



# [12] 发明专利申请公开说明书

[21] 申请号 02815184.4

[43] 公开日 2004年12月22日

[11] 公开号 CN 1556972A

[22] 申请日 2002.6.4 [21] 申请号 02815184.4

[30] 优先权

[32] 2001.6.1 [33] IE [31] S20010524

[86] 国际申请 PCT/IE2002/000072 2002.6.4

[87] 国际公布 WO2002/097752 英 2002.12.5

[85] 进入国家阶段日期 2004.2.2

[71] 申请人 欧洲免税购物有限公司

地址 爱尔兰戈尔韦

[72] 发明人 格拉尔德·J·巴里

[74] 专利代理机构 永新专利商标代理有限公司

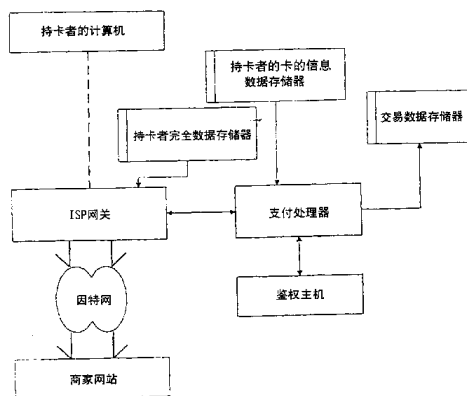
代理人 王英

权利要求书6页 说明书19页 附图6页

[54] 发明名称 安全的在线支付系统

[57] 摘要

本发明涉及电子商务领域，尤其涉及使用诸如借记卡、赊帐卡或信用卡这类支付卡来进行在线购物。本发明的概念是采用当前所用的安全方法的一种替换途径来保护持卡者。所述概念使持卡者在购物时不必发送卡号及其他购物详细资料并且将此与口令特征的使用相结合。由此提出了一种与银行现金提取相似的交易以确保安全，从安全性角度来看，所述银行/卡的形式完全是恰当的，但是难以允许电子商务和/或对其“网络”的任何其它访问。



1. 一种用于处理在线支付交易的计算机数据处理方法，包括如下步骤：

从支付卡的持卡者那里接收一个连接到网络的请求，所述请求包括持卡者口令，

5 对所述持卡者请求进行鉴定，并且提供所述持卡者所要求的网络接入，接收一个与持卡者相关联的支付请求，其中所述请求识别包括商业代码标识符以及交易价格在内的商业信息，

从一个持卡者详细资料数据库中为持卡者检索支付卡的详细资料，

10 将一个包括商业代码和交易价格在内的涉及支付卡资料的支付授权请求提交到一个用于授权所述交易的鉴权主机，由此接收一个授权而将授权的确认转发给商家。

2. 根据权利要求 1 的计算机数据处理方法，还包括从商家那里  
15 请求一个商业代码的步骤。

3. 权利要求 1 或 2 的用于处理在线支付交易的计算机数据处理方法，还包括将所述支付请求投寄到一个用于处理支付交易的支付主机的步骤。

20

4. 根据权利要求 3 的用于处理在线支付交易的计算机数据处理方法，还包括在接收到交付确认之前延迟投寄所述支付请求的步骤。

5. 权利要求 1 到 4 中任何一个权利要求的计算机数据处理方法，

还包括验证步骤，以确保提供到商家的持卡者信息与存储在持卡者详细资料数据库中的持卡者信息匹配。

6. 一种用于处理在线支付交易的计算机数据处理方法，其中包  
5 括如下步骤：

从持卡者那里接收一个连接到网络的请求，所述请求包括持卡者口令，

对所述持卡者的请求进行鉴定并且提供所述持卡者请求的网络接入，接收一个与商家和持卡者之间的交易相关联的第一交易请求，

10 从一个数据库中检索持卡者的支付卡详细资料，

将一个包含系统商业代码和交易价格在內并且涉及支付卡详细资料的支付授权请求提交给一个用于授权所述交易的鉴权主机，以及

一旦接收到授权，则将一个包含持卡者的支付卡代码的交易请求转发到商家。

15

7. 根据权利要求 6 的计算机数据处理方法，还包括从商家那里请求一个商业代码标识符的步骤。

8. 根据权利要求 6 或 7 的用于处理在线支付交易的计算机数据  
20 处理方法，还包括将所述支付请求投寄到一个用于处理支付交易的支付主机的步骤。

9. 根据权利要求 8 的用于处理在线支付交易的计算机数据处理  
25 方法，还包括在接收到交付的确认之前延迟投寄所述支付请求的步骤。

10. 根据权利要求 6 到 9 中任何一个的用于处理在线支付交易的计算机数据处理方法，其中执行另外一个验证，以确保提供到商家的持卡者信息与保存在数据库中的持卡者信息匹配。

5 11. 一种用于处理在线支付交易的系统，所述系统具有一个与因特网的连接，还具有经由本地网络而与持卡者终端的另外一个连接，其中包括：

接收装置，用于从持卡者那里接收一个连接到网络的请求，所述请求包括持卡者口令，

10 鉴定装置，用于鉴定持卡者请求并且提供持卡者所请求的网络接入，

接收装置，用于接收一个与商家和持卡者之间的交易相关联的第一交易请求，

检索装置，用于从一个数据库中检索持卡者的支付卡详细资料，

15 授权装置，用于将一个关于支付卡详细资料的支付授权请求提交到一个用于授权所述交易的鉴权主机，其中所述授权请求包括系统商业代码和交易价格，

以及交易装置，用于对从鉴权主机接收到一个授权做出响应并且适于将一个包括系统持卡者帐号的交易请求转发到商家。

20

12. 权利要求 11 的系统，还包括商家请求装置，用于从商家那里请求一个商业代码标识符。

13. 权利要求 11 或 12 的系统，还包括一个支付投寄装置，用于  
25 将支付请求投寄到一个用于处理支付交易的支付主机。

14. 权利要求 13 的系统，其中支付投寄装置在接收到交付的确认之前延迟投寄所述支付请求。

15. 根据权利要求 11 到 14 中任何一个的系统，其中验证装置适于执行一个第二验证，以便确保提供到商家的持卡者信息与保存在数据库中的持卡者信息匹配。

16. 一种用于处理商家和持卡者之间的在线支付交易的支付处理系统，其中包括：

10 用于接收一个支付交易请求的装置，所述支付请求标识包括商业代码标识符和交易价格在内的商家信息，

用于将持卡者与所接收的支付请求相关联的关联装置，

用于从一个持卡者卡的详细资料的数据库中检索那些涉及持卡者的支付卡详细资料的装置，

15 用于将一个包括所检索的支付卡详细资料、支付请求的商业代码和支付请求的交易价格在内的支付授权请求提交到一个用于授权所述交易的鉴权主机的授权装置，

适于响应所提交的支付授权请求来转发所接收到的一个授权的确认的确认装置。

20

17. 权利要求 16 的系统，还包括商家请求装置，用于从商家那里请求一个商业代码标识符。

18. 权利要求 16 或 17 的系统，还包括一个支付投寄装置，用于  
25 将支付请求投寄到一个用于处理支付交易的支付主机。

19. 权利要求 18 的系统，其中支付投寄装置在接收到交付的确认之前延迟投寄所述支付请求。

20. 根据权利要求 16 到 19 中任何一个的系统，其中验证装置适于执行一个第二验证，以便确保提供到商家的持卡者信息与保存在数据库中的持卡者信息匹配。

21. 一种用于处理商家与持卡者之间的在线支付交易的支付处理系统，包括：

10 用于接收一个支付交易请求的装置，所述支付请求标识包括商业代码标识符和交易价格的商家信息，

用于将一个持卡者与所接收的支付请求相关联的关联装置，

用于从一个持卡者卡的详细资料的数据库中检索那些涉及持卡者的支付卡详细资料的装置，

15 用于将一个涉及所检索的支付卡详细资料的支付授权请求提交到一个用于授权所述交易的鉴权主机的授权装置，所述支付授权请求包括所检索的支付卡详细资料、系统商业代码以及支付请求的交易价格，

20 用于对一个授权的接收作出响应并且适于将一个包含系统持卡者帐号的交易请求转发到商家的响应装置。

22. 权利要求 21 的系统，还包括商家请求装置，用于从商家那里请求一个商业代码标识符。

25 23. 权利要求 21 或 22 的系统，还包括一个支付投寄装置，用于将所述支付请求投寄到一个用于处理支付交易的支付主机。

---

24. 权利要求 23 的系统，其中支付投寄装置在接收到交付的确认之前延迟投寄所述支付请求。

- 5        25. 根据权利要求 21 到 24 中任何一个的系统，其中验证装置适于执行一个第二验证，以便确保提供到商家的持卡者信息与保存在数据库中的持卡者信息匹配。

---

## 安全的在线支付系统

### 技术领域

本发明涉及电子商务领域，尤其涉及使用诸如借记卡、赊帐卡或  
5 信用卡这类支付卡来进行在线购物。

### 背景技术

目前在开发、实施和维护安全支付系统的方面已经应用了效果显  
著的研究和资源，它们促进了持卡者在经由因特网所实施的商品交易  
10 中的信用卡/赊帐卡的使用。

所有这些安全系统是以持卡者每次都必须“处理”其卡号为基础  
的，而这将会导致在每次购物的时候对所传送的卡号和相关信息的  
“捕获”，而将其公开给黑客和/或可以获得卡号及有效期限访问权的  
其他诈财者。

15 一种解决方案是将安全（加密）通信方法应用在购物时经由因特  
网进行的信用卡资料的发送过程中。这种安全方法的实例包括安全套  
接层（SSL）和安全电子交易（SET）协议。为了在因特网上执行信  
用卡资料的电子传输，通过对计算机公司和信用卡行业的企业进行明  
确的引导，已发展了这些方法。然而在以某种程度的安全性来发送信  
20 用卡/赊帐卡详细资料的同时，并没有担保所述详细资料在被保存到  
商家系统的时候不易受到攻击。此外，商家或商家雇员很有可能会出  
于欺诈目的而使用或窃取所述卡的详细资料。

如持卡者察觉的那样，缓和在线商务中的坏处的进一步关注的问  
题是电子商务商家的可靠性以及可提供给进行购物的持卡者的追索

权的缺乏。持卡者没有得到及时交付所订购物品的保证，也没有得到所定购物品具有相宜质量和/或数量等等的保证。对于持卡者而言，一旦将所述卡的详细资料和适当的资金记入持卡者帐户的借方，则很难从商家那里得到适当的补偿。

- 5           更为关心的是在这里并未保证商家或是可以访问持卡者资料的相关人员不会在以后的无授权交易中使用持卡者资料或是出于犯罪目的而将这些信息传递给第三方。

另一方面，对商家而言，值得关注的是在发货之前已经明确结算了所述物品，也就是说，卡的形式（card scheme）的获取者（acquirer）  
10 已经出于结算目的而对所述卡的资料和金额进行了“批准”，并且所述卡的详细资料和持卡者信息都是真实的。

EP0801479 公开了一种安全通信机制，用于在经由数据网络（例如因特网）通信的持卡者终端与服务器之间传递信用卡或其他敏感信息。为了经由数据网络来传递安全地或秘密地传递敏感信息，在持卡者为了接入数据网络而连接的始发因特网服务供应商（ISP）的服务器与敏感信息所针对的服务器供应商之间建立一个电话连接。然而，任何通往包含信用卡或其它敏感信息的终端 ISP 服务器通信或交易都是通过一个定位到终端 ISP 服务器的电话号码的电话呼叫在第二连接上实现的。在接收到一个呼叫之后，通过在因特网上将这个呼叫与涉  
20 及信息和/或交互服务、和/或不可电子递送的商品或服务的持卡者请求相关联，ISP 可以向持卡者提供所请求的信息和/或服务，或者批准交付那些非电子递送的商品或服务。通过使用这种安排，可以在不借助因特网路由服务器提供信用卡信息以及没有与 ISP 建立财务关系的情况下实现支付。较为优选的是，还可以对始发服务器与终端 ISP 服  
25 务器之间经由电话线的信息传递进行加密。然而这种方法的问题在

于,ISP 与商家有必要就所述想法以及附加通信设备的安装进行签约,以促进辅助信道上的安全通信。此外,对独立电话呼叫的需要给所述处理添加了额外费用,从持卡者的角度而言,也还是没有得到任何确保。

5           WO97/03410 公开了一种因特网记帐方法,其包括在因特网接入提供商与顾客之间建立一个协定,并且在因特网接入提供商与厂商之间建立一个协定,其中因特网接入提供商与顾客以及厂商达成一致,以为顾客进行记帐并且向厂商汇出有关顾客经由因特网而从厂商那里购买的产品和服务的款项。所述提供商为顾客创建因特网接入。当  
10 顾客经由因特网而从厂商那里订购产品或服务时,顾客与厂商之间所传送的交易信息也发送到提供商。然后,提供商记录顾客交易金额的帐目并且将一部分交易金额汇至厂商,保留差额作为提供服务的费用。这种方法的结果的是不必经由因特网来发送顾客帐号或厂商帐号,由此保持信息的安全性。然而这种方法的一个很大的难点则是在  
15 进行任何交易之前都要在 ISP 与商家之间达成协定。

          US5,905,736 公开了一种方法,其用于为那些经由因特网而在持卡者与因特网服务供应商之间经由因特网接入提供商(IAP)进行的交易进行集中记帐。一旦将持卡者终端连至 IAP,则 IAP 会向记帐平台发送一个消息,所述消息将持卡者的身份以及 IAP 指派给持卡者的  
20 交易(session)以便供其使用的临时因特网协议(IP)地址关联到持卡者终端。响应于与 ISP 的可记帐的交易,ISP 把进行交易的持卡者的 IP 地址和涉及所述交易的费用发送到记帐平台。涉及所有这些交易的费用由一个交易服务器累积并且保存在用请求终端的 IP 地址所识别的相关数据库上的一个帐户之中。在持卡者的交易(session)结  
25 束时,在交易(session)期间保存在用 IP 地址所识别的帐户中的交

易服务器数据库上的所有交易费用都被记入一个与持卡者的身份相关联的帐户中，其中所述身份是通过从先前所接收并保存的消息中交叉引用对于持卡者的身份的 IP 地址而被保存在记帐服务器的数据库中的。

- 5 有鉴于现有技术，如果可以提供一种在线购物方法，在发生投诉的情况下，所述方法允许持卡者具有针对电子商务商家的简单有效的追索权，那么将会是非常有利的。

如果可以提供一种方法，所述方法允许顾客在不向第三方公开他们的卡的资料的情况下进行在线购物，那将是更为合乎需要的。

10

#### 发明内容

- 本发明的概念是采用当前所用安全方法的一种替换途径来保护持卡者。所述概念使持卡者在购物时不必发送卡号及其他购物的详细资料并且将其与口令特征的使用相结合。由此提出了一种与银行现金
- 15 提取相似的交易，从安全性角度来看，银行/卡的形式完全是恰当的，但是为了确保安全而难以允许电子商务和/或其它访问其“网络”。

在第一实施例中提供了一种用于处理在线支付交易的计算机数据处理方法，其中包括如下步骤：

- 从持卡者那里接收一个连接到网络的请求，所述请求包括持卡者
- 20 口令，

对所述持卡者请求进行鉴定，并且提供所述持卡者所要求的网络接入，接收一个与持卡者相关联的支付请求，其中所述请求识别的是包括商业代码标识符以及交易价格在内的商家信息，

- 从持卡者详细资料数据库中为持卡者检索支付卡的详细资料，
- 25 将一个包括商业代码和交易价格在内的涉及支付卡资料的支付

授权请求提交到一个用于授权所述交易的鉴权主机，由此接收一个授权而将授权确认转发给商家。

所述计算机数据处理方法还可以包括从商家那里请求一个商业代码标识符的步骤。所述计算机数据处理方法可以包括将所述支付请求投寄到一个用于处理支付交易的支付主机的步骤。在执行投寄的情况下，所述计算机数据处理方法还可以包括在接收到投寄确认之前延迟投寄所述支付请求的步骤。可选地，所述计算机数据处理方法还可以包括验证步骤，以确保提供到商家的持卡者信息与保存在持卡者详细资料数据库中的持卡者信息匹配。

10 在第二实施例中，提供了一种用于处理在线支付交易的计算机数据处理方法，所述方法包括如下步骤：

从持卡者那里接收一个连接到网络的请求，所述请求包括持卡者口令，

对持卡者的请求进行鉴定并且提供所述持卡者请求的网络接入，  
15 接收一个与商家和持卡者之间的交易相关联的第一交易请求，

从一个数据库中检索持卡者的支付卡详细资料，

将一个包含系统商业代码和交易价格在内并且涉及支付卡详细资料的支付授权请求提交给一个用于授权所述交易的鉴权主机，以及

一旦接收到授权，则将一个包含持卡者的支付卡代码的交易请求  
20 转发到商家。

所述计算机数据处理方法还可以包括从商家那里请求一个商业代码标识符的步骤。所述计算机数据处理方法可以包括将所述支付请求投寄到一个处理支付交易的支付主机的步骤。在执行投寄的情况下，所述计算机数据处理方法还可以包括在接收到投寄确认之前延迟投寄所述支付请求的步骤。可选地，所述计算机数据处理方法还可以  
25

包括验证步骤，以确保提供到商家的持卡者信息与保存在持卡者资料数据库中持卡者信息匹配。

在第三实施例中提供了一种用于处理在线支付交易的系统，所述系统具有一个与因特网的连接，并且具有一个经由本地网络而与持卡者终端相连的另外一个连接，其中包括：

接收装置，用于从持卡者那里接收一个连接到网络的请求，所述请求包括持卡者口令，

鉴定装置，用于鉴定持卡者请求并且提供持卡者所请求的网络接入，

接收装置，用于接收一个与商家和持卡者之间的交易相关联的第一交易请求，

检索装置，用于从一个数据库中检索持卡者的支付卡详细资料，

授权装置，用于将一个关于支付卡详细资料的支付授权请求提交到一个用于授权所述交易的鉴权主机，其中所述授权请求包括系统商业代码和交易价格，以及

交易装置，用于对从鉴权主机接收到一个授权做出响应并且适于将一个包括系统持卡者帐号的交易请求转发到商家。

在这个实施例中，所述系统还可以包括一个用于从商家那里请求一个商业代码标识符的商家请求装置。所述系统可以包括一个用于将所述支付请求投寄到一个用于处理支付交易的支付主机的支付投寄装置。在这种选择的情况下，所述支付装置在接收到一个投寄确认之前将会延迟投寄所述支付请求。

可选地，所述系统可以包括一个适于执行第二验证的验证装置，以确保提供给商家的持卡者信息与数据库中保存的持卡者信息相匹配。

在第四实施例中提供了一个用于处理商家与持卡者之间的在线支付交易的支付处理系统，所述系统包括：

用于接收一个支付交易请求的装置，所述支付请求标识商家信息，其中包括商业代码标识符以及交易价格，

5 用于将持卡者与所接收的支付请求相关联的关联装置，

用于从持卡者的卡的详细资料的数据库中检索那些涉及持卡者的支付卡的详细资料的装置，

用于将一个涉及所检索的支付卡的详细资料的支付授权请求提交到一个用于授权所述交易的鉴权主机的授权装置，其中所述支付授权请求包括所检索的支付卡的详细资料、支付请求的商业代码和支付请求的交易价格，

适于响应所提交的支付授权请求来转发一个所接收的授权的确认的确认装置。

在这个实施例中，所述系统还可以包括一个用于从商家那里请求一个商业代码标识符的商家请求装置。所述系统可以包括一个用于将所述支付请求投寄到一个用于处理支付交易的支付主机的支付投寄装置。在这种选择的情况下，所述支付装置在接收到一个投寄确认之前延迟投寄所述支付请求。

20 可选地，所述系统可以包括一个适于执行第二验证的验证装置，以确保提供给商家的持卡者信息与数据库中保存的持卡者信息相匹配。

在第五实施例中提供了一种用于处理商家与持卡者之间的在线支付交易的支付处理系统，其中包括：

25 用于接收一个支付交易请求的装置，所述支付请求标识商家信息，其中包括商业代码标识符和交易价格，

用于将一个持卡者与所接收的支付请求相关联的关联装置，

用于从持卡者的卡的详细资料的数据库中检索那些涉及持卡者的支付卡的详细资料的装置，

5 用于将一个涉及所检索的支付卡的详细资料的支付授权请求提交到一个用于授权所述交易的鉴权主机的授权装置，所述支付授权请求包括所检索的支付卡的详细资料，系统商业代码以及所述支付请求的交易价格，以及

用于对一个授权的接收进行响应并且适于将一个包含系统持卡者帐号的交易请求转发到商家的响应装置。

10 在该实施例中，所述系统还可以包括一个用于从商家那里请求一个商业代码标识符的商家请求装置。所述系统可以包括一个用于将所述支付请求投寄到一个用于处理支付交易的支付主机的支付投寄装置。在这种选择的情况下，所述支付装置在接收到一个投寄确认之前将会延迟投寄所述支付请求。

15 可选地，所述系统可以包括一个适于执行第二验证的验证装置，以确保提供给商家的持卡者信息与数据库中保存的持卡者信息相匹配。

20 在一个实施例中，第一组信息识别的是持卡者，第二组信息识别的是商家，这两组信息是使用一个因特网提交协议来接收的，例如与HTML表格相关联的POST操作。

本发明的这些及其他方面将通过参考下文所述的一个或多个实施例而变得清楚并且得到阐明。

#### 附图说明

25 现在参考附图而对本发明进行更进一步的详细描述，其中：

图1是根据本发明的支付交易系统的布置的图示，

图 2 是图 1 布置的更详细显示，  
图 3 是与本发明一起使用的示范性数据库的图解，  
图 4 是根据本发明的第一方面的方法的流程图，  
图 5 显示的是与本发明一起使用的表单，以及  
5 图 6 是根据本发明的第二方面的方法的流程图。

### 具体实施方式

如图 1 所示，根据本发明的在线交易方案的布置包括处于一个网络中的不同节点的许多不同的当事者。特别地，所述处理涉及的是在  
10 支付卡（通常是借记卡、信用卡或赊帐卡）的持卡者 4 与商家 2 之间实施的在线（电子商务）交易。

商家与持卡者之间的通信是通过网络 3（因特网）来实施的。通常，商家，更确切的说，商家服务器，连续不断地连接到网络，以使消费者能够毫无阻碍地访问商家网站。

15 另一方面，持卡者的计算机可以配置为仅仅按照需要而与因特网 3 相连。通常，持卡者的计算机经由一个因特网服务供应商（ISP）5 而与因特网 3 相连。可以使用调制解调器并经由常规的或 ISDN 电话线或是借助其他适当的通信装置来实现与 ISP 的连接。

一旦连接到 ISP 5，则持卡者可能需要输入持卡者姓名和/或持卡  
20 者口令。诸如安全软件模块这样的鉴定装置执行一个验证处理，所述处理通常是相对于在 ISP 服务器或是 ISP 服务器的相关服务器或网络上本地保存的有效持卡者姓名和口令的持卡者安全数据库来比较所输入的持卡者姓名和口令。一旦验证了持卡者姓名和口令，则准许持卡者的计算机经由 ISP 网络而接入因特网。

25 通常，ISP 服务器 5 可以使用路由器或其他相关硬件设备连接到因特网 3。对于 ISP 服务器和相关的本地网络而言，可以通过防火墙

装置或是软件来提供安全和保护。这种路由器技术与安全特征的组合允许 ISP 进行那些在 ISP 服务器上可以提供的服务，其中所述服务器可以由经由 ISP 连接的持卡者直接访问而不需要经由因特网来发送持卡者请求和服务器响应。用这种方式，ISP 网络上的服务器与经由 ISP 网络而与因特网相连的持卡者的计算机之间的通信通常不会由因特网上第三方的截取。

图 2 描述了一种用于向持卡者提供因特网接入的 ISP 系统的示范性结构，并且描述了一个用于根据本发明实施例而对持卡者与商家之间的在线交易进行处理的相关的支付/验证处理系统。所述相关的支付处理系统既可以集成在 ISP 内部，或保持在一个与 ISP 相关联的分立系统中。在这个示范性结构中，将上述 ISP 的持卡者数据库 100、101 进一步扩展为包括进一步的持卡者信息，如图 3 的示范性数据库结构中描述的那样，其可以包括持卡者 14、15、16 的姓名 12、地址 13 以及支付卡详细资料。支付卡的关键详细资料通常包括单独的持卡者的卡的支付形式 14（例如 VISA<sup>TM</sup>、AMERICAN EXPRESS<sup>TM</sup>、DINERS CLUB<sup>TM</sup>、MASTER CARD<sup>TM</sup> 等等）、卡号 15 以及有效期限 16 的详细资料。

这些关键的支付卡详细资料可以是在持卡者用 ISP 或是方便于持卡者和 ISP 的某个后续时间建立帐户时建立的。出于安全原因，有人建议在从持卡者提交给 ISP 的书面申请中提供所述关键详细资料。作为选择，这些关键详细资料可以通过一个连至 ISP 的电话呼叫来提供。使用上述方法中的任何一种方法则确保持卡者的关键资料不经由因特网来发送。而一个较不优选的实施例则允许持卡者在线输入其关键详细资料。

可以理解的是，可以使用有关和数据库中的一个或多个表格 100、

101 来实现所述数据库结构。每一个持卡者的帐户可能具有一个以上的相关的关键的卡的详细资料组，即持卡者具有一张以上的信用卡。在这种情况下，本领域技术人员将会理解，多表格数据库将具有识别持卡者及其口令的第一表格并且使用第二表格来保持持卡者详细资料，而这将是非常适当的。此外，还可以使用一个附加字段来链接表格，例如，在向数据库中输入持卡者时创建的持卡者号码，其中对每一个持卡者而言，所述持卡者号码都是唯一的。此外还可以理解的是，持卡者的卡的详细资料 101 可以完全存入一个分立的系统中，由此与所述系统一起存入持卡者安全数据存储器 100，特报是在交易处理系统不同于 ISP 的情况下。

通常，本发明的方法是从持卡者经由 ISP 而与因特网建立一个连接 20 开始，其中包括常规的持卡者验证（鉴定）步骤 21。在连接时，ISP 可以将持卡者的计算机的连接 ID（例如所分配的 IP 号码）与持卡者相关联。可以由 ISP 随后使用以在交易处理中识别持卡者。

一旦持卡者经由 ISP 而与因特网建立了连接 22，则持卡者可以使用 NETSCAPE NAVIGATOR 或 MICROSOFT INTERNET EXPLORER 这类适当的浏览器软件来导航因特网或浏览商家网站。

图 4 显示了本发明的第一操作方法。在这个实施例中，商家与 ISP 直接或间接地建立一个协定，在本发明的上下文中，应该以此来表示一个具有相关的支付处理器的 ISP，以使用本发明的交易方案。所述方法是从持卡者访问商家网站开始的。根据商家的网站的结构，持卡者可以查看关于待售商品或服务的描述，并且可以查看所述商品或服务的图片以及选择所要购买的物品 23。在本领域中，用于在网站服务器上实现这些功能的技术是众所周知的。

一旦从持卡者那里接收到购买物品的请求，则商家服务器可以通

过转发一个由持卡者填完的表格来做出响应。所述表格可以是包括小型 JAVASCRIPT 程序的超文本标记语言 (HTML) 文档, 由此确保适当地填写所要求的字段, 虽然在这里可以使用任何浏览器可读取的表格。

- 5           在本领域中, HTML 表格是众所周知的, 这些表格允许包含多个字段, 所述字段为浏览器软件指示了使用这个表格采取什么操作、怎样和向哪里发送持卡者在表格中所提供的信息。

          在图 4 中显示了一个实例表格 40。所述表格允许持卡者使用浏览器软件来输入一些信息, 例如, 他们的姓名 44a、地址 44b 和电话  
10       号码 44c。

          表格 40 还可以包括那些详细描述所述交易的信息, 举例来说, 其中可以包括关于商品 43b、数量 43c、价格 43d 以及商业交易参考号 43a 的描述。所有这些信息都可作为字段而被存在表格中。可以将某些字段标记为隐藏, 例如商家的交易参考号。

- 15           一旦持卡者填写了表格 24 并且点击了恰当按钮 41, 则由浏览器软件将表格 40 提交到一个在表格自身当中定义的位置。嵌入在 HTML 文档中的适当脚本可以对所输入的字段和价格的有效性进行检查。举例来说, 如果姓名字段一直为空白, 则脚本可以提示持卡者重新输入他们的详细资料。

- 20           本发明的方法可以配置为用多种不同方式来进行操作。在第一实施例中, 其中商家的系统适于与 ISP 的交易处理系统进行合作, 所述商家系统将涉及卡的形式的事家的商业代码提供给 ISP。

- 这可以通过商家提供与 ISP 服务相对应的购买支付选项 45 来实现。例如, 持卡者可以从表格中的下拉列表或使用一个复选框能够选  
25       择 ISP 的支付形式或是相关事物。

在一个实施例中，其中持卡者是在完成上述表格之前选择支付方法的，一旦选择了持卡者希望使用保存在 ISP 或相关事物上的持卡者信用卡详细资料来进行购物的选项，则商家将上述表格转发到持卡者来完成填写。所述表格包括那些对诸如商家的商业代码、卡的形式标识符这类的商家卡的信息加以识别的字段，并且这些字段可以是隐藏的。

一旦持卡者完成了表格，则将表格提交 25 到 ISP 服务器或是作为交易处理器 102 的主机的相关服务器。交易处理器 102 包括一个用于接收表格并从该表格中提取 26 包括商家的商业代码和交易金额在 10 内的信息的接收装置。

交易处理器包括一个关联装置，所述关联装置例如使用发送请求的计算机的 IP 地址来确定提交所述表格的持卡者并且将交易与持卡者相关联。

一旦交易处理器确定了持卡者的身份，则交易处理器使用适当的检索装置来从持卡者的卡的信息数据库中检索 26 涉及相关持卡者的持卡者卡的详细资料。然后，交易处理器 102（或相关的授权设备）与卡的形式鉴权主机 7 建立（如果还未建立）一个连接并且提交 27 支付卡详细资料、商业代码以及交易价格来得到许可。举例来说，与鉴权主机的连接可以通过一个专用的安全网络或是电话线来进行。

20 如果鉴权主机拒绝所述交易，则交易处理器通过向持卡者和/或商家发送一个恰当的消息来做出响应，并且所述交易被取消。

如果批准所述交易，则鉴权主机按照常规支付交易向交易处理器 102 提供一个交易授权编号。然后，交易处理器使用一个确认装置来转发 28 授权的确认，例如通过将作为字段的授权码与持卡者填写的 25 表格资料一起插入到商家服务器。

交易的详细资料包括商家信息和持卡者信息，并且交易详细资料既可以由交易处理器保存，也可以本地保存在交易数据存储器中或是相关的服务器上，以便进行后续处理 29（例如通过一个将交易信息投寄到用于处理交易的卡的支付形式的交易处理器的投寄装置）。尽管  
5 如此，这个步骤也可以与所述授权同时完成。

一旦用交易资料接收到一个确认，诸如授权码，则商家将会具有一个有效保障来保障交易是有效的，并且商家将会及时地从卡的形式中接收结算。用这种保障，商家可以允许交易，例如，提供所请求的商品或服务。

10 可以理解的是，在整个交易处理过程中都没有将持卡者的卡的关键详细资料泄漏给商家。

在另外一个实施例中，交易处理器保存交易的详细资料，但在商家确认处理订购或是持卡者接收到商品之前，交易处理器保持所述交易用于投寄。例如，在从商家那里接收到一个详细描述交付业务公司  
15 及其交付交易记录的消息之前，交易处理器可以保持所述交易。一旦接收并且可能验证这种信息，则交易处理器将释放所述交易用于由恰当的卡的形式处理。

对本领域技术人员而言，显然可以使用许多不同的方法和技术来允许持卡者提交信息并使交易处理器获取商家的卡的形式详细资料。例如，在与商家相连的时候，商家或商家的服务器软件可以只从  
20 持卡者的浏览器软件提供的标题信息中识别 ISP 网关的域。商家或商家的服务器软件可以将一个交易请求转发到一个预先指定的子域（先前由 ISP 指示给商家）或是预先定义的标准域。举例来说，如果从持卡者所接收的标题信息指示其发自域 TESTISP.COM，那么，商家的  
25 软件可以选择 PAYMENT.TESTISP.COM 的标准子域，以发送所述请

求。

在第二实施例中，商家也可以与 ISP 或相关的交易处理器没有协定，从而促进上述方法的使用。在该第二实施例中，交易处理器截取 31 持卡者已经填写好 30 的交易表格。举例来说，这种截取有可能会受到持卡者点击其图形界面上的按钮的影响，对其所做的选择将会影响到将已经填写好的表格引导到 ISP 交易处理器的软件模块的运行。

一旦接收到表格，则交易处理器 102 最初可以进行检查，以确定是否准许商家直接或是经由另一方而与 ISP 或是相关的交易系统结合使用。该许可也可以使用一种否定表达方式，其中商家将被禁止使用所述系统，例如其中在商家先前并未令人满意地执行发货或服务的情况下。用这种方式，可以在持卡者与商家进行交易的时候包含一个可靠性因素。在持卡者成功投诉之后，商家有可能会列于一个禁止列表之上。

交易处理器还可以使用一个商家请求装置，尝试向商家提交一个消息，要求商家提供其商业详细资料来允许交易处理继续进行。举例来说，可以通过在交易表格的字段中输入所述消息并将这些详细资料提交给商家服务器来提交所述消息。这尤其适于手动执行在商家网站上的交易处理的情况，即个人经由销售点（POS）或虚拟 POS 支付卡设备来手动重新键入所提交的卡的信息的情况。在这些情况中，使网站的支付交易处理部分自动化，商家服务器有可能产生一个错误消息。

如果商家对这种请求做出响应并且提供了其商业卡的形式详细资料，则可以如上所述，相对于第一实施例中的交易请求处理来处理所述交易。

如果商家做出否定响应或是没能在一段时间以内做出响应，则所

述方法会沿着以下线路继续进行：

如上所述，相对于第一实施例而言，交易处理器确定持卡者的身份并且从持卡者卡的关键详细资料数据存储单元中提取持卡者的持卡者信息。

- 5 可选地，交易处理器可以包括一个验证装置，所述验证装置适于执行检查，以确保数据库上的姓名和/或地址等与由持卡者在交易表格中所提供的姓名和/或地址等相匹配。

在该第二实施例中，交易处理器不具有商家的商业代码信息。因此不可能像在所述第一实施例中所述的情况那样来直接处理所述交易。

10 为了克服这个问题，支付处理器使用了自身的商业代码，即，与交易处理器的运营商（例如 ISP）相关联的商业代码，在下文中将其称为系统\_商业代码。然后，交易处理器向一个恰当的鉴权主机发送一个支付授权请求，并且提交系统\_商业代码、交易金额（从表格中提取）以及持卡者的支付卡详细资料（卡号及有效期限）。

15 如果鉴权主机拒绝所述交易，那么如先前所述，将会向持卡者发送一个恰当的消息，并且所述交易将被取消。

如果鉴权主机批准所述交易，则将一个授权码转发到交易处理器

- 20 一旦接收到授权码，则交易处理器将其与交易数据存储单元中的其他的交易详细资料一起保存，用于进一步的处理（例如支付）35。

可以理解的是，一旦交易用卡的形式进行结算处理，则交易金额将从持卡者那里记入借方并且存入与系统\_商业代码相对应的系统\_商家（交易处理器的方案运营商）帐户。该第一交易并不涉及商家，而只涉及交易处理器方案运营商和持卡者。

为了将所述结算(从交易处理器的方案运营商那里)传递到商家,交易处理器向商家提供与交易处理器的运营商的帐户(下文将其称为系统\_持卡者帐户)相对应的持卡者信息、卡号和有效期限。商家可以使用常规方式来处理这个系统\_持卡者信息。在该第二交易中,交易处理器的方案运营商系统\_持卡者帐户是记入借方的,并且已经将其存入商家帐户。在与第一交易相结合的情况下,将会从持卡者帐户中产生一个有效付款(effective debit),而商家收取交易金额。这两个交易的交易处理器段(segments)有效地取消了。

交易处理器可以把它的系统\_持卡者信息提供给商家的一个方法是通过在持卡者先前完成并且提交到交易处理器的表格的适当字段中插入相关的系统\_持卡者的卡的信息并将这个经过修订的表格转发到商家服务器来实现的。

一旦接收到表格,则商家服务器使用常规方式处理表格。而在这种情况下,商家服务器将会提交一个关于系统\_持卡者号的授权和(后续)支付请求,而不是持卡者的卡号详细资料。

交易处理器转而将交易的验收的确认与授权码一起转发到商家。商家则不转发持卡者的支付卡详细资料。

交易处理器保存交易的详细资料,随后根据常规方法来投寄用于支付的交易(例如在一天中的最后时间进行投寄中)。作为选择,也可以在授权时投寄所述交易。

在该第二实施例中存在两个等价交易。第一个交易处于交易处理器的方案运营商与持卡者之间。第二个交易则处于交易处理器的方案运营商与商家之间。为了防止欺诈,交易处理器可以恰当地适用于在这两组交易之间进行调解,识别不寻常的交易。

在另外一个实施例中,持卡者可以具有属于一个或多个卡的形式

的一张以上的卡。在该实施例中，每个单独卡的详细资料可以保存在一个数据库中。在与 ISP 相连或在其他一些合适的时候，当输入持卡者姓名和口令时，可以让持卡者识别他们希望哪个卡用于所述交易（session）。

5        作为选择，持卡者可以在提交表格时识别用于一个交易的一张特定卡，例如选择一个恰当的按钮。为了确保更高的安全性，持卡者可以在向 ISP 提交资料的时候为各个卡分配一个参考标识符。举例来说，持卡者可以向主要用于购买家用设备的 VISA™ 信用卡分配一个名称“VISA-household”，或是分配名称“AMEX-business”来识别一张用  
10        于商业目的的美国捷运信用卡（AMERICAN EXPRESS card）。通过为持卡者提供一个卡标识符的列表以从中选择，持卡者可以识别他们希望使用的卡而不需要持卡者或交易处理器向持卡者发送那些公开所述卡详细资料的数据。

非常频繁的是，持卡者具有与一张或多个张卡相关联的一个以上  
15        的地址。举例来说，持卡者可以具有一个用于与工作相关联的卡的办公地址，并且具有一个用于其他卡的家庭地址。此外，持卡者常常可以希望将商品递送到一个地址，而所述地址并不是持卡者的实际地址，例如给爱人寄送一件礼物。

在本系统的另外一个实施例中构造了持卡者的卡的关键详细资  
20        料数据库，以便允许一个以上的地址与一特定的卡或是持卡者帐户相关联。这些地址可以在持卡者向 ISP 提供所述卡的详细资料的同时进行输入，也可以在后续的日子进行修改，以便针对所述地址来进行删除或添加。

在执行一个有效性检查的时候，交易处理器可以进行检查，以确  
25        认持卡者在交易时所提供的地址与数据库上的所述特定卡或持卡者

的地址匹配。

尽管已经依照 HTML 表格而对本发明进行了描述，但是本领域技术人员将明白，可以使用各种不同的方法来实施本发明，而不脱离本发明的实质和范围。举例来说，持卡者可以下载一个用于其浏览器的特定附加项 (add-in)，在检测到持卡者做出的选择或是来自商家服务器的响应的时候，例如，在商家服务器一旦从持卡者那里接收到一个购买请求就用一特定的文件格式做出响应的情况下，所述附加项将会自动进行操作。

如这里所述，本发明针对的是经由 ISP 进行的支付交易的路由安排以及仅仅受到使用口令的持卡者许可的访问，它包括对持卡者数据库姓名/地址等等与交易订购的姓名/地址的一致进行校正/验证的可能性，并且允许获取独立于商家但却代表商家的支付授权。如果被拒绝的话，则将所述拒绝传递到持卡者，并且所述交易不会被处理。如果被批准的话，则向持卡者和商家发送一个确认。

作为另一个分立的建立信任的措施，在已接收到独立的发货确认之前，可以延迟相对于商家所进行的交易结算。

当在这里参考本发明而使用单词“包含/由……组成”以及单词“具有/包括”时，这些单词是用于指示存在所描述的特征、整体、步骤或部件，但是并不排除存在或添加一个或多个其他特征、整体、步骤、组件或是它们组成的组。

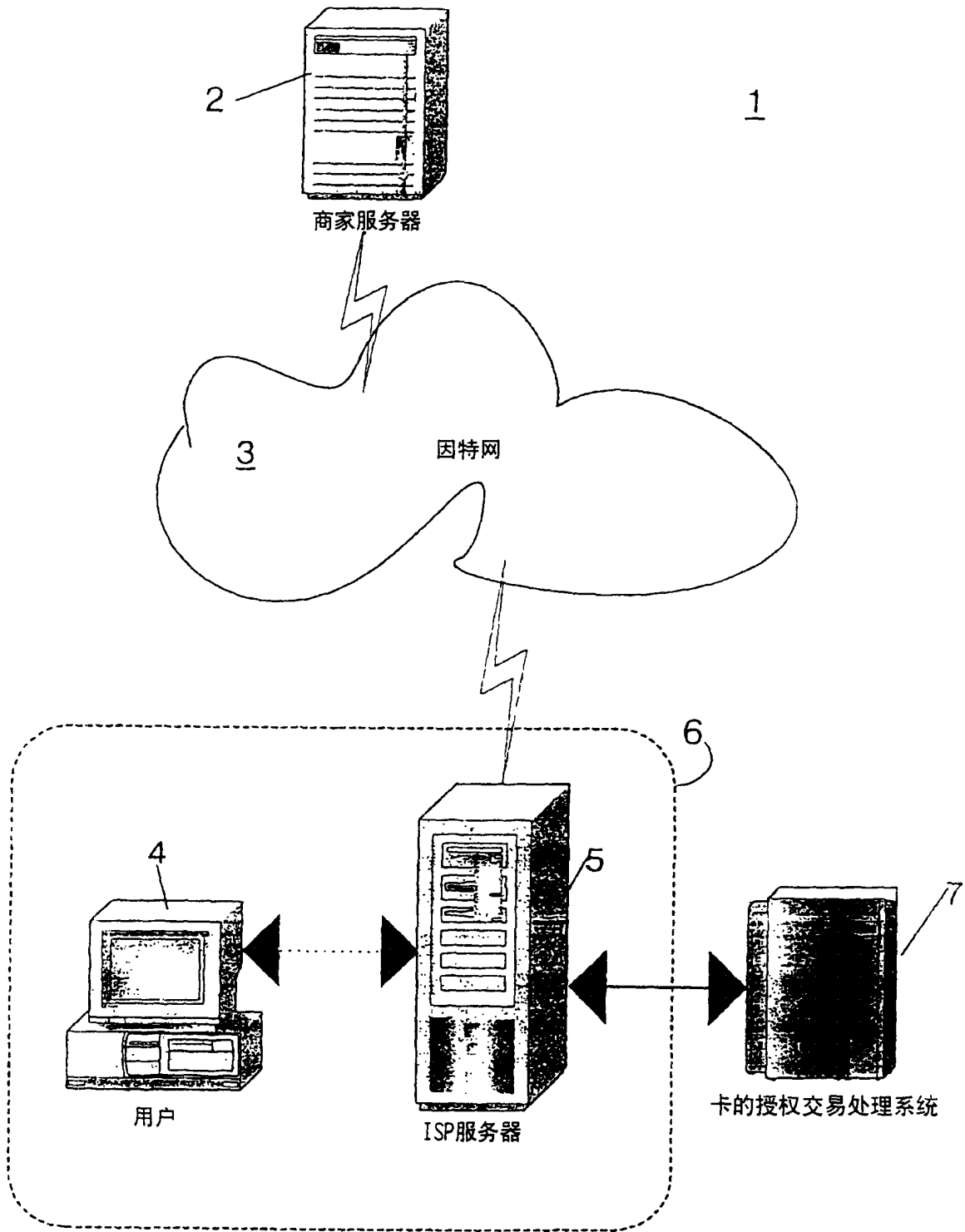


图1

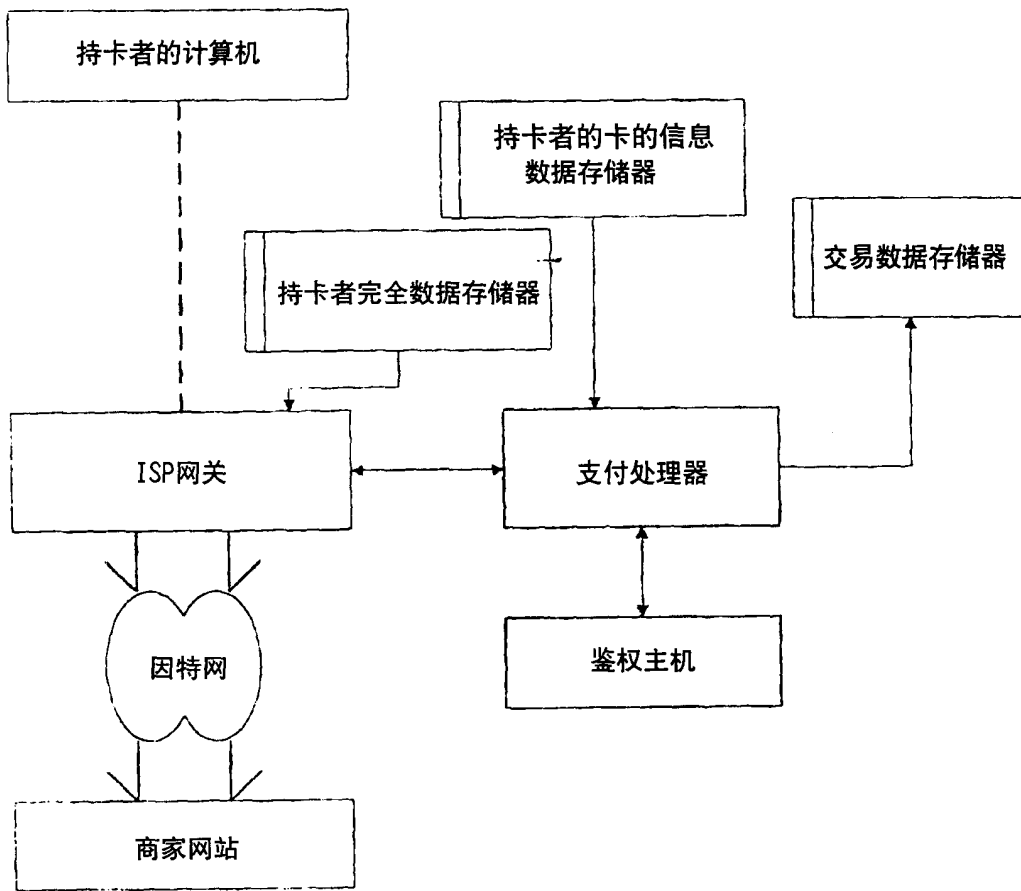


图2

10 用户名	11 口令	12 卡的名称	13 卡的地址	14 卡的方案	15 卡的编号	16 有效期限
17 User 1	PW1	CardName 1	CardAddress	CardScheme A	CardNo. 1	Date 1
18 User 2	PW2	CardName 2	CardAddress2	CardScheme B	CardNo. 2	Date 2
...	...	...	...	...	...	...
User n	PW n	CardName n	CardAddress n	CardScheme X	CardNo. n	Date n

图3

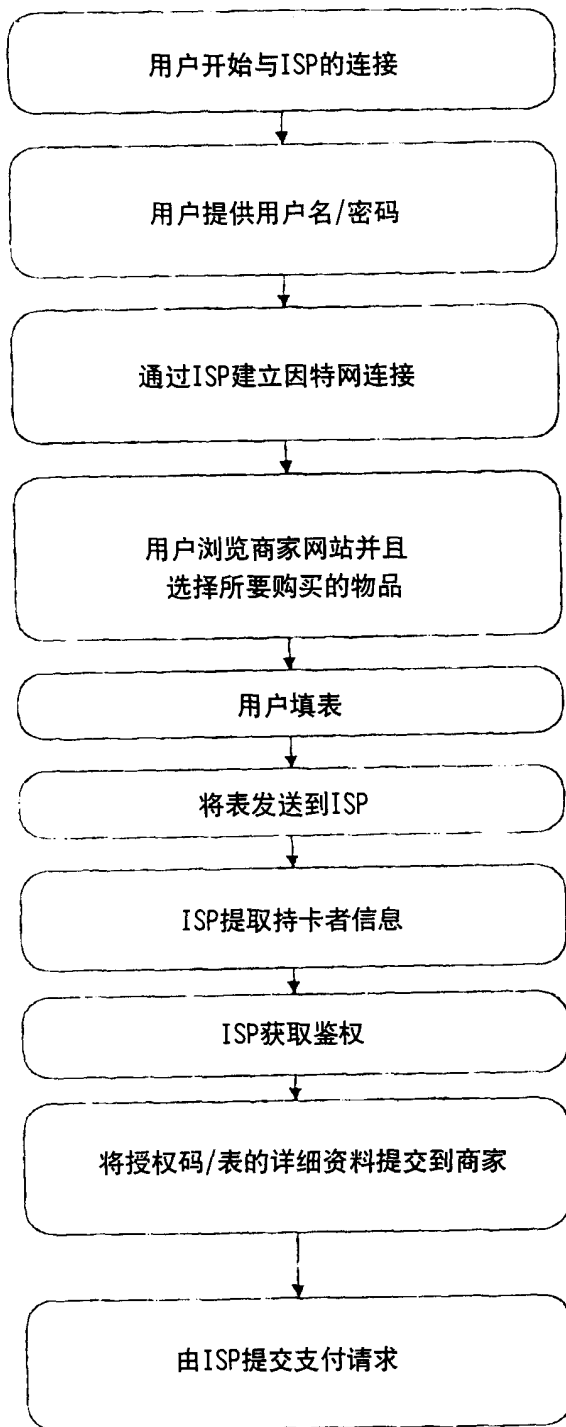


图4

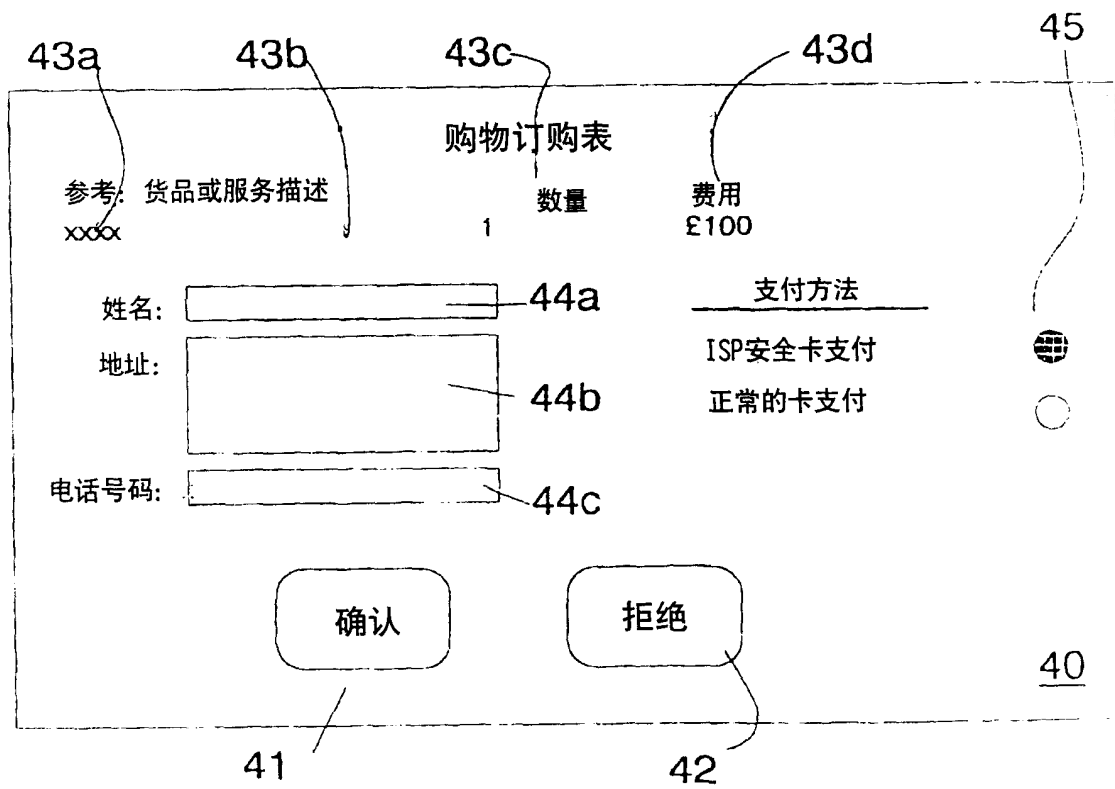


图5

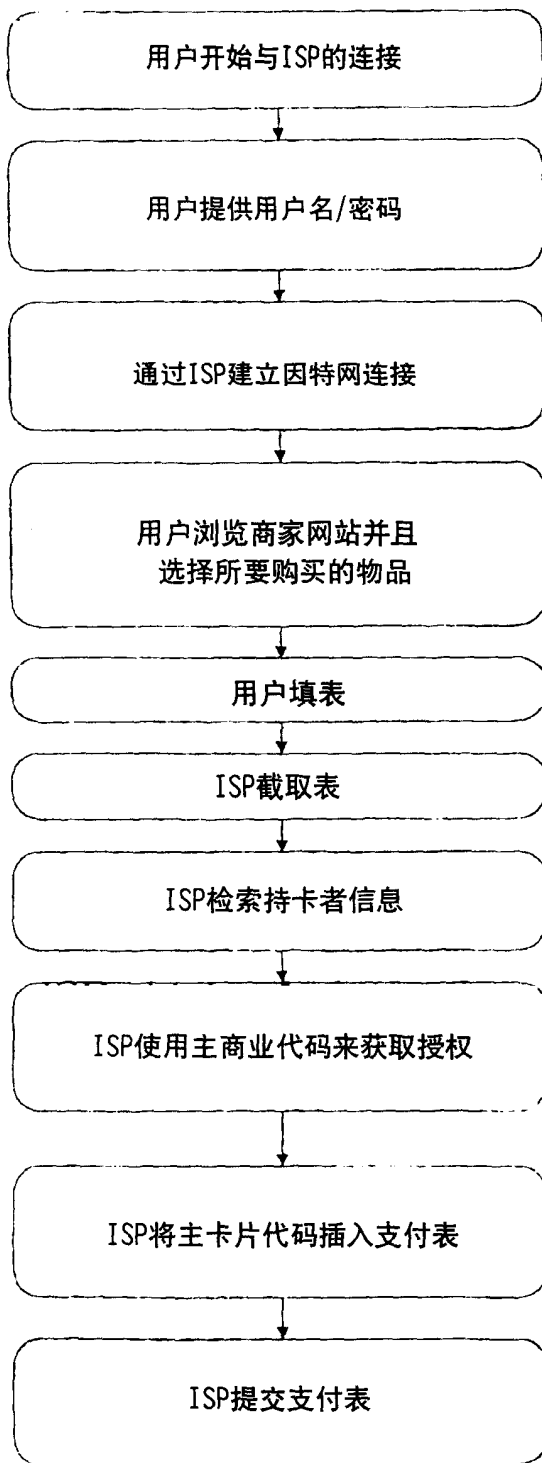


图6