

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
C06Q 20/00 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200610076282.9

[43] 公开日 2006 年 9 月 20 日

[11] 公开号 CN 1835008A

[22] 申请日 2006.4.21

[74] 专利代理机构 北京清亦华知识产权代理事务所
代理人 廖元秋

[21] 申请号 200610076282.9

[71] 申请人 李黎军

地址 100052 北京市宣武门外大街 6 号庄胜
广场中央办公楼北翼 1008 室

共同申请人 曾之俊 徐 竹

[72] 发明人 李黎军 曾之俊 徐 竹

权利要求书 1 页 说明书 4 页

[54] 发明名称

一种移动支付方法

[57] 摘要

本发明涉及一种移动支付方法，属于电子交易服务技术领域，包括：用户申请开通移动支付服务，并获取初始的用户数字身份证明；移动支付系统对用户终端号码进行验证；用户通过短信提交其数字身份证明；移动支付系统首先进行用户身份的认证；对数字身份认证通过的用户，请求用户提交支付信息；并向用户发送一次性支付密码；用户反馈该一次性支付密码；移动支付系统向银行支付系统发送该笔交易的实时支付信息，并获得银行支付系统对该笔交易的处理反馈结果；移动支付系统向用户反馈扣费结算处理的结果信息。本发明可实现用户使用移动设备能够如同操作 POS 机一样，方便、安全地完成支付、转账等金融交易。

1、一种移动支付方法，其特征在于，包括以下步骤：

1) 用户申请开通移动支付服务，并获取初始的用户数字身份证明；

2) 用户发起支付请求；

3) 移动支付系统对用户终端号码进行验证，验证通过的请求用户数字身份证明；

4) 用户通过短信提交其数字身份证明；

5) 移动支付系统首先进行用户身份的认证；

6) 移动支付系统对数字身份认证通过的用户，请求用户提交支付信息；

7) 移动支付系统接收到用户支付信息后，向用户发送一次性支付密码；

8) 用户反馈该一次性支付密码给移动支付系统；

9) 移动支付系统向银行支付系统发送该笔交易的实时支付信息，并获得银行支付系统对该笔交易的处理反馈结果；

10) 移动支付系统向用户反馈扣费结算处理的结果信息；

2、如权利要求1所述的移动支付方法，其特征在于，所述步骤1)具体实现方法为：用户通过短信，发送相关的开通服务指令，并提供相关的银行账户凭证信息直接给移动支付系统，成为移动支付服务的签约用户，并获取初始的用户数字身份证明。

3、如权利要求1所述的移动支付方法，其特征在于，所述步骤1)中的用户数字身份证明是通过单向加密算法，采用用户手机号码、开户的时间信息来生成的。

4、如权利要求1所述的移动支付方法，其特征在于，所述步骤5)的认证方法为采用将用户的移动终端号码以及开户时间等信息使用单向加密算法加密后和用户发送过来的数字身份证明进行对比，相同则通过认证，否则没有通过认证。

5、如权利要求1所述的移动支付方法，其特征在于，所述步骤7)一次性支付密码是采用双向加密算法生成动态一次性密码，该密码在使用一次后即失效。

一种移动支付方法

技术领域

本发明属于电子交易服务技术领域，特别涉及用于对移动设备的用户提供与应用服务系统实现进行安全的支付、转账等金融交易，具有开通、支付、查询和取消功能的方法。

背景技术

移动支付业务是移动运营商与金融部门合作推出的，通过手机进行支付行为、缴费或消费的电子交易服务。移动支付作为未来电子支付的手段之一，尤其是在3G大规模商用、智能手机普及后，将成为人们最便捷的日常支付方式，市场发展潜力巨大！截止到2005年底，中国移动支付业务市场规模达到了1.87亿元（主要用短信进行确认、支付），中国近4亿的移动手机用户，将成为世界上最大的支付网点，移动支付的市场需求巨大，一旦手机“金融POS机化”，移动支付就不再是手机用户的“选择性业务”，而成为每个用户的“必需性业务”，这种转变对移动支付产业来说，充满无限的想象。

注：POS（Point of sales）的中文意思是“销售点”，是一种配有条码或OCR码（Optical character recognition 光字符码）终端阅读器，有现金或易货额度出纳功能。品种有有线和无线两种或有、无线兼用。POS机与广告易货交易平台的结算系统相联，其主要任务是对商品与媒体交易提供数据服务和管理功能，并进行非现金结算。

在已有移动支付方式中，主要有以下几种：短信(STK)方式、IVR方式(Interactive Voice Response 交互式语音应答)、USSD方式、WAP协议方式实现、WEB(WWW)方式实现，但主要以短信方式为主（主要由于操作方便以及终端支持率高）

现有短信方式移动支付的方法主要有以下步骤：

- 1) 用户将交易信息以及移动支付账户的口令通过短信发送到移动支付系统；
- 2) 移动支付系统校验用户信息，确认无误后完成交易；
- 3) 移动支付系统发送短信通知用户交易完成。

目前大多数通过短信实现的移动支付的方法采用静态支付口令，存在以下安全缺陷：

口令字相对固定，可反复使用，因而易被泄露、窃听。

口令字长度较短（通常是4~6位十进制数），易遭试探攻击。

口令字直接在短信中明文发送，未进行处理，容易泄漏。

当前，制约移动支付、手机“信用卡”化的主要因素在于：

(一) 支付安全性担心，出于对新业务的疑虑和使用安全性担心，害怕个人的银行卡信息泄露，目前移动支付市场中用户的应用行为，仅限于小额支付、虚拟物品支付，如：手机银行、手机钱包，“e路通”等；

(二) 用户的认知度较低，第三方支付公司无论在公信力、安全性的认可度，都无法

建立；用户对移动支付业务出于小心翼翼的尝试阶段，对于大额支付和实物商品的移动支付还有待与培育和发展。

发明内容

本发明的目的是为克服已有的移动支付方法存在的不足之处，提出了一种移动支付方法，用于对移动设备的用户提供与应用服务系统进行安全、方便的支付、转账等金融交易，具有开通、支付、查询和取消功能，可实现用户使用移动设备能够如同操作 POS 机一样，方便、安全地完成支付、转账等金融交易。

本发明提出的一种移动支付方法，包括以下步骤：

- 1) 用户申请开通移动支付服务，并获取初始的用户数字身份证明；
- 2) 用户发起支付请求；
- 3) 移动支付系统对用户终端号码进行验证，验证通过后请求用户数字身份证明；
- 4) 用户通过短信提交其数字身份证明；
- 5) 移动支付系统首先进行用户身份的认证；
- 6) 移动支付系统对数字身份认证通过的用户，请求用户提交支付信息；
- 7) 移动支付系统接收到用户支付信息后，向用户发送一次性支付密码；
- 8) 用户反馈该一次性支付密码给移动支付系统；
- 9) 移动支付系统向银行支付系统发送该笔交易的实时支付信息，并获得银行支付系统对该笔交易的处理反馈结果；
- 10) 移动支付系统向用户反馈扣费结算处理的结果信息。

本发明的特点及效果：

在本发明提出的移动支付方法中，改善了目前应用的移动支付方法中信息交互的简单和安全性差的方面，提出了身份认证的安全方式（采用数字身份证明）以及支付方式的安全方式（采用一次性支付密码方法）。

由于本发明有效地提供了一种对用户使用移动设备进行安全和方便支付的系统和方法，从而让用户无需对支付安全性担心，可扩展到更多的应用场合和更大数额的支付，并且可以解决第三方支付公司在公信力、安全性的用户认可度低的问题，极大增强了用户使用移动支付业务的信心和增加用户的使用机会直接促进移动支付市场的高速发展。

具体实施方式

本发明的移动支付方法结合实施例作进一步详细说明。

本发明的方法实施例包括：建立与银行支付系统或运营商指定的营业网点相连通的一移动支付系统，该移动支付系统是采用一套能够完成移动支付流程的平台，包括可实现开通、支付、查询、注销等功能的平台。该系统包括：

用户认证模块，用于对用户通过移动设备发出的身份信息，进行采集，并传送给信息分析中心进行认证，同时将认证记录、移动设备的信息和时间信息关联地存储在海量日志

信息存贮装置中。

数字身份证明验证模块，用于基于应用层的安全认证，确保用户的动作和数据在网络中被侦听，也不能被轻易非法冒充，即用户在登录或交易过程中的密码是不可重用的。

一次性支付密码生成模块，用于在移动设备终端没有计算和运算能力的应用环境下，提供现有静态密码所不具备的安全性和保密性；

移动支付网关模块，用于解决基于移动通信网络设备的网上安全支付问题的交易平台，位于移动通信网络和传统的金融机构内部网之间，将两个网络安全的连接起来，保证交易信息传给安全的金融网络，主要完成：通信、协议转换和数据加解密的功能。

上述系统中各模块均可采用常规具有相同功能的模块，或在已有的移动支付系统结构的基础上根据其所需完成的功能采用常规技术手段实现。

上述运营商的营业网点、银行支付系统均为可实现电子交易的现有的运营商、银行内部的相应设备，其本身不属于本发明的保护内容，在此不以赘述。

该方法包括以下步骤：

1) 用户申请开通移动支付服务，并获取初始的用户数字身份证明：

用户可以通过三种实施方式，即：

(1) 用户通过短信，发送相关的开通服务指令，并提供相关的银行账户凭证信息直接给移动支付系统，成为移动支付服务的签约用户，并获取初始的用户数字身份证明；

(2) 用户持本人有效证件，到运营商指定的营业网点进行身份确认和开通，并完成开通移动支付服务的相关服务合约的签署，而成为移动支付服务的签约用户，并获取初始的用户数字身份证明；

(3) 用户持本人有效证件原件及账户凭证原件（银行卡或存折）到账户所在地的银行营业网点进行身份确认，并完成开通移动支付服务的相关服务合约的签署，而成为移动支付服务的签约用户，并获取初始的用户数字身份证明。

所述的数字身份证明的生成可通过单向加密算法（如 SHA-1 算法等），采用用户手机 MDN（手机号码）、开户的时间等信息来生成。数字身份证明是不重复且不可解密的，可唯一标识用户身份的证明。

2) 用户发起支付请求：

在有支付需要的环境下，用户使用移动终端（例如手机），通过发送短信到移动支付特定服务代码的方式发起支付请求（例如：发送短信 ZF 到移动支付的服务代码 95555）。

3) 移动支付系统对用户终端号码进行验证，验证通过后请求用户数字身份证明：

移动支付系统通过对发送短信的用户终端号码进行验证，确认该终端号码是已经开通移动支付服务的终端号码，则向用户发送短信请求数字身份证明（对于没有验证通过的用户终端号码，将会取消请求数字身份证明及后续流程）。

4) 用户通过短信提交其数字身份证明：

用户使用移动终端以短信的方式将数字身份证明发送到移动支付特定服务代码（如发送到 95555）

5) 移动支付系统进行用户身份的认证;

移动支付系统根据用户发送的数字身份证明，在系统中进行认证；认证的实施方式可采用将用户的移动终端号码以及开户时间等信息使用单向加密算法（如 SHA-1 单向散列算法）加密后和用户发送过来的数字身份证明进行对比，相同则通过认证，否则没有通过认证。

6) 移动支付系统对数字身份证明认证通过的用户，请求用户提交支付信息：

移动支付系统对用户数字身份证明认证通过后，向用户发送短信，请求用户发送支付信息。

所述支付信息是指完成一次交易所需的信息，包括接受付款的商户名称、代号以及交易金额等必要信息。

7) 移动支付系统接收到用户支付信息后，向用户发送一次性支付密码：

移动支付系统收到用户支付信息后，生成一次性支付密码，并通过短信发送给用户。

移动支付系统生成一次性支付密码的实施例是采用双向加密算法（如 Blowfish 对称加密算法）生成动态一次性密码。该密码在使用一次后即失效，同时该密码具有时效性，过期后同样失效。通过这种方式确保用户支付安全。

8) 用户反馈该一次性支付密码给移动支付系统：

用户收到移动支付系统发送过来的一次性支付密码后，将该密码重新发送回移动支付系统，以确认该次交易。

9) 移动支付系统向银行支付系统发送该笔交易的实时支付信息，并获得银行支付系统对该笔交易的处理反馈结果；

移动支付系统收到用户反馈的一次性支付密码后，通过和银行支付系统之间的接口向银行支付系统发送该笔交易的支付信息，并获得银行支付系统对该笔交易的处理反馈结果。处理结果包括支付成功、支付失败等其它账户资金结算状态。状态为支付成功则表明用户的该笔支付交易成功完成。

10) 移动支付系统向用户反馈支付处理结果信息：

移动支付系统将该支付处理反馈结果通过短信发送给用户。该次支付请求流程即为完成。