(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102768744 B
(45)授权公告日 2016.03.16

(21)申请号 201210147405.9

(22)申请日 2012.05.11

(73)专利权人 福建联迪商用设备有限公司
地址 350003 福建省福州市软件大道 89 号
福州软件园一区 23 号楼

(72)发明人 彭波涛 苏龙

(74)专利代理机构 福州市鼓楼区博深专利代理事务所（普通合伙） 35214
代理人 林志峥

(51)Int.Cl.
H04L 9/32(2006.01)
G06Q 20/40(2012.01)

(56)对比文件
CN 102006275 A,2011.04.06,
WO 2007/135619 A2,2007.11.29,
CN 101394615 A,2009.03.25,

审查员 李腾

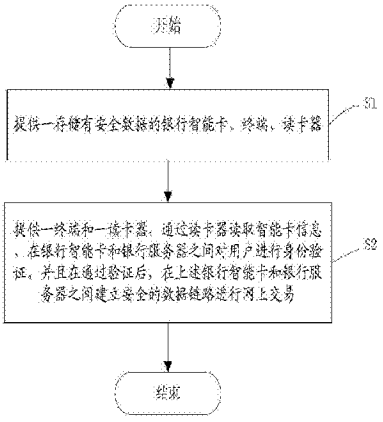
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种远程安全支付方法和系统

(57)摘要

本发明公开一种远程安全支付方法，包括以下步骤：提供一存储有安全数据的银行智能卡；提供一终端和一读卡器，通过读卡器读取智能卡信息，在银行智能卡和远程服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和远程服务器之间建立安全的数据链路进行网上交易。本发明为用户使用网上银行提供了一种安全防护措施。



CN 102768744 B

1. 一种远程安全支付方法，其特征在于，包括以下步骤：

提供一存储有安全数据的银行智能卡；所述安全数据包括数字证书和私人密钥；

提供一终端和一读卡器，通过读卡器读取智能卡信息，在银行智能卡和远程服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和远程服务器之间建立安全的数据链路进行网上交易；

所述身份验证包括以下步骤：所述终端读取银行智能卡的安全数据，所述远程服务器通过互联网向上述终端发起一个密钥协商过程，所述终端密钥协商成功后，返回成功信息给上述远程服务器，双方通过该密钥协商过程进行双向认证并产生一个过程密钥，该过程密钥在后续通信过程中作为所述远程服务器和所述终端交换数据的加密密钥，从而在所述服务器和该银行智能卡之间形成一个安全的数据传输链路；

其中，银行智能卡与远程服务器交互过程如下：

终端让银行智能卡产生 32 字节随机数，打包生成终端握手信息；

终端将终端握手信息传输到远程服务器；

远程服务器产生 32 字节随机数，打包生成服务器握手信息；

远程服务器将服务器握手信息和服务器证书发送到终端；

终端将远程服务器证书发送到银行智能卡，由银行智能卡对收到的远程服务器证书进行验证，如果验证通过，则登录成功；否则登录失败；

终端使用银行智能卡进行如下过程：

产生一个 48 字节的随机数作为共享主密钥；

该主密钥用远程服务器证书中的公钥进行加密，生成加密共享主密钥；

将终端握手信息和远程服务器握手信息算出握手信息哈希值，然后用终端私钥进行加密，生成握手信息数字签名；

终端从银行智能卡中获得加密共享主密钥、握手信息数字签名；

终端将终端证书、加密共享主密钥、握手信息数字签名发送到远程服务器；

远程服务器检查终端证书有效性，如果有效，则握手成功；否则握手失败；

远程服务器使用终端证书中的公钥验证握手信息数字签名是否与终端和服务端握手信息匹配，如果匹配，则握手成功；否则握手失败，返回错误；

远程服务器使用服务器私钥将进行解密共享主密钥，得出共享主密钥；

双方都使用共享主密钥算出会话密钥；后续通信过程，都使用会话密钥对数据包进行加密，即建立了安全通道，登录成功；

所述银行智能卡设有 ISO7816 接口，所述读卡器通过该接口读取卡内安全数据。

2. 根据权利要求 1 所述的一种远程安全支付方法，其特征在于，所述终端为手机，所述远程服务器为银行的网银服务器。

3. 根据权利要求 1 所述的一种远程安全支付方法，其特征在于，所述终端为 PAD，所述远程服务器为银行的网银服务器。

4. 根据权利要求 1 所述的一种远程安全支付方法，其特征在于，所述终端为 POS 机，所述远程服务器为 POS 服务器。

5. 根据权利要求 1 所述的一种远程安全支付方法，其特征在于，所述终端为手机，所述远程服务器为网上银行服务器，所述手机通过计算机与所述网上银行服务器通信。

6. 根据权利要求 1 所述的一种远程安全支付方法，其特征在于，所述银行智能卡设有符合 ISO14443 标准的非接触式通信接口，所述读卡器通过该接口读取卡内安全数据。

7. 一种远程安全支付系统，其特征在于，包括：

银行智能卡，用以存储安全数据；所述安全数据包括数字证书和私人密钥；

读卡器，用以读取上述安全数据；

终端，安装有客户端软件，用以进行网上交易；

所述终端通过读卡器读取智能卡信息，在银行智能卡和远程服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和远程服务器之间建立安全的数据链路进行网上交易；

其中，银行智能卡与远程服务器交互过程如下：

终端让银行智能卡产生 32 字节随机数，打包生成终端握手信息；

终端将终端握手信息传输到远程服务器；

远程服务器产生 32 字节随机数，打包生成服务器握手信息；

远程服务器将服务器握手信息和服务器证书发送到终端；

终端将远程服务器证书发送到银行智能卡，由银行智能卡对收到的远程服务器证书进行验证，如果验证通过，则登录成功；否则登录失败；

终端使用银行智能卡进行如下过程：

产生一个 48 字节的随机数作为共享主密钥；

该主密钥用远程服务器证书中的公钥进行加密，生成加密共享主密钥；

将终端握手信息和远程服务器握手信息算出握手信息哈希值，然后用终端私钥进行加密，生成握手信息数字签名；

终端从银行智能卡中获得加密共享主密钥、握手信息数字签名；

终端将终端证书、加密共享主密钥、握手信息数字签名发送到远程服务器；

远程服务器检查终端证书有效性，如果有效，则握手成功；否则握手失败；

远程服务器使用终端证书中的公钥验证握手信息数字签名是否与终端和服务端握手信息匹配，如果匹配，则握手成功；否则握手失败，返回错误；

远程服务器使用服务器私钥将进行解密共享主密钥，得出共享主密钥；

双方都使用共享主密钥算出会话密钥；后续通信过程，都使用会话密钥对数据包进行加密，即建立了安全通道，登录成功；

所述银行智能卡设有 ISO7816 接口，所述读卡器通过该接口读取卡内安全数据。

8. 根据权利要求 7 所述的一种远程安全支付系统，其特征在于，所述终端为手机，所述远程服务器为银行的网银服务器。

9. 根据权利要求 7 所述的一种远程安全支付系统，其特征在于，所述终端为 POS 机，所述远程服务器为 POS 服务器。

10. 根据权利要求 7 所述的一种远程安全支付系统，其特征在于，所述终端为手机，所述远程服务器为网上银行服务器，所述手机通过计算机与所述网 上银行服务器通信。

11. 根据权利要求 7 所述的一种远程安全支付系统，其特征在于，所述银行智能卡设有符合 ISO14443 标准的非接触式通信接口，所述读卡器通过该接口读取卡内安全数据。

一种远程安全支付方法和系统

技术领域

[0001] 本发明涉及电子支付领域，尤其是一种远程安全支付方法和系统。

背景技术

[0002] 随着电子商务的发展，网上交易已经越来越普及。此外，随着智能手机的价格下降，其销量也与日俱增。这就使得通过手机进行网上支付的需求日益明显，各大银行也推出了各自的手机银行。目前，常见的基于手机的移动支付方式有：

[0003] 方式 1：通过本地文件证书，对远程支付提供安全认证。

[0004] 方式 2：通过短信码，对远程支付提供安全认证。

[0005] 方式 3：对于部分提供 USB-OTG 接口的手机，已经有特定的 U-key 可用。通过这种 U-key 来保证远程支付的安全。

[0006] 上述方式的缺点：

[0007] 方式 1 和方式 2 的缺点：由于智能手机可能受病毒和黑客入侵，方式 1 和方式 2 中的文件证书或短信码可能被恶意软件获取，从而危及网络交易安全

[0008] 方式 3 缺点：银行需要专门发行 U-key，这种 U-key 常常只用于一个银行的网上交易。这提高了银行的运营成本，也使得用户除了银行卡外，还需要携带多种 U-key，在使用上很不方便。

发明内容

[0009] 为解决上述问题，本发明为用户使用网上银行提供了一种安全防护措施。

[0010] 本发明采用的具体技术手段如下：一种远程安全支付方法，其特征在于，包括以下步骤：

[0011] 提供一存储有安全数据的银行智能卡；

[0012] 提供一终端和一读卡器，通过读卡器读取智能卡信息，在银行智能卡和远程服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和远程服务器之间建立安全的数据链路进行网上交易。

[0013] 特别地，所述身份验证包括以下步骤：所述终端读取银行智能卡的安全数据，所述远程服务器通过互联网向上述终端发起一个密钥协商过程，所述终端密钥协商成功后，返回成功信息给上述远程服务器，双方通过该密钥协商过程进行双向认证并产生一个过程密钥，该过程密钥在后续通信过程中作为所述远程服务器和所述终端交换数据的加密密钥，从而在所述服务器和该银行智能卡之间形成一个安全的数据传输链路。

[0014] 特别地，所述终端为手机，所述远程服务器为手机银行服务器。

[0015] 特别地，所述终端为 POS 机，所述远程服务器为 POS 服务器。

[0016] 特别地，所述终端为手机，所述远程服务器为网上银行服务器，所述手机通过计算机与所述网上银行服务器通信。

[0017] 特别地，所述银行智能卡设有 ISO7816 接口，所述读卡器通过该接口读取卡内安

全数据。

[0018] 特别地，所述银行智能卡设有符合 ISO14443 标准的非接触式通信接口，所述读卡器通过该接口读取卡内安全数据。

[0019] 特别地，所述安全数据包括数字证书和私人密钥。

[0020] 本发明还一种远程安全支付系统，其特征在于，包括：

[0021] 银行智能卡，用以存储安全数据；

[0022] 读卡器，用以读取上述安全数据；

[0023] 终端，安装有客户端软件，用以进行网上交易；

[0024] 所述终端通过读卡器读取智能卡信息，在银行智能卡和远程服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和远程服务器之间建立安全的数据链路进行网上交易。

[0025] 特别地，所述终端为手机，所述远程服务器为银行的网银服务器。

[0026] 特别地，所述终端为 POS 机，所述远程服务器为 POS 服务器。

[0027] 特别地，所述终端为手机，所述远程服务器为网上银行服务器，所述手机通过计算机与所述网上银行服务器通信。

[0028] 特别地，所述银行智能卡设有 ISO7816 接口，所述读卡器通过该接口读取卡内安全数据。

[0029] 特别地，所述银行智能卡设有符合 ISO14443 标准的非接触式通信接口，所述读卡器通过该接口读取卡内安全数据。

[0030] 特别地，所述安全数据包括数字证书和私人密钥。

[0031] 本发明有益效果：

[0032] 本发明在现有金融 IC 卡基础上，增加数字证书的存储和软件接口，用以对用户身份进行验证，保证用户网上交易的安全，可以实现现有 U 盾的功能，且 IC 卡处理芯片体积小，且使用广泛存在的 ISO7816 接口，从而本发明为用户使用网上银行提供了一种安全防护措施。

附图说明

[0033] 图 1 为本发明实施例的银行智能卡的结构图；

[0034] 图 2 为本发明实施例的一种远程安全支付方法流程图；

[0035] 图 3 为本发明实施例的远程安全支付系统结构图；

[0036] 图 4 为本发明智能卡、网银客户端、服务器之间身份验证交互图。

具体实施方式

[0037] 为详细说明本发明的技术内容、构造特征、所实现目的及效果，以下结合实施方式并配合附图详予说明。

[0038] 请参阅图 1，为本发明实施例的银行智能卡的结构图。该银行智能卡是在银行向客户发行的金融卡 IC 卡基础上，增加安全模块，在安全模块中存储有客户数字证书和私人密钥的存储和软件接口，数字证书和私人密钥统称为安全数据，且具备逻辑加密运算功能，可替代 USB KEY 实现用户身份认证的功能。IC 卡片体积小巧，且各银行均会发行相应 IC 卡。

在本实施例中，银行 IC 卡具有 ISO7816 接口，读卡器可以通过 ISO7816 接口读取卡内安全数据，也可以通过无线方式，比如符合 ISO14443 标准的非接触式通信接口，读取卡内信息。

[0039] 请参考图 2，为本发明实施例的一种远程安全支付方法流程图。其中安全支付方法包括以下步骤：

[0040] S1. 提供一存储有安全数据的银行智能卡；

[0041] S2. 提供一终端和一读卡器，通过读卡器读取智能卡信息，在银行智能卡和远程服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和远程服务器之间建立安全的数据链路进行网上交易。

[0042] 其中，身份验证包括以下步骤：所述终端读取银行智能卡的安全数据，所述远程服务器通过互联网向上述终端发起一个密钥协商过程，所述终端密钥协商成功后，返回成功信息给上述远程服务器，双方通过该密钥协商过程进行双向认证并产生一个过程密钥，该过程密钥在后续通信过程中作为所述远程服务器和所述终端交换数据的加密密钥，从而在所述服务器和该银行智能卡之间形成一个安全的数据传输链路。

[0043] 在本实施例中，终端包括移动终端，也包括非移动终端，包括个人终端，也包括商用终端。所述移动终端包括手机、PAD、移动 PC 等，其对应的远程服务器为银行的网银服务器；所述非移动终端可以使台式 PC，对应的服务器为网上银行，PC 通过读卡器读取卡内信息，登陆网上银行交易；所述商用终端可以使商用 POS 机，其对应的服务器是 POS 服务器。

[0044] 其中，所述银行智能卡设有 ISO7816 接口，当所述终端没有读卡功能，就可以通过读卡器通过该接口读取卡内安全数据。所述银行智能卡还可以设有射频卡近场通信接口，读卡器通过采用无线方式比如无线射频方式读取卡内信息。

[0045] 图 4 是本发明智能卡、网银客户端、服务器之间身份验证交互图。在此以常见的网上银行登录过程为例对该流程进行说明。终端安装有网银客户端，需要使用一张接触式智能卡对交易过程进行保护。该智能卡相当于 U-key 的作用，里面存放网上银行用于识别客户身份的数字证书和私人密钥，卡片内部的处理器可以完成加密和数字签名算法。

[0046] 在登录过程中，主要是智能卡与系统服务器（远端系统）之间进行交互。客户端软件通过终端、读卡器与智能卡进行交互，发送服务器命令并从智能卡接收响应，从而完成登录过程。

[0047] 为了进行交互，智能卡和系统服务器各存有一个数字证书和对应私钥。智能卡上的证书和私钥分别称为客户端证书和客户端私钥，服务器上证书和私钥分别称为服务器证书和服务器私钥。此外，智能卡和服务器都有这些证书对应的根证书。

[0048] 智能卡和远程服务器交互过程如下：

[0049] 1. 客户端让智能卡产生 32 字节随机数，加上一些信息打包生成客户端握手信息，这里客户端是相对于服务器的一种叫法，是将客户端软件、终端、智能卡、证书等等一些列组件当做一个整体来看待的。从服务器的角度来看，与服务器交互的对象就是客户端；

[0050] 2. 客户端将客户端握手信息传输到服务器；

[0051] 3. 服务器产生 32 字节随机数，加上一些信息打包，生成服务器握手信息；

[0052] 4. 服务器将服务器握手信息和服务器证书发送到客户端；

[0053] 5. 客户端将服务器证书发送到智能卡，由智能卡对收到的服务器证书进行验证，如果验证通过，则登录成功；否则登录失败；

[0054] 6. 客户端使用智能卡进行如下过程：

[0055] 产生一个 48 字节的随机数作为共享主密钥

[0056] 该主密钥用服务器证书中的公钥进行加密，生成加密共享主密钥

[0057] 将客户端握手信息和服务端握手信息算出握手信息哈希值，然后用客户端私钥进行加密，生成握手信息数字签名；

[0058] 7. 客户端从智能卡中获得加密共享主密钥、握手信息数字签名；

[0059] 8. 客户端将客户端证书、加密共享主密钥、握手信息数字签名发送到服务器；

[0060] 9. 服务器检查客户端证书有效性，如果有效，则握手成功；否则握手失败；

[0061] 10. 服务器使用客户端证书中的公钥验证握手信息数字签名是否与客户端和服务端握手信息匹配，如果匹配，则握手成功；否则握手失败，返回错误；

[0062] 11. 服务器使用服务器私钥将进行解密共享主密钥，得出共享主密钥；

[0063] 12. 双方都使用共享主密钥算出会话密钥。后续通信过程，都使用会话密钥对数据包进行加密，即建立了安全通道，登录成功。

[0064] 请参考图 3，为本发明实施例的安全支付系统结构图。安全支付系统包括：银行智能卡，用以存储安全数据；读卡器，用以读取上述安全数据；终端，安装有客户端软件，用以进行网上交易；所述终端通过读卡器读取智能卡信息，在银行智能卡和远程服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和远程服务器之间建立安全的数据链路进行网上交易。其中，安全数据包括数字证书和私人密钥。在本实施例中，以 PC 和网上银行服务器为例，所述网上银行服务器通过互联网向上述 PC 端发起一个密钥协商过程，该 PC 端密钥协商成功后，返回成功信息给上述网上银行服务器，双方通过该密钥协商过程进行双向认证并产生一个过程密钥，该过程密钥在后续通信过程中作为该网上银行服务器和所述终端交换数据的加密密钥，从而在该网上银行服务器和该智能卡之间形成一个安全的数据传输链路，后续的交易数据在此链路上进行传输。

[0065] 本发明在现有金融 IC 卡基础上，增加数字证书的存储和软件接口，用以对用户身份进行验证，保证用户网上交易的安全，可以实现现有 U 盾的功能，且 IC 卡处理芯片体积小，且使用广泛存在的 ISO7816 接口，成本低廉，加工技术成熟，从而为用户使用网上银行提供了一种安全、低成本的防护措施。

[0066] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

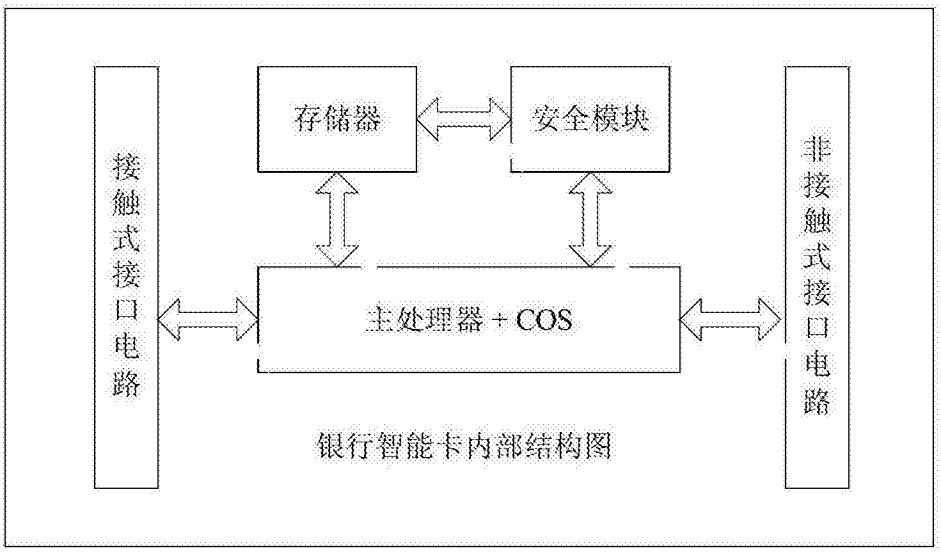

存储器
安全模块
接触式接口电路
主处理器 + COS
非接触式接口电路
银行智能卡内部结构图

图 1

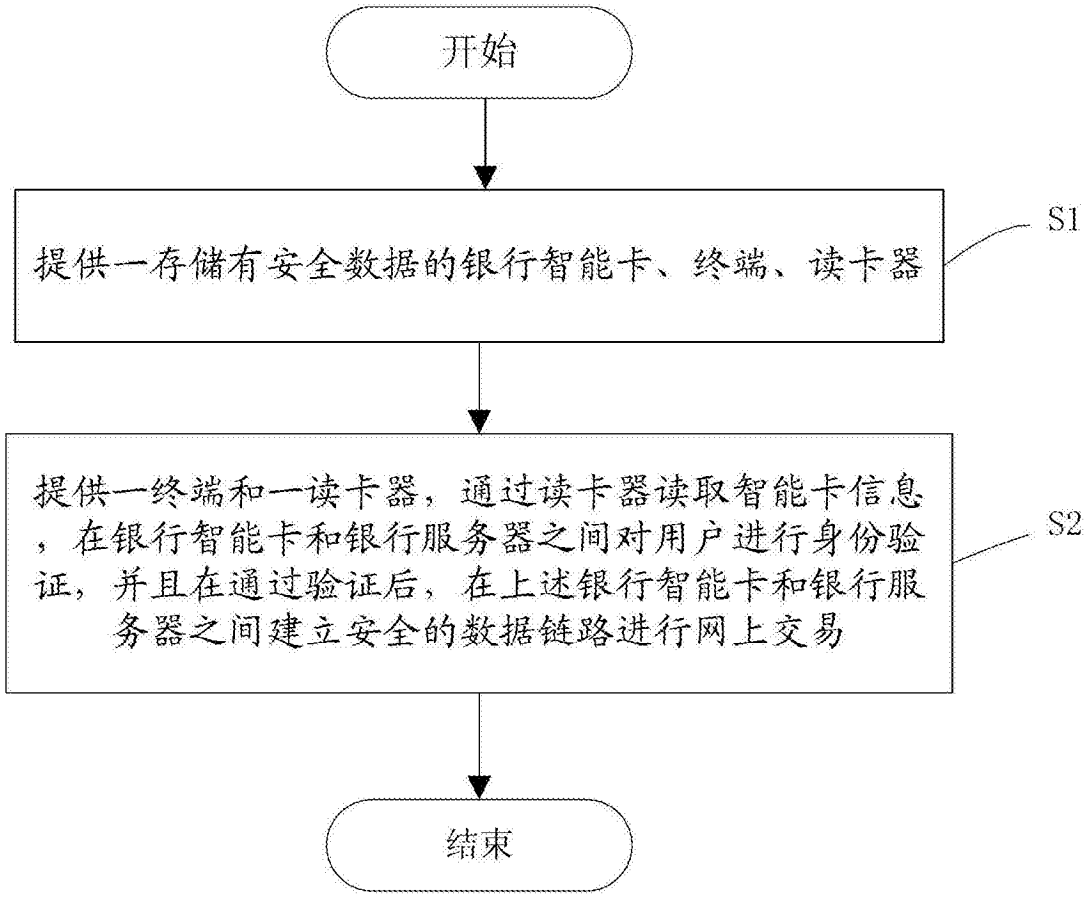

开始
提供一存储有安全数据的银行智能卡、终端、读卡器
S1
提供一终端和一读卡器，通过读卡器读取智能卡信息，在银行智能卡和银行服务器之间对用户进行身份验证，并且在通过验证后，在上述银行智能卡和银行服务器之间建立安全的数据链路进行网上交易
S2
结束

图 2

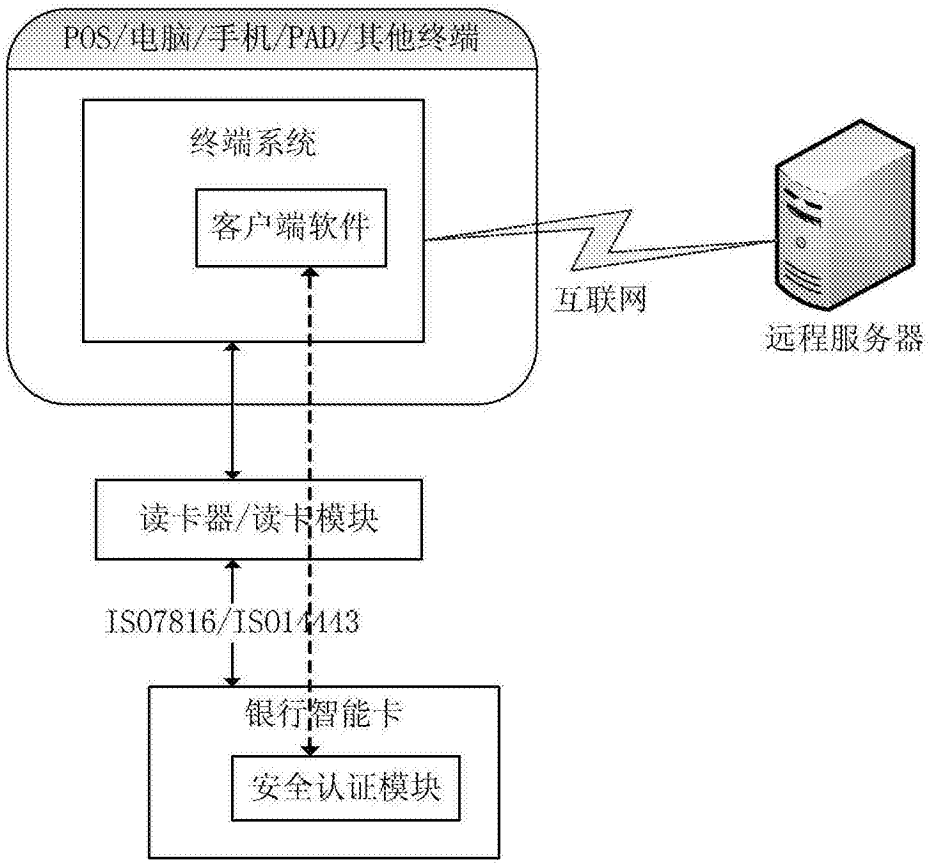

POS/电脑/手机/PAD/其他终端
终端系统
客户端软件
互联网
远程服务器
读卡器/读卡模块
IS07816/IS014443
银行智能卡
安全认证模块

图 3

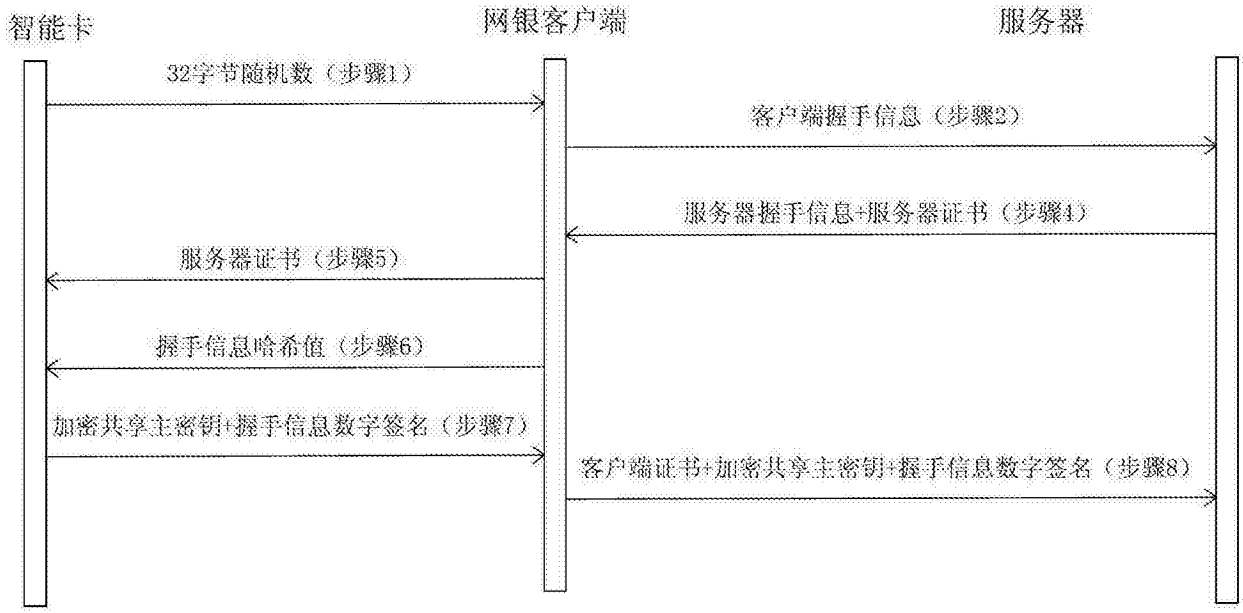

智能卡
网银客户端
服务器
32字节随机数（步骤1）
客户端握手信息（步骤2）
服务器握手信息+服务器证书（步骤4）
服务器证书（步骤5）
握手信息哈希值（步骤6）
加密共享主密钥+握手信息数字签名（步骤7）
客户端证书+加密共享主密钥+握手信息数字签名（步骤8）

图 4