(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104835038 A
(43)申请公布日 2015.08.12

(21)申请号 201510144962.9

(22)申请日 2015.03.30

(71)申请人 恒宝股份有限公司
地址 212355 江苏省镇江市丹阳市横塘工业区

(72)发明人 罗广文 许荣均

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 杨立

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/34(2012.01)
G06Q 20/40(2012.01)

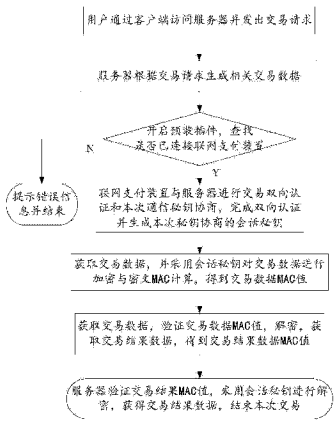
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种联网支付装置及方法

(57)摘要

本发明涉及一种联网支付装置及方法，其方法包括：步骤1：用户通过客户端访问服务器并发出交易请求；步骤2：根据交易请求生成相关交易数据；步骤3：开启预装插件，查找是否已连接联网支付装置，如果是，建立链接，执行步骤4；否则，提示错误信息并结束；步骤4：进行交易双向认证，完成双向认证并生成本次通信的会话秘钥；步骤5：获取交易数据，并采用会话秘钥对交易数据进行加密与密文MAC计算，得到交易数据密文与MAC值；步骤6：验证交易数据MAC值，解密并处理，获取交易结果数据，得到交易结果数据密文与MAC值；步骤7：获得交易结果数据，结束本次交易。本发明支持一对多应用场景，大大节约持卡人、金融机构、行业的成本。



CN 104835038 A

1.一种联网支付方法，其特征在于，具体包括以下步骤：

步骤1：用户通过客户端访问服务器并输入交易请求；

步骤2：服务器根据交易请求生成相关交易数据；

步骤3：客户端接收相关交易数据，开启预装插件，查找是否已连接联网支付装置，如果是，联网支付装置与服务器建立链接，执行步骤4；否则，提示错误信息并结束；

步骤4：联网支付装置与服务器进行交易双向认证和本次通信秘钥协商，完成双向认证并生成本次通信的会话秘钥；

步骤5：服务器获取交易数据，并采用会话秘钥对交易数据进行加密与密文MAC计算，得到交易数据MAC值；

步骤6：联网支付装置获取交易数据，验证交易数据MAC值，并采用会话秘钥进行解密，根据解密结果得到的数据进行交易，获取交易结果数据，并将交易结果数据采用会话秘钥进行加密与密文MAC计算，得到交易结果数据MAC值；

步骤7：服务器验证交易结果数据MAC值，采用会话秘钥进行解密，获得交易结果数据，结束本次交易。

2.根据权利要求1所述的一种联网支付方法，其特征在于，所述步骤4具体包括以下步骤：

步骤4.1：服务器接收客户端反馈的提示信息，发送获取随机数指令，联网支付装置返回随机数与算法标识；

步骤4.2：服务器发送服务器证书、服务器算法标识和服务器随机数RS；

步骤4.3：联网支付装置根据预制的根证书验证收到的服务器证书的合法性，如合法，执行步骤4.4；否则，发送出错消息，结束；

步骤4.4：联网支付装置产生新随机数作为共享主密钥，采用服务器证书中的公钥对共享主密钥进行加密，得到加密数据；

步骤4.5：服务器收到加密数据进行私钥运算，得到加密数据明文，读取得到的联网支付装置的支付装置证书和签名数据；

步骤4.6：使用根证书验证联网支付装置的合法性，判断验证是否通过，如果是，执行步骤4.7；否则，发送出错消息，结束；

步骤4.7：服务器对服务器证书、支付装置证书进行运算生成秘钥协商完成信息；

步骤4.8：联网支付装置对接收到的秘钥协商完成信息进行验证，如通过验证，联网支付装置将秘钥协商完成信息进行转换为新秘钥协商完成信息，执行步骤4.9；否则，返回错误的状态码，结束链接；

步骤4.9：服务器接收到新秘钥协商完成信息，进行验证，判断验证是否通过；如通过，完成双向验证，计算获得会话秘钥和MAC秘钥，执行步骤5；否则，结束链接。

3.根据权利要求2所述的一种联网支付方法，其特征在于，所述步骤4.7具体包括以下步骤：

步骤4.7.1：对服务器证书进行摘要运算得到服务器证书摘要，对支付装置证书进行摘要运算得到支付装置摘要；

步骤4.7.2：将支付装置随机数、服务器随机数、服务器证书摘要、支付装置摘要、支付装置签名数据和加密数据连接得到连接数据，连接数据＝（支付装置随机数 ‖ 服务器随机

数 ‖ 服务器证书摘要 ‖ 支付装置摘要 ‖ 支付装置签名数据 ‖ 加密数据）；

步骤 4.7.3：对连接数据进行摘要运算得到连接摘要，将 ASCII 码“SERVER”和连接摘要连接后得到新连接数据，对新连接数据进行 HMAC 运算得到秘钥协商完成信息。

4. 根据权利要求 3 所述的一种联网支付方法，其特征在于，所述步骤 4.8 采用与步骤 4.7 中相同的算法进行验证。

5. 根据权利要求 4 所述的一种联网支付方法，其特征在于，所述步骤 4.8 中如验证通过，联网支付装置对秘钥协商完成信息转换得到新秘钥协商完成信息的过程采用的转换方法为，将 ASCII 码”SERVER”改为“CLIENT”。

6. 一种联网支付装置，其特征在于，包括输入模块、指令处理模块、判断模块、主控制模块、计算模块、加解密交易模块和交易结束模块；

所述输入模块用于用户通过客户端访问服务器并输入交易请求；

所述指令处理模块用于控制服务器根据交易请求生成及处理相关交易数据；

所述判断模块用于控制客户端接收相关交易数据，开启预装插件，查找是否已连接联网支付装置，如果是，联网支付装置与服务器建立链接；否则，提示错误信息并结束；

所述主控制模块用于控制联网支付装置与服务器进行交易双向认证和本次通信秘钥协商，完成双向认证并协商本次通信的会话秘钥；

所述加解密交易模块用于控制客户端获取交易数据，验证交易数据 MAC 值，并采用会话秘钥进行解密，根据解密结果得到的数据进行交易，获取交易结果数据，并将交易结果数据采用会话秘钥进行加密与密文 MAC 计算，得到交易结果数据 MAC 值；

所述交易结束模块用于控制服务器验证交易结果数据 MAC 值，采用会话秘钥进行解密，获得交易结果数据，结束本次交易。

7. 根据权利要求 6 所述的一种联网支付装置，其特征在于，所述一种联网支付装置还包括信息显示模块，所述信息显示模块用于显示操作过程及操作结果。

8. 根据权利要求 6 所述的一种联网支付装置，其特征在于，所述一种联网支付装置还包括提示模块，所述提示模块用于根据判断模块的控制发出提示或告警。

9. 根据权利要求 6-8 任一项所述的一种联网支付装置，其特征在于，所述一种联网支付装置还包括包括接触式读写卡模块和 / 或非接触式读写卡模块；

所述接触式读写卡模块用于通过接触的方式获取 IC 卡信息，并将获取的信息传输到主控制模块；

所述非接触式读写卡模块用于通过非接触的方式获取 IC 卡信息，并将获取的信息传输到主控制模块。

一种联网支付装置及方法

技术领域

[0001] 本发明涉及一种联网支付装置及方法。

背景技术

[0002] 目前互联网金融活动快速发展，磁条式卡片的安全性已经无法满足其安全性要求。金融 IC 卡片内部由其全安芯片组成从而可提升金融活动安全级别，所以近年各类银行机构快速推行金融 IC 卡替换原有磁条卡；由于目前网络上的交易活动大多数以无卡进行，带来较多便利，但其安全问题也随之增多，虽然各银行发行的Usb Key可以解决某方面安全问题，但各银行实施方案不尽相同，导致用户一卡一 Key 现象，这样不但增加银行的成本问题，也使用户随身携带带来一定的影响；POS 成本高，不易申请等诸多因素。

发明内容

[0003] 本发明所要解决的技术问题是提供一种解决联网支付需办理相关业务或无卡支付存在安全风险等问题，利用金融 IC 卡的参与，达到有卡交易从而保证用卡相对安全的，便携且成本低的联网支付装置及方法。由于该装置具有认证、签名、加解密运算等功能，从而可以使用不同的金融 IC 卡均可在该设备上进行金融交易。

[0004] 本发明解决上述技术问题的技术方案如下：一种联网支付方法，具体包括以下步骤：

[0005] 步骤 1：用户通过客户端访问服务器并输入交易请求；

[0006] 步骤 2：服务器根据交易请求生成相关交易数据；

[0007] 步骤 3：客户端接收相关交易数据，开启预装插件，查找是否已连接联网支付装置，如果是，联网支付装置与服务器建立链接，执行步骤 4；否则，提示错误信息并结束；

[0008] 步骤 4：联网支付装置与服务器进行交易双向认证和本次通信秘钥协商，完成双向认证并生成本次通信的会话秘钥；

[0009] 步骤 5：服务器获取交易数据，并采用会话秘钥对交易数据进行加密与密文 MAC 计算，得到交易数据 MAC 值；

[0010] 步骤 6：联网支付装置获取交易数据，验证交易数据 MAC 值，并采用会话秘钥进行解密，根据解密结果得到的数据进行交易，获取交易结果数据，并将交易结果数据采用会话秘钥进行加密与密文 MAC 计算，得到交易结果数据 MAC 值；

[0011] 步骤 7：服务器验证交易结果数据 MAC 值，采用会话秘钥进行解密，获得交易结果数据，结束本次交易。

[0012] 本发明的有益效果是：由于 IC 具有动态数据加解密与不可伪造等特性，因此本发明针对该特性采用该方法比较现在网络支付具有以下特点：在整个网络支付交易中，需要持卡人持卡参与，在网络实现与现实中相同的有卡支付，从而使安全级别更进一步提高；由于本发明内置数据加解密与认证特征，从而保证了交易双方不可抵赖性以及交易数据保密性；所述发明可以扩展多应用，不仅应用于联网金融支付交易，而且还可用于行业应用；本

发明支持一对多应用场景，大大节约持卡人、金融机构、行业的成本。

[0013] 在上述技术方案的基础上，本发明还可以做如下改进。

[0014] 进一步，所述步骤 4 具体包括以下步骤：

[0015] 步骤 4.1：服务器接收客户端反馈的提示信息，发送获取随机数指令，联网支付装置返回随机数与算法标识；

[0016] 步骤 4.2：服务器发送服务器证书、服务器算法标识和服务器随机数 RS；

[0017] 步骤 4.3：联网支付装置根据预制的根证书验证收到的服务器证书的合法性，如合法，执行步骤 4.4；否则，发送出错消息，结束；

[0018] 步骤 4.4：联网支付装置产生新随机数作为共享主密钥，采用服务器证书中的公钥对共享主密钥进行加密，得到加密数据；

[0019] 步骤 4.5：服务器收到加密数据进行私钥运算，得到加密数据明文，读取得到的联网支付装置的支付装置证书和签名数据；

[0020] 步骤 4.6：使用根证书验证联网支付装置的合法性，判断验证是否通过，如果是，执行步骤 4.7；否则，发送出错消息，结束；

[0021] 步骤 4.7：服务器对服务器证书、支付装置证书进行运算生成秘钥协商完成信息；

[0022] 步骤 4.8：联网支付装置对接收到的秘钥协商完成信息进行验证，如通过验证，联网支付装置将秘钥协商完成信息进行转换为新秘钥协商完成信息，执行步骤 4.9；否则，返回错误的状态码，结束链接；

[0023] 步骤 4.9：服务器接收到新秘钥协商完成信息，进行验证，判断验证是否通过；如通过，完成双向验证，计算获得会话秘钥和 MAC 秘钥，执行步骤 5；否则，结束链接。

[0024] 进一步，所述步骤 4.7 具体包括以下步骤：

[0025] 步骤 4.7.1：对服务器证书进行摘要运算得到证书摘要，对支付装置证书进行摘要运算得到支付装置证书摘要；

[0026] 步骤 4.7.2：将支付装置随机数、服务器随机数、服务器证书摘要、支付装置摘要、支付装置签名数据和加密数据连接得到连接数据，连接数据＝（支付装置随机数 ‖ 服务器随机数 ‖ 服务器证书摘要 ‖ 支付装置证书摘要 ‖ 支付装置签名数据 ‖ 加密数据）；

[0027] 步骤 4.7.3：对连接数据进行摘要运算得到连接摘要，将 ASCI I 码“SERVER”和连接摘要连接后得到新连接数据，对新连接数据进行 HMAC 运算得到秘钥协商完成信息。

[0028] 进一步，所述步骤 4.8 采用与步骤 4.7 中相同的算法进行验证。

[0029] 进一步，所述步骤 4.8 中如验证通过，联网支付装置对秘钥协商完成信息转换得到新秘钥协商完成信息的过程采用的转换方法为，将 ASCI I 码”SERVER”改为“CLIENT”。

[0030] 本发明解决上述技术问题的技术方案如下：一种联网支付装置，包括输入模块、指令处理模块、判断模块、主控制模块、计算模块、加解密交易模块和交易结束模块；

[0031] 所述输入模块用于用户通过客户端访问服务器并输入交易相关信息（如：交易密码等）；

[0032] 所述指令处理模块用于控制服务器根据交易请求生成及处理相关交易数据；

[0033] 所述判断模块用于控制客户端接收相关交易数据，开启预装插件，查找是否已连接联网支付装置，如果是，联网支付装置与服务器建立链接；否则，提示错误信息并结束；

[0034] 所述主控制模块用于控制联网支付装置与服务器进行交易双向认证和本次通信

秘钥协商，完成双向认证并协商本次通信的会话秘钥；

[0035] 所述加解密交易模块用于控制客户端获取交易数据，验证交易数据 MAC 值，并采用会话秘钥进行解密，根据解密结果得到的数据进行交易，获取交易结果数据，并将交易结果数据采用会话秘钥进行加密与密文 MAC 计算，得到交易结果数据 MAC 值；

[0036] 所述交易结束模块用于控制服务器验证交易结果数据 MAC 值，采用会话秘钥进行解密，获得交易结果数据，结束本次交易。

[0037] 本发明的有益效果是：由于 IC 具有动态数据加解密与不可伪造等特性，因此本发明针对该特性采用该方法比较现在网络支付具有以下特点：在整个网络支付交易中，需要持卡人持卡参与，在网络实现与现实中相同的有卡支付，从而使安全级别更进一步提高；由于所述发明内置数据加解密与认证特征，从而保证了交易双方不可抵赖性以及交易数据保密性；所述发明可以扩展多应用，不仅应用于联网金融支付交易，而且还可用于行业应用；所述发明支持一对多应用场景，大大节约持卡人、金融机构、行业的成本。

[0038] 在上述技术方案的基础上，本发明还可以做如下改进。

[0039] 进一步，所述一种联网支付装置还包括信息显示模块，所述信息显示模块用于显示操作过程及操作结果。

[0040] 进一步，所述一种联网支付装置还包括提示模块，所述提示模块用于根据判断模块的控制发出提示或告警。

[0041] 进一步，所述一种联网支付装置还包括包括接触式读写卡模块和 / 或非接触式读写卡模块；

[0042] 所述接触式读写卡模块用于通过接触的方式获取 IC 卡信息，并将获取的信息传输到主控制模块；

[0043] 所述非接触式读写卡模块用于通过非接触的方式获取 IC 卡信息，并将获取的信息传输到主控制模块。

附图说明

[0044] 图 1 为本发明所述的一种联网支付方法流程图；

[0045] 图 2 为本发明所述的一种联网支付装置结构图；

[0046] 图 3 为本发明具体实施例所示的联网支付方法流程图。

[0047] 附图中，各标号所代表的部件列表如下：

[0048] 1、输入模块，2、指令处理模块，3、判断模块，4、主控制模块，5、计算模块，6、加解密交易模块，7、交易结束模块，8、信息显示模块，9、提示模块，10、接触式读写卡模块，11、非接触式读写卡模块。

具体实施方式

[0049] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0050] 如图 1 所示，为本发明所述的一种联网支付方法，具体包括以下步骤：

[0051] 步骤 1：用户通过客户端访问服务器并输入交易请求；

[0052] 步骤 2：服务器根据交易请求生成相关交易数据；

[0053] 步骤 3 :客户端接收相关交易数据,开启预装插件,查找是否已连接联网支付装置,如果是,联网支付装置与服务器建立链接,执行步骤 4 ;否则,提示错误信息并结束 ;

[0054] 步骤 4 :联网支付装置与服务器进行交易双向认证和本次通信秘钥协商,完成双向认证并协商本次通信的会话秘钥 ;

[0055] 步骤 5 :服务器获取交易数据,并采用会话秘钥对交易数据进行加密与密文 MAC 计算,得到交易数据 MAC 值 ;

[0056] 步骤 6 :联网支付装置获取交易数据,验证交易数据 MAC 值,并采用会话秘钥进行解密,根据解密结果得到的数据进行交易,获取交易结果数据,并将交易结果数据采用会话秘钥进行加密与密文 MAC 计算,得到交易结果数据 MAC 值 ;

[0057] 步骤 7 :服务器验证交易结果数据 MAC 值,采用会话秘钥进行解密,获得交易结果数据,结束本次交易。

[0058] 所述步骤 4 具体包括以下步骤 :

[0059] 步骤 4.1 :服务器接收客户端反馈的提示信息,发送获取随机数指令,联网支付装置返回支付装置随机数与算法标识 ;

[0060] 步骤 4.2 :服务器发送服务器证书、算法标识和以及随机数 RS ;

[0061] 步骤 4.3 :联网支付装置根据预制的根证书验证收到的服务器证书的合法性,如合法,执行步骤 4.4 ;否则,发送出错消息,结束 ;

[0062] 步骤 4.4 :联网支付装置产生新随机数作为共享主密钥 , 采用服务器证书中的公钥对共享主密钥进行加密,得到加密数据 ;

[0063] 步骤 4.5 :服务器收到加密数据进行私钥运算,得到加密数据明文,读取得到的联网支付装置的支付装置证书和证书签名数据 ;

[0064] 步骤 4.6 :服务器使用根证书验证联网支付装置的合法性,判断验证是否通过,如果是,执行步骤 4.7 ;否则,发送出错消息,结束 ;

[0065] 步骤 4.7 :服务器对服务器证书、支付装置证书进行运算生成秘钥协商完成信息 ;

[0066] 步骤 4.8 :联网支付装置对接收到的秘钥协商完成信息进行验证,如通过验证,联网支付装置将秘钥协商完成信息进行转换为新秘钥协商完成信息,执行步骤 4.9 ;否则,返回错误的状态码,结束链接 ;

[0067] 步骤 4.9 :服务器接收到新秘钥协商完成信息,进行验证,判断验证是否通过 ;如通过,完成双向验证,计算获得会话秘钥和 MAC 秘钥,执行步骤 5 ;否则,结束链接。

[0068] 所述步骤 4.7 具体包括以下步骤 :

[0069] 步骤 4.7.1 :对服务器证书进行摘要运算得到证书摘要,对支付装置证书进行摘要运算得到证书摘要 ;

[0070] 步骤 4.7.2 :将支付装置随机数、服务器随机数、服务器证书摘要、支付装置证书摘要、支付装置签名数据和加密数据连接得到连接数据,连接数据 = (支付装置随机数 ‖ 服务器随机数 ‖ 服务器证书摘要 ‖ 支付装置证书摘要 ‖ 支付装置签名数据 ‖ 加密数据) ;

[0071] 步骤 4.7.3 :对连接数据进行摘要运算得到连接摘要,将 ASC Ⅱ 码“SERVER”和连接摘要连接后得到新连接数据,对新连接数据进行 HMAC 运算得到秘钥协商完成信息。

[0072] 所述步骤 4.8 采用与步骤 4.7 中相同的算法进行验证。

[0073] 所述步骤 4.8 中如验证通过，联网支付装置对秘钥协商完成信息转换得到新秘钥协商完成信息的过程采用的转换方法为，将 ASCI I 码”SERVER”改为“CLIENT”。

[0074] 如图 2 所示，为本发明所述的一种联网支付装置，包括输入模块 1、指令处理模块 2、判断模块 3、主控制模块 4、计算模块 5、加解密交易模块 6 和交易结束模块 7；

[0075] 所述输入模块 1 用于用户通过客户端访问服务器并输入交易相关信息（如：交易密码等）；

[0076] 所述指令处理模块 2 用于控制服务器根据交易请求生成及处理相关交易数据；

[0077] 所述判断模块 3 用于控制客户端接收相关交易数据，开启预装插件，查找是否已连接联网支付装置，如果是，联网支付装置与服务器建立链接；否则，提示错误信息并结束；

[0078] 所述主控制模块 4 用于控制联网支付装置与服务器进行交易双向认证和本次通信秘钥协商，完成双向认证并协商本次通信的会话秘钥；

[0079] 所述加解密交易模块 6 用于控制客户端获取交易数据，验证交易数据 MAC 值，并采用会话秘钥进行解密，根据解密结果得到的数据进行交易，获取交易结果数据，并将交易结果数据采用会话秘钥进行加密与密文 MAC 计算，得到交易结果数据 MAC 值；

[0080] 所述交易结束模块 7 用于控制服务器验证交易结果数据 MAC 值，采用会话秘钥进行解密，获得交易结果数据，结束本次交易。

[0081] 所述一种联网支付装置还包括信息显示模块 8，所述信息显示模块 8 用于显示操作过程及操作结果。

[0082] 所述一种联网支付装置还包括提示模块 9，所述提示模块 9 用于根据判断模块的控制发出提示或告警。

[0083] 所述一种联网支付装置还包括包括接触式读写卡模块 10 和 / 或非接触式读写卡模块 11；

[0084] 所述接触式读写卡模块 10 用于通过接触的方式获取 IC 卡信息，并将获取的信息传输到主控制模块；

[0085] 所述非接触式读写卡模块 11 用于通过非接触的方式获取 IC 卡信息，并将获取的信息传输到主控制模块。

[0086] 实施案例：以实施案例来说明本发明方法的实现过程。

[0087] A. 用户通过联网访问交易网站服务器系统进行交易。

[0088] B. 提交相关交易数据，并转至相关的付款界面。

[0089] C. 用户客户端启动预安装的插件，并查找当前已连接的本发明设备。然后利用主芯片自带安全算法模块进行交易双向认证和本次通信密钥协商流程。

[0090] D. 以 TLV 格式进行交易数据的封装后采用上述协商完成的密钥进行加密与密文 MAC 计算操作，再发送给本发明设备。

[0091] E. 本发明设备收到数据，通过主芯片自带安全算法模块对通信数据的 MAC 验证以及解密操作，然后对解密后的明文进行指令二次分发处理。

[0092] F. 本发明设备首先通过非接式读写卡模块或接触式读写卡模块查询 IC 卡是否已插入，如未检测到 IC 卡片时，通过声音或显示方式提示用户插入或挥入 IC 卡并等待有限时间；如果已插入或挥入后，需通过声音或显示等提示用户输入交易必备的私密数据。

[0093] G. 本发明设备采用触控按键，当用户每按下按键时利用声音和马达震动进行按键反馈；同时采用 OLED 材质屏进行显示输入。

[0094] H. 当用户输入完交易的私密数据后，立即利用本发明设备中已预置的公钥证书的公钥通过主芯片的安全算法模块对其进行非对称运算得到密文后消毁该明文。然后通过非接触式或接触式读写卡模块读取 IC 卡应用数据。

[0095] I. 本发明设备对已读取的 IC 卡应用数据进行长度、必备数据是否存在、交易金额、IC 卡应用生 / 失效等规则检查。最后根据设备与卡片当前配置分析，以判断本次交易以联机交易，并向 IC 卡请求联机交易数据。

[0096] J. IC 卡响应联机交易请求同时返回 IC 卡应用密文数据与发卡行数据，支付装置接收到数据后，采用上述协商完成的密钥通过主芯片自带安全算法模块对返回数据进行密钥与密文 MAC 运算，然后发送到交易服务器请求交易。

[0097] K. 服务器接收到数据后进行 MAC 验证与解密操作后，对其请求数据判断 IC 卡与支付装置信息是否合法，如果请求数据认证通过，则发送发卡行数据、以及相关交易数据。

[0098] L. 支付装置收到数据后通过安全算法模块对数据的 MAC 验证与解密操作。然后对部分数据元通过非接触 / 接触读写卡模块发送到 IC 卡对其进行认证，并接收 IC 卡处理结果。通过 IC 卡响应结果判断本次交易是否成功，并通过安全算模块采用协商密钥对其加密与密文 MAC 计算后发送给交易服务器，同时通过声音或显示提示用户交易结果。

[0099] M. 交易服务器端接收完数据后进行数据 MAC 验证与解密操作，对交易结束数据进行存储、运算等操作。最终提示用户本次交易状态。

[0100] 本发明联网支付装置方法包括：

[0101] A. 通过对本装置上电后，其主 MCU 加载程序进行防篡改检查（图 1）以及外围模块初始化。然后系统进入到 Standby 状态，等待接收上位机程序发送的指令数据以及外部模块发出中断事件。

[0102] B. 当用户在服务器发起金融交易时，上位机检查已连接的装置系统。如果未找到则不发起交易，提示错误信息并退出；如果找到已连接本装置后，进入本次通信身份双向认证与密钥协商过程（图 1 所示）：

[0103] (1). 服务器发送取随机数指令。支付装置返回 32 字节随机数 (rt) 与 1 字节的算法标识 (at = 11h 代表 RSA1024 与 3DES 算法；51 代表 RSA2048 与 3DES 算法)：RT = rt|at，用于表示支付装置在后续处理中用到的非对称与对称算法。

[0104] (2). 服务器发送服务器证书、算法标识 (as) 以及 32 字节的随机数 (rs) 到支付装置中。

[0105] (3). 支付装置利用预制的根证书验证收到的服务器发送的服务器证书合法性，如果验证不通过，则发送出错消息，结束操作。

[0106] (4). 支付装置产生 48 字节随机数作为共享主密钥 MK，并且使用服务器的服务器证书中公钥采用之前的非对称算法对 MK 加密得到 E1，并发送给服务器。

[0107] (5). 服务器收到 E1 后，进行私钥运算，得到 MK 明文。然后读取支付装置证书与签名数据。并使用根证书验证支付装置合法性，如果验证不通过，则发送出错消息，结束操作。

[0108] (6). 服务器对服务器证书进行摘要运算得到 H1，对支付装置证书进行摘要运算得到 H2，将 RT, TS, H1, H2, S1, E1 连接后得到 T1 = (RT||RS||H1||H2||S1||E1)，然后对 T1

进行摘要运算得到 H3 ;将 ASCI I 码"SERVER"和 H3 连接后得到 D1 使用 M1 前 16 字节对 D1 进行 HMAC 运算得到 F1。

[0109] (7). 服务器发送 F1 到支付装置。支付装置使用同样的算法进行验证。如果验证不成功,则返回错误的状态码,结束链接 ;否则支付装置进行与 F1 运算方法 (只是将 ASCI I 码"SERVER"改为"CLIENT"得到 F2,并发送验证信息到服务器。

[0110] (8). 服务器接收到 F2 后,使用同样的运算方法进行验证,如果验证不通过,则结束链接,否则以下方法计算本次会话密钥 X = HMAC(M1,key_label||rt||rs),并取 X 前 16 字节为对称算法密钥, 后 16 字节作为 MAC 密钥。

[0111] C. 服务器将交易指令及其数据以 ISO7816-4 部分中 APDU 格式封装后,然后对其加密后链接数据 MAC 值打包发送到支付装置。

[0112] D. 当支付装置通过数据传输管理模块接收到数据后,用上述产生的密钥校验数据 MAC 正确性,如果验证失败,则返回错误状态码并结束本次交易,回到 Standby 状态 ;否则解出明文数据后,进行指令集的二次分发处理。

[0113] E. 指令集解析模块首先进行指令码匹配。如果匹配不成功,则返回错误状态码并返回 Standby 状态 ;否则再交于安全控制模块进行安全状态控制检查,如果安全状态不满足运行条件,则返回错误状态码并返回 Standby 状态 ;否则交于各业务指令进行功能处理。

[0114] F. 交易指令处理流程 :

[0115] (1). 查询设备上 IC 卡是否插入,如果未插入,则采用声音或显示方式提示用户插入或挥卡并等待有限时间 ;如果已检测到已有卡片。则采用声音、显示等方式提示用户输入交易必要的私密数据 (包括但不限于交易密码,交易金额等),然后利用支付装置已预置的公钥证书对其进行非对称运算得理密文后,消毁明文。最后进行读取卡片应用数据操作。

[0116] (2). 读取卡片应用数据后,检查 IC 卡片返回数据的格式是否合法,然后对交易数据的必备数据元存在进行检查、交易金额、IC 卡应用生效、失效等数据元进行相关的风险处理。最后支付装置根据当前配置与卡片配置,以判断本次交易是否以联机交易,并向 IC 卡片请求联机交易信息。

[0117] (3). 如果 IC 卡片响应联机交易请求同时返回应用密文数据与发卡片相关数据,支付装置接收到此数据后,向服务器请求交易。否则返回错误。

[0118] (4). 服务器接收到此请求后,根据请求数据判断 IC 卡与支付装置信息是否合法,如果此请求为非法,则拒绝本次交易,并提示交易失败同时与支付装置断开链接 ;反之服务器发送发卡行数据、以及相关交易数据到支付装置。

[0119] (5). 支付装置接收到数据后,判断数据合法性,如果不合法则返回错误,结束交易。否则根据规则对部份数据元转发到 IC 卡中进行交易认证,如果认证失败,则返回错误并结束交易 ;否则 IC 卡响应支付装置成功处理。支付装置根据响应结果返回给服务器并结束链接,同时提示用户成功交易。

[0120] (6). 服务器收到交易结束响应后,对必要的数据信息进行存储、运算等操作。

[0121] (7). 上述过程描述中服务器与支付装置的数据交互均采用密文方式 + 校验值方式进行传输。密钥值采用交易之前的已完成密钥协商的密钥值。

[0122] (8). 上述交易流程处理过程中,需要相关私密数据文件时,需要交于文件系统管理模块,由该模块对当前状态与私密数据文件读写权限进行检查。如果权限满足,则进行文

件数据的读写；否则返回错误。

[0123] (9). 上述流程支付装置处理中，任何出现错误时，均返回错误到服务器并通过声音或显示提示用户交易失败，同时系统返回到 Standby 状态等待下一指令接收。

[0124] G. 支付装置与服务器的通信方式包括有线、无线（包括但不限于 USB、串口、蓝牙、WIFI）。

[0125] 本发明联网支付装置嵌入式系统包括以下模块：

[0126] A. 数据通讯模块：负责本系统通过 USB 接口与计算机或支持 OTG 移动终端程序之间的数据收发过程。

[0127] B. 指令处理模块：对接收到的指令数据进行指令查找、格式、长度、安全状态等检查，然后对指令进行分发处理。

[0128] C. 安全控制模块：负责控制设备运行状态、文件读写权限与当前权限检查。

[0129] D. 文件系统模块：对于应用层的数据以文件形式出现，因此采用文件系统模块对其进行管理（包括但不限于：建立、删除、修改、激活等功能）。

[0130] E. 算法运算模块：用于主控制芯片自带的硬件密码运算模块，提供统一对称、非对称、摘要计算统一接口管理。

[0131] F. 数据存储模块：负责用户私密数据逻辑存储与掉电备份机制等功能。

[0132] G. 外围硬件控制模块：负责对本系统所用到的外围芯片驱动接口管理。

[0133] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

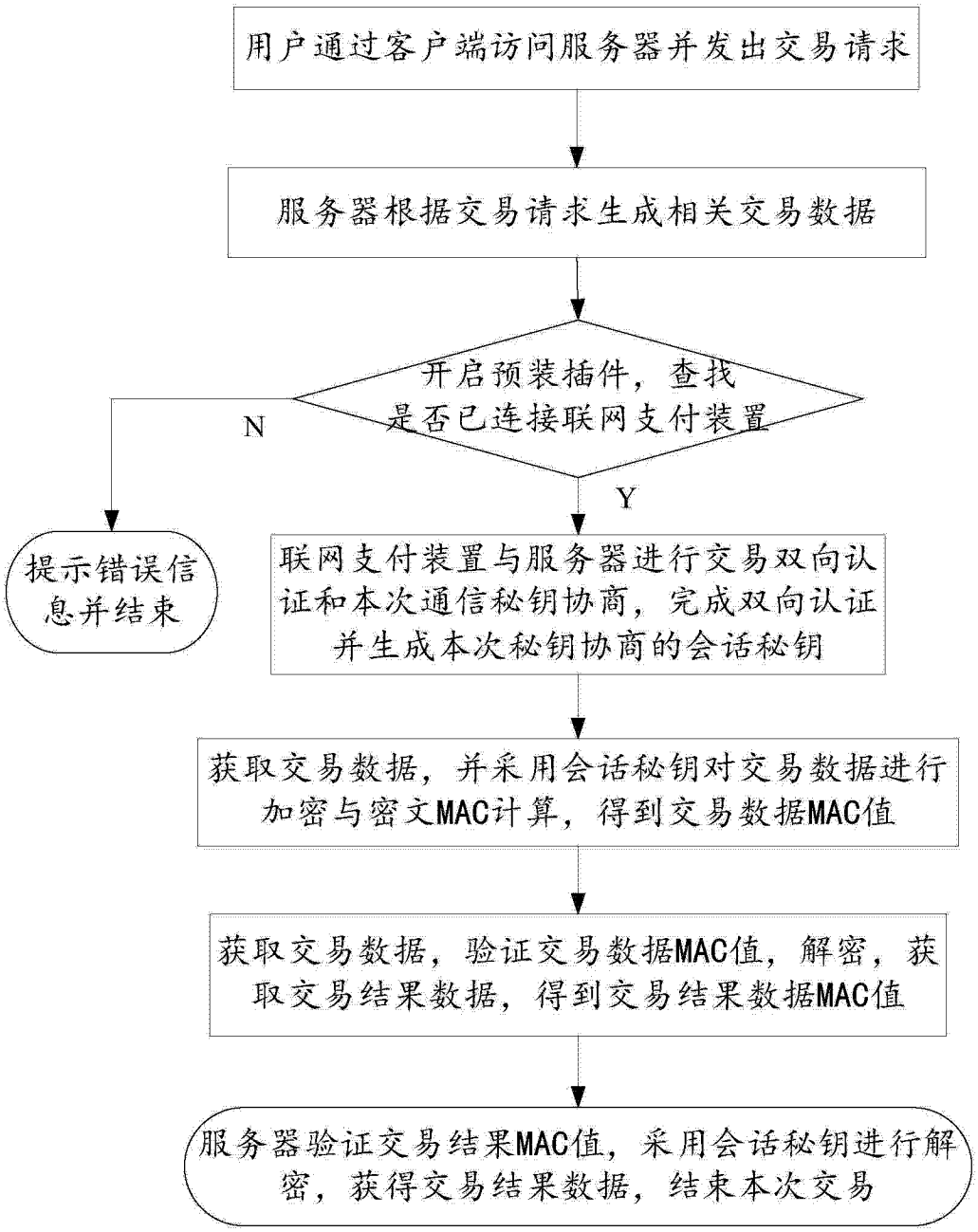

用户通过客户端访问服务器并发出交易请求
服务器根据交易请求生成相关交易数据
开启预装插件，查找是否已连接联网支付装置
N
Y
提示错误信息并结束
联网支付装置与服务器进行交易双向认证和本次通信秘钥协商，完成双向认证并生成本次秘钥协商的会话秘钥
获取交易数据，并采用会话秘钥对交易数据进行加密与密文MAC计算，得到交易数据MAC值
获取交易数据，验证交易数据MAC值，解密，获取交易结果数据，得到交易结果数据MAC值
服务器验证交易结果MAC值，采用会话秘钥进行解密，获得交易结果数据，结束本次交易

图 1

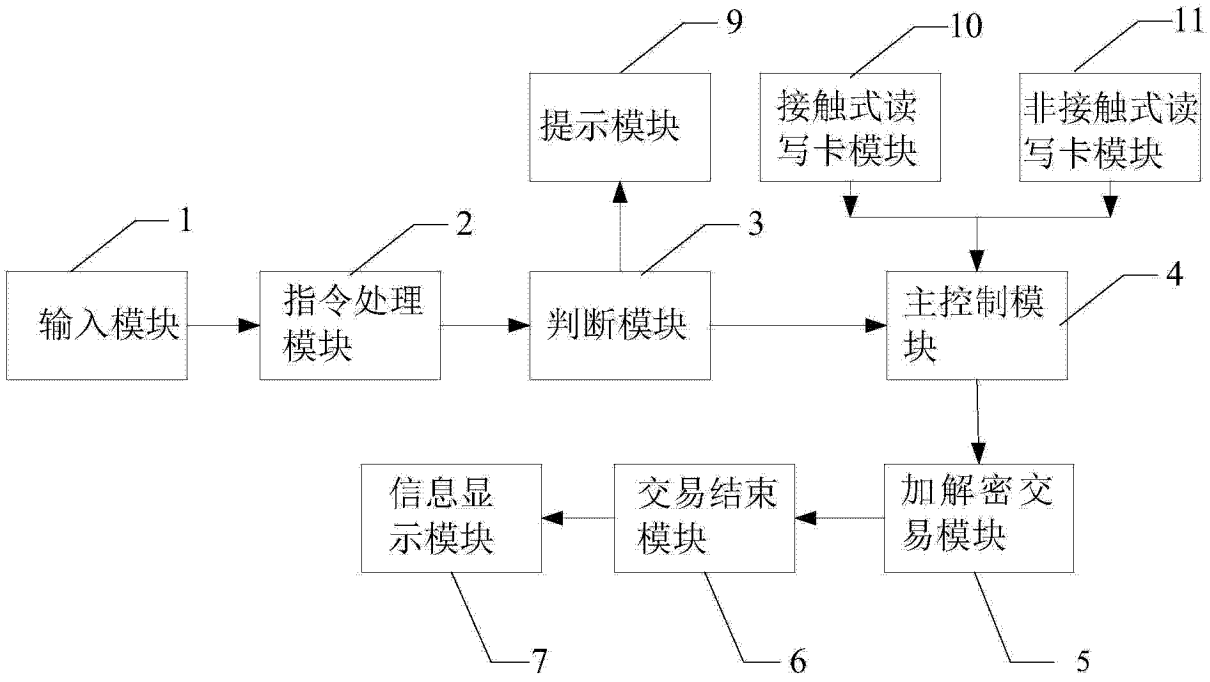

9
10
11
提示模块
接触式读写卡模块
非接触式读写卡模块
1
2
3
4
输入模块
指令处理模块
判断模块
主控制模块
信息显示模块
交易结束模块
加解密交易模块
7
6
5

图 2

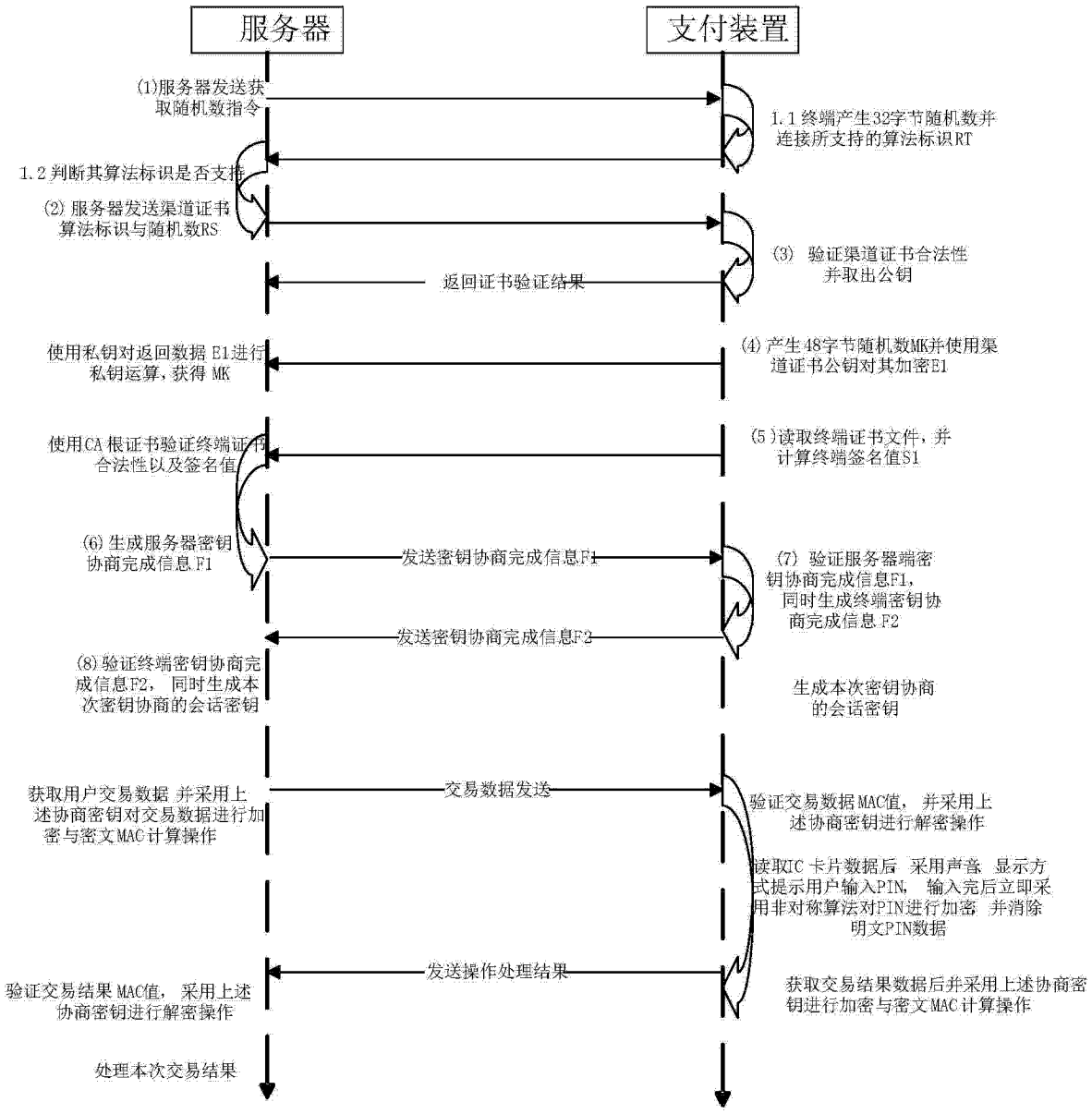

服务器
支付装置
(1)服务器发送获取随机数指令
1.1 终端产生32字节随机数并连接所支持的算法标识RT
1.2 判断其算法标识是否支持
(2) 服务器发送渠道证书算法标识与随机数RS
(3) 验证渠道证书合法性并取出公钥
返回证书验证结果
使用私钥对返回数据 E1进行私钥运算，获得 MK
(4) 产生48字节随机数MK并使用渠道证书公钥对其加密E1
使用CA 根证书验证终端证书合法性以及签名值
(5)读取终端证书文件，并计算终端签名值S1
(6) 生成服务器密钥协商完成信息 F1
发送密钥协商完成信息F1
(7) 验证服务器端密钥协商完成信息F1，同时生成终端密钥协商完成信息 F2
发送密钥协商完成信息F2
(8)验证终端密钥协商完成信息F2， 同时生成本次密钥协商的会话密钥
生成本次密钥协商的会话密钥
获取用户交易数据 并采用上述协商密钥对交易数据进行加密与密文MAC 计算操作
交易数据发送
验证交易数据MAC值， 并采用上述协商密钥进行解密操作
读取IC 卡片数据后 采用声音 显示方式提示用户输入PIN， 输入完后立即采用非对称算法对PIN进行加密 并消除明文PIN数据
发送操作处理结果
验证交易结果 MAC值， 采用上述协商密钥进行解密操作
获取交易结果数据后并采用上述协商密钥进行加密与密文MAC 计算操作
处理本次交易结果

图 3