[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
G06Q 20/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810200736.8

[43] 公开日 2010 年 3 月 31 日

[11] 公开号 CN 101686225A

[22] 申请日 2008.9.28
[21] 申请号 200810200736.8
[71] 申请人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路 36 号银联大厦
[72] 发明人 何 朔 孟宏文

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 臧霁晨 王小衡

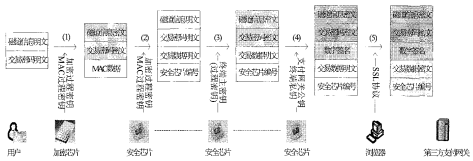
权利要求书 3 页 说明书 14 页 附图 8 页

[54] 发明名称

一种用于网上支付的数据加密和密钥生成方法

[57] 摘要

本发明揭示了一种用于网上支付的数据加密方法，包括：用户通过键盘刷卡和输入交易密码；对磁道信息和交易密码加密；接收和解密磁道信息、交易密码和 MAC 数据，并对其进行二次加密和组织报文；对报文数据进行数字签名；以及网络浏览器将全部报文发送至支付网关。 本发明也揭示了一种密钥生成方法，包括：设定加密主密钥和 MAC 主密钥；向支付网关申请下载终端主密钥；调取支付网关加密机中的根密钥；根据安全芯片编号生成终端主密钥和获取终端公钥。 采用本发明的数据加密和密钥生成方法，在互联网上传输银行卡的敏感数据及交易数据时，采用对称加密、非对称加密和 SSL 通道的三重加密，实现“一机一密”和“一次一密”，具有极高的安全性。



1. 一种用于网上支付的数据加密方法，其特征在于，它包括步骤：

用户订购商品后，通过键盘刷卡并输入交易密码，以产生磁道信息明文和交易密码明文；

加密芯片对所述磁道信息明文和交易密码明文进行加密，并转换为相应的磁道信息密文、交易信息密文和 MAC 数据；

安全芯片接收和解密所述磁道信息密文、交易密码密文和 MAC 数据，并转换为磁道信息明文、交易密码明文、交易数据明文和安全芯片编号；

安全芯片对所述磁道信息明文、交易密码明文进行二次加密并组织报文，在报文中加入交易数据明文和安全芯片编号；

安全芯片对报文数据进行数字签名，并加密所述数字签名和所述交易数据明文；以及

网络浏览器通过 SSL 协议将全部报文发送至支付网关。

2. 如权利要求 1 所述的方法，其特征在于，所述加密芯片设置在计算机的键盘内，并且所述安全芯片设置在计算机的主板上。

3. 如权利要求 1 所述的方法，其特征在于，所述加密芯片具有加密主密钥和 MAC 主密钥。

4. 如权利要求 1 所述的方法，其特征在于，所述安全芯片具有加密主密钥、MAC 主密钥、终端主密钥和终端证书。

5. 如权利要求 3 或 4 所述的方法，其特征在于，所述加密芯片的加密主密钥和所述安全芯片的加密主密钥的密钥生成算法相同，并且所述加密芯片和所述安全芯片基于加密主密钥进行对称加密。

6. 如权利要求 5 所述的方法，其特征在于，键盘的加密芯片使用加密主密钥与主板的安全芯片协商加密过程密钥，并利用所述加密过程密钥来加密磁道信息明文和交易密码明文。

7. 如权利要求 6 所述的方法，其特征在于，所述协商加密过程密钥的步骤包括：

加密芯片预设密钥生成算法；

安全芯片预设与所述加密芯片相同的密钥生成算法；

加密芯片随机生成一个随机因子，并根据加密主密钥和随机因子计算加密过程密钥；

加密芯片向安全芯片发送连接请求和随机因子；

安全芯片根据加密主密钥和随机因子计算加密过程密钥；以及

完成基于对称根密钥的过程密钥协商。

8. 如权利要求 1 所述的方法，其特征在于，所述二次加密是指，安全芯片通过终端主密钥与支付网关协商过程密钥，并使用过程密钥及 3DES 算法加密磁道信息明文和交易密码明文。

9. 如权利要求 1 所述的方法，其特征在于，安全芯片通过终端私钥对报文数据进行数字签名，并且使用支付网关公钥加密数字签名和交易数据明文及协商过程密钥的随机因子。

10. 如权利要求 1 所述的方法，其特征在于，所述安全芯片和所述加密芯片间实现密钥同步包括：

设定加密主密钥和 MAC 主密钥；

通过 BIOS 向安全芯片发出申请密钥的请求；

利用键盘驱动程序由 BIOS 自动将申请到的密钥注入加密芯片；以及

完成安全芯片和加密芯片间的密钥同步。

11. 一种在如权利要求 1 所述的数据加密方法中的密钥生成方法，其特征在于，该方法包括：

设定加密主密钥和 MAC 主密钥，以同步安全芯片和加密芯片间的密钥；

向支付网关发送请求，申请下载终端主密钥；

调取所述支付网关加密机中的根密钥；

根据安全芯片编号由所述根密钥分散生成终端主密钥；以及

根据安全芯片编号来获取终端公钥。

12. 如权利要求 11 所述的方法，其特征在于，所述加密芯片设置在计算机的键盘内，并且所述安全芯片设置在计算机的主板上。

13. 如权利要求 11 所述的方法，其特征在于，所述加密芯片具有加密主密钥和 MAC 主密钥。

14. 如权利要求 11 所述的方法，其特征在于，所述安全芯片具有加密主密钥、MAC 主密钥、终端主密钥和终端证书。

15. 如权利要求 11 所述的方法，其特征在于，计算机上的钱包程序向安全芯片发送终端证书初始化命令后，所述安全芯片生成并保存 RSA 密钥对。

一种用于网上支付的数据加密和密钥生成方法

技术领域

本发明涉及电子商务应用领域，尤其涉及电子商务应用中的安全支付技术。

背景技术

随着经济的发展和人们生活水平的提高，银行卡已经成为日常生活中随处可见的支付工具和支付手段。例如，在商场、超市、机场或者酒店中的POS终端为用户提供了便捷的服务，持卡人只需输入银行卡的密码就可以实现无币支付。此外，随着互联网上电子商务的蓬勃发展，银行卡的网上支付业务也呈现出迅速增长的态势，与银行卡的传统业务相比，网上支付属于新兴的业务领域，网上买家在进行网上支付时提供银行卡账号和个人密码，就可以完成商品购买。

然而，在繁荣的网络经济时代，由于风险管理制度和风险防范措施尚未完善，给网上支付业务带来较高的潜在风险，也给持卡人使用该网上支付业务带来诸多的负面影响。甚至，一些网民利用自制的虚假网站来骗取持卡人的银行卡账号和交易密码，以冒领银行卡内余额的网上经济案件层出不穷，一定程度上也使得持卡人使用网上支付的积极性大打折扣。

如何提供一个安全、易用、足够安全的支付手段是持卡人最为关注的技术问题，与此同时，安全、易用和备受信任的支付手段对于网络商户拓展商机和增长利润也是巨大的推动力。虽然，在现有技术中，发卡行针对电子商务的发展推出了网上银行业务，并采用硬件安全芯片作为交易证书的载体来提高交易的安全性，通过将银行卡和交易证书在后台绑定的方式提供网上支付业务，但是用户必须首先到银行购买硬件安全芯片，并绑定某张银行卡，成本较高，操作步骤繁琐，后续的业务变更还只能到银行柜台办理，给用户带来诸多不便。

另一方面，个人PC在家庭生活中日益普及，能否通过扩展普通家用电脑的理财功能，将刷卡交易引入到网上购物的支付环节，以实现“网上订购、刷卡支付”，是摆在银行服务业的技术人员面前迫切需要解决的难题。

发明内容

针对现有技术中用户在进行网上支付时所存在的上述技术缺陷，本发明提供了一种用于网上支付的数据加密方法和密钥生成方法。通过分别在电脑的主板和键盘上设计安全芯片和加密芯片来完成银行卡敏感数据的加密和/或解密，以实现数据的安全传输。与现有的网上支付业务不同，在该支付系统中用户不仅要输入银行卡密码，而且还需要在电脑的键盘上执行刷卡操作以获取银行卡的磁道信息数据，并通过键盘上的加密芯片进行加密而发送至电脑主板上的安全芯片。

按照本发明的一个方面，提供了一种用于网上支付的数据加密方法。该数据加密方法包括:

用户订购商品后，通过键盘刷卡并输入交易密码，以产生磁道信息明文和交易密码明文;

加密芯片对磁道信息明文和交易密码明文进行加密，并转换为相应的磁道信息密文、交易信息密文和 MAC 数据;

安全芯片接收和解密磁道信息密文、交易密码密文和 MAC 数据，并转换为磁道信息明文、交易密码明文、交易数据明文和安全芯片编号;

安全芯片对磁道信息明文、交易密码明文进行二次加密并组织报文，在报文中加入交易数据明文和安全芯片编号;

安全芯片对报文数据进行数字签名，并加密数字签名和交易数据明文；以及

网络浏览器通过 SSL 协议将全部报文发送至支付网关。

其中，加密芯片设置在计算机的键盘内，并且安全芯片设置在计算机的主板上。

其中，加密芯片具有加密主密钥和 MAC 主密钥。

其中，安全芯片具有加密主密钥、MAC 主密钥、终端主密钥和终端证书。进一步，终端证书包括终端公钥、终端私钥和支付网关公钥。

其中，加密芯片的加密主密钥和安全芯片的加密主密钥的密钥生成算法相同，并且加密芯片和安全芯片基于加密主密钥进行对称加密。此外，键盘的加密芯片使用加密主密钥与主板的安全芯片协商加密过程密钥，并利用该加密过程密钥来加密磁道信息明文和交易密码明文。

其中，主板的安全芯片使用加密过程密钥来解密来自加密芯片的磁道信息密文和交易密码密文。

其中，键盘上的加密芯片和主板上的安全芯片协商加密过程密钥的步骤包括：

加密芯片预设密钥生成算法；

安全芯片预设与加密芯片相同的密钥生成算法；

加密芯片随机生成一个随机因子，并根据加密主密钥和随机因子计算加密过程密钥；

加密芯片向安全芯片发送连接请求和随机因子；

安全芯片根据加密主密钥和随机因子计算加密过程密钥；以及

完成基于对称根密钥的过程密钥协商。

其中，二次加密是指安全芯片通过终端主密钥与支付网关协商过程密钥，并使用过程密钥及3DES算法加密磁道信息明文和交易密码明文，3DES算法采用128位的长密钥。

其中，安全芯片通过终端私钥对报文数据进行数字签名，并且使用支付网关公钥加密数字签名和交易数据明文及协商过程密钥的随机因子，数字签名的算法使用1024位长密钥的RSA算法。

其中，安全芯片和所述加密芯片间实现密钥同步包括：

设定加密主密钥和MAC主密钥；

通过BIOS向安全芯片发出申请密钥的请求；

利用键盘驱动程序由BIOS自动将申请到的密钥注入加密芯片；以及

完成安全芯片和加密芯片间的密钥同步。

按照本发明的又一个方面，提供了一种在用于网上支付的数据加密方法中的密钥生成方法，该方法包括：

设定加密主密钥和MAC主密钥，以同步安全芯片和加密芯片间的密钥；

向支付网关发送请求，申请下载终端主密钥；

调取所述支付网关加密机中的根密钥；

根据安全芯片编号由所述根密钥分散生成终端主密钥；以及

根据安全芯片编号来获取终端公钥。

其中，加密芯片设置在计算机的键盘内，并且安全芯片设置在计算机的主板上。

其中，加密芯片具有加密主密钥和MAC主密钥；并且，安全芯片具有加密主密钥、MAC主密钥、终端主密钥和终端证书。更为具体地，终端证书包括终端公钥、终端私钥和支付网关公钥。

其中，计算机上的钱包程序向安全芯片发送终端证书初始化命令后，安全芯片生成并保存 RSA 密钥对。该 RSA 密钥对包括终端私钥和终端公钥。

采用本发明的数据加密和密钥生成方法，能够以个人 PC 为平台，为持卡人提供一个安全的网上支付环境，将互联网上电子商务的便捷性和理财电脑的安全性集于一体，从计算机键盘、计算机主板、支付网关到清算转接机构均采用数据加密传输，将传统的刷卡交易引入网上交易的支付环节，实现“网上订购、刷卡支付”，在提升网上支付安全级别的同时，也极大地方便了网络用户。而且，利用本发明的数据加密和密钥生成方法，在互联网上传输银行卡的敏感数据及交易数据时，采用对称加密、非对称加密和 SSL 通道的三重加密，实现“一机一密”和“一次一密”，具有极高的安全性。

附图说明

读者在参照附图阅读了本发明的具体实施方式以后，将会更清楚地了解本发明的各个方面。其中，

图 1 示出了本发明基于理财电脑来实现网上支付的流程示意图；

图 2 示出了本发明用于实现网上支付的理财电脑的结构示意图；

图 3 示出了本发明在使用网上支付业务前激活理财电脑的原理示意图；

图 4 示出了采用本发明的理财电脑进行网上支付时，从持卡人刷卡到第三方支付网关接收报文过程中的数据加密示意图；

图 5 示出了依据本发明进行网上支付而采用的各种密钥的存储示意图；

图 6 示出了本发明理财电脑的主板上所存储的终端主密钥和终端公钥的生成示意图；

图 7 示出了本发明理财电脑的主板上的安全芯片和键盘上的加密芯片基于加密主密钥而协商加密过程密钥的原理示意图；

图 8 示出了本发明中实现安全芯片和加密芯片间密钥同步的原理框图；

图 9 示出了本发明理财电脑的主板上的安全芯片进行初始化的流程示意图；

图 10 示出了本发明用于网上支付的银行卡在支付网关上注册的流程示意图；

图 11 示出了本发明基于理财电脑的网上支付系统的支付流程示意图；而

图 12 示出了本发明基于理财电脑的网上支付系统的收款流程示意图。

具体实施方式

下面参照附图，对本发明的具体实施方式作进一步的详细描述。

图 1 示出了本发明基于理财电脑来实现网上支付的流程示意图。这里，理财电脑是指具有网上支付功能的家用电脑。本领域的技术人员应当理解，图 1 不仅可以表示本发明的支付系统的结构组成，而且还可以说明该支付系统进行网上支付的具体流程示意图。

参照图 1，该支付系统包括：网络用户的理财电脑 10、支付网关 20、清算转接机构 30、发卡行 40、以及网络商户 50。其中，网络用户是发卡行和中国银联的用户，持有银联卡并且是理财电脑的所有者，对理财电脑上发生的刷卡行为负责；支付网关 20（也称为收单服务机构）拓展使用理财电脑支付的互联网 B2C 商户，为网络商户提供资金结算、差错请求提交等收单服务；清算转接机构 30 是运营理财电脑接入前置和交换的网络，并进行跨行支付清算服务；发卡行 40 是网络用户持有的银行卡的发卡机构；以及网络商户 50 是通过互联网为持卡人提供商业服务的单位或机构。需要指出的是，发卡行可以不经过清算转接机构中转，直接接收来自所述支付网关的敏感数据和交易数据，并返回响应信息至所述支付网关。更加具体地，理财电脑 10 至少包括主板 104 和键盘 102。

当采用上述支付系统进行网上支付时，主要包括以下步骤：

步骤 S1，作为持卡人的网络用户通过理财电脑 10 访问在线网络商户 50，订购商品并选择理财电脑支付方式进行支付；

步骤 S2，接受理财电脑支付方式，将网页重定向至中国银联统一的支付页面；

步骤 S3，网络用户的理财电脑 10 检测到来自支付网关 20 的等待支付信息，理财电脑 10 键盘上的专用指示灯亮起，以提示用户刷卡并输入密码；

步骤 S4，持卡人通过集成了读卡器的键盘进行刷卡，当输入交易密码后，将磁道信息和交易密码以加密的方式送往理财电脑 10 主板上的安全芯片；

步骤 S5，安全芯片接收来自键盘的磁道信息和交易密码，再次加密后连同交易数据一起发送至支付网关 20；

步骤 S6，支付网关 20 判断所接收的信息是否合法，如果合法则将交易信息发送到清算转接机构 30；如果不合法则结束并返回；

步骤 S7，清算转接机构 30 转发交易信息至发卡行 40；

步骤 S8，发卡行 40 返回应答至清算转接机构 30；

步骤 S9，清算转接机构 30 将发卡行的返回应答转发至支付网关 20;

步骤 S10，支付网关 20 将交易结果通知在线网络商户 50;

步骤 S11，在线网络商户 50 将交易结果和订单匹配，返回交易结果通知应答;

步骤 S12，支付网关 20 向理财电脑 10 返回支付结果页面，用户通过支付结果页面中的链接返回在线网络商户网站以查询确认支付结果；以及

步骤 S13，该在线网络商户 50 将相应的商品发送至持卡人。

其中，在上述步骤里，支付网关是指中国银联的支付网关，其主要用于拓展基于理财电脑支付方式的互联网 B2C 商户，并为商户提供资金结算、差错请求提交等收单服务。

其中，在上述步骤里，持卡人在理财电脑上进行刷卡支付。但是，刷卡人和持卡人可以是同一个人，也可以是不同的人。

图 2 示出了本发明用于实现网上支付的理财电脑的结构示意图。参照图 2，理财电脑 10 至少包括主板 104 和键盘 102，其中，主板 104 具有安全芯片 1041，以及键盘 102 具有加密芯片 1021、读卡器和支付指示灯等。如图 1 所述，本发明的支付系统在进行网上安全支付时，首先网页重定向至银联统一的支付页面，当键盘的专用指示灯亮起，持卡人利用读卡器进行刷卡并输入交易密码，此时，加密芯片 1021 将持卡人输入的磁道信息和交易密码以加密方式传送至主板上的安全芯片 1041，并且安全芯片 1041 解密该加密信息后组织交易报文，再次通过安全芯片加密交易报文中的敏感交易数据后发送至后台。至于安全芯片 1041 和加密芯片 1021 之间的密钥机制和协商将在后续的附图中具体描述。

优选地，用于输入交易密码的小键盘采用密码键盘，或者至少采用达到密码键盘的安全水平的 PIN 输入设备。其中，键盘设置专用切换键，只有切换到基于理财电脑的网上支付方式时，读卡器才接收银行卡的磁道信息，同时由键盘内置的加密芯片对用户输入的交易密码进行加密。

其中，键盘也设置专用的指示灯及其驱动程序，当网络用户在支付网关提交支付请求时，电脑将接收到等待支付的信息，键盘的专用指示灯亮起，以提示用户可以进行刷卡操作。进一步，等待支付设置超时处理，当持卡人超过一定时间仍未刷卡支付时，键盘的专用指示灯熄灭，持卡人须重新到支付网关的统一支付页面上提交支付请求。这样就可以防止伪造刷卡键盘，因为伪造的刷卡键盘无法对等待支付信息作出实时响应。

图 3 示出本发明在使用网上支付业务前激活理财电脑的原理示意图。参照图 3，本发明中在其主板上具有安全芯片和在其键盘上具有加密芯片的家用电脑在使用理财功能前，必须予以激活。其具体的激活流程为：

首先，网络用户进入基本输入输出系统(BIOS)设置中相应的菜单项，选择激活电脑的理财功能；

接着，BIOS 向键盘发送指令以查询键盘状态，确认键盘上装有加密芯片；向主板发送指令以查询主板状态，确认主板上装有安全芯片；此时，键盘和主板均接收相应的查询指令，并返回状态信息；

步骤 S3，BIOS 发送初始化激活命令并接收主板的响应信息；并且主板返回唯一的响应信息；

步骤 S4，分析响应信息并将新的传输密钥发送到键盘，接收键盘的响应信息；并且键盘写入新密钥，锁定键盘的加密芯片和主板的安全芯片之间的通讯机制；

步骤 S5，BIOS 发送激活键盘命令，以激活计算机的理财功能；主板设置新的传输密钥，记录键盘串号并启动理财功能。

图 4 示出了采用本发明的理财电脑进行网上支付时，从持卡人刷卡到第三方支付网关接收报文过程中的数据加密示意图。参照图 4，在该加密数据的传输流程中主要涉及键盘的加密芯片、主板的安全芯片以及第三方支付网关。并且，数据加密主要存在于从持卡人利用集成了读卡器的键盘刷卡到主板的安全芯片、从主板的安全芯片到第三方支付网关。以下，分别使用流程中的节点(1)、(2)、(3)、(4)和(5)进行详细描述。

需要指出的是，图 4 中的磁道信息密文、交易密码密文、交易数据密文以及数字签名均表示加密数据，而磁道信息明文、交易密码明文、交易数据明文和安全芯片编号均表示未加密数据或者已加密数据解密后的数据。

节点(1)，网络用户通过键盘刷卡并输入交易密码，以产生对应于磁道信息的磁道信息明文和对应于交易密码的交易密码明文，键盘的加密芯片利用加密过程密钥以及 MAC 过程密钥将磁道信息明文和交易密码明文转换为磁道信息密文、交易信息密文和 MAC 数据；

节点(2)，主板的安全芯片接收到来自加密芯片的磁道信息密文、交易信息密文和 MAC 数据后，首先使用 MAC 过程密钥验证数据未被更改，再使用加密过程密钥来解密磁道信息密文和交易密码密文，并转换为磁道信息明文、交易密码明文、

交易数据明文和安全芯片编号，这里，键盘的加密芯片和主板的安全芯片之间的通讯采用对称加密的机制，键盘的加密芯片使用加密主密钥与主板的安全芯片协商加密过程密钥，并利用加密过程密钥来解密磁道信息密文和交易密码密文；以及键盘的加密芯片使用 MAC 主密钥协商 MAC 过程密钥，再用 MAC 过程密钥计算密文的消息验证码，以确保数据未被更改；

节点(3)，主板的安全芯片通过终端主密钥与第三方支付网关协商过程密钥，并使用过程密钥及 3DES 算法加密产生磁道信息密文和交易密码密文，其中 3DES 算法采用 128 位长密钥，并在报文中加入订单信息等交易数据明文及安全芯片编号；

节点(4)，主板的安全芯片通过终端私钥对报文数据进行数字签名，再使用终端证书中的支付网关公钥加密数字签名和节点(3)中的交易数据明文及协商过程密钥的随机因子。其中非对称加密和数字签名算法使用 1024 位长密钥的 RSA 算法；以及

节点(5)，网络浏览器通过 SSL 协议将全部报文发送至第三方支付网关，该第三方支付网关接收到报文后，首先通过安全芯片编号分散出终端对应的公钥，使用自身私钥解密交易数据密文、随机因子和数字签名，并使用终端公钥核对数字签名，再使用随机因子和终端主密钥计算得出过程密钥，最后使用过程密钥解密得到磁道信息明文和交易密码明文。在获得所有数据明文后，第三方支付网关使用与清算转接机构协商的工作密钥加密交易密码，并与磁道信息、交易数据一起通过金融网转发至清算转接机构。

通过上述数据传输流程可以知晓，本发明的支付系统相对于现有技术中的网上支付方法，具有如下特点：

通过键盘的加密芯片将用户刷卡产生的磁道信息和输入的交易密码进行加密以传输到主板的安全芯片；

在互联网上传输数据时，采用对称加密、非对称加密和 SSL 通道的三重加密，实现“一机一密”和“一次一密”；这里，一机一密是指每台理财电脑具有唯一性的密钥；一次一密是指在每个传输节点上采用不同的加密密钥；

磁道信息和交易密码在网络的任何节点上均为加密传输；

密码键盘通过 MAC 保证敏感数据到达主板的安全芯片前不被更改；通过终端证书签名及 HTTP 通信协议保证交易在互联网上传输的完整性；以及通过终端证书签

名保证交易的不可否认性，保存金融交易的原始报文（含签名），以确保在发生争议时有据可查。

图 5 示出了依据本发明进行网上支付而采用的各种密钥的存储示意图。如图 5 所示，键盘的加密芯片 1021 具有加密主密钥和 MAC 主密钥，主板的安全芯片 1041 具有加密主密钥、MAC 主密钥、终端主密钥和终端证书。其中，终端证书包括自身公钥和私钥以及第三方支付网关公钥，用于与第三方支付网关进行非对称加密；加密主密钥用于在安全芯片和加密芯片间进行对称加密，并协商加密过程密钥；和 MAC 主密钥用于协商 MAC 过程密钥。此外，终端主密钥用于主板的安全芯片与第三方支付网关进行对称加密。

图 6 示出了本发明理财电脑的主板上所存储的终端主密钥和终端公钥的生成示意图。如上所述，终端主密钥用于主板的安全芯片与第三方支付网关进行对称加密，更为详细地，主板上的安全芯片通过终端主密钥与第三方支付网关协商过程密钥，使用该过程密钥及 3DES 算法加密交易密码明文和磁道信息明文。参照图 6，生成终端主密钥和终端公钥包括：

步骤 600，向第三方支付网关发送请求，申请下载终端主密钥；

步骤 602，调取该第三方支付网关加密机中的根密钥；

步骤 604，根据安全芯片编号由该根密钥分散生成终端主密钥；以及

步骤 606，根据安全芯片编号来获取终端公钥。

其中，所获取的终端公约用于核对数字签名。

其中，第三方支付网关的加密机主要用于加密和解密操作，包括：使用支付网关自身私钥解密交易数据密文、随机因子和数字签名；基于随机因子和终端主密钥计算得出的过程密钥，解密得到磁道信息明文和交易密码明文；使用与清算转接机构协商的工作密钥加密交易密码。

图 7 示出了本发明理财电脑的主板上的安全芯片和键盘上的加密芯片基于加密主密钥而协商加密过程密钥的原理示意图。如上所述，键盘的加密芯片和主板的安全芯片间采用对称加密的通讯机制，具体来说，键盘的加密芯片使用加密主密钥与主板的安全芯片协商加密过程密钥，并用该加密过程密钥加密磁道信息明文和交易密码明文；另一方面，安全芯片在接收到磁道信息密文和交易密码密文后，利用相同的加密过程密钥来解密磁道信息密文和交易密码密文。该协商加密过程密钥包括：

步骤 700，加密芯片预设密钥生成算法；

步骤 702，安全芯片预设与加密芯片相同的密钥生成算法；

步骤 704，加密芯片随机生成一个随机因子，并根据加密主密钥和随机因子计算加密过程密钥；

步骤 706，键盘的加密芯片向主板的安全芯片发送连接请求和随机因子；

步骤 708，安全芯片根据加密主密钥和随机因子计算加密过程密钥；以及

步骤 710，完成基于对称根密钥的过程密钥协商。

本领域的技术人员应当理解，键盘的加密芯片可以采用与上述流程类似的方法使用 MAC 主密钥协商 MAC 过程密钥，同样，主板的安全芯片可以使用终端主密钥与第三方支付网关协商过程密钥；以及第三方支付网关可以与清算转接机构协商工作密钥。

图 8 示出了本发明中实现安全芯片和加密芯片间密钥同步的原理框图。参照图 8,键盘的加密芯片和主板的安全芯片采用加密主密钥和 MAC 主密钥进行数据传输，并且加密主密钥和 MAC 主密钥仅仅用于保证从键盘到安全芯片传输数据信息的完整性，与第三方支付网关无关。实现安全芯片和加密芯片间密钥同步包括：

步骤 800，设定加密主密钥和 MAC 主密钥；

步骤 802，通过 BIOS 向安全芯片发出申请密钥的请求；

步骤 804，利用键盘驱动程序由 BIOS 自动将申请到的密钥注入加密芯片；以及

步骤 806，完成安全芯片和加密芯片之间的密钥同步。

图 9 示出了本发明理财电脑的主板上的安全芯片进行初始化的流程示意图。当网络用户在理财电脑上使用银行卡进行网上支付时，首先须将银行卡在第三方支付网关上注册后才可以使用，即第三方支付网关能够识别持卡人的银行卡。为此，在理财电脑上专门设置有一个用来管理注册银行卡的程序，其主要是将用户的银行卡信息安全地传送到第三方支付网关进行注册。只有在支付网关进行了注册的银行卡才可以办理网上支付业务，因该注册银行卡的程序类似于钱包的功能，我们不妨将其称为钱包程序。该钱包程序可以是单独的应用程序，或者在网页上运行的程序，用于初始化主板上的安全芯片，管理注册的银行卡并设置默认的支付卡片。

从安全支付的角度考虑，用户的银行卡信息每次在交易时都将由安全芯片进行加密处理后才在互联网上进行传输。其初始化的流程包括：

钱包程序查询证书的有效性;

安全芯片返回证书状态到钱包程序，若证书有效，则结束该初始化过程，若证书无效，则向安全芯片发送证书初始化命令;

安全芯片接收初始化命令后，生成RSA密钥对，并保存安全芯片的私钥，返回安全芯片的公钥至钱包程序;

钱包程序接收安全芯片的公钥，取得个人信息后发送支付网关进行数字签名;

将待签名信息送CA签名，返回数字证书至钱包程序；以及

钱包程序接收证书并发送命令STORE_CERT以保存至安全芯片。

其中，存储在安全芯片上的数字证书可以在交易时用来加密或进行签名，如果证书失效或者不存在，则网上支付行为将无法完成。

如图9所述，持卡人的银行卡只有在第三方支付网关上注册后才可以使用。因而，图10示出了本发明用于网上支付的银行卡在支付网关上注册的流程示意图。该注册流程包括:

用户打开钱包程序，选择注册银行卡功能;

理财电脑提示用户刷卡并输入PIN;

用户进行刷卡操作并输入PIN;

理财电脑将卡片的磁道信息及交易密码加密后送往第三方支付网关;

第三方支付网关将收到的银行卡的磁道信息和交易密码解密后，发送至相应的发卡行进行验证，根据发卡行的验证结果向理财电脑返回响应信息；以及

理财电脑接收该响应信息，提示银行卡注册成功或失败。

以上简要描述了用于网上支付的银行卡在支付网关上注册的主要步骤。这里，为了更加详细地介绍注册流程，我们不妨将其划分为四个节点，具体为：钱包程序提示用户刷卡及输入PIN、主板上的安全芯片对来自加密芯片的磁道信息密文和交易密码密文进行处理、钱包程序发送数据至第三方支付网关、以及第三方支付网关绑定银行卡。下面对该四个节点的详细操作步骤说明如下:

（1）钱包程序提示用户刷卡及输入PIN

a.理财电脑的钱包程序向键盘发送刷卡信号，键盘的专用指示灯亮起以提示用户进行刷卡操作;

b.用户刷卡，键盘将银行卡的磁道信息加密后等待读取;

c.钱包程序读取磁道信息密文后送至安全芯片;

d.钱包程序提示用户输入PIN；以及

e.用户输入PIN，键盘将交易密码加密后等待读取。

（2）主板上的安全芯片对来自加密芯片的磁道信息密文和交易密码密文进行处理

a.安全芯片只有在接收磁道信息密文和交易密码密文后才替换密文和签名；

b.安全芯片接收磁道信息密文后，对其进行解密，检查格式是否正确，如果成功则设置标志位，指示磁道信息就绪；

c.安全芯片接收交易密码密文后，对其进行解密，检查格式是否正确，如果成功则设置标志位，指示交易密码就绪；

d.每次设置标志位后均检查是否磁道信息和交易密码都具备，如果具备则进行下一步，否则等待设置标志位；

e.安全芯片生成一个16位长的随机对称密钥SK，将交易密码和磁道信息使用SK进行加密；

f.用第三方支付网关公钥对SK加密得到的信息称为信封，用安全芯片私钥对交易密码密文和磁道信息密文按照一定的格式签名，得到签名信息；

g.返回交易密码密文和磁道信息密文；以及

h.返回信封和签名信息。

（3）钱包程序发送数据至第三方支付网关

a.提示输入银行卡名称和电子邮件等信息；以及

b.将个性化信息和信封、签名信息及磁道信息密文和交易密码密文一起组成报文发送至第三方支付网关。

（4）第三方支付网关绑定银行卡

a.第三方支付网关收到报文后，用私钥解开信封，得到SK；

b.用SK磁道信息密文解密PIN，并用银行的终端密钥重新加密磁道信息；

c.将磁道信息和交易密码发送至发卡行进行验证；以及

d.返回成功与否的响应报文至钱包程序

其中，若验证成功，则对银行卡卡号和理财电脑的硬件序号进行绑定，形成对应关系并保存到安全芯片；若验证失败，则返回响应信息提示用户注册不成功。

图11示出了本发明基于理财电脑的网上支付系统的支付流程示意图。该支付流程包括：

网络用户浏览网站，选购商品并指定使用理财电脑支付方式；

用户选择支付的银行卡并确定；

理财电脑激活钱包程序，提示用户刷卡并输入 PIN；

用户在键盘上执行刷卡操作并输入 PIN；

理财电脑接收加密磁道信息和加密 PIN；

检查当前的银行卡是否在安全芯片的认证卡列表里，如果不在，提示用户无法进行支付，如果存在，则获取订单信息和银行卡信息后组织报文发送到支付网关；

支付网关收到报文，检查绑定关系，确认可以交易后，转发报文至清算转接机构，并取得清算转接机构的响应信息；

支付网关发送付款成功消息至商户，并得到订单查询 URL；

商户接收付款成功消息，匹配订单，准备发货；

支付网关返回响应信息至理财电脑，理财电脑接收该响应信息，提示交易结束；以及

用户选择继续购物或者退出。

其中，激活钱包程序进行网上支付可以分为两种，一种是在购物网站上选择支付时自动跳转到支付网关的统一支付页面，由支付页面通过钱包接口调用钱包程序；另一种是点击支付页面时，目标页面自动导向到由商户网站自动生成一定格式的购物信息文件，该文件类型和钱包程序在理财电脑形成关联。

图 12 示出了本发明基于理财电脑的网上支付系统的收款流程示意图。与图 11 所示的支付流程相类似，该收款流程包括：

网络用户选购商品并指定使用理财电脑支付方式；

商户启用理财电脑进行收款转账，要求用户刷卡和输入 PIN；

理财电脑激活收款程序；

用户刷卡并输入 PIN；

理财电脑接收加密磁道信息和加密 PIN，并组织报文发送至支付网关；

支付网关收到报文，检查绑定关系，确认可以交易后，转发报文至清算转接机构，并取得清算转接机构的响应信息；

支付网关发送付款成功消息至商户，并得到订单查询 URL；

商户接收转账通知，确认收款成功；

支付网关返回该响应信息至理财电脑，理财电脑接收该响应信息，提示交易结

束；以及

商户交付商品给该用户。

上文中，参照附图描述了本发明的具体实施方式。但是，本领域中的普通技术人员能够理解，在不偏离本发明的精神和范围的情况下，还可以对本发明的具体实施方式作各种变更和替换。这些变更和替换都落在本发明权利要求书所限定的范围内。

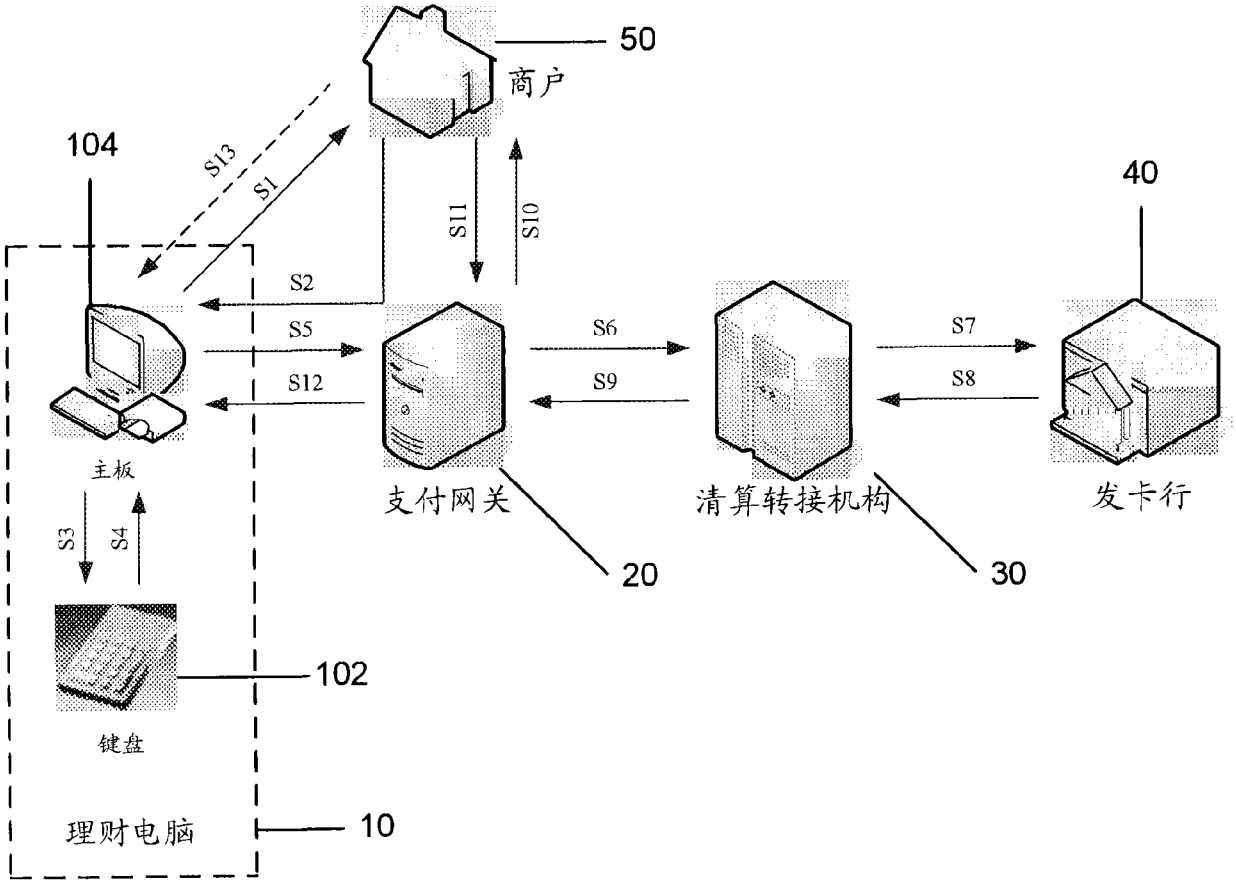

50
商户
104
S13
S1
S11
S10
40
S2
S5
S6
S7
S12
S9
S8
主板
S3
S4
支付网关
清算转接机构
发卡行
20
30
102
键盘
理财电脑
10

图 1

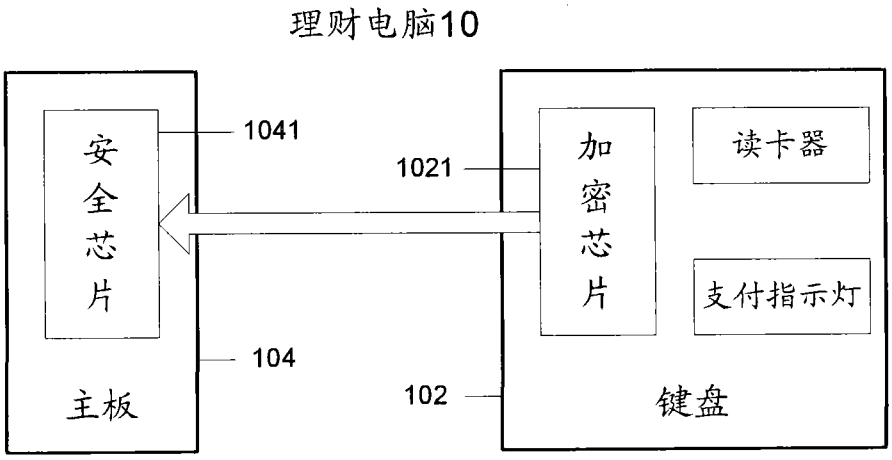

理财电脑10
安全芯片
1041
1021
加密芯片
读卡器
支付指示灯
104
主板
102
键盘

图 2

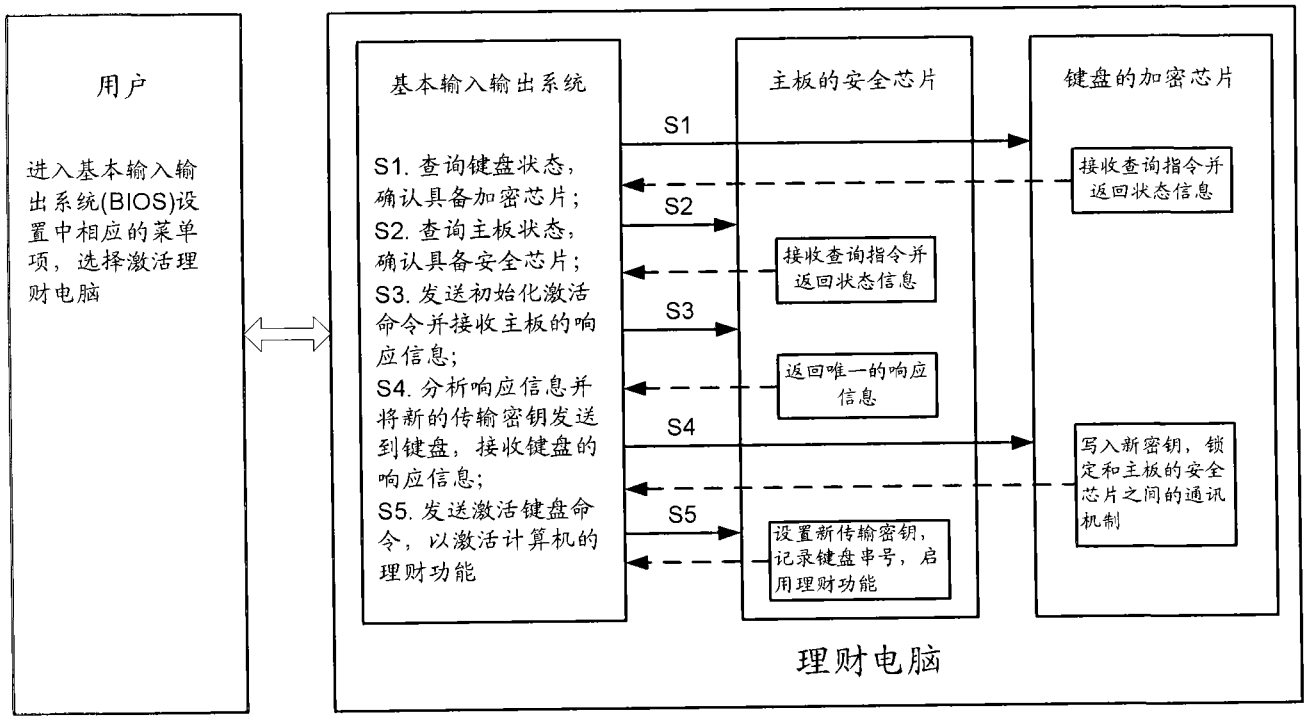

用户
进入基本输入输出系统(BIOS)设置中相应的菜单项，选择激活理财电脑
基本输入输出系统
S1. 查询键盘状态，确认具备加密芯片；
S2. 查询主板状态，确认具备安全芯片；
S3. 发送初始化激活命令并接收主板的响应信息；
S4. 分析响应信息并将新的传输密钥发送到键盘，接收键盘的响应信息；
S5. 发送激活键盘命令，以激活计算机的理财功能
主板的安全芯片
键盘的加密芯片
S1
接收查询指令并返回状态信息
S2
接收查询指令并返回状态信息
S3
返回唯一的响应信息
S4
写入新密钥，锁定和主板的安全芯片之间的通讯机制
S5
设置新传输密钥，记录键盘串号，启用理财功能
理财电脑

图 3

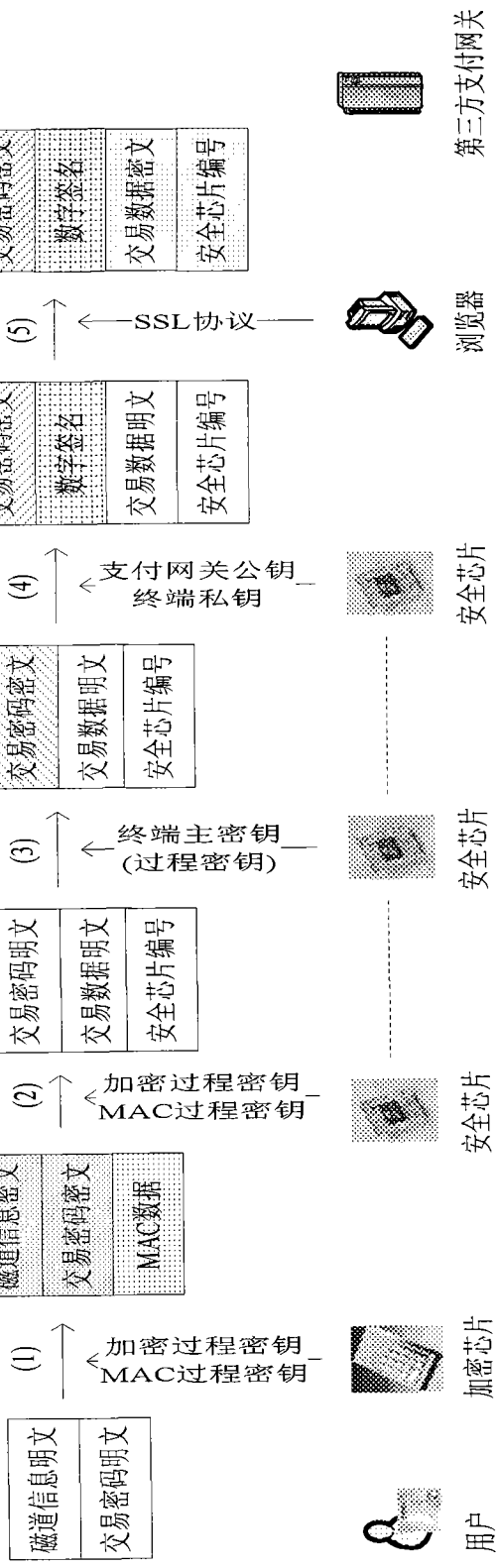

磁道信息明文
交易密码明文
(1)
加密过程密钥_
MAC过程密钥
磁道信息密文
交易密码密文
MAC数据
(2)
加密过程密钥_
MAC过程密钥
磁道信息明文
交易密码明文
交易数据明文
安全芯片编号
(3)
终端主密钥
(过程密钥)
磁道信息密文
交易密码密文
交易数据明文
安全芯片编号
(4)
支付网关公钥_
终端私钥
磁道信息密文
交易密码密文
数字签名
交易数据明文
安全芯片编号
(5)
SSL协议
磁道信息密文
交易密码密文
数字签名
交易数据密文
安全芯片编号
用户
加密芯片
安全芯片
安全芯片
浏览器
第三方支付网关

图 4

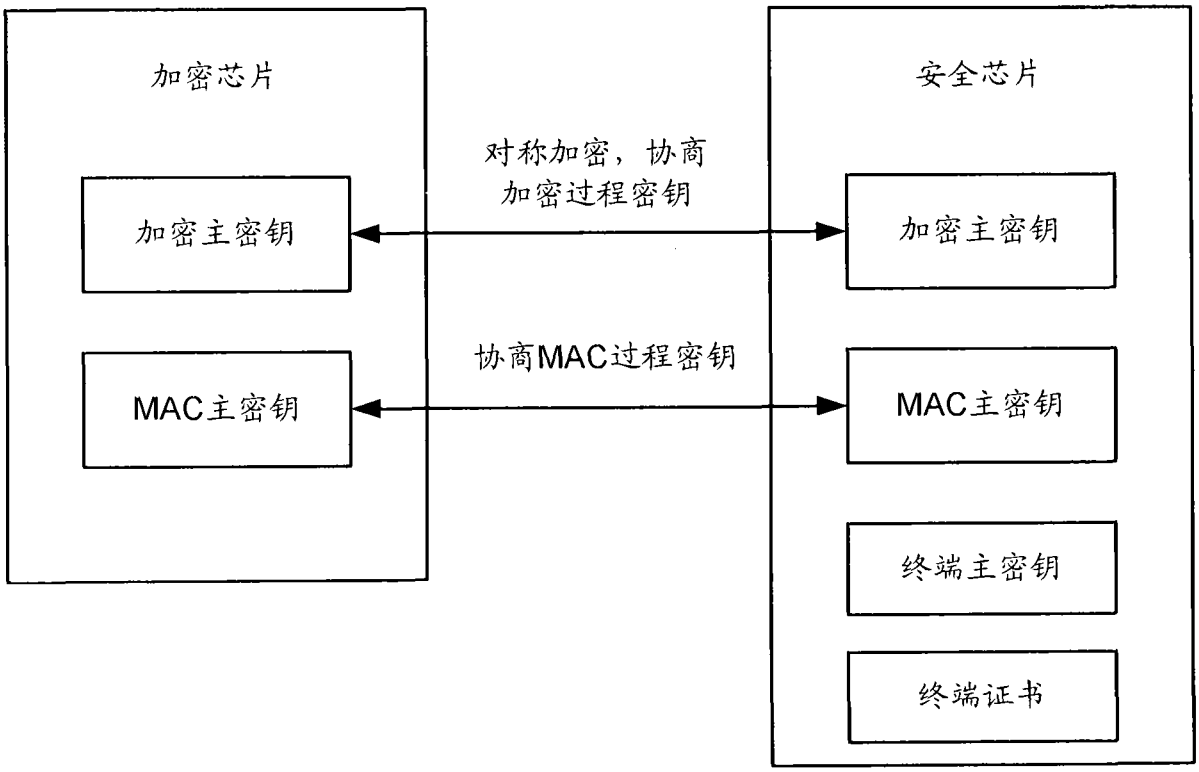

加密芯片
安全芯片
对称加密，协商
加密过程密钥
加密主密钥
加密主密钥
协商MAC过程密钥
MAC主密钥
MAC主密钥
终端主密钥
终端证书

图 5

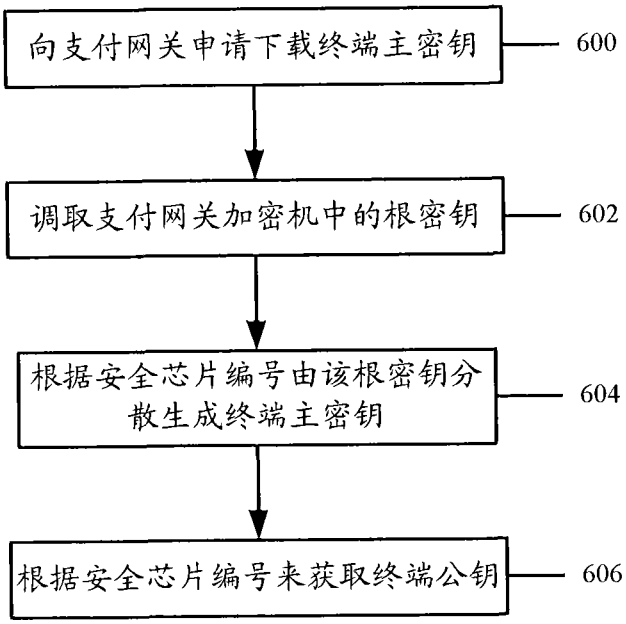

向支付网关申请下载终端主密钥
600
调取支付网关加密机中的根密钥
602
根据安全芯片编号由该根密钥分
散生成终端主密钥
604
根据安全芯片编号来获取终端公钥
606

图 6

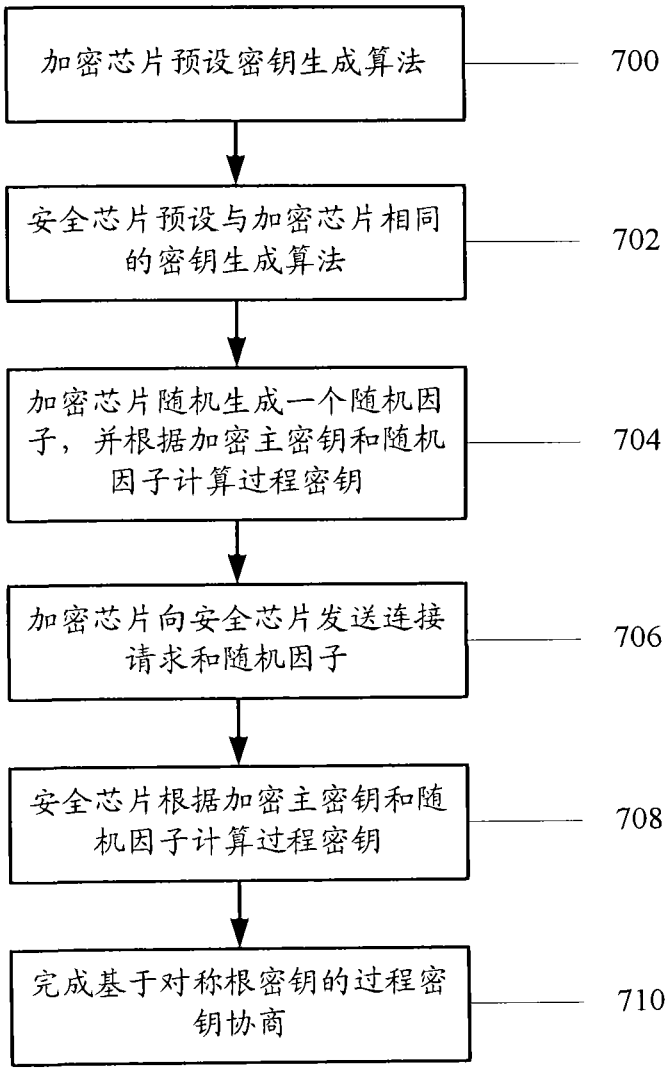

加密芯片预设密钥生成算法
700
安全芯片预设与加密芯片相同的密钥生成算法
702
加密芯片随机生成一个随机因子，并根据加密主密钥和随机因子计算过程密钥
704
加密芯片向安全芯片发送连接请求和随机因子
706
安全芯片根据加密主密钥和随机因子计算过程密钥
708
完成基于对称根密钥的过程密钥协商
710

图 7

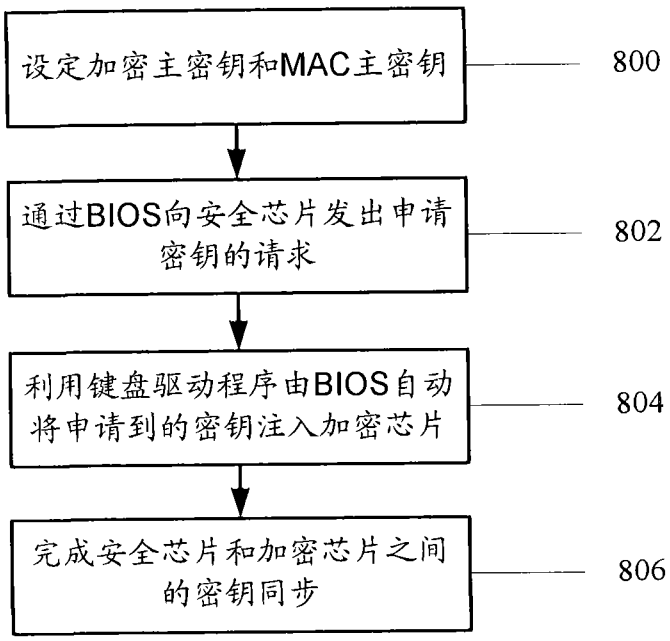

设定加密主密钥和MAC主密钥
800
通过BIOS向安全芯片发出申请密钥的请求
802
利用键盘驱动程序由BIOS自动将申请到的密钥注入加密芯片
804
完成安全芯片和加密芯片之间的密钥同步
806

图 8

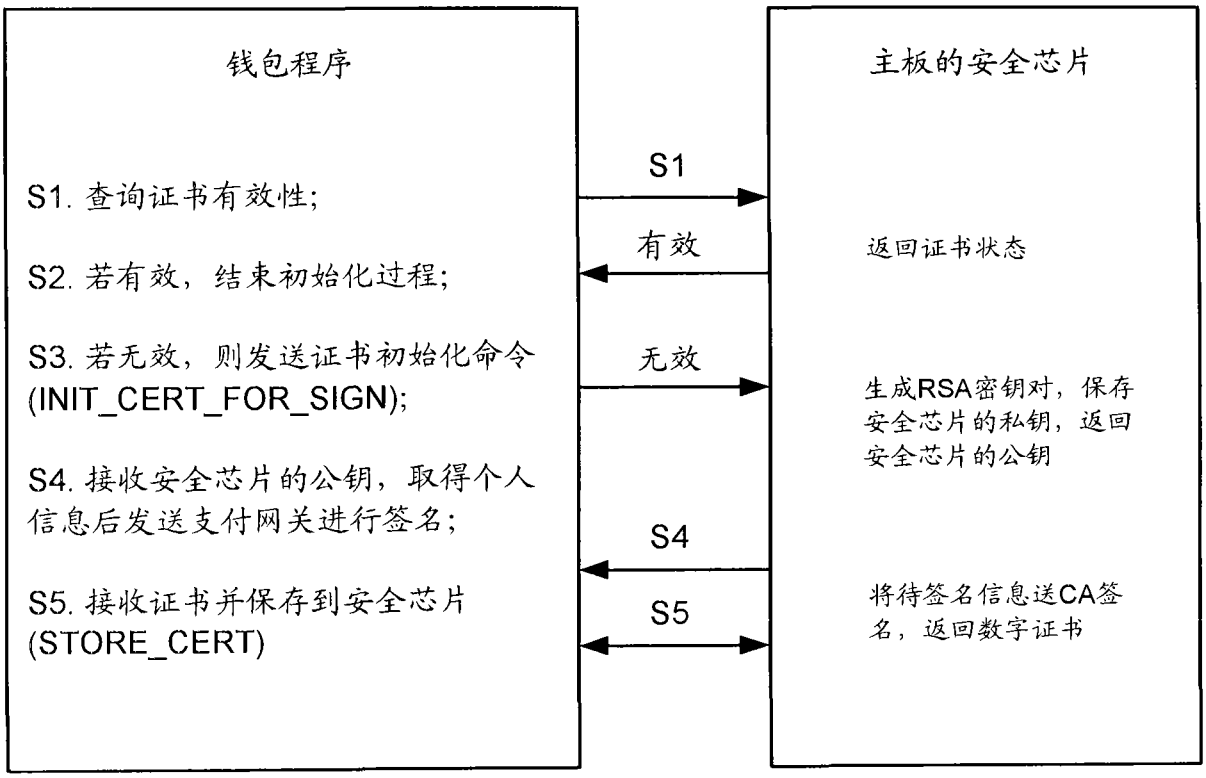

钱包程序
主板的安全芯片
S1. 查询证书有效性;
S2. 若有效，结束初始化过程;
S3. 若无效，则发送证书初始化命令(INIT_CERT_FOR_SIGN);
S4. 接收安全芯片的公钥，取得个人信息后发送支付网关进行签名;
S5. 接收证书并保存到安全芯片(STORE_CERT)
S1
有效
返回证书状态
无效
生成RSA密钥对，保存安全芯片的私钥，返回安全芯片的公钥
S4
将待签名信息送CA签名，返回数字证书
S5

图 9

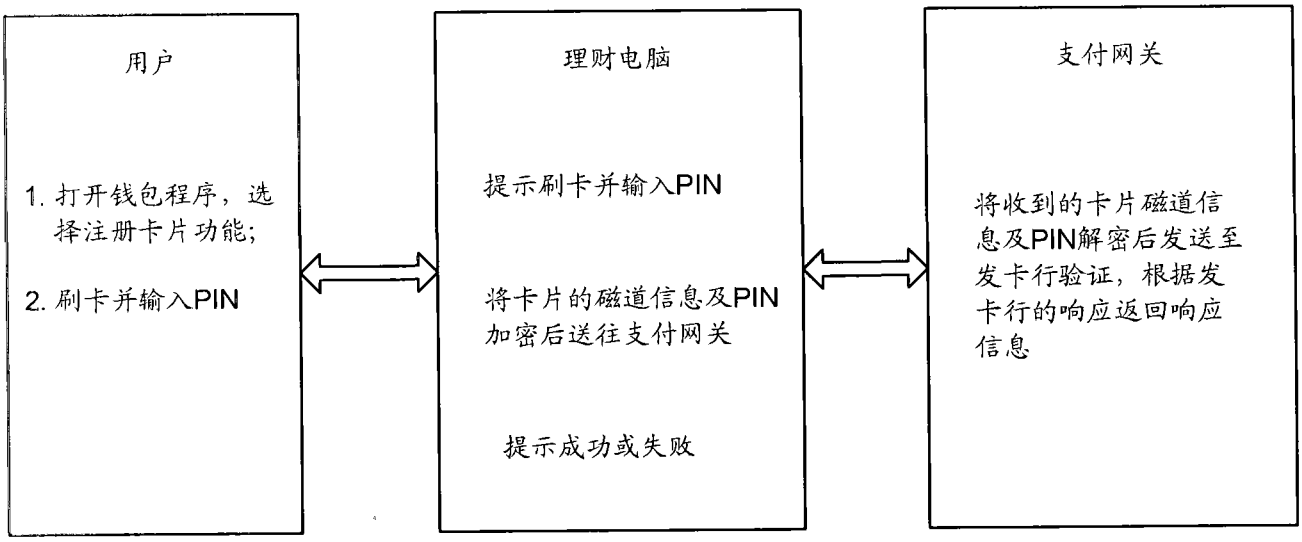

用户
1. 打开钱包程序，选择注册卡片功能;
2. 刷卡并输入PIN
理财电脑
提示刷卡并输入PIN
将卡片的磁道信息及PIN加密后送往支付网关
提示成功或失败
支付网关
将收到的卡片磁道信息及PIN解密后发送至发卡行验证，根据发卡行的响应返回响应信息

图 10

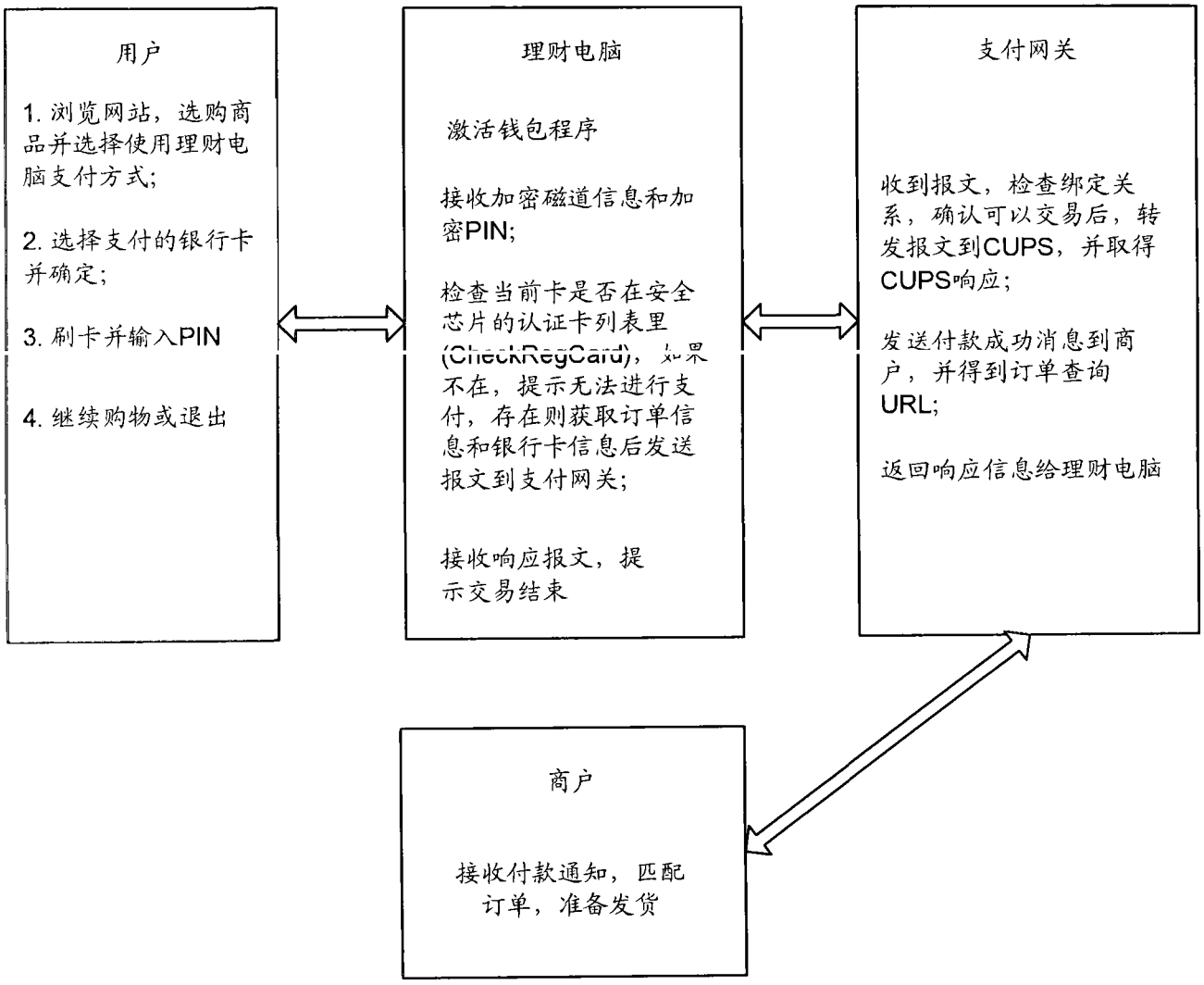

用户
1. 浏览网站，选购商品并选择使用理财电脑支付方式;
2. 选择支付的银行卡并确定;
3. 刷卡并输入PIN
4. 继续购物或退出
理财电脑
激活钱包程序
接收加密磁道信息和加密PIN;
检查当前卡是否在安全芯片的认证卡列表里(CheckRegCard)，如果不在，提示无法进行支付，存在则获取订单信息和银行卡信息后发送报文到支付网关;
接收响应报文，提示交易结束
支付网关
收到报文，检查绑定关系，确认可以交易后，转发报文到CUPS，并取得CUPS响应;
发送付款成功消息到商户，并得到订单查询URL;
返回响应信息给理财电脑
商户
接收付款通知，匹配订单，准备发货

图 11

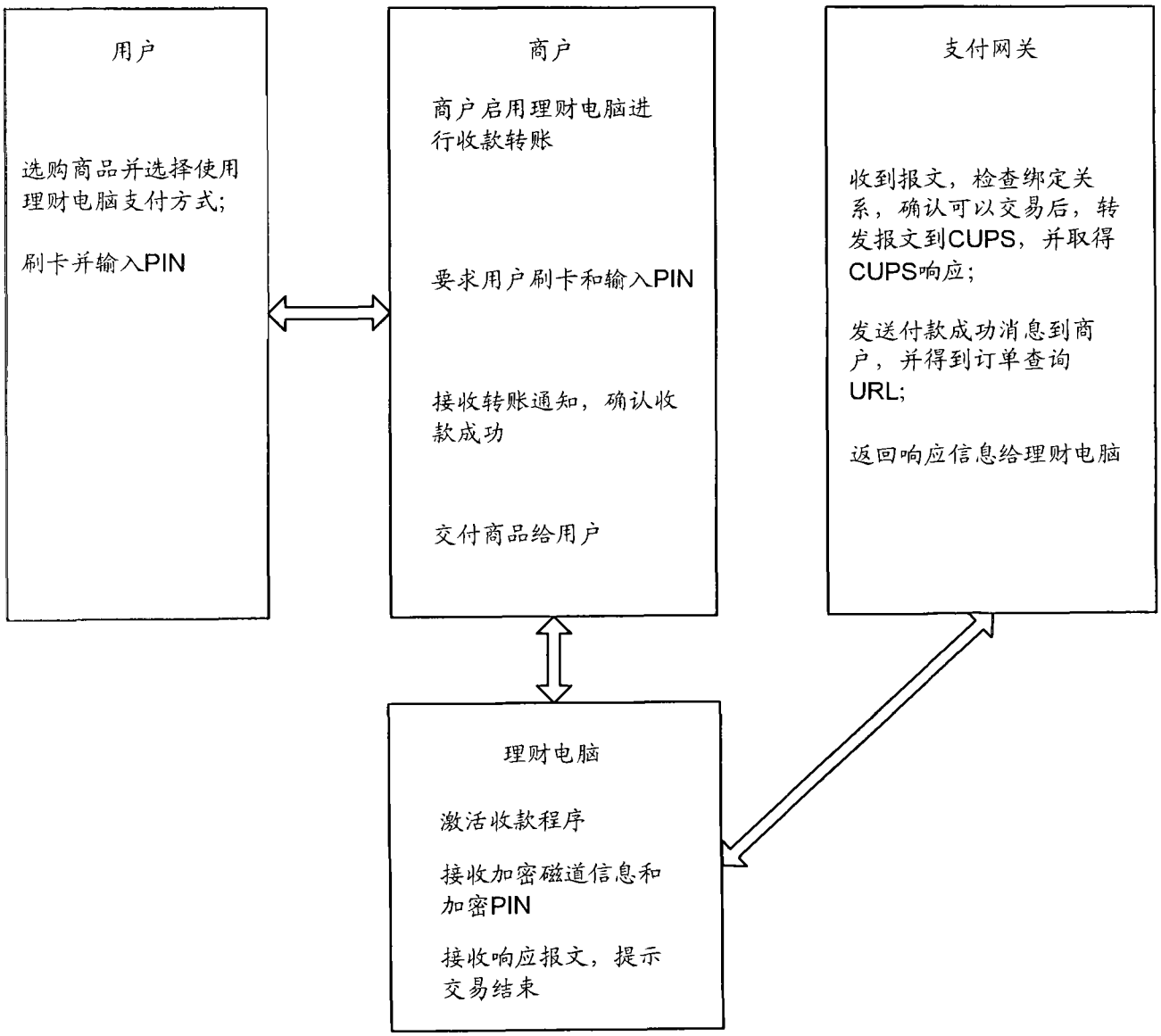

用户
选购商品并选择使用理财电脑支付方式;
刷卡并输入PIN
商户
商户启用理财电脑进行收款转账
要求用户刷卡和输入PIN
接收转账通知，确认收款成功
交付商品给用户
支付网关
收到报文，检查绑定关系，确认可以交易后，转发报文到CUPS，并取得CUPS响应;
发送付款成功消息到商户，并得到订单查询URL;
返回响应信息给理财电脑
理财电脑
激活收款程序
接收加密磁道信息和加密PIN
接收响应报文，提示交易结束

图 12