

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 12 月 29 日 (29.12.2016)



(10) 国际公布号
WO 2016/206385 A1

- (51) 国际专利分类号:
G06Q 20/40 (2012.01)
- (21) 国际申请号: PCT/CN2016/073748
- (22) 国际申请日: 2016 年 2 月 14 日 (14.02.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510359713.1 2015 年 6 月 25 日 (25.06.2015) CN
- (71) 申请人: 深圳市中兴微电子有限公司 (ZTE MICROELECTRONICS TECHNOLOGY CO.,LTD.) [CN/CN]; 中国广东省深圳市盐田区大梅沙 1 号厂房, Guangdong 518085 (CN)。
- (72) 发明人: 孙奥 (SUN, Ao); 中国广东省深圳市盐田区大梅沙 1 号厂房, Guangdong 518085 (CN)。 童龙仓 (TONG, Longcang); 中国广东省深圳市盐田区大梅沙 1 号厂房, Guangdong 518085 (CN)。 陈天明 (CHEN, Tianming); 中国广东省深圳市盐田区大梅沙 1 号厂房, Guangdong 518085 (CN)。
- (74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OF-

FICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: PAYMENT METHOD, DEVICE AND SYSTEM, AND COMPUTER STORAGE MEDIUM

(54) 发明名称: 一种支付的方法、设备、系统及计算机存储介质

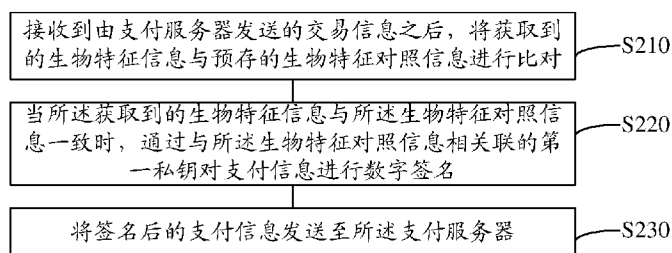


图 2

S210 AFTER TRANSACTION INFORMATION SENT BY A PAYMENT SERVER IS RECEIVED, COMPARE ACQUIRED BIOLOGICAL CHARACTERISTIC INFORMATION WITH PRE-STORED BIOLOGICAL CHARACTERISTIC REFERENCE INFORMATION

S220 WHEN THE ACQUIRED BIOLOGICAL CHARACTERISTIC INFORMATION IS CONSISTENT WITH THE BIOLOGICAL CHARACTERISTIC REFERENCE INFORMATION, SIGN A DIGITAL SIGNATURE ON THE PAYMENT INFORMATION BY MEANS OF A FIRST PRIVATE KEY ASSOCIATED WITH THE BIOLOGICAL CHARACTERISTIC REFERENCE INFORMATION

S230 SEND, TO THE PAYMENT SERVER, THE PAYMENT INFORMATION ON WHICH THE DIGITAL SIGNATURE IS SIGNED

(57) Abstract: A payment method, device and system, and a computer storage medium. The method comprises: after transaction information sent by a payment server is received, comparing acquired biological characteristic information with pre-stored biological characteristic reference information (S210); when the acquired biological characteristic information is consistent with the biological characteristic reference information, signing a digital signature on payment information by means of a first private key associated with the biological characteristic reference information (S220); and sending, to the payment server, the payment information on which the digital signature is signed (S230).

(57) 摘要: 一种支付的方法、设备、系统及计算机存储介质, 该方法包括: 接收到由支付服务器发送的交易信息之后, 将获取到的生物特征信息与预存的生物特征对照信息进行比对 (S210); 当所述获取到的生物特征信息与所述生物特征对照信息一致时, 通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名 (S220); 将签名后的支付信息发送至所述支付服务器 (S230)。

WO 2016/206385 A1

一种支付的方法、设备、系统及计算机存储介质

技术领域

本发明涉及信息安全技术，尤其涉及一种支付的方法、设备、系统及计算机存储介质。

5 背景技术

二维码支付作为一种新型便捷的支付手段凭借其时尚、便捷的用户体验得到迅速普及，但由于二维码本身具有易捕获、易截取、易传播的特点，用于支付的终端设备后台运行的病毒程序可以通过截屏等技术手段获取二维码信息，抢先发送支付请求，从而给客户造成损失，具有较大的安全隐患。

目前，为了提高二维码支付的安全性，一些基于生物特征信息的确认手段，如指纹等被加入到二维码支付过程中，具体的过程可以包括：首先，认证服务器预存用户的指纹模板一枚，身份扫描设备的机器指纹一份，用户二维码一份；然后，用户移动终端向认证服务器发起认证请求；接着，身份扫描设备扫描用户指纹信息，提取指纹特征；随后，身份扫描设备扫描用户二维码，提取设备的机器指纹；接着，通过设备的机器指纹对用户二维码、指纹特征进行加密保护，传输至远端认证服务器进行认证；最后，认证服务器用预存的设备机器指纹解密用户认证请求，比对用户二维码与指纹特征，一致，则认证通过，不一致，则认证失败。

上述方案可以保证用户身份凭据的唯一性，也能够满足用户无需记忆密钥的需求。但是上述方案在具体实现过程中，用户终端内的病毒程序可以在用户输入指纹时获取指纹特征，并生成伪造的交易信息采取发给认证服务器认证；进一步地，指纹特征在网络上的传输过程以及指纹特征直接

保存在服务器侧均会导致指纹特征的泄露，再加上用户的指纹信息具有不可撤销性，无法像改密码一样随意修改，一旦泄露则可以通过指纹信息模板反推出用户侧指纹图像，给用户带来更严重的损失，因此，上述方案仍然具有较大的安全隐患。

5 发明内容

为解决上述技术问题，本发明实施例期望提供一种支付的方法、设备、系统及计算机存储介质，避免生物特征信息的泄露，提高了移动支付过程中的安全性。

本发明的技术方案是这样实现的：

10 第一方面，本发明实施例提供了一种支付终端，所述支付终端包括：通过加密通道进行连接的获取单元和支付信息处理单元、以及安装有支付应用程序的且与所述支付信息处理单元相连接的终端设备；其中，

所述终端设备，配置为接收由支付服务器发送的交易信息；其中，所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；

15 所述获取单元，配置为获取生物特征信息，并将所述生物特征信息传输至所述支付信息处理单元，

所述支付信息处理单元，配置为将所述生物特征信息与预存的生物特征对照信息进行比对；以及，

20 当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名；并将签名后的支付信息传输至所述终端设备；其中，所述支付信息用于确认对所述交易信息进行支付；

25 所述终端设备，还配置为将所述签名后的支付信息发送至所述支付服务器；其中，所述签名后的支付信息用于所述支付服务器通过与所述生物特征对照信息相关联的第一公钥进行数字签名验证，且当验证成功时按照

支付信息将所述支付终端对应的用户账号中的所述待支付的金额划拨至收款端。

在上述方案中，所述获取单元，还可以配置为获取生物特征对照信息；并将生物特征对照信息传输至所述支付信息处理单元；

5 所述支付信息处理单元，还配置为按照预设的密钥生成策略生成与生物特征对照信息相关联的密钥对；并将密钥对中的第一公钥传输至所述终端设备；其中，密钥对包括第一公钥和第一私钥；

 所述终端设备，还配置为将密钥对中的第一公钥发送至支付服务器；所述第一公钥用于支付服务器将第一公钥与支付终端对应的用户账号进行
10 绑定。

 在上述方案中，所述终端设备，还配置为向所述支付服务器发送临时账号请求；其中，所述临时账号请求用于所述支付服务器生成与所述用户账号相关联的临时账号；以及，接收所述支付服务器发送的临时账号，并生成与所述临时账号相关联的二维码；其中，所述临时账号用于在预设的
15 有效期内具有与用户账号相同的支付功能且仅用于预设次数的支付；所述二维码用于收款端扫描后向所述支付服务器发送交易请求；所述交易请求包括所述收款端通过解析所述二维码获取到的所述临时账号和待支付金额。

 在上述方案中，当所述临时账号处于有效期内，则所述交易信息中所
20 包括的用户账号信息为所述临时账号；

 当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为所述支付服务器重新生成的临时账号。

 在上述方案中，所述支付信息处理单元存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法通过所述终端设备进行获
25 取。

第二方面，本发明实施例提供了一种支付服务器，所述支付服务器包括：发送单元、接收单元、验证单元和划拨单元；其中，

所述发送单元，配置为向支付终端发送交易消息；其中，所述交易消息包括所述支付终端对应的用户账号信息和待支付的金额；

5 所述接收单元，配置为接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后的支付消息；所述支付消息用于确认对所述交易信息进行支付；

所述验证单元，配置为通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；并在验证成功后触发所述划拨单元；

10 所述划拨单元，配置为将所述支付终端对应的用户账号中的所述待支付金额划拨至收款端。

在上述方案中，所述接收单元，还配置为接收由所述支付终端发送的第一公钥；

所述支付服务器还包括绑定单元，配置为将所述第一公钥与所述支付
15 终端对应的用户账号进行绑定。

在上述方案中，所述接收单元，还配置为接收由所述支付终端发送的临时账号请求；

所述支付服务器还包括生成单元，配置为生成与所述用户账号相关联的临时账号；其中，所述临时账号用于在预设的有效期内具有与所述用户
20 账号相同的支付功能且仅用于预设次数的支付；

发送单元，还配置为向支付终端发送临时账号，以使得支付终端生成与临时账号相关联的二维码。

在上述方案中，所述接收单元，还配置为接收由所述收款端通过扫描所述二维码后发送的交易请求；其中，所述交易请求包括所述收款端通过
25 解析所述二维码获取到的所述临时账号和待支付金额。

在上述方案中，当所述临时账号处于有效期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为所述生成单元重新生成的临时账号。

5 第三方面，本发明实施例提供了一种支付的方法，所述方法应用于一支付终端，所述方法包括：

接收到由支付服务器发送的交易信息之后，将获取到的生物特征信息与预存的生物特征对照信息进行比较；其中，所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；

10 当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名；其中，所述支付信息用于确认对所述交易信息进行支付；

将签名后的支付信息发送至所述支付服务器；其中，所述签名后的支付信息用于所述支付服务器通过与所述生物特征对照信息相关联的第一公
15 钥进行数字签名验证，且当验证成功时按照支付信息将所述支付终端对应的用户账号中的所述待支付的金额划拨至收款端。

在上述方案中，所述接收到由支付服务器发送的交易信息之前，所述方法还包括：

获取生物特征对照信息；

20 按照预设的密钥生成策略生成与所述生物特征对照信息相关联的密钥对；所述密钥对包括第一公钥和第一私钥；

将密钥对中的第一公钥发送至支付服务器；所述第一公钥用于所述支付服务器将所述第一公钥与所述支付终端对应的用户账号进行绑定。

在上述方案中，所述支付终端发起支付时，所述方法还包括：

25 所述支付终端向所述支付服务器发送临时账号请求；其中，所述临时

账号请求用于所述支付服务器生成与所述用户账号相关联的临时账号；

所述支付终端接收所述支付服务器发送的所述临时账号，并生成与所述临时账号相关联的二维码；其中，所述临时账号用于在预设的有效期内具有与所述用户账号相同的支付功能且仅用于预设次数的支付；所述二维码用于收款端扫描后向所述支付服务器发送交易请求；所述交易请求包括所述收款端通过解析所述二维码获取到的所述临时账号和待支付金额。

在上述方案中，当所述临时账号处于有效期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为所述支付服务器重新生成的临时账号。

在上述方案中，所述支付终端存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法进行获取。

第四方面，本发明实施例提供了一种支付的方法，所述方法应用于一支付服务器，所述方法包括：

所述支付服务器向支付终端发送交易消息；其中，所述交易消息包括所述支付终端对应的用户账号信息和待支付的金额；

所述支付服务器接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后的支付消息；所述支付消息用于确认对所述交易信息进行支付；

所述支付服务器通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；

当验证成功时，所述支付服务器将所述支付终端对应的用户账号中的所述待支付金额划拨至收款端。

在上述方案中，所述支付服务器向支付终端发送交易消息之前，所述方法还包括：

所述支付服务器接收由所述支付终端发送的第一公钥；并将所述第一公钥与所述支付终端对应的用户账号进行绑定。

在上述方案中，所述支付终端发起支付时，所述方法还包括：

所述支付服务器接收由所述支付终端发送的临时账号请求；并生成与
5 所述用户账号相关联的临时账号，所述临时账号用于在预设的有效期内具有与
所述用户账号相同的支付功能且仅用于预设次数的支付；

所述支付服务器向所述支付终端发送所述临时账号，以使得所述支付终端生成与
所述临时账号相关联的二维码。

在上述方案中，所述支付服务器向所述支付终端发送所述临时账号之
10 后，且所述支付服务器向支付终端发送交易消息之前，所述方法还包括：

所述支付服务器接收由所述收款端通过扫描所述二维码后发送的交易请求；其中，
所述交易请求包括所述收款端通过解析所述二维码获取到的所述临时账号和待支付金额。

在上述方案中，当所述临时账号处于有效期内，则所述交易信息中所
15 包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为
所述支付服务器重新生成的临时账号。

第五方面，本发明实施例提供了一种支付系统，所述系统包括支付终端、收款端
和支付服务器；其中，

20 所述支付终端，配置为接收到由所述支付服务器发送的交易信息之后，将获取到的生物特征信息
与预存的生物特征对照信息进行比对；所述交易信息包括所述支付终端对应的用户账号信息
和待支付的金额；以及，

当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过与所述生物特征对照信息
相关联的第一私钥对支付信息进行数字签名；其中，
25 所述支付信息用于确认对所述交易信息进行支付，并且，所述支付终

端存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法进行获取；以及，

将签名后的支付信息发送至所述支付服务器；

所述支付服务器，配置为向所述支付终端发送交易消息；其中，所述
5 交易消息包括所述支付终端对应的用户账号信息和待支付的金额；以及，

接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后的支付消息；所述支付消息用于确认对所述交易信息进行支付；以及，

通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；以及，

10 当验证成功时，将所述支付终端对应的用户账号中的所述待支付金额划拨至所述收款端。

本发明实施例提供了一种计算机存储介质，所述计算机存储介质中存储有计算机程序，所述计算机程序用于执行以上所述的支付方法。

本发明实施例提供了一种支付的方法、设备和系统，通过与生物特征
15 信息对应的密钥对来执行支付中的验证过程，避免用户的生物特征信息的泄露，也避免了用户真实账号的泄露，提高了移动支付过程中的安全性。

附图说明

图 1 为本发明实施例提供的一种支付终端的结构示意图；

图 2 为本发明实施例提供的一种应用于支付终端的支付方法流程示意图；
20 图；

图 3 为本发明实施例提供的一种生物特征对照信息及对应的密钥对的生成流程示意图；

图 4 为本发明实施例提供的一种生成与用户账号对应的临时账号相关联的二维码的流程示意图；

25 图 5 为本发明实施例提供的一种支付服务器的结构示意图；

图 6 为本发明实施例提供的另一种支付服务器的结构示意图；

图 7 为本实施例提供的一种应用于支付服务器的支付方法流程示意图；

图 8 为本发明实施例提供的一种支付方法的详细流程示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述。

实施例一

如图 1，其示出了本发明实施例提供的一种支付终端 10 的结构，该终端 10 可以包括通过加密通道进行连接的获取单元 110 和支付信息处理单元 120、以及安装有支付应用程序的与支付信息处理单元 120 相连接的终端设备 130；终端设备 130 可以按照支付应用程序的指示实现本发明实施例所述的支付过程的功能；其中，

终端设备 130，配置为接收由支付服务器发送的交易信息；其中，所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；

获取单元 110，配置为获取生物特征信息，并将该生物特征信息传输至支付信息处理单元 120；在本发明实施例中，生物特征信息以指纹信息为例对技术方案进行说明，可以理解地，本领域技术人员可以将本发明实施例的技术方案应用于其他生物特征信息，例如眼纹、声纹等。本发明实施例对此不做赘述；

支付信息处理单元 120，配置为将生物特征信息与预存的生物特征对照信息进行比对；以及，

当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名；并将签名后的支付信息传输至终端设备 130；其中，所述支付信息用于确认对所述交易信息进行支付；

终端设备 130, 还配置为将签名后的支付信息发送至所述支付服务器; 其中, 所述签名后的支付信息用于所述支付服务器通过与所述生物特征对照信息相关联的第一公钥进行数字签名验证, 且当验证成功时按照支付信息将所述支付终端对应的用户账号中的所述待支付的金额划拨至收款端。

5 需要说明的是, 本实施例中所述的终端设备 130 可以是任一种具有支付应用的终端设备, 例如手机、平板电脑等。支付信息处理单元 120 可以是一种包括存储区域和处理器的具有硬件保护性能的装置, 该装置可以具有存储、运算及加解密的能力, 并且具有对存储的数据进行安全存储的能力, 使得被安全存储的数据能够不被导出和获取。获取单元 110 的具体结构可对应于处理器, 所述处理器具体的结构可以为中央处理器(CPU, Central Processing Unit)、微处理器(MCU, Micro Controller Unit)、数字信号处理器(DSP, Digital Signal Processing)或可编程逻辑器件(PLC, Programmable Logic Controller)等具有处理功能的电子元器件或电子元器件的集合。获取单元 110 和支付信息处理单元 120 可以通过 USB 等外设接口与终端设备 130 10 相连, 也可以通过总线连接设计成为终端设备 130 的一部分, 本实施例对此不做具体赘述。

示例性地, 获取单元 110, 还可以配置为获取生物特征对照信息; 并将生物特征对照信息传输至支付信息处理单元 120;

支付信息处理单元 120, 还配置为按照预设的密钥生成策略生成与生物特征对照信息相关联的密钥对; 并将密钥对中的第一公钥传输至终端设备 130; 其中, 密钥对包括第一公钥和第一私钥;

终端设备 130, 还配置为将密钥对中的第一公钥发送至支付服务器; 所述第一公钥用于支付服务器将第一公钥与支付终端对应的用户账号进行绑定。

25 示例性地, 终端设备 130, 还配置为向支付服务器发送临时账号请求;

其中，临时账号请求用于支付服务器生成与用户账号相关联的临时账号；以及，接收支付服务器发送的临时账号，并生成与临时账号相关联的二维码；其中，临时账号用于在预设的有效期内具有与用户账号相同的支付功能且仅用于预设次数的支付；所述二维码用于收款端扫描后向所述支付服务器发送交易请求；所述交易请求包括所述收款端通过解析所述二维码获取到的所述临时账号和待支付金额。

进一步地，当所述临时账号处于有效期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为所述支付服务器重新生成的临时账号；可以理解地，此时终端设备 130 可以重新向支付服务器发送临时账号请求，从而获得支付服务器重新生成的临时账号。

示例性地，由于支付信息处理单元 120 具有硬件保护性能，因此，支付信息处理单元 120 所存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法通过终端设备 130 进行获取。

本实施例提供了一种支付终端 10 的结构，通过与生物特征信息对应的密钥对来执行支付中的验证过程，避免用户的生物特征信息的泄露，也避免了用户真实账号的泄露，提高了移动支付过程中的安全性。

实施例二

基于实施例一所述的支付终端，参见图 2，其示出了本实施例提供的一种应用于前述实施例中所所述的支付终端的支付方法流程，该方法可以包括：

S210：接收到由支付服务器发送的交易信息之后，将获取到的生物特征信息与预存的生物特征对照信息进行比对；

其中，所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；

S220: 当所述获取到的生物特征信息与所述生物特征对照信息一致时, 通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名;

其中, 所述支付信息用于确认对所述交易信息进行支付;

5 S230: 将签名后的支付信息发送至所述支付服务器;

其中, 所述签名后的支付信息用于所述支付服务器通过与所述生物特征对照信息相关联的第一公钥进行数字签名验证, 且当验证成功时按照支付信息将所述支付终端对应的用户账号中的所述待支付的金额划拨至收款端。

10 需要说明的是, 所述支付终端存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法通过终端进行获取。

示例性地, 参见图 3, 在接收到由支付服务器发送的交易信息之前, 该方法还包括生物特征对照信息及对应的密钥对的生成过程:

S200: 获取生物特征对照信息;

15 S201: 按照预设的密钥生成策略生成与所述生物特征对照信息相关联的密钥对; 所述密钥对包括第一公钥和第一私钥;

S202: 将密钥对中的第一公钥发送至支付服务器; 所述第一公钥用于所述支付服务器将所述第一公钥与所述支付终端对应的用户账号进行绑定。

20 示例性地, 参见图 4, 支付终端发起支付时, 该方法还包括生成与用户账号对应的临时账号相关联的二维码的过程, 具体包括:

S203: 支付终端向支付服务器发送临时账号请求;

其中, 所述临时账号请求用于所述支付服务器生成与所述用户账号相关联的临时账号;

25 S204: 支付终端接收支付服务器发送的临时账号, 并生成与临时账号

相关联的二维码;

其中, 所述临时账号用于在预设的有效期内具有与所述用户账号相同的支付功能且仅用于预设次数的支付; 所述二维码用于收款端扫描后向所述支付服务器发送交易请求; 所述交易请求包括所述收款端通过解析所述
5 二维码获取到的所述临时账号和待支付金额。

进一步地, 当所述临时账号处于有效期内, 则所述交易信息中所包括的用户账号信息为所述临时账号;

当所述临时账号不处于有效期内, 则所述交易信息中所包括的用户账号信息为所述支付服务器重新生成的临时账号, 可以理解地, 此时支付终端可以重新向支付服务器发送临时账号请求, 从而获得支付服务器重新生成
10 的临时账号。

本实施例提供了一种应用于支付终端的支付方法, 通过与生物特征信息对应的密钥对来执行支付中的验证过程, 避免用户的生物特征信息的泄露, 也避免了用户真实账号的泄露, 提高了移动支付过程中的安全性。

15 实施例三

基于前述实施例相同的技术构思, 参见图 5, 其示出了本发明实施例提供的一种支付服务器 50 的结构, 该支付服务器 50 可以包括: 发送单元 510、接收单元 520、验证单元 530 和划拨单元 540; 其中,

发送单元 510, 配置为向支付终端发送交易消息; 其中, 所述交易消息
20 包括所述支付终端对应的用户账号信息和待支付的金额;

接收单元 520, 配置为接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后的支付消息; 所述支付消息用于确认对所述交易信息进行支付;

验证单元 530, 配置为通过所述支付终端的第一公钥对所述签名后的支付消息进行验证; 并在验证成功后触发划拨单元 540;

25

划拨单元 540, 配置为将所述支付终端对应的用户账号中的所述待支付金额划拨至收款端。

示例性地, 接收单元 520, 还配置为接收由所述支付终端发送的第一公钥; 参见图 6, 支付服务器 50 还包括绑定单元 550, 配置为将所述第一公
5 钥与所述支付终端对应的用户账号进行绑定。

示例性地, 接收单元 520, 还配置为接收由支付终端发送的临时账号请求;

参见图 6, 支付服务器 50 还包括生成单元 560, 配置为生成与用户账号相关联的临时账号; 其中, 所述临时账号用于在预设的有效期内具有与
10 所述用户账号相同的支付功能且仅用于预设次数的支付;

发送单元 510, 还配置为向支付终端发送临时账号, 以使得支付终端生成与临时账号相关联的二维码。

进一步地, 接收单元 520, 还配置为接收由所述收款端通过扫描所述二维码后发送的交易请求; 其中, 所述交易请求包括所述收款端通过解析所
15 述二维码获取到的所述临时账号和待支付金额。

进一步地, 当所述临时账号处于有效期内, 则所述交易信息中所包括的用户账号信息为所述临时账号;

当所述临时账号不处于有效期内, 则所述交易信息中所包括的用户账号信息为生成单元 560 重新生成的临时账号, 可以理解地, 此时接收单元
20 520 可以接受由支付终端重新发送的临时账号请求, 从而生成单元 560 能够重新生成的临时账号。

实际应用中, 所述接发送单元 510、接收单元 520、验证单元 530、划拨单元 540、绑定单元 550、生成单元 560 的具体结构均可对应于处理器。
所述处理器具体的结构可以为 CPU、MCU、DSP 或 PLC 等具有处理功能的
25 电子元器件或电子元器件的集合。其中, 所述处理器包括可执行代码, 所

述可执行代码存储在存储介质中，所述处理器可以通过总线等通信接口与所述存储介质中相连，在执行具体的各模块的对应功能时，从所述存储介质中读取并运行所述可执行代码。所述存储介质用于存储所述可执行代码的部分优选为非瞬间存储介质。

5 上述接发送单元 510、接收单元 520、验证单元 530、划拨单元 540、绑定单元 550、生成单元 560 可以集成对应于同一处理器，或分别对应不同的处理器；当集成对应于同一处理器时，所述处理器采用时分处理所述接发送单元 510、接收单元 520、验证单元 530、划拨单元 540、绑定单元 550、生成单元 560 对应的功能。

10 本实施例提供了一种支付服务器 50 的结构，通过与生物特征信息对应的密钥对来执行支付中的验证过程，避免用户的生物特征信息的泄露，也避免了用户真实账号的泄露提高了移动支付过程中的安全性。

实施例四

15 基于实施例三所述的支付服务器，参见图 7，其示出了本实施例提供了一种应用于前述实施例中所所述的支付服务器的支付方法流程，该方法可以包括：

S710: 支付服务器向支付终端发送交易消息；

其中，所述交易消息包括支付终端对应的用户账号信息和待支付的金额；

20 S720: 支付服务器接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后的支付消息；

其中，所述支付消息用于确认对所述交易信息进行支付；

S730: 支付服务器通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；

25 S740: 当验证成功时，支付服务器将所述支付终端对应的用户账号中

的所述待支付金额划拨至收款端。

示例性地，在支付服务器向支付终端发送交易消息之前，还可以包括：

支付服务器接收由所述支付终端发送的第一公钥；并将所述第一公钥与所述支付终端对应的用户账号进行绑定。

5 示例性地，支付终端发起支付时，还可以包括：

支付服务器接收由所述支付终端发送的临时账号请求；并生成与所述用户账号相关联的临时账号；以及，

支付服务器向所述支付终端发送所述临时账号，以使得所述支付终端生成与所述临时账号相关联的二维码。

10 其中，所述临时账号用于在预设的有效期内具有与所述用户账号相同的支付功能且仅用于预设次数的支付。

需要说明的是，当所述临时账号处于有效期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为支付服务器重新生成的临时账号，可以理解地，此时支付服务器
15 可以接受由支付终端重新发送的临时账号请求，从而支付服务器能够重新生成的临时账号。

进一步地，在支付服务器向所述支付终端发送所述临时账号之后，且所述支付服务器向支付终端发送交易消息之前，还可以包括：

20 所述支付服务器接收由所述收款端通过扫描所述二维码后发送的交易请求；其中，所述交易请求包括所述收款端通过解析所述二维码获取到的所述临时账号和待支付金额。

本实施例提供了一种应用于支付服务器的支付方法，通过与生物特征信息对应的密钥对来执行支付中的验证过程，避免用户的生物特征信息的
25 泄露，也避免了用户真实账号的泄露提高了移动支付过程中的安全性。

实施例五

基于前述实施例相同的技术构思，参见图 8，其示出了本发明实施例提供的一种支付方法的详细流程，该流程中，生物特征信息以指纹为例进行技术方案的说明，该流程可以包括：

5 S801：支付终端通过鉴权之后，向支付服务器发送指纹绑定请求；

 S802：支付服务器向支付终端发送指纹绑定指令；

 S803：支付终端获取对照指纹，并按照预设的密钥生成策略生成与对照指纹相关联的密钥对；

 其中，密钥对包括第一公钥和第一私钥；

10 具体地，可以由支付终端中的获取单元来获取对照指纹，可以由支付信息处理单元生成并存储与对照指纹相关联的密钥对；

 S804：支付终端将密钥对中的第一公钥发送至支付服务器；

 S805：支付服务器将第一公钥与支付终端对应的用户账号进行绑定；

15 可以理解地，S801 至 S805 实现了对照指纹的获取以及对照指纹对应的密钥对的生成，从而可以使得在后续支付验证过程中，通过验证密钥对而非验证指纹信息来进行支付验证，从而可以降低指纹信息的泄露风险。

 当需要发起支付交易时，该流程继续可以包括：

 S806：支付终端向支付服务器发送临时账号请求；

20 其中，所述临时账号请求用于所述支付服务器生成与用户账号相关联的临时账号；

 S807：支付服务器生成与用户账号相关联的临时账号；

 需要说明的是，临时账号与用户账号的组成结构一致，因此，临时账号可以用于在预设的有效期内具有与所述用户账号相同的支付功能且仅用于预设次数的支付；由于使用了临时账号来替代用户账号的支付功能，因此，在具体支付过程中，支付终端和商户收款端均无法获取真实的用户账

25

号信息，从而保证了真实的用户账号的安全，而且，由于临时账号仅用于预设次数的支付，因此，还能保证了用户账号中的资金安全。

S808: 支付服务器向支付终端发送所述临时账号；

S809: 支付终端生成与临时账号相关联的二维码；

5 S810: 收款端扫描二维码，并根据二维码解析出临时账号；

可以理解地，收款端可以是进行交易的商户，通过二维码扫描器对临时账号相关联的二维码进行扫描。

S811: 收款端将解析出的临时账号和待支付金额封装成交易请求发送至支付服务器；

10 S812: 支付服务器根据交易请求向支付终端发送交易信息；

其中，交易信息包括支付终端对应的用户账号信息和待支付的金额；

需要说明的是，当临时账号处于有效期内，则交易信息中所包括的用户账号信息为所述临时账号；当临时账号不处于有效期内，则交易信息中所包括的用户账号信息为所述支付服务器重新生成的临时账号；

15 S813: 支付终端获取用户的指纹，并将获取到的指纹与对照指纹进行比对；

S814: 当获取到的指纹与对照指纹一致时，支付终端通过与对照指纹相关联的第一私钥对支付信息进行数字签名；

其中，支付信息用于确认对所述交易信息进行支付；

20 可以理解地，支付终端可以通过获取单元来获取用户的指纹，可以通过支付信息处理单元进行指纹比对以及对支付信息的数字签名。

S815: 支付终端将签名后的支付信息发送至支付服务器；

S816: 支付服务器通过支付终端的第一公钥对签名后的支付消息进行验证；

25 S817: 当验证成功时，支付服务器将所述支付终端对应的用户账号中

的所述待支付金额划拨至收款端。

可以理解地，当资金划拨完毕后，支付服务器可以通知收款端和支付终端。

本实施例提供了一种支付方法的详细流程，通过与生物特征信息对应的
5 的密钥对来执行支付中的验证过程，避免用户的生物特征信息的泄露，也避免了用户真实账号的泄露提高了移动支付过程中的安全性。

实施例六

前述实施例对本发明实施例的技术方案中的两个重要的执行主体，即支付终端和支付服务器的结构进行了描述，在此基础上本实施例还提出了一种支付的系统，该系统可以包括支付终端、收款端和支付服务器；其中，
10 一种支付的系统，该系统可以包括支付终端、收款端和支付服务器；其中，

支付终端，配置为接收到由支付服务器发送的交易信息之后，将获取到的生物特征信息与预存的生物特征对照信息进行比较；所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；以及，

当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过
15 与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名；其中，所述支付信息用于确认对所述交易信息进行支付，并且，所述支付终端存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法通过终端进行获取；以及，

将签名后的支付信息发送至所述支付服务器；其中，所述签名后的支付信息用于所述支付服务器通过与所述生物特征对照信息相关联的第一公
20 钥进行数字签名验证，且当验证成功时按照支付信息将所述支付终端对应的用户账号中的所述待支付的金额划拨至收款端；

支付服务器，配置为向支付终端发送交易消息；其中，所述交易消息包括所述支付终端对应的用户账号信息和待支付的金额；以及，

25 接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后

的支付消息；所述支付消息用于确认对所述交易信息进行支付；以及，

通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；当验证成功时，将所述支付终端对应的用户账号中的所述待支付金额划拨至收款端。

5 可以理解地，本实施例中所涉及的支付终端可以为前述实施例中所述的支付终端；本实施例中所涉及的支付服务器可以为前述实施例中所述的支付服务器。

本发明实施例还记载了一种计算机存储介质，所述计算机存储介质中存储有计算机可执行指令，所述计算机可执行指令用于前述各实施例所述
10 的支付的方法。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘
15 存储器和光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、
20 嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理
25 设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存

存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

5 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

10 工业实用性

本发明实施例中，通过与生物特征信息对应的密钥对来执行支付中的验证过程，避免用户的生物特征信息的泄露，也避免了用户真实账号的泄露，提高了移动支付过程中的安全性。

权利要求书

1、一种支付终端，所述支付终端包括：通过加密通道进行连接的获取单元和支付信息处理单元、以及安装有支付应用程序的且与所述支付信息处理单元相连接的终端设备；其中，

5 所述终端设备，配置为接收由支付服务器发送的交易信息；其中，所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；

 所述获取单元，配置为获取生物特征信息，并将所述生物特征信息传输至所述支付信息处理单元；

 所述支付信息处理单元，配置为将所述生物特征信息与预存的生物特征对照信息进行比对；以及，

 当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名；并将签名后的支付信息传输至所述终端设备；其中，所述支付信息用于确认对所述交易信息进行支付；

15 所述终端设备，还配置为将所述签名后的支付信息发送至所述支付服务器；其中，所述签名后的支付信息用于所述支付服务器通过与所述生物特征对照信息相关联的第一公钥进行数字签名验证，且当验证成功时按照支付信息将所述支付终端对应的用户账号中的所述待支付的金额划拨至收款端。

20 2、根据权利要求 1 所述的支付终端，其中，所述获取单元，还可以配置为获取生物特征对照信息；并将生物特征对照信息传输至所述支付信息处理单元；

 所述支付信息处理单元，还配置为按照预设的密钥生成策略生成与生物特征对照信息相关联的密钥对；并将密钥对中的第一公钥传输至所述终端设备；其中，密钥对包括第一公钥和第一私钥；

25

所述终端设备，还配置为将密钥对中的第一公钥发送至支付服务器；
所述第一公钥用于支付服务器将第一公钥与支付终端对应的用户账号进行绑定。

3、根据权利要求 1 所述的支付终端，其中，所述终端设备，还配置为
5 向所述支付服务器发送临时账号请求；其中，所述临时账号请求用于所述
支付服务器生成与所述用户账号相关联的临时账号；以及，接收所述支付
服务器发送的临时账号，并生成与所述临时账号相关联的二维码；其中，
所述临时账号用于在预设的有效期内具有与用户账号相同的支付功能且仅
用于预设次数的支付；所述二维码用于收款端扫描后向所述支付服务器发
10 送交易请求；所述交易请求包括所述收款端通过解析所述二维码获取到的
所述临时账号和待支付金额。

4、根据权利要求 3 所述的支付终端，其中，当所述临时账号处于有效
期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账
15 号信息为所述支付服务器重新生成的临时账号。

5、根据权利要求 1 所述的支付终端，其中，所述支付信息处理单元存
储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法
通过所述终端设备进行获取。

6、一种支付服务器，其中，所述支付服务器包括：发送单元、接收单
20 元、验证单元和划拨单元；其中，

所述发送单元，配置为向支付终端发送交易消息；其中，所述交易消
息包括所述支付终端对应的用户账号信息和待支付的金额；

所述接收单元，配置为接收由所述支付终端发送的经过所述支付终端
的第一私钥数字签名后的支付消息；所述支付消息用于确认对所述交易信
25 息进行支付；

所述验证单元，配置为通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；并在验证成功后触发所述划拨单元；

所述划拨单元，配置为将所述支付终端对应的用户账号中的所述待支付金额划拨至收款端。

- 5 7、根据权利要求6所述的支付服务器，其中，所述接收单元，还配置为接收由所述支付终端发送的第一公钥；

所述支付服务器还包括绑定单元，配置为将所述第一公钥与所述支付终端对应的用户账号进行绑定。

- 10 8、根据权利要求6所述的支付服务器，其中，所述接收单元，还配置为接收由所述支付终端发送的临时账号请求；

所述支付服务器还包括生成单元，配置为生成与所述用户账号相关联的临时账号；其中，所述临时账号用于在预设的有效期内具有与所述用户账号相同的支付功能且仅用于预设次数的支付；

- 15 发送单元，还配置为向支付终端发送临时账号，以使得支付终端生成与临时账号相关联的二维码。

9、根据权利要求8所述的支付服务器，其中，所述接收单元，还配置为接收由所述收款端通过扫描所述二维码后发送的交易请求；其中，所述交易请求包括所述收款端通过解析所述二维码获取到的所述临时账号和待支付金额。

- 20 10、根据权利要求8所述的支付服务器，其中，当所述临时账号处于有效期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为所述生成单元重新生成的临时账号。

- 25 11、一种支付的方法，其中，所述方法应用于一支付终端，所述方法包括：

接收到由支付服务器发送的交易信息之后，将获取到的生物特征信息与预存的生物特征对照信息进行比较；其中，所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；

5 当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名；其中，所述支付信息用于确认对所述交易信息进行支付；

将签名后的支付信息发送至所述支付服务器；其中，所述签名后的支付信息用于所述支付服务器通过与所述生物特征对照信息相关联的第一公钥进行数字签名验证，且当验证成功时按照支付信息将所述支付终端对应的
10 的用户账号中的所述待支付的金额划拨至收款端。

12、根据权利要求 11 所述的方法，其中，所述接收到由支付服务器发送的交易信息之前，所述方法还包括：

获取生物特征对照信息；

按照预设的密钥生成策略生成与所述生物特征对照信息相关联的密钥
15 对；所述密钥对包括第一公钥和第一私钥；

将密钥对中的第一公钥发送至支付服务器；所述第一公钥用于所述支付服务器将所述第一公钥与所述支付终端对应的用户账号进行绑定。

13、根据权利要求 11 所述的方法，其中，所述支付终端发起支付时，所述方法还包括：

20 所述支付终端向所述支付服务器发送临时账号请求；其中，所述临时账号请求用于所述支付服务器生成与所述用户账号相关联的临时账号；

所述支付终端接收所述支付服务器发送的所述临时账号，并生成与所述临时账号相关联的二维码；其中，所述临时账号用于在预设的有效期内具有与所述用户账号相同的支付功能且仅用于预设次数的支付；所述二维
25 码用于收款端扫描后向所述支付服务器发送交易请求；所述交易请求包括

所述收款端通过解析所述二维码获取到的所述临时账号和待支付金额。

14、根据权利要求 13 所述的方法，其中，当所述临时账号处于有效期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为所述支付服务器重新生成的临时账号。

15、根据权利要求 11 所述的方法，其中，所述支付终端存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法进行获取。

16、一种支付的方法，其中，所述方法应用于一支付服务器，所述方法包括：

10 所述支付服务器向支付终端发送交易消息；其中，所述交易消息包括所述支付终端对应的用户账号信息和待支付的金额；

所述支付服务器接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后的支付消息；所述支付消息用于确认对所述交易信息进行支付；

15 所述支付服务器通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；

当验证成功时，所述支付服务器将所述支付终端对应的用户账号中的所述待支付金额划拨至收款端。

17、根据权利要求 16 所述的方法，其中，所述支付服务器向支付终端发送交易消息之前，所述方法还包括：

所述支付服务器接收由所述支付终端发送的第一公钥；并将所述第一公钥与所述支付终端对应的用户账号进行绑定。

18、根据权利要求 16 所述的方法，其中，所述支付终端发起支付时，所述方法还包括：

25 所述支付服务器接收由所述支付终端发送的临时账号请求；并生成与

所述用户账号相关联的临时账号，所述临时账号用于在预设的有效期内具有与所述用户账号相同的支付功能且仅用于预设次数的支付；

所述支付服务器向所述支付终端发送所述临时账号，以使得所述支付终端生成与所述临时账号相关联的二维码。

- 5 19、根据权利要求 18 所述的方法，其中，所述支付服务器向所述支付终端发送所述临时账号之后，且所述支付服务器向支付终端发送交易消息之前，所述方法还包括：

所述支付服务器接收由所述收款端通过扫描所述二维码后发送的交易请求；其中，所述交易请求包括所述收款端通过解析所述二维码获取到的
10 所述临时账号和待支付金额。

20、根据权利要求 18 所述的方法，其中，当所述临时账号处于有效期内，则所述交易信息中所包括的用户账号信息为所述临时账号；

当所述临时账号不处于有效期内，则所述交易信息中所包括的用户账号信息为所述支付服务器重新生成的临时账号。

- 15 21、一种支付系统，其中，所述系统包括支付终端、收款端和支付服务器；其中，

所述支付终端，配置为接收到由所述支付服务器发送的交易信息之后，将获取到的生物特征信息与预存的生物特征对照信息进行比对；所述交易信息包括所述支付终端对应的用户账号信息和待支付的金额；以及，

- 20 当所述获取到的生物特征信息与所述生物特征对照信息一致时，通过与所述生物特征对照信息相关联的第一私钥对支付信息进行数字签名；其中，所述支付信息用于确认对所述交易信息进行支付，并且，所述支付终端存储的所述生物特征对照信息及所述生物特征对照信息对应的第一私钥无法进行获取；以及，

- 25 将签名后的支付信息发送至所述支付服务器；

所述支付服务器，配置为向所述支付终端发送交易消息；其中，所述交易消息包括所述支付终端对应的用户账号信息和待支付的金额；以及，

接收由所述支付终端发送的经过所述支付终端的第一私钥数字签名后的支付消息；所述支付消息用于确认对所述交易信息进行支付；以及，

5 通过所述支付终端的第一公钥对所述签名后的支付消息进行验证；以及，

当验证成功时，将所述支付终端对应的用户账号中的所述待支付金额划拨至所述收款端。

22、一种计算机存储介质，所述计算机存储介质中存储有计算机可执行指令，所述计算机可执行指令用于执行权利要求 11 至 15 任一项所述的方法、和/或用于执行权利要求 16 至 20 任一项所述的方法。

10

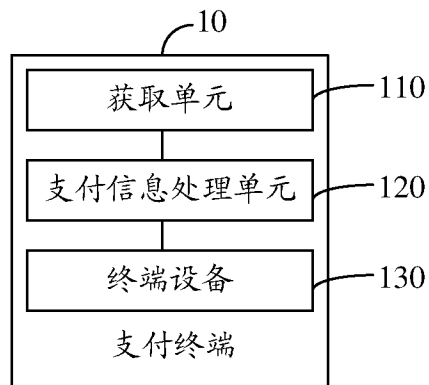


图 1

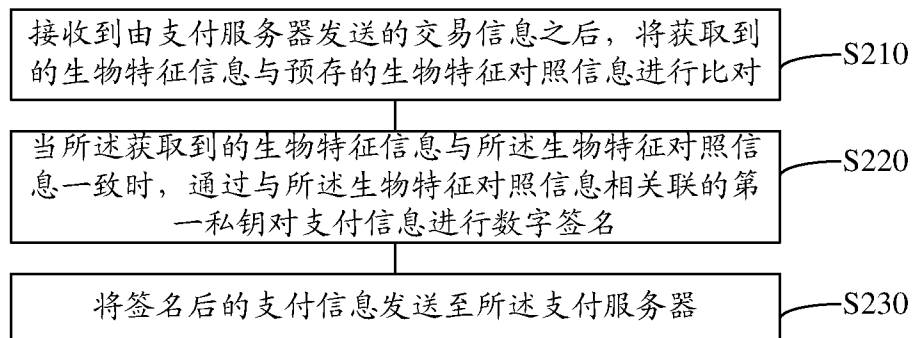


图 2

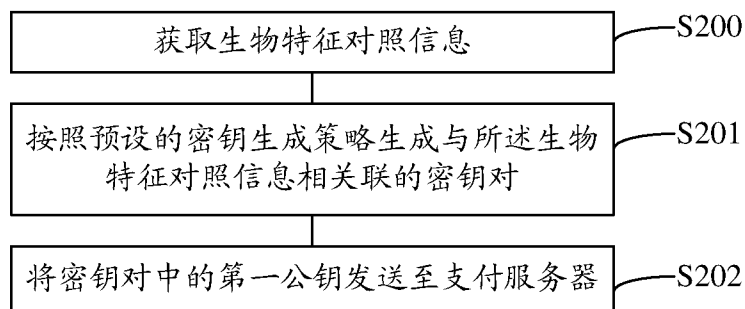


图 3

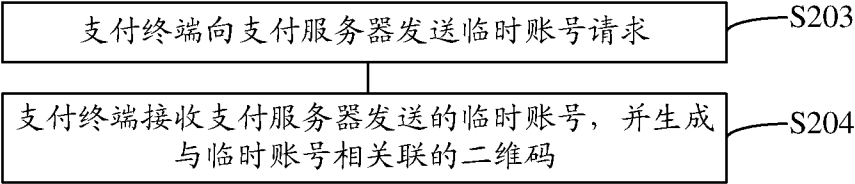


图 4

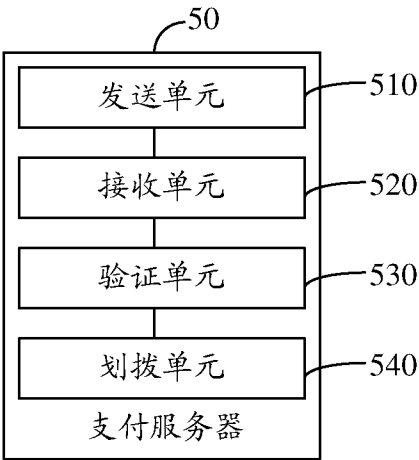


图 5

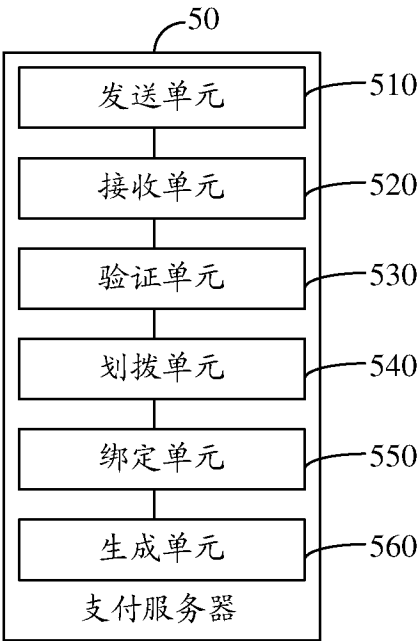


图 6

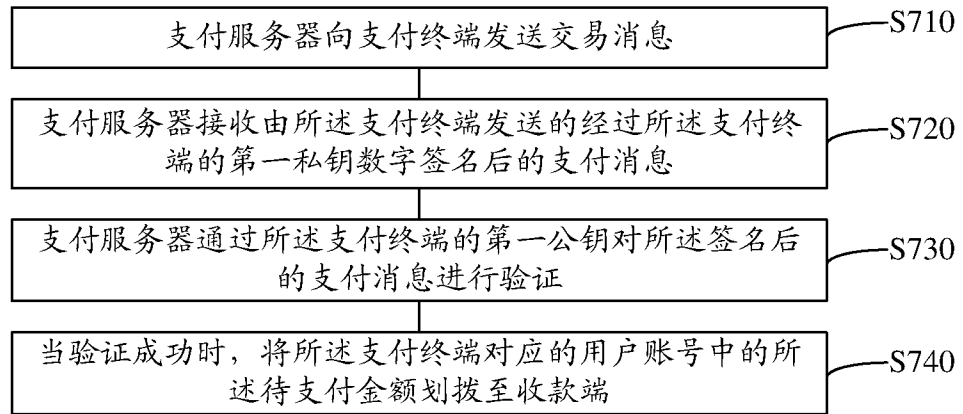


图 7

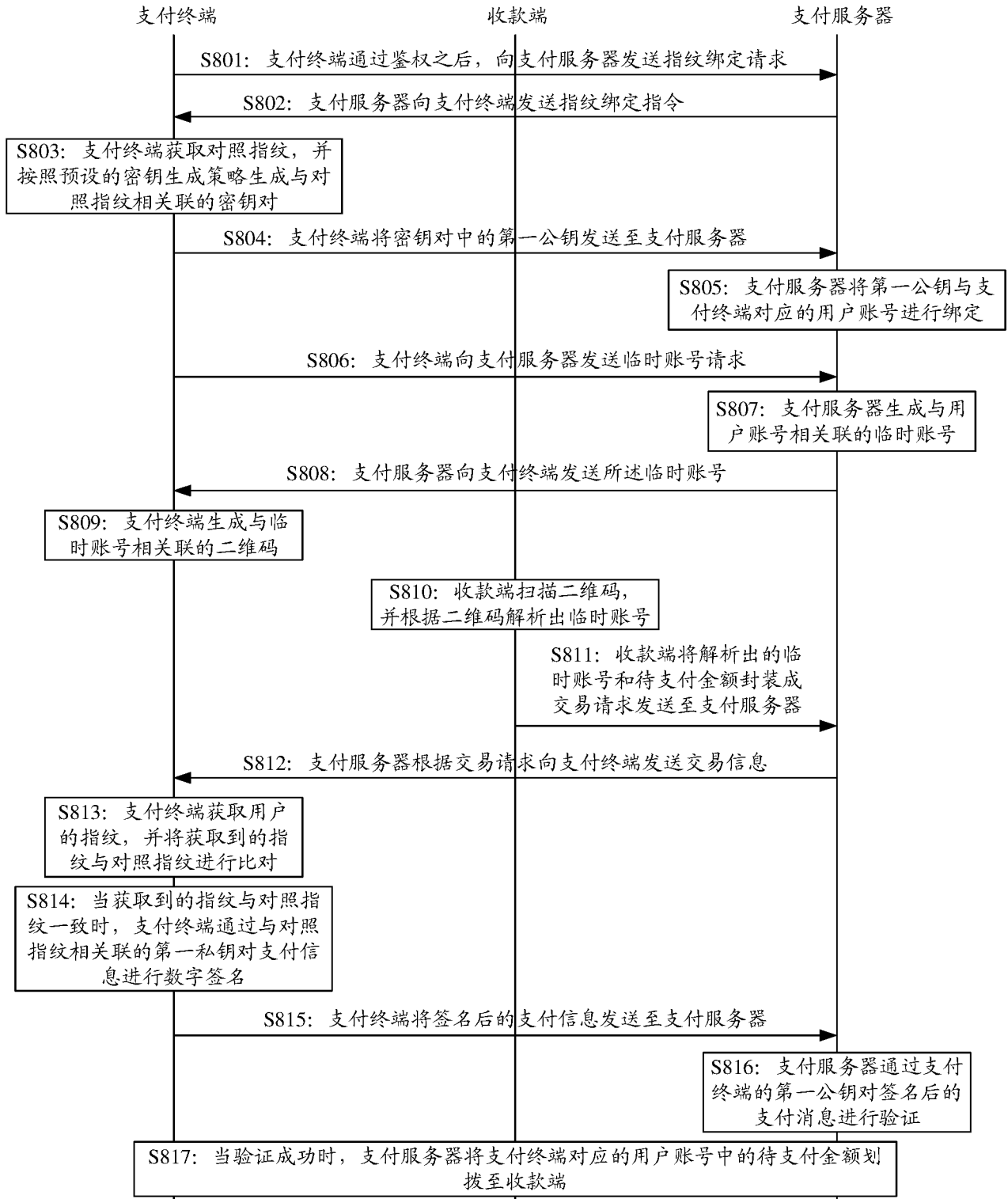


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/073748

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: digital signature, cipher, private key, pay, bio+, iris, fingerprint, key, digital, signature

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102880960 A (SHENZHEN ARATEK BIOMETRICS TECHNOLOGY CO., LTD.), 16 January 2013 (16.01.2013), description, [0038]-[0064], and figures 1 and 2	6-10, 16-20, 22
A	CN 102880960 A (SHENZHEN ARATEK BIOMETRICS TECHNOLOGY CO., LTD.), 16 January 2013 (16.01.2013), the whole document	1-5, 11-15, 21
A	CN 101340285 A (MIAXIS BIOMETRICS CO., LTD.), 07 January 2009 (07.01.2009), the whole document	1-22
A	CN 101692277 A (SUN YAT-SEN UNIVERSITY), 07 April 2010 (07.04.2010), the whole document	1-22
A	CN 103049850 A (SHENZHEN ZTE MOBILE TELECOM CO., LTD.), 17 April 2013 (17.04.2013), the whole document	1-22
A	CN 102521744 A (ZTE CORP.), 27 June 2012 (27.06.2012), the whole document	1-22

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 15 April 2016 (15.04.2016)	Date of mailing of the international search report 27 April 2016 (27.04.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer SU, Fei Telephone No.: (86-10) 62413632

International application No.
PCT/CN2016/073748

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2016/073748

A. 主题的分类

G06Q 20/40(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI, EPODOC, CNPAT, CNKI: 支付, 数字签名, 密码, 密钥, 私钥, 生物, 指纹, 虹膜, pay, bio+, iris, fingerprint, key, digital, signature

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 102880960 A (深圳市亚略特生物识别科技有限公司) 2013年 1月 16日 (2013 - 01 - 16) 说明书[0038]-[0064]、附图1-2	6-10, 16-20, 22
A	CN 102880960 A (深圳市亚略特生物识别科技有限公司) 2013年 1月 16日 (2013 - 01 - 16) 全文	1-5, 11-15, 21
A	CN 101340285 A (杭州中正生物认证技术有限公司) 2009年 1月 7日 (2009 - 01 - 07) 全文	1-22
A	CN 101692277 A (中山大学) 2010年 4月 7日 (2010 - 04 - 07) 全文	1-22
A	CN 103049850 A (深圳市中兴移动通信有限公司) 2013年 4月 17日 (2013 - 04 - 17) 全文	1-22
A	CN 102521744 A (中兴通讯股份有限公司) 2012年 6月 27日 (2012 - 06 - 27) 全文	1-22

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 4月 15日

国际检索报告邮寄日期

2016年 4月 27日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

苏菲

传真号 (86-10)62019451

电话号码 (86-10)62413632

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/073748

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	102880960	A	2013年 1月 16日	无			
CN	101340285	A	2009年 1月 7日	无			
CN	101692277	A	2010年 4月 7日	无			
CN	103049850	A	2013年 4月 17日	无			
CN	102521744	A	2012年 6月 27日	WO	2013097358	A1	2013年 7月 4日

表 PCT/ISA/210 (同族专利附件) (2009年7月)