(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 103985036 A
(43)申请公布日 2014.08.13

(21)申请号 201410196695.5

(22)申请日 2014.05.09

(71)申请人 杭州晟元芯片技术有限公司
地址 311121 浙江省杭州市余杭区五常街道文一西路998号9幢东楼

(72)发明人 黄权 夏舒畅 邱柏云

(74)专利代理机构 浙江杭州金通专利事务所有限公司 33100
代理人 徐关寿

(51)Int.Cl.
G06Q 20/16(2012.01)
G06Q 20/40(2012.01)
G06K 19/06(2006.01)

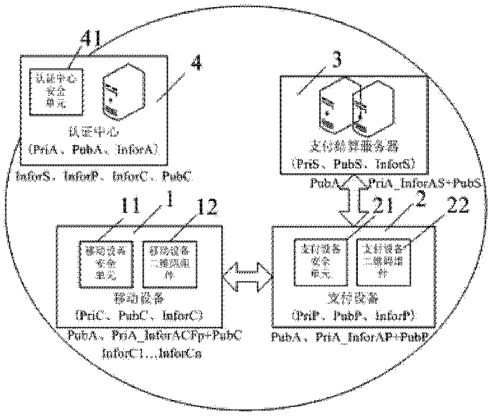
权利要求书3页 说明书7页 附图1页

(54)发明名称

一种带生物特征的二维码支付方法

(57)摘要

一种带生物特征的二维码支付方法，包括移动设备、支付设备、支付结算服务器、认证中心，移动设备、支付设备和支付结算服务器均向认证中心申请安全认证，认证后移动设备采集支付设备生成的带随机扰动码的消费二维码图片，并在相关信息认证后根据相关信息生成支付二维码图片供支付设备刷码支付，支付设备与支付结算服务器对支付二维码进行解码进行信息认证后完成后续支付。由于支付二维码加入了从支付设备获得的随机扰动码，因此可以保证每次消费的二维码都是动态变化，可以有效防止静态码被截取后反复使用的问题；通过对认证中心识别信息及所有权用户指纹特征的核验，从设备到使用者双方面保证了信息的防伪性。



CN 103985036 A

1. 一种带生物特征的二维码支付方法，其特征在于：包括移动设备、支付设备、支付结算服务器、认证中心，所述移动设备包括用于安全存储移动设备安全认证信息及用户银行信息和身份信息并可以进行安全认证的移动设备安全单元和用于采集支付设备生成的消费二维码并基于解码后的支付账户信息生成支付二维码的移动设备二维码组件；

所述支付设备包括用于安全存储支付设备安全认证信息及支付设备自身信息并可以将传输数据进行加解密安全处理后传输给支付结算服务器的支付设备安全单元和用于生成消费二维码给移动设备及采集移动设备生成的支付二维码并进行解码的支付设备二维码组件；

所述支付结算服务器包括用于安全存储支付结算服务器安全认证信息及对支付设备的传输数据进行解码并进行相关认证支付的支付结算服务器安全单元；

所述认证中心包括用于安全存储认证中心认证信息、认证中心识别信息及经认证中心认证过的所有设备信息记录的认证中心安全单元；

二维码支付的步骤如下：

（1）移动设备、支付设备和支付结算服务器均向认证中心申请安全认证，并各自将经认证中心认证的安全认证信息存储于各自的安全单元中，移动设备还将用户银行信息和身份信息存储于移动设备安全单元中；

（2）向支付设备输入消费金额；

（3）支付设备基于消费金额、自身的安全认证信息、关联消费账号信息、随机扰动码等信息生成消费二维码图片，并将随机扰动码导入支付设备安全单元中暂存；

（4）移动设备通过移动设备二维码组件拍照获取消费二维码图片并通过二维码组件的解码单元提取获得消费金额、支付设备的安全认证信息、关联消费账号信息、随机扰动码等消费二维码图片所包含的相关信息；

（5）移动设备通过移动设备安全单元内存储的认证中心公钥解码支付设备的安全认证信息，按约定格式提取认证中心识别信息，与认证中心在进行移动设备认证申请通过后导入认证中心识别信息进行比对，通过则进入下一步骤，失败则提示支付设备非法，停止支付；

（6）移动设备对支付设备进行认证通过后，移动设备的 CPU 会将消费金额、关联消费账号信息、随机扰动码等导入移动设备安全单元，并以命令码的方式触发移动设备安全单元对消费金额、指定的消费账号、随机扰动码、移动设备的安全认证信息基于支付设备公钥进行加密输出消费认证信息；

（7）移动设备的二维码组件获取到由自身的安全单元输出的消费认证信息生成支付二维码图片并进行显示；

（8）将移动设备生成的支付二维码图片到支付设备上进行刷码支付；

（9）支付设备获取到移动设备的支付二维码图片后自动进行解码，得到被支付设备公钥加密的消费认证信息，并将其导入支付设备安全单元用自身的私钥进行解密，生成解密后的消费信息；

（10）支付设备在支付设备安全单元内对解密获得的消费信息中的随机扰动码与支付设备安全单元中暂存的随机扰动码进行核对，核对通过则进入下一步骤，核对失败则提示支付失败，并终止支付流程；

（11）支付设备通过判断消费信息中是否包含消费认证指纹特征，如果无则提示消费者进行指纹认证，支付设备通过指纹传感器获取到消费者的指纹图片后，生成消费认证指纹特征，并导入支付设备安全单元中；如果移动设备本身配备指纹传感器则可以由移动设备提示用户认证，获取消费认证指纹特征，并叠加到加密的消费认证信息中，通过支付二维码图片传输过来；

（12）支付设备通过安全网络向支付结算服务器获取支付结算服务器公钥，并且用该公钥在支付设备安全单元中对消费信息、消费认证指纹特征进行加密后生成加密消费信息；

（13）支付设备通过安全网络通道将加密消费信息传输给支付结算服务器，支付结算服务器安全单元用其自身的私钥对加密消费信息进行解码获得消费金额、消费账号、随机扰动码、移动设备的安全认证信息、移动设备公钥、消费认证指纹特征；

（14）支付结算服务器安全单元通过认证中心公钥对移动设备的安全认证信息进行解码，获得认证中心识别信息、移动设备信息、所有权用户指纹特征，通过对认证中心识别信息核对可以确定移动设备的可靠性，成功则继续通过所有权用户指纹特征与消费认证指纹特征核对用户身份，失败则反馈支付设备提示用户消费认证失败；

（15）用户身份核对成功，则继续使用消费账号进行后续支付，不管成功 / 失败都可以通过安全网络将信息回传给支付设备进行相关提示。

2. 根据权利要求 1 所述的一种带生物特征的二维码支付方法，其特征在于：所述移动设备向认证中心申请安全认证的步骤如下：

A. 移动设备通过自身的安全单元生成公私钥密码对，公钥可导出发布，私钥不可导出；

B. 移动设备通过指纹传感器采集申请人的指纹信息，并生成所有权用户指纹特征数据并提交给认证中心服务器安全单元进行备档存储；如果移动设备没有自带指纹传感器也可以通过认证中心的指纹采集设备设生成申请人的指纹特征数据；

C. 移动设备将自身的公钥及移动设备信息，提交给认证中心服务器安全单元进行备档存储；

D. 认证中心以自身私钥对自身认证信息、移动设备信息、所有权用户指纹特征、移动设备公钥进行签名，产生移动设备的安全认证信息；

E. 认证中心的服务器将自身的公钥及移动设备的安全认证信息导出给移动设备的安全单元进行安全存存储；

F. 用户可向认证中心下载安装二维码应用及安全账户管理软件，用户通过安全账户管理软件平台将银行卡帐号、信用卡帐号，第三方支付用户帐户号、预付卡帐号等支付卡帐号输入于移动设备安全单元，并可由移动设备公钥加密后存储于移动设备安全单元。

3. 根据权利要求 1 所述的一种带生物特征的二维码支付方法，其特征在于：所述支付设备和支付结算服务器向认证中心申请安全认证的步骤如下：

a. 支付设备和支付结算服务器均通过自身的安全单元生成公私钥密码对，公钥可导出发布，私钥不可导出；

b. 支付设备和支付结算服务器均将自身的设备信息、公钥提交给认证中心进行设备认证申请；

c. 认证中心以自身私钥对自身认证信息、支付设备和支付结算服务器的各自设备信息

和公钥进行签名，产生支付设备和支付结算服务器的各自安全认证信息；

d. 认证中心的服务器将自身的公钥及支付设备和支付结算服务器的各自安全认证信息分别导出给支付设备和支付结算服务器的各自安全单元进行安全存储。

4. 根据权利要求 1~3 之一所述的一种带生物特征的二维码支付方法，其特征在于：所述移动单元二维码组件和支付设备二维码组件均由摄像头、显示屏、二维码生成及解码单元组成。

一种带生物特征的二维码支付方法

技术领域

[0001] 本发明涉及一种带生物特征的二维码支付方法。

背景技术

[0002] 随着技术的成熟，移动设备的普及，二维码支付作为移动支付的主力军，凭借时尚、便捷的客户体验，在支付领域得到了广泛推广，用户数的增长非常快速，但是由于其易捕获、易截取、易传播的特性，不断爆发欺诈事件，其在支付方面的安全性备受质疑。

[0003] 专利 2011101720434 中公开了一种移动电话生成二维码并实现移动支付的方法，虽然用户拥有的银行卡帐号、信用卡帐号，第三方支付用户帐户号、预付卡帐号等支付卡帐号信息虽然经过加密后保存在移动电话中，但是这些信息都是固定不变的，完全可以被运行在手机上的二维码生成软件直接获取，因此一旦手机系统平台被植入病毒程序，完全有可能被窃取后通过软件破解的方式盗用他人支付卡账号信息（支付卡账号信息只要是固定的，不管是明文还是密文，只要是被病毒程序获取到了，一旦运行在移动电话上的该系列支付二维码生成管理软件被破解，具有支付凭证的二维码就可被随意生成）以相同的方式进行二维码生成支付应用；而且支付二维码生成管理软件虽然会自动将当前时间、移动电话指纹，移动电话位置等信息编入到支付信息中，并加密后再生成支付二维码，虽然增加了一些防伪核对信息，但是二维码是以图片显示的方式存在，容易被拍照截获，被截取的二维码与原版不存在真假问题，因此无法解决类似网络上的“钓鱼”欺诈事件。打个比方说：某用户在某商户用移动电话生成二维码进行消费支付，如果商户让该消费用户在他自己伪造的具有拍照功能的支付设备上进行刷移动电话二维码支付，紧接着以设备故障为由要求用户以现金支付，那么刚才拍照截取的二维码图片完全可以被用来在正真的支付设备以图片还原的方式及时进行盗刷支付。在互联网络上的话就更加容易造就类似机理的“钓鱼”欺诈事件。

[0004] 还有专利 2011100353368 中公开了非对称加密二维码防伪方法，以二维码为载体，采用私钥加密与公钥解密相结合的方式构成完整的防伪、鉴别系统。私钥加密采用电子签名的方式对需要防伪产品中的明文唯一信息进行加密，加密后的密文信息转换成二维码图形与明文唯一信息同时出现，并将对应的解密公钥公开发布且动态发布伪品 ID 黑名单。该技术通过明文唯一信息与二维码密文信息的核对确定产品发行方的可信性，但是无法避免产品的唯一性，比方说仿冒者虽然无法通过明文唯一信息的变更仿冒出相应的密文二维码，但是仿冒者完全可以通过对正品包装上的二维码图形与明文唯一信息同时拷贝的方式大量复制伪冒产品，虽然正品生产方可以根据市场反馈通过事后追查的方式动态发布伪品 ID 黑名单，但是毕竟是伪冒产品流通过后的补救办法，此时即使是正品生产也无法用该方法确定收缴回来的这些问题产品中到底哪一件才是正品。

发明内容

[0005] 本发明提供了一种具有唯一二维码、可避免二维码被复制重复使用、提高了可信

任认证度的带生物特征的二维码支付方法。

[0006] 本发明采用的技术方案是：

一种带生物特征的二维码支付方法，其特征在于：包括移动设备、支付设备、支付结算服务器、认证中心，所述移动设备包括用于安全存储移动设备安全认证信息及用户银行信息和身份信息并可以进行安全认证的移动设备安全单元和用于采集支付设备生成的消费二维码并基于解码后的支付账户信息生成支付二维码的移动设备二维码组件；

所述支付设备包括用于安全存储支付设备安全认证信息及支付设备自身信息并可以将传输数据进行加解密安全处理后传输给支付结算服务器的支付设备安全单元和用于生成消费二维码给移动设备及采集移动设备生成的支付二维码并进行解码的支付设备二维码组件；

所述支付结算服务器包括用于安全存储支付结算服务器安全认证信息及对支付设备的传输数据进行解码并进行相关认证支付的支付结算服务器安全单元；

所述认证中心包括用于安全存储认证中心认证信息、认证中心识别信息及经认证中心认证过的所有设备信息记录的认证中心安全单元；

二维码支付的步骤如下：

(1)移动设备、支付设备和支付结算服务器均向认证中心申请安全认证，并各自将经认证中心认证的安全认证信息存储于各自的安全单元中，移动设备还将用户银行信息和身份信息存储于移动设备安全单元中；

(2)向支付设备输入消费金额；

(3)支付设备基于消费金额、自身的安全认证信息、关联消费账号信息、随机扰动码等信息生成消费二维码图片，并将随机扰动码导入支付设备安全单元中暂存；

(4)移动设备通过移动设备二维码组件拍照获取消费二维码图片并通过二维码组件的解码单元提取获得消费金额、支付设备的安全认证信息、关联消费账号信息、随机扰动码等消费二维码图片所包含的相关信息；

(5)移动设备通过移动设备安全单元内存储的认证中心公钥解码支付设备的安全认证信息，按约定格式提取认证中心识别信息，与认证中心在进行移动设备认证申请通过后导入的认证中心识别信息进行比对，通过则进入下一步骤，失败则提示支付设备非法，停止支付；

(6)移动设备对支付设备进行认证通过后，移动设备的CPU会将消费金额、关联消费账号信息、随机扰动码等导入移动设备安全单元，并以命令码的方式触发移动设备安全单元对消费金额、指定的消费账号、随机扰动码、移动设备的安全认证信息基于支付设备公钥进行加密输出消费认证信息；

(7)移动设备的二维码组件获取到由自身的安全单元输出的消费认证信息生成支付二维码图片并进行显示；

(8)将移动设备生成的支付二维码图片到支付设备上进行刷码支付；

(9)支付设备获取到移动设备的支付二维码图片后自动进行解码，得到被支付设备公钥加密的消费认证信息，并将其导入支付设备安全单元用自身的私钥进行解密，生成解密后的消费信息；

(10)支付设备在支付设备安全单元内对解密获得的消费信息中的随机扰动码与支付

设备安全单元中暂存的随机扰动码进行核对，核对通过则进入下一步骤，核对失败则提示支付失败，并终止支付流程；

（11）支付设备通过判断消费信息中是否包含消费认证指纹特征，如果无则提示消费者进行指纹认证，支付设备通过指纹传感器获取到消费者的指纹图片后，生成消费认证指纹特征，并导入支付设备安全单元中；如果移动设备本身配备指纹传感器则可以由移动设备提示用户认证，获取消费认证指纹特征，并叠加到加密的消费认证信息中，通过支付二维码图片传输过来；

（12）支付设备通过安全网络向支付结算服务器获取支付结算服务器公钥，并且用该公钥在支付设备安全单元中对消费信息、消费认证指纹特征进行加密后生成加密消费信息；

（13）支付设备通过安全网络通道将加密消费信息传输给支付结算服务器，支付结算服务器安全单元用其自身的私钥对加密消费信息进行解码获得消费金额、消费账号、随机扰动码、移动设备的安全认证信息、移动设备公钥、消费认证指纹特征；

（14）支付结算服务器安全单元通过认证中心公钥对移动设备的安全认证信息进行解码，获得认证中心识别信息、移动设备信息、所有权用户指纹特征，通过对认证中心识别信息核对可以确定移动设备的可靠性，成功则继续通过所有权用户指纹特征与消费认证指纹特征核对用户身份，失败则反馈支付设备提示用户消费认证失败；

（15）用户身份核对成功，则继续使用消费账号进行后续支付，不管成功／失败都可以通过安全网络将信息回传给支付设备进行相关提示。

[0007] 进一步，所述移动设备向认证中心申请安全认证的步骤如下：

A. 移动设备通过自身的安全单元生成移动设备公私钥密码对，移动设备公钥可导出发布，移动设备私钥不可导出；

B. 移动设备通过指纹传感器采集申请人的指纹信息，生成所有权用户指纹特征数据并提交给认证中心服务器安全单元进行备档存储；如果移动设备没有自带指纹传感器也可以通过认证中心的指纹采集设备设生成申请人的所有权用户指纹特征数据；

C. 移动设备将自身的公钥及移动设备信息，提交给认证中心服务器安全单元进行备档存储；

D. 认证中心以自身私钥对自身认证信息、移动设备信息、所有权用户指纹特征、移动设备公钥进行签名，产生移动设备的安全认证信息；

E. 认证中心的服务器将自身的公钥及移动设备的安全认证信息导出给移动设备的安全单元进行安全存存储；

F. 用户可向认证中心下载安装二维码应用及安全账户管理软件，用户通过安全账户管理软件平台将银行卡帐号、信用卡帐号，第三方支付用户帐户号、预付卡帐号等支付卡帐号输入于移动设备安全单元，并可由移动设备公钥加密后存储于移动设备安全单元。

[0008] 进一步，所述支付设备和支付结算服务器向认证中心申请安全认证的步骤如下：

a. 支付设备和支付结算服务器均通过自身的安全单元生成公私钥密码对，公钥可导出发布，私钥不可导出；

b. 支付设备和支付结算服务器均将自身的设备信息、公钥提交给认证中心进行设备认证申请；

c. 认证中心以自身私钥对自身认证信息、支付设备和支付结算服务器的各自设备信息

和公钥进行签名，产生支付设备和支付结算服务器的各自安全认证信息；

d. 认证中心的服务器将自身的公钥及支付设备和支付结算服务器的各自安全认证信息分别导出给支付设备和支付结算服务器的各自安全单元进行安全存储。

[0009] 进一步，所述移动单元二维码组件和支付设备二维码组件均由摄像头、显示屏、二维码生成及解码单元组成。

[0010] 本发明的有益效果：由于支付二维码加入了从支付设备获得的随机扰动码，因此可以保证每次消费的二维码都是动态变化，可以有效防止静态码被截取后反复使用的问题；通过对认证中心识别信息及所有权用户指纹特征的核验，从设备到使用者双方面保证了信息的防伪性；二维码支付信息中携带使用者的具有唯一识别功用的生物特征信息，可有效防止他人非法盗用个人移动支付设备；个人移动支付设备基于二维码识别技术实现对商户收款设备的可信任认证。

附图说明

[0011] 图 1 是本发明的结构示意图。

具体实施方式

[0012] 下面结合具体实施例来对本发明进行进一步说明，但并不将本发明局限于这些具体实施方式。本领域技术人员应该认识到，本发明涵盖了权利要求书范围内所可能包括的所有备选方案、改进方案和等效方案。

[0013] 参照图 1，一种带生物特征的二维码支付方法，包括移动设备 1、支付设备 2、支付结算服务器 3、认证中心 4，所述移动设备 1 包括用于安全存储移动设备安全认证信息及用户银行信息和身份信息并可以进行安全认证的移动设备安全单元 11 和用于采集支付设备生成的消费二维码并基于解码后的支付账户信息生成支付二维码的移动设备二维码组件 12；

所述支付设备 2 包括用于安全存储支付设备安全认证信息及支付设备自身信息并可以将传输数据进行加解密安全处理后传输给支付结算服务器的支付设备安全单元 21 和用于生成消费二维码给移动设备及采集移动设备生成的支付二维码并进行解码的支付设备二维码组件 22；

所述支付结算服务器 3 包括用于安全存储支付结算服务器安全认证信息及对支付设备传输数据进行解码并进行相关认证支付的支付结算服务器安全单元；

所述认证中心 4 包括用于安全存储认证中心认证信息、认证中心识别信息及经认证中心认证过的所有设备信息记录的认证中心安全单元 41；其中，认证中心认证信息包括安全认证中心自身的认证私钥和认证公钥。

[0014] 二维码支付的步骤如下：

（1）移动设备 1、支付设备 2 和支付结算服务器 3 均向认证中心 4 申请安全认证，并各自将经认证中心 4 认证的安全认证信息存储于各自的安全单元中，移动设备 1 还将用户银行信息和身份信息存储于移动设备安全单元 11 中；

（2）向支付设备 2 输入消费金额 Sum；

（3）支付设备 2 基于消费金额 Sum、自身的安全认证信息 PriA_InforAP+PubP、关联消

费账号信息、随机扰动码 RandCodeP 等信息生成消费二维码图片 ImageP，并将随机扰动码 RandCodeP 导入支付设备安全单元 21 中暂存；

（4）移动设备 1 通过移动设备二维码组件 12 拍照获取消费二维码图片 ImageP 并通过二维码组件 12 的解码单元提取获得消费金额 Sum、支付设备 2 的安全认证信息 PriA_InforAP+PubP、关联消费账号信息、随机扰动码 RandCodeP 等消费二维码图片 ImageP 所包含的相关信息；

（5）移动设备 1 通过移动设备安全单元 11 内存储的认证中心公钥 PubA 解码支付设备 2 的安全认证信息 PriA_InforAP+PubP，按约定格式提取认证中心 4 识别信息 InforA，与认证中心 4 在进行移动设备 1 认证申请通过后导入的认证中心识别信息 InforA 进行比对，通过则进入下一步骤，失败则提示支付设备非法，停止支付；

（6）移动设备 1 对支付设备 2 进行认证通过后，移动设备 1 的 CPU 会将消费金额 Sum、关联消费账号信息、随机扰动码 RandCodeP 等导入移动设备安全单元 11，并以命令码的方式触发移动设备安全单元 11 对消费金额 Sum、指定的消费账号 InforCn、随机扰动码 RandCodeC、移动设备 1 的安全认证信息 PriA_InforACFp+PubC 基于支付设备公钥 PubP 进行加密输出消费认证信息 PubP_InforPay=PubP(Sum+InforCn+ RandCodeC+PriA_InforACFp+PubC)；

（7）移动设备 1 的二维码组件 12 获取到由自身的安全单元输出的消费认证信息 PubP_InforPay 生成支付二维码图片 ImageC 并进行显示；

（8）将移动设备 1 生成的支付二维码图片 ImageC 到支付设备 2 上进行刷码支付；

（9）支付设备 2 获取到移动设备 1 的支付二维码图片 ImageC 后自动进行解码，得到被支付设备公钥 PubP 加密的消费认证信息 PubP_InforPay，并将其导入支付设备安全单元 21 用自身的私钥进行解密，生成解密后的消费信息 InforPay=Sum+InforCn+RandCodeC+PriA_InforACFp+PubC；

（10）支付设备 2 在支付设备安全单元 21 内对解密获得的消费信息中的随机扰动码 RandCodeC 与支付设备安全单元 21 中暂存的随机扰动码 RandCodeP 进行核对，核对通过则进入下一步骤，核对失败则提示支付失败，并终止支付流程；

（11）支付设备 2 通过判断消费信息 InforPay 中是否包含消费认证指纹特征 InforFpN，如果无则提示消费者进行指纹认证，支付设备 2 通过指纹传感器获取到消费者的指纹图片 ImageFpN 后，生成消费认证指纹特征 InforFpN，并导入支付设备安全单元 21 中；如果移动设备 1 本身配备指纹传感器则可以由移动设备 1 提示用户认证，获取消费认证指纹特征 InforFpN，并叠加到加密的消费认证信息 PubP_InforPay 中，通过支付二维码图片 ImageC 传输过来；

（12）支付设备 2 通过安全网络向支付结算服务器 3 获取支付结算服务器公钥 PubS，并且用该公钥在支付设备安全单元 12 中对消费信息 InforPay、消费认证指纹特征 InforFpN 进行加密后生成加密消费信息 PubS_InforPay=PubS(Sum+InforCn+RandCodeC+PriA_InforACFp+PubC+ InforFpN)；

（13）支付设备 2 通过安全网络通道将加密消费信息 PubS_InforPay 传输给支付结算服务器 3，支付结算服务器 3 安全单元用其自身的私钥对加密消费信息 PubS_InforPay 进行解码获得消费金额 Sum、消费账号 InforCn、随机扰动码 RandCodeC、移动设备的安全认证信息

PriA_InforACFp、移动设备公钥 PubC、消费认证指纹特征 InforFpN；

（14）支付结算服务器 3 安全单元通过认证中心 4 公钥 PubA 对移动设备的安全认证信息 PriA_InforACFp 进行解码，获得认证中心识别信息 InforA、移动设备信息 InforC、所有权用户指纹特征 InforFp，通过对认证中心识别信息 InforA 核对可以确定移动设备的可靠性，成功则继续通过所有权用户指纹特征 InforFp 与消费认证指纹特征 InforFpN 核对用户身份，失败则反馈支付设备 2 提示用户消费认证失败；

（15）用户身份核对成功，则继续使用消费账号 InforCn 进行后续支付，不管成功 / 失败都可以通过安全网络将信息回传给支付设备 2 进行相关提示。

[0015] 所述移动设备 1 向认证中心 4 申请安全认证的步骤如下：

A. 移动设备 1 通过自身的安全单元生成公私钥密码对，公钥 PubC 可导出发布，私钥 PriC 不可导出；

B. 移动设备 1 通过指纹传感器采集申请人的指纹信息，并生成所有权用户指纹特征数据 InforFp 并提交给认证中心 4 服务器安全单元进行备档存储；如果移动设备 1 没有自带指纹传感器也可以通过认证中心 4 的指纹采集设备设生成申请人的指纹特征数据；

C. 移动设备 1 将自身的公钥 PubC 及移动设备信息 InforC，如果指纹特征是由移动设备 1 生成，移动设备信息则包括指纹特征，提交给认证中心 4 服务器安全单元进行备档存储；

D. 认证中心 4 以自身私钥 PriA 对自身认证信息 InforA、移动设备信息 InforC、所有权用户指纹特征 InforFp、移动设备公钥 PubC 进行签名，产生移动设备的安全认证信息 PriA_InforACFp+PubC = PriA（InforA+InforC+ InforFp+PubC）；

E. 认证中心的服务器将自身的公钥 PubA 及移动设备的安全认证信息 PriA_InforACFp+PubC 导出给移动设备安全单元 11 进行安全存存储；

F. 用户可向认证中心 4 下载安装二维码应用及安全账户管理软件，用户通过安全账户管理软件平台将银行卡帐号、信用卡帐号，第三方支付用户帐户号、预付卡帐号等支付卡帐号 InforC1~ InforCn 输入于移动设备安全单元 11，并可由移动设备公钥 PubC 加密后存储于移动设备安全单元 11。

[0016] 所述支付设备 2 和支付结算服务器 3 向认证中心 4 申请安全认证的步骤如下：

a. 支付设备 2 和支付结算服务器 3 均通过自身的安全单元生成公私钥密码对，公钥 PubP 和 PubS 可导出发布，私钥 PriP 和 PriS 不可导出；

b. 支付设备 2 和支付结算服务器 3 均将自身的设备信息 InforP 和 InforS、公钥 PubP 和 PubS 提交给认证中心 4 进行设备认证申请；

c. 认证中心 4 以自身私钥 PriA 对自身认证信息 InforA、支付设备 2 和支付结算服务器 3 的各自设备信息 InforP 和 InforS 以及公钥 PubP 和 PubS 进行签名，产生支付设备 2 和支付结算服务器 3 的各自安全认证信息 PriA_InforAP+PubP=PriA（InforA+InforP+PubP）和 PriA_InforAS+PubS = PriA（InforA+InforS+PubS）；

d. 认证中心 4 的服务器将自身的公钥 PubA 及支付设备 2 和支付结算服务器 3 的各自安全认证信息分别导出给支付设备 2 和支付结算服务器 3 的各自安全单元进行安全存储。

[0017] 所述移动单元二维码组件 12 和支付设备二维码组件 22 均由摄像头、显示屏、二维码生成及解码单元组成。

[0018] 本实施例中的移动设备 1 主要由移动设备安全单元 11 与移动各设备二维码组件 12 两部分组成，用于对支付设备 2 的认证及基于支付账户数据的支付二维码生成。移动设备安全单元 11 可以以 SIM 卡、TF 卡、指纹传感器、移动设备 CPU 的内嵌 SE 单元等形态存在，可独立生成客户公私钥对，私钥 PriC 存储于安全单元不可导出，公钥 PubC 可被导出由移动设备的 CPU 进行发布处理，另外用户的银行卡帐号、信用卡帐号，第三方支付用户帐户号、预付卡帐号等支付卡帐号（InforC1~ InforCn）及指纹特征等身份信息 InforC 也可以导入由公钥 PubC 加密存储于该安全单元。移动设备二维码组件 12 主要包括摄像头、显示屏、二维码生成及解码软件组成。摄像头用于采集支付设备 2 基于安全认证信息 PriA_InforAP+PubP、消费金额、关联消费账号信息、随机扰动码 RandCodeP 等信息生成的消费二维码；二维码解码软件用于将二维码进行解码提取相关信息 PriA_InforAP+PubP 进行设备认证，认证通过则将提取的消费金额、关联消费账号信息、随机扰动码送入移动设备安全单元 11，由移动设备安全单元 11 将相关支付账号、设备身份信息（可包含指纹信息）、消费金额、随机扰动码等信息通过支付设备公钥 PubP 加密后输出给二维码生成软件生成支付二维码图片，并且显示于移动设备 1 屏幕上。

[0019] 本实施例中支付设备 2 主要有支付设备安全单元 21 与支付设备二维码组件 22 两部分组成，用于消费二维码生成及用户数据的安全传输。支付设备安全单元 21 用于安全存储认证中心公钥 PubA、支付设备自身信息以及经过认证中心私钥 PriA 签名后的设备认证信息 PriA_InforAP+PubP，同时可以对传输信息进行一下加解密安全处理。支付设备二维码组件 22 主要包括摄像头、显示屏、二维码生成及解码软件组成。一方面用于产生消费二维码供移动设备 1 进行认证识别，一方面则用来采集移动设备 1 生成的支付二维码图片，再经由二维码解码软件生成字节数据后，通过支付设备安全单元 21 经进行相关安全处理，最终传输给支付结算服务器 3。

[0020] 本实施例中支付结算服务器 3 用于对支付设备 2 通过安全网络通道提供的用户支付账户等相关数据进行解码认证支付。

[0021] 本实施例中认证中心 4 是整个系统平台的可信交互基础，用于保证移动设备 1、支付设备 2、支付结算服务器 3 相互认证识别。认证中心安全单元 41 用于安全存储安全认证中心自身的认证私钥 PriA、认证公钥 PubA、认证中心识别信息 InforA 以及经认证中心认证过的所有设备信息记录，如：支付结算服务器设备信息 InforS、支付设备信息 InforP、移动设备信息 InforC、移动设备公钥 PubC 等；同时可进行一些基于公私钥对的加解密认证。

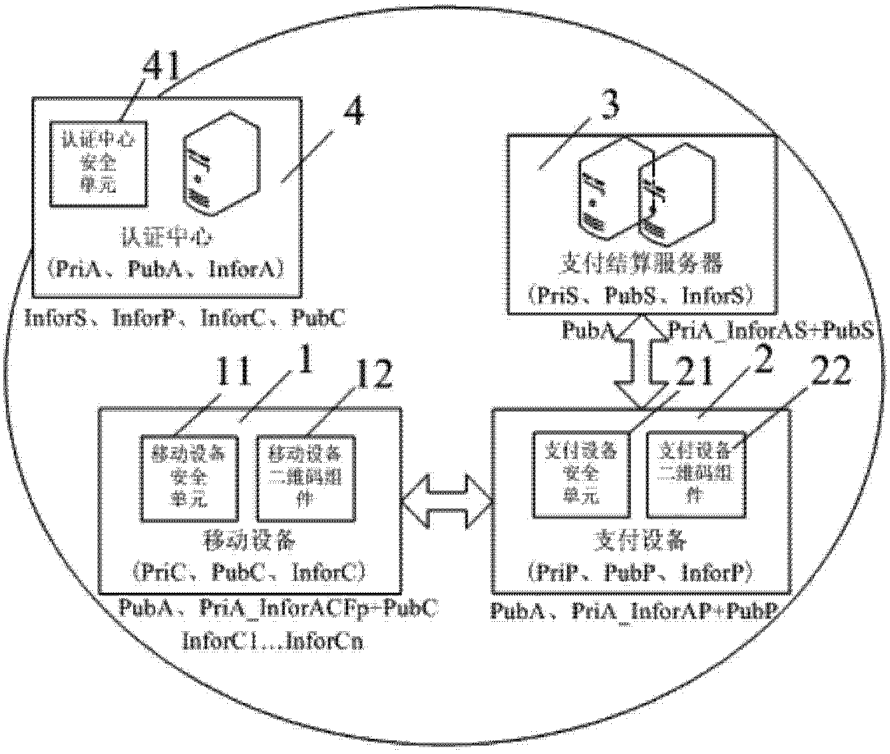

41
认证中心
安全
单元
4
认证中心
(PriA、PubA、InforA)
InforS、InforP、InforC、PubC
3
支付结算服务器
(PriS、PubS、InforS)
PubA
PriA_InforAS+PubS
11
1
12
移动设备
安全
单元
移动设备
二维码组
件
移动设备
(PriC、PubC、InforC)
PubA、PriA_InforACFp+PubC
InforC1...InforCn
21
2
22
支付设备
安全
单元
支付设备
二维码组
件
支付设备
(PriP、PubP、InforP)
PubA、PriA_InforAP+PubP

图 1