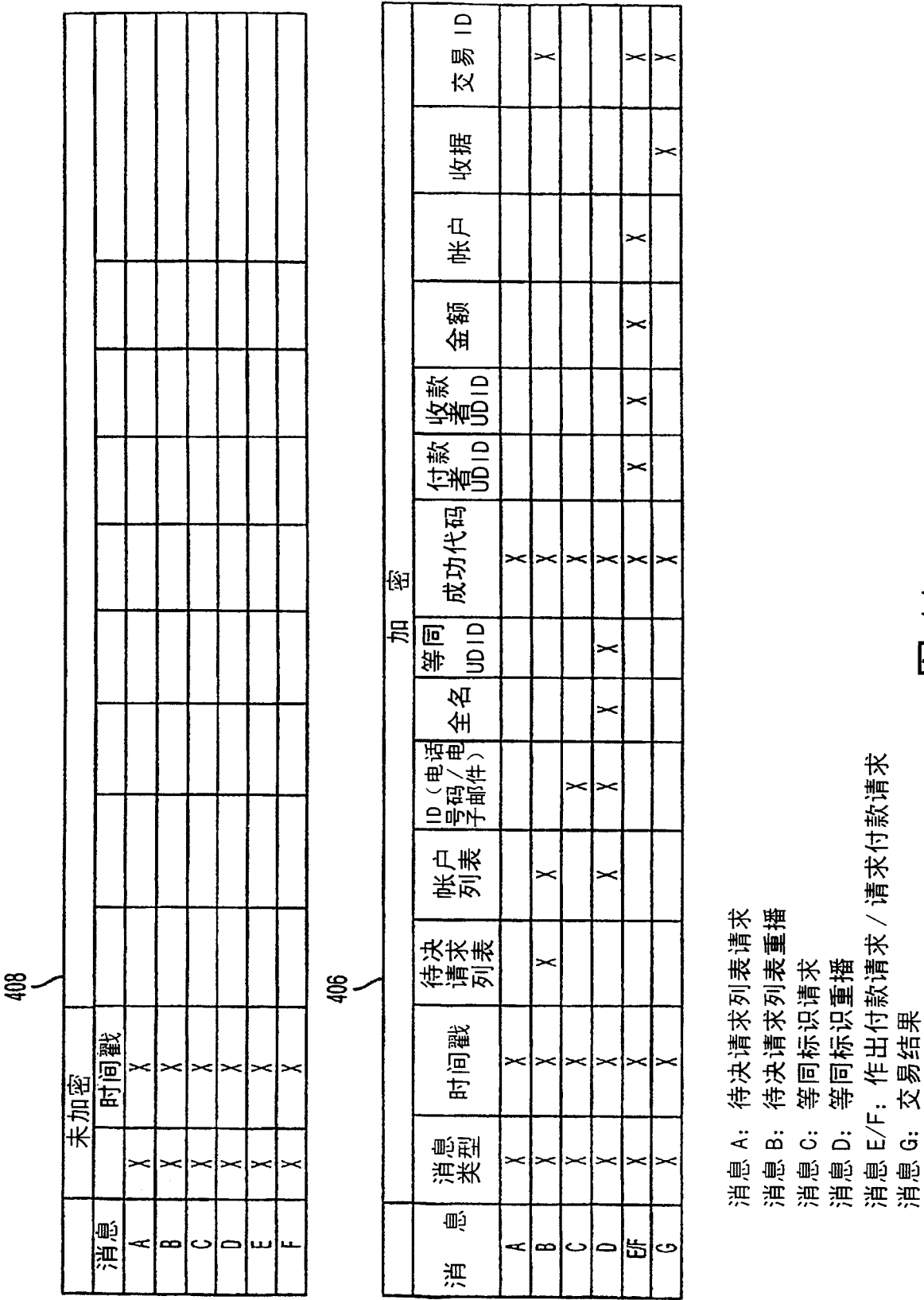


图 11

1202 { 帐户列表格式: 帐户 1\帐户 1\帐户 1\帐户 3...
待决请求列表格式: ID1\UDID1/全名 1\金额 1\TID1\全名 2\金额 2\TID2\UD\ID3\全名 3\TID3\n...
消息封包: 无格式的, 加密, 消息摘要

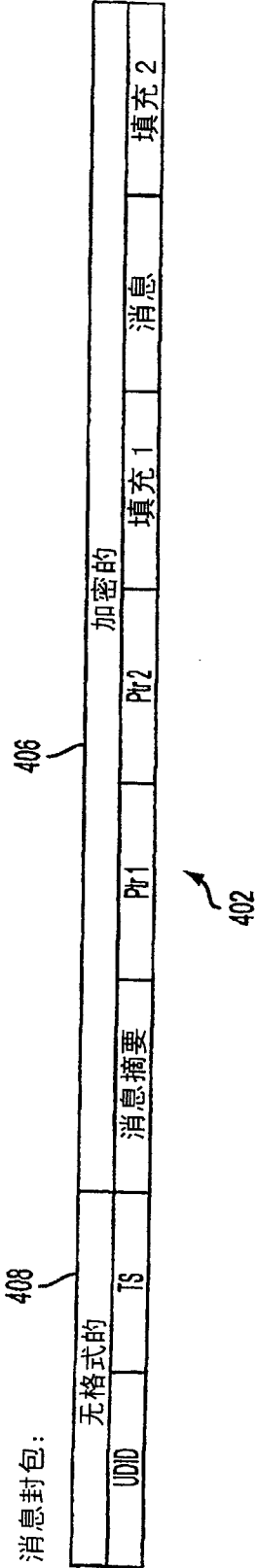


图 12