(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
2018 年 1 月 4 日 (04.01.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/000275 A1

(51) 国际专利分类号:
G06Q 20/38 (2012.01)

(21) 国际申请号: PCT/CN2016/087763

(22) 国际申请日: 2016 年 6 月 29 日 (29.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 李国庆 (LI, Guoqing); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 梅敬青 (MEI, Jingqing); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区知春路7号致真大厦A1304-05室, Beijing 100191 (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)。

(54) **Title:** PAYMENT VERIFICATION METHOD AND APPARATUS

(54) **发明名称**: 一种支付验证方法及装置

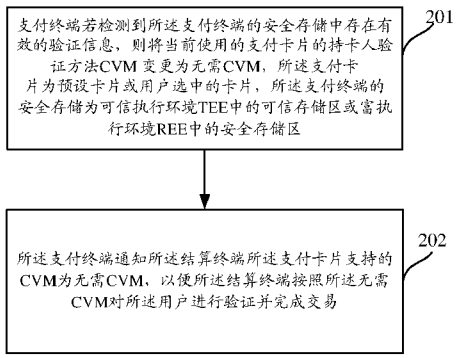


图 2

201 If a payment terminal detects that valid verification information is present in a secure memory of said payment terminal, then a cardholder verification method (CVM) for the payment card currently being used is altered to a non-CVM, said payment card being a default card or a card selected by a user, said secure memory of said payment terminal being a trusted memory area within a trusted execution environment (TEE) or a secure memory area within a rich execution environment (REE)

202 Said payment terminal informs a settlement terminal that the CVM supported by said payment card is a non-CVM, so that said settlement terminal carries out validation of said user and completes a transaction according to the non-CVM.

(57) **Abstract:** A payment verification method and apparatus, comprising: if a payment terminal detects that valid verification information is present in a secure memory of said payment terminal, then a cardholder verification method (CVM) for the payment card currently being used is altered to a non-CVM, said payment card being a default card or a card selected by a user, and said secure memory of said payment terminal being a trusted memory area within a trusted execution environment (TEE) or a secure memory area within a rich execution environment (REE); said payment terminal informs a settlement terminal that the CVM supported by said payment card is a non-CVM, so that said settlement terminal carries out validation of said user and completes a transaction according to the non-CVM.

(57) **摘要**: 一种支付验证方法及装置，包括：支付终端若检测到所述支付终端的安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法CVM变更为无需CVM，所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境TEE中的可信存储区或富执行环境REE中的安全存储区；所述支付终端通知所述结算终端所述支付卡片支持的CVM为无需CVM，以便所述结算终端按照所述无需CVM对所述用户进行验证并完成交易。

WO 2018/000275 A1

[见续页]

根据细则4.17的声明：

— 关于申请人有权申请并被授予专利(细则4.17(ii))

本国际公布：

— 包括国际检索报告(条约第21条(3))。

一种支付验证方法及装置

技术领域

本申请涉及移动支付技术领域，尤其涉及一种支付验证方法及装置。

背景技术

持卡人验证方法（Cardholder Verification Method，CVM）是银行卡发卡行验证持卡人身份、防止银行卡被盗用的方法，CVM 要求持卡人使用银行卡支付时向发卡行提供证明自己是卡片主人的验证数据(如 PIN（Personal Identification Number，个人识别码）码，签名等)，发卡行收到验证数据后对验证数据进行验证(联机验证)，根据验证的结果确定此次交易成功或拒绝此次交易。近年来，Mastercard、Visa 等国际卡组织定义了一种新的持卡人验证方法：消费者设备持卡人验证方法(Consumer Device Cardholder Verification Method，CD-CVM)，该验证方法主要应用于使用移动终端作为支付终端进行非接触支付的场景，例如 Apple Pay，Samsung Pay 等，可避免用户交易时在 POS(Point of Sale，销售点) 机上输入 PIN 码。在进行非接触支付交易时，持卡人可以先在支付终端上选择一张卡片，通过支付终端输入身份验证数据，然后持卡人使用支付终端触碰非接触(Contactless)POS 机，非接触 POS 机接收支付终端发送的交易数据后进行处理，如 POS 机也支持 CD-CVM，则 POS 认为正在使用的卡片已经通过持卡人验证，可继续后续流程完成支付交易。

然而，目前市场上存在大量已经部署的非接触 POS 机，并未支持新出现的持卡人验证方式 CD-CVM。在 POS 机不支持 CD-CVM 的情况下，用户使用支付终端进行非接触支付时，POS 机即使收到卡片发送的支持 CD-CVM 的交易请求消息，也不能正确的通过持卡人验证，这将导致用户需要额外的在 POS 机上输入 PIN 码或签名，否则支付交易无法完成。这导致了非接触支付用户体验的降低。

发明内容

本申请实施例提供一种支付验证方法及装置，用于在 POS 机不支持 CD-CVM 的情况下，实现使用支付终端利用终端侧的用户身份验证来取代非接触 POS 机要求的输入 PIN 码或签名操作。

本申请实施例提供一种支付验证方法，包括:

支付终端若检测到所述支付终端的安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区;

所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

根据本申请实施例提供的方法，支付终端在确定持卡人的身份验证通过后，向结算终端发送持卡人验证方法变更消息，从而将当前支付交易的持卡人身份验证方法变更为无需持卡人验证，从而无需结算终端对持卡人进行身份验证，从而实现使用支付终端利用终端侧的用户身份验证来取代非接触 POS 机要求的输入 PIN 码或签名操作。

可选的，所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM 之前，还包括:

所述支付终端若检测到所述支付终端的安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求;

所述支付终端接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

通过上述方法，所述支付终端可以通过云验证服务器获得验证信息，从而可以避免在本地不存在有效的验证信息时，无法获得验证信息，从而可以在保证交易安全的同时提高支付交易体验。

可选的，所述支付终端检测到所述支付终端的安全存储中存在有效的验

证信息之前，还包括:

所述支付终端接收第一身份验证数据，并确定所述第一身份验证数据与所述支付终端的安全存储中保存的第二身份验证数据匹配。

通过上述方法，支付终端通过第二身份验证数据对用户的第一身份验证数据进行验证，从而提高支付交易的安全性。

可选的，所述验证信息包含有效期参数;

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在所述预设有效时间内有效;

所述支付终端检测到所述支付终端的安全存储中存在有效的验证信息，包括:

所述支付终端检测到所述支付终端的安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

可选的，所述验证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效;

所述支付终端检测到所述支付终端的安全存储中存在有效的验证信息，包括:

所述支付终端检测到所述支付终端的安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

可选的，所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM 之前，还包括:

所述支付终端获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法;

所述支付终端根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证方法 CD-CVM。

通过上述方法，可以预先根据结算终端的终端交易属性确定所述结算终

端是否支持 CD-CVM，从而可以在确定所述结算终端不支持 CD-CVM 时，将当前使用的支付卡片的 CVM 变更为无需 CVM。

可选的，所述支付终端获取所述结算终端的终端交易属性，包括:

所述支付终端向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述支付终端在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的；或者

所述支付终端通过扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

所述支付终端通过接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

可选的，所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM 之后，还包括:

所述支付终端接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易;

所述支付终端将所述交易日志同步到云验证服务器。

本申请实施例提供一种支付验证装置，该装置包括:

处理单元，用于若检测到安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区;

收发单元，用于通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

可选的，所述处理单元还用于:

若检测到所述安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求;

所述收发单元，还用于接收所述云验证服务器返回的验证信息；所述验

证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

可选的，所述收发单元还用于：

接收第一身份验证数据，并确定所述第一身份验证数据与所述安全存储中保存的第二身份验证数据匹配。

可选的，所述验证信息包含有效期参数；

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在所述预设有效时间内有效；

所述处理单元具体用于：

检测到所述安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

可选的，所述验证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效；

所述处理单元具体用于：

检测到所述安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

可选的，所述收发单元还用于：

获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法；

根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证方法 CD-CVM。

可选的，所述收发单元具体用于：

向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述装置在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的；或者

通过扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

通过接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

可选的，所述收发单元还用于:

接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易;

将所述交易日志同步到云验证服务器。

本申请实施例提供一种支付终端，包括：处理器、近场通信 NFC 模块;

所述处理器，用于若检测到所述支付终端的安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区;

所述 NFC 模块，用于通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

可选的，所述支付终端中还包括收发机和 Wi-Fi 模块;

所述处理器还用于:

若检测到所述安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求;

所述收发机或所述 Wi-Fi 模块，还用于接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

可选的，所述支付终端中还包括收发机和 Wi-Fi 模块;

所述收发机或所述 Wi-Fi 模块，用于接收第一身份验证数据;

所述处理器，用于确定所述第一身份验证数据与所述安全存储中保存的第二身份验证数据匹配。

可选的，所述验证信息包含有效期参数;

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在所述预设有效时间内有效;

所述处理器具体用于:

检测到所述安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

可选的，所述验证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效;

所述处理器具体用于:

检测到所述安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

可选的，所述 NFC 模块还用于:

获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法;

所述处理器还用于：根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证方法 CD-CVM。

可选的，所述支付终端中还包括蓝牙模块以及图像采集模块:

所述支付终端通过所述 NFC 模块向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述支付终端在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的;

或者

所述支付终端通过所述图像采集模块扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

所述支付终端通过所述蓝牙模块接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

可选的，所述支付终端中还包括收发机和 Wi-Fi 模块：所述收发机或所述 Wi-Fi 模块用于:

接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交

易的类型标记为 CVM 降级交易;

将所述交易日志同步到云验证服务器。

附图说明

图 1 为本申请实施例提供的一种支付终端系统结构示意图;

图 2 为本申请实施例提供的一种支付验证方法流程示意图;

图 3 为本申请实施例提供的一种支付交易示意图;

图 4 为本申请实施例提供的一种支付交易流程示意图;

图 5 为本申请实施例提供的一种支付交易流程示意图;

图 6 为本申请实施例提供的一种支付验证装置结构示意图;

图 7 为本申请实施例提供的一种支付终端结构示意图。

具体实施方式

下面结合说明书附图对本申请实施例做详细描述。

本申请实施例中，支付终端可以是无线终端，例如可以为移动电话、计算机、平板电脑、个人数码助理（英文：personal digital assistant，缩写：PDA）、移动互联网设备（英文：mobile Internet device，缩写：MID）、可穿戴设备和电子书阅读器（英文：e-book reader）等。

本申请实施例中，结算终端可以是非接触 POS 机，或者具有非接触 POS 机功能的其他设备。

利用具有非接触通信接口(例如，NFC（Near Field Communication，近场通信）接口)和 SE(Secure Element，安全单元)的支付终端可模拟物理卡片，进行非接触支付，这个功能称之为卡模拟(Card Emulation，CE)功能。支付终端需要将其模拟的卡片数据(如用户主账号、有效期、卡片密钥等)保存在 SE 中。近年来为了推广非接触支付(例如，NFC 支付)，Google 在 Android 系统中增加了对主机卡模拟(Host-based Card Emulation，HCE)的支持，使得银行或第三方支付机构可以更方便的开发和部署利用支付终端的非接触通信接口的支付应

用。与将卡片数据保存于 SE 中不同，HCE 一般将支付相关数据保存在云端即支付平台端，运行于 Android 系统中的应用获取云端保存的账户数据后可利用支付终端的 CPU（Central Processing Unit，中央处理器）模拟一张物理卡片完成非接触支付。为确保 HCE 支付应用的信息安全，一般支付应用可以设置数字或图案锁定密码，进入 HCE 支付应用需用户提供解码锁。此外，银行为了防欺诈，使用支付终端模拟卡片进行非接触支付时也需要执行持卡人验证如输入 PIN 码或签名等，这导致了 HCE 应用需要输入两次 PIN 码，降低了非接触支付的优良体验。

本申请实施例中，支付终端具有非接触通信接口(例如，近场通信 NFC 接口)，可以安装 HCE 应用程序，支付终端还可包括 TEE（Trust Execution Environment，可信执行环境）以及 REE（Rich Execution Environment，富执行环境）。HCE 应用程序主要的业务逻辑在 REE 中运行。

具体的，如图 1 所示，为本申请实施例提供的一种支付终端系统结构示意图。图 1 中，支付终端包括身份验证数据输入模块、本地身份验证数据验证模块、云身份验证数据管理模块、POS 信息获取模块(非必选)以及卡片 CVM 管理模块，优选地，上述模块在 TEE 中实现。

其中，身份验证数据输入模块用于为用户提供输入 PIN、签名、指纹等身份验证数据的输入界面，可以通过可信用户界面（Trusted User Interface，TUI）实现。

本地身份验证数据验证模块，用于对用户输入的 PIN、签名、指纹等身份验证数据进行本地验证。

云身份验证数据管理模块，用于管理保存在 TEE 的可信存储中的验证信息；验证信息通过支付终端向云验证服务器提交包含验证参数的身份验证请求获得，验证信息可以包含有效期参数。验证信息可以为 Access Tocken（接入令牌）或者云验证服务器设置的支付交易次数等。用户输入身份验证数据，通过本地身份认证之后，用户程序可以访问 TEE 可信存储中自己的存储区，并获得保存在存储区中的验证信息并检查其有效期；如验证信息失效，则用

户程序还可获得保存于 TEE 可信存储中的用户数据(如用户程序账户及密码、用户程序绑定的卡片的主账号、有效期、持卡人联系电话等)并向云验证服务器发送验证请求，以便重新获取验证信息。

POS 信息获取模块，用于获取 POS 机的描述信息和/或终端交易属性，例如，商户编号、POS 机编号、收单行信息等描述信息，和/或 POS 支持的 CVM 方法等终端交易属性信息。

卡片 CVM 管理模块，用于管理支付终端模拟的卡片的 CVM 列表。支付终端有能力模拟多张支付卡片，每张支付卡片具有一个 CVM 列表，每个 CVM 列表可包含一个或多个 CVM。

举例来说，一张支付卡片的 CVM 列表可以如表 1 所示。

CVM 编码	CVM
0100 0010 0000 0011	联机 PIN
0100 0001 0000 0011	脱机 PIN
0001 1110 0000 0011	签名
0001 1111 0000 0000	无需 CVM

表 1

需要说明的是，无需 CVM 是一种特殊的 CVM，它的安全级别最低，在进行支付交易时，结算终端若确定支付卡片的验证方法为无需 CVM，则直接确认持卡人验证成功，不需要再进行持卡人验证。一般情况下，在交易金额小于预设值时可以采用此方法，从而可以提高交易速度，提升用户的交易体验。

基于上述论述，如图 2 所示，本申请实施例提供的一种支付验证方法流程示意图。

如图 2 所示，该方法具体包括以下步骤:

步骤 201: 支付终端若检测到所述支付终端的安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，

所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区；

步骤 202：所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

步骤 201 之前，支付终端会接收到用户启动 HCE 应用程序的请求，此时支付终端会提示用户输入第一身份验证数据以便通过本地身份验证后进入 HCE 应用程序界面。支付终端接收到的第一身份验证数据包括但不限于指纹、PIN、声音（声纹）、签名、虹膜图像。

结合图 1，支付终端可以通过身份验证数据输入模块接收用户输入的第一身份验证数据。

支付终端在获得用户输入的第一身份验证数据之后，可以对用户输入的第一身份验证数据进行本地验证。结合图 1，支付终端可以通过本地身份验证数据验证模块对用户输入的第一身份验证数据进行验证。

举例来说，支付终端可以将用户输入的第一身份验证数据与支付终端的安全存储中存储的第二身份验证数据进行对比，若确定用户输入的第一身份验证数据与支付终端的安全存储中存储的第二身份验证数据是匹配的，则确定第一身份验证数据验证成功，否则确定第一身份验证数据验证失败。

支付终端在确定第一身份验证数据验证成功之后，响应用户启动 HCE 应用程序的请求，进入 HCE 应用程序界面，用户从可选择卡片列表中选择一张支付卡片（当然，HCE 应用程序也可以直接将默认的卡片作为支付卡片），之后支付终端检测 TEE 中的可信存储区中是否存在对应于 HCE 应用程序正在使用的支付卡片的有效的验证信息，所述验证信息由云身份验证数据管理模块管理。支付终端在检测到存在有效的验证信息时，执行步骤 201。

步骤 201 中，支付卡片可以为通过绑定借记卡、信用卡等卡片到支付终端产生的虚拟卡片，一个 HCE 应用程序可绑定多张支付卡片，本申请实施例对此并不限定。

本申请实施例中，验证信息可以包含有效期参数；所述有效期参数可以为云验证服务器预设的有效时间，所述验证信息在所述预设有效时间内有效。所述验证信息还可以为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功，则所述支付交易次数减一，所述支付交易次数不为 0 时有效。

需要说明的是，所述验证信息为支付交易次数时，所述支付交易次数与 HCE 应用程序的标识和/或 HCE 应用程序绑定的支付卡片相关联，即一个 HCE 应用程序和/或 HCE 应用程序绑定的支付卡片对应一个支付交易次数。

所述支付终端检测到所述支付终端的安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息；或者，所述支付终端检测到所述支付终端的安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

举例来说，在支付终端应用 OAuth 协议向云验证服务器请求验证信息的场景下，验证信息为 Access Token，Access Token 的有效期参数可以为预设有效时间。支付终端在确定第一身份验证数据验证成功之后，响应用户启动 HCE 应用程序的请求，然后根据 HCE 应用程序的标识和/或 HCE 应用程序当前使用的支付卡片的标识检测支付终端中是否存在与所述 HCE 应用程序的标识和/或 HCE 应用程序当前使用的支付卡片的标识相关联且有效的 Access Token。若 Access Token 存在且 Access Token 的预设有效时间未过期，则确定存在有效的验证信息，并执行步骤 201 后面的流程。

再举例来说，验证信息为与支付卡片相关联的支付交易次数，支付交易次数标记保存于 TEE 中，支付终端每次执行非接支付交易成功一次则将支付交易次数减一。支付终端在确定第一身份验证数据验证成功之后，响应用户启动 HCE 应用程序的请求，然后判断所述支付终端中的支付交易次数是否为 0，若不为 0，则确定存在有效的验证信息，并执行步骤 201 后面的流程。

可选的，本申请实施例中，所述支付终端若检测到所述支付终端的安全

存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求；所述支付终端接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器根据所述验证参数对持卡人的身份验证通过后生成并发送的。

所述验证参数可以为支付终端标识、HCE 应用程序的账户和密码、当前 Access Token 对应的 Refresh token，还可以为 HCE 应用程序绑定卡片的主账户、有效期、联系人电话等，具体根据实际情况确定。

结合前面的描述，可选的，支付终端若确定 Access Token 不存在，则由 TEE 中的云身份验证信息管理模块将 HCE 应用程序的标识、HCE 应用程序的账户和密码发送给云验证服务器，用于向云验证服务器请求授权码（Authorization Code），然后再由 HCE 应用程序将 Authorization Code、HCE 应用程序标识和 HCE 应用程序账户通过验证请求发送给云验证服务器，用于向云验证服务器请求验证 Authorization Code 有效后下发 Access Token 和 Refresh Token；若 Access Token 存在，则检查 Access Token 的预设有效时间是否过期，若 Access Token 的预设有效时间过期但与 Access Token 对应的刷新令牌（Refresh Token）有效，则由 HCE 应用程序将 HCE 应用程序账户以及 Refresh Token 通过验证请求发送给云验证服务器，用于向云验证服务器请求 Access Token。

需要说明的是，Authorization Code 和 HCE 应用程序相关联，HCE 应用程序可以通过与之关联的 Authorization Code、HCE 应用程序标识和 HCE 应用程序账户申请 Access Token。用户在通过 HCE 应用程序进行支付交易时，需要获得一定的交易权限，以便 HCE 应用程序通过支付卡片完成交易。HCE 应用程序所需的权限需要由 Access Token 进行授权，Access Token 是有时间限制，避免 HCE 应用程序永久保留权限。为了避免 Access Token 失效时，用户需要不停的通过 Authorization Code、HCE 应用程序标识和 HCE 应用程序账户的方式重新为 HCE 应用程序申请 Access Token，可以在 Access Token 失效时，通过与 Access Token 关联的 Refresh Token 重新申请 Access Token。关于

Authorization Code、Access Token 以及 Refresh Token 的具体内容可以参考 OAuth2.0 协议中的规定，在此不再赘述。

再举例来说，支付终端若确定支付交易次数为 0，则将根据用户输入的第一身份验证数据获得的用户程序绑定的卡片的主账号、有效期、持卡人联系电话等通过验证请求发送给云验证服务器，用于向云验证服务器请求验证信息，即一个不为 0 的支付交易次数。

需要说明的是，云验证服务器可以为所述支付卡片对应的发卡行服务器。本申请实施例中，支付终端可以通过 Wi-Fi 模块与云验证服务器进行通信，也可以通过移动通信模块（例如，2G 模块、3G 模块、4G 模块等通信模块）与云验证服务器进行通信。支付终端通过非接触通信模块与结算终端进行通信，例如 NFC 模块。

可选的，支付终端在检测到所述支付终端的安全存储中存在有效的验证信息之后，在将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM 之前，还可以先确定当前支付交易所需支付的支付金额，若确定支付金额小于预设阈值，则执行将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM 的步骤；若确定支付金额大于或等于预设阈值，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为联机 PIN 或签名等验证方法。

本申请实施例中，支付终端可以通过以下方式将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM:

支付终端可以在支付卡片的 AIP（Application Interchange Profile，应用交互特征）中将第一字节的第 5 个比特位设置为 1，从而指示该支付卡片支持持卡人验证，并初始化支付卡片的 CVM 列表，将“无需 CVM”设置为卡片支持的 CVM 列表中的第一个条目，或者将 CVM 列表设置为只包含“无需 CVM”一个条目，从而实现将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM。

可选的，本申请实施例中，支付终端在执行步骤 202 之前，还可以先获取结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的

CVM 方法。当支付终端根据所述终端交易属性确定所述结算终端不支持CD-CVM后，可以执行步骤202。

当然，以上只是可选步骤，支付终端还可以在确定所述结算终端支持CD-CVM后，也执行步骤202，或不判断结算终端是否支持CD-CVM，直接执行步骤202。

结合图1，支付终端可以通过POS信息获取模块获取结算终端的终端交易属性，进而判断结算终端是否支持CD-CVM，当结算终端不支持CD-CVM时，执行步骤202。

本申请实施例中，支付终端可以通过多种方式获取所述结算终端的终端交易属性，下面详细描述。

第一种可能的实现方式：在所述结算终端与所述支付终端通信，选择应用程序的过程中，所述支付终端可通过向所述结算终端发送PDOL（Processing Data Object List，处理选项数据对象列表）获取所述结算终端的终端交易属性。具体的，支付终端通过非接触通信模块响应结算终端发送的选择应用程序标识（SELECT AID）命令时，在应答消息的PDOL中设置标签“9F66”，用于指示结算终端需要向支付终端提供其终端交易属性；之后支付终端通过非接触通信模块接收结算终端发送的GPO（Get Processing Option，获得处理选项）命令，所述GPO命令中包括PDOL中要求结算终端提供的终端交易属性，结算终端可利用其终端交易属性第一字节的第1个比特位或第二字节、第三字节中的预留比特位来指示结算终端是否支持CD-CVM。对于不支持CD-CVM的传统终端，上述比特位应初始化设置为0。

需要说明的是，由于支付终端通过HCE技术模拟所述支付卡片，因此支付终端不能主动向结算终端发送消息，只能在支付终端进入到结算终端的电磁场范围内时，接收到结算终端通过非接触模块向支付终端发送命令之后，在应答结算终端发送的命令时向结算终端发送请求。

举例来说，如图3所示，为本申请实施例提供的一种支付交易示意图。图3中，支付终端301接收到用户启动支付终端301中的HCE应用程序的请

求，此时支付终端 301 会提示用户输入第一身份验证数据，并在对第一身份验证数据验证通过后，在 HCE 应用程序中确定支付卡片。之后支付终端检测 TEE 中的可信存储区中是否存在对应于 HCE 应用程序正在使用的支付卡片的有效的验证信息。所述支付终端 301 若检测到所述支付终端 301 的安全存储中不存在有效的验证信息，则向云验证服务器 303 发送包括验证参数的验证请求。向云验证服务器 303 在核实所述验证参数通过后，向所述支付终端 301 返回新的验证信息。此时，支付终端 301 将当前使用的支付卡片的 CVM 变更为无需 CVM。支付终端 301 在靠近结算终端 302 之后，感应到结算终端 302 的电磁信号，从而通过支付终端的非接触通信模块接收结算终端 302 发送的交易命令。支付终端 301 响应结算终端 302 的交易命令，并通知结算终端 302 当前使用的支付卡片的 CVM 为无需 CVM。结算终端 302 确定支付终端 301 当前使用的支付卡片的 CVM 为无需 CVM 后，确定持卡人验证通过，并向收单机构的收单服务器 304 发送交易请求。结算终端 302 向收单服务器 304 发送的交易请求中包括支付卡片的账号、交易金额等信息。结算终端 302 在收到收单服务器 304 返回的交易授权通知消息之后，确认支付交易完成。

第二种可能的实现方式：所述支付终端通过扫描包含所述结算终端的终端交易属性的 URL (Uniform Resoure Locator，统一资源定位符)的二维码获取所述结算终端的终端交易属性。在部署结算终端的环境如商场、超市中，结算终端管理者可主动提供二维码，用户使用支付终端扫描二维码可以访问一个 URL，通过这个 URL 可以获得结算终端的终端交易属性，进而判断结算终端是否支持 CD-CVM；支付终端还可通过访问 URL 获得结算终端描述信息，如商户编号、终端编号等。

第三种可能的实现方式：所述支付终端通过接收 BLE（Bluetooth Low Energy，蓝牙低功耗）广播消息获取所述结算终端的终端交易属性。在部署结算终端的环境如商场、超市中，结算终端管理者可部署 BLE 广播用作推送广告和支付相关信息，如结算终端支持的 CVM 方式；所述 BLE 广播消息可以为所述结算终端发送的，也可以为其他终端发送的。支付终端接收到 BLE 广

播后可解析广播获得结算终端的终端交易属性，进而判断结算终端是否支持CD-CVM。支付终端还可通过解析 BLE 广播获得结算终端描述信息，如商户编号、终端编号等。

步骤 202 中，支付终端在接收到结算终端发送的 GPO 命令后，所述支付终端向所述结算终端发送包括所述 AIP 的应答消息。之后结算终端使用 READ RECORD（读取记录）命令读取应用数据时，支付终端使用调整后的 CVM 方法列表响应结算终端，结算终端读取到 CVM 列表后，根据 CVM 列表中的第一个条目确定持卡人验证方法为“无需 CVM”，从而确定持卡人验证流程通过，从而执行支付交易后面的流程。

通过上述方法，支付终端通过将支付卡片的 CVM 调整为“无需 CVM”后，结算终端无论支不支持 CD-CVM 等持卡人验证方法，只需要根据“无需 CVM”直接确定持卡人验证流程通过，从而不需要用户再输入 PIN 码持卡人验证操作，从而简化了交易流程，提高了交易体验。

可选的，支付终端还可以在支付卡片的发卡行应用数据中包含的支付卡片验证结果(Card Verification Result，CVR)部分指示支付卡片已通过支付终端执行持卡人验证，以便结算终端将 CVR 上送到发卡行，同时将支付卡片的 CVM 方法设置为联机 PIN，以便用户可在结算终端上输入任意数字或直接按确认，之后结算终端可确认持卡人验证通过继续执行交易。

可选的，所述支付终端可以接收结算终端或云验证行服务器发送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易。支付终端还可在标记为 CVM 降级交易的记录中添加结算终端描述信息，如商户标号、终端编号等。

进一步的，所述支付终端还可以将所述交易日志同步到云验证服务器。

下面通过具体的实施例描述上面的过程。

如图 4 所示，为本申请实施例提供的一种支付交易流程示意图。

图 4 为在采用 OAuth2.0 协议获取验证信息的场景下进行支付交易的流程，验证信息为 Access Token。

步骤 401：支付终端接收用户启动 HCE 应用程序的请求。此后，支付终端显示第一身份验证数据输入界面，提示用户输入身份验证数据。该输入界面可通过 TUI 实现。

步骤 402：支付终端接收用户输入的第一身份验证数据，并对所述第一身份验证数据进行本地验证，若验证成功，则转至步骤 403，否则转至步骤 412。

步骤 403：支付终端启动 HCE 应用程序，并根据 HCE 应用程序的标识检测支付终端中是否存在与所述 HCE 应用程序的标识或与所述 HCE 应用程序当前使用的支付卡片相关联的 Access Token，若存在，则转至步骤 404，否则转至步骤 407。

步骤 404：支付终端判断 Access Token 是否有效，若有效，则转至步骤 409，否则转至步骤 405。

支付终端检查 Access Token 的预设有效时间，如果预设有效时间未超过有效期时间，则判定 Access Token 有效。

步骤 405: 支付终端获取与 Access Token 对应的 Refresh Token 以及与 HCE 应用程序相关联的支付卡片标识，然后将 Refresh Token 和 HCE 应用账户数据，或将 Refresh Token 和 HCE 应用当前使用的卡片标识通过验证请求发送给云验证服务器，用于向云验证服务器请求一个新的 Access Token。

发卡行服务器可以使用 Access Token 控制一定时间内累计不超过特定限额的支付，Refresh Token 用于 Access Token 的有效期时间已超期时向云验证服务器申请一个新的 Access Token，此时云验证服务器不再伴随 Access Token 下发一个 Refresh Token，支付终端收到新的 Access Token 后删除 Refresh Token。

步骤 406：支付终端接收云验证服务器返回的 Access Token。

步骤 407：支付终端将支付卡片持卡人验证方法设置为无需 CVM，转至步骤 410。

具体的，支付终端可将支付卡片支持的 CVM 列表的第一个条目设置为“无需 CVM”，或者将 CVM 列表设置为只包含“无需 CVM”一个条目。

步骤 408：支付终端通过云验证信息管理模块将 HCE 应用程序的标识、HCE 应用账户和密码等数据发送给云验证服务器，用于向云验证服务器请求 Authorization Code。

步骤 409：支付终端接收 Authorization Code，然后再由 HCE 应用程序将 HCE 应用程序标识和 Authorization Code，或者 HCE 应用程序正在使用的卡片标识和 Authorization Code 发送给云验证服务器，用于向云验证服务器请求 Access Token。

步骤 410：支付终端接收到结算终端的 GPO 命令后，通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM。

具体的，支付终端通过应答结算终端发送的 GPO 命令通知结算终端支付卡片支持持卡人验证，并通过应答结算终端发送的 READ RECORD 命令向结算终端提供支付卡片的 CVM 列表；结算终端接收应答，获得支付卡片的 CVM 列表，读取第一个条目，确认支付卡片“无需 CVM”，进而确认持卡人验证通过，继续其他数据的处理并完成支付交易。

需要说明的是，步骤 410 发生于用户将支付终端靠近结算终端，使得支付终端感应到结算终端电磁信号进行非接触支付交易时。

步骤 411：支付终端可接收结算终端或云验证服务器发送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易。

其中，交易成功通知是结算终端确认支付卡片支持“无需 CVM”之后，直接确认支付卡片的持卡人验证通过后发送的。由于结算终端根据“无需 CVM”直接确定支付卡片的持卡人验证通过，避免了用户需要输入 PIN 等持卡人验证操作，从而简化了交易流程，提高了用户体验。

可选的，支付终端还可以将所述交易日志同步到云验证服务器。

步骤 412：结束整个交易流程。

如图 5 所示，为本申请实施例提供的一种支付交易流程示意图。

图 5 所示的支付交易流程中，验证信息为支付交易次数。

步骤 501：支付终端接收用户启动 HCE 应用程序的请求。

步骤 502：支付终端接收用户输入的第一身份验证数据，并对所述第一身份验证数据进行本地验证，若验证成功，则转至步骤 503，否则转至步骤 511。

步骤 503：支付终端启动 HCE 应用程序，并根据 HCE 应用程序的标识和/或 HCE 应用程序绑定的支付卡片检测支付终端中与 HCE 应用程序相关联的验证成功标记对应的支付交易次数是否为 0，若为 0，则转至步骤 504，否则转至步骤 507。

步骤 504：支付终端向云验证服务器发送包含验证参数的验证请求，以便云验证服务器通过验证后返回一个不为 0 的支付交易次数限制。所述验证参数可以是支付终端标识；所述验证参数还可以是支付终端标识和支付卡片主账户、主账户有效期、持卡人电话号码等。验证服务器可根据支付终端提交的不同验证参数，设置不同的支付交易次数限制。

支付终端在接收到云验证服务器返回的支付交易次数限制后，对支付终端本地的验证成功标记进行重置。

可选的，在步骤 504 之前，支付终端还可以提示用户需要向云验证服务器请求一个不为 0 的支付交易次数，并接收用户的输入和确认操作。

步骤 505：支付终端获取所述结算终端的终端交易属性。

具体的，支付终端可以通过非接触通信模块接收结算终端发送的 SELECT AID 命令，然后支付终端向所述结算终端发送包含终端交易属性查询请求字段(即标签“9F66”)的 PDOL，随后通过非接触通信模块接收结算终端发送的 GPO 命令，并根据所述 GPO 命令确定结算终端的终端交易属性，判断结算终端是否支持 CD-CVM。

当然，支付终端还可通过扫描二维码获取所述结算终端的终端交易属性；或者，所述支付终端还可通过接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性，在此不再赘述。

步骤 506：支付终端根据所述结算终端的终端交易属性判断所述结算终端是否支持 CD-CVM，若否，则转至步骤 507，否则转至步骤 508。

步骤 507：支付终端将支付卡片的持卡人验证方法设置为无需 CVM，转

至步骤 509。

具体的，支付终端可将支付卡片的 CVM 列表的第一个条目设置为“无需 CVM”，或将支付卡片的 CVM 列表设置为仅包含“无需 CVM”一个条目。

步骤 508：支付终端指示结算终端已经执行了 CD-CVM，结算终端确认持卡人验证通过，继续其他处理并完成支付交易。

以上步骤 505，506，508 为可选步骤；

步骤 509：支付终端接收到结算终端的查询消息后，通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM。具体的，支付终端接收到结算终端发送的读取应用数据命令 READ RECORD，并使用步骤 507 设置的 CVM 列表应答，以便结算终端可确认支付卡片支持“无需 CVM”并确认持卡人验证通过。

步骤 510：支付终端接收结算终端或云验证服务器发送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易。

其中，交易成功通知是结算终端确认支付卡片支持“无需 CVM”之后，直接确认支付卡片的持卡人验证通过后发送的。由于结算终端根据“无需 CVM”直接确定支付卡片的持卡人验证通过，避免了用户需要输入 PIN 等持卡人验证操作，从而简化了交易流程，提高了用户体验。

可选的，支付终端还可以将所述交易日志同步到云验证服务器。

步骤 511：结束整个交易流程。

基于相同的发明构思，本申请实施例还提供一种支付验证装置，该装置可以执行上述方法。

如图 6 所示，为本申请实施例提供的一种支付验证装置结构示意图。

参见图 6，该装置包括：

处理单元 601，用于若检测到安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区；

收发单元 602，用于通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

可选的，所述处理单元 601 还用于：

若检测到所述安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求；

所述收发单元 602，还用于接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

可选的，所述收发单元 602 还用于：

接收第一身份验证数据，并确定所述第一身份验证数据与所述安全存储中保存的第二身份验证数据匹配。

可选的，所述验证信息包含有效期参数；

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在所述预设有效时间内有效；

所述处理单元 601 具体用于：

检测到所述安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

可选的，所述验证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效；

所述处理单元 601 具体用于：

检测到所述安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

可选的，所述收发单元 602 还用于：

获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法；

根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证

方法 CD-CVM。

可选的，所述支付终端中还包括蓝牙模块以及图像采集模块：

所述支付终端通过所述 NFC 模块向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述支付终端在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的；或者

所述支付终端通过所述图像采集模块扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

所述支付终端通过所述蓝牙模块接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

可选的，所述收发单元 602 还用于：

接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易；

将所述交易日志同步到云验证服务器。

基于相同的发明构思，本申请实施例还提供一种支付终端，该支付终端可以执行上述方法。

如图 7 所示，为本申请实施例提供的一种支付终端结构示意图。

参见图 7，该支付终端包括：处理器 701、NFC 模块 702、存储器 703；

处理器 701 可以是中央处理器（英文：central processing unit，缩写：CPU），网络处理器（英文：network processor，缩写：NP）或者 CPU 和 NP 的组合。处理器 701 还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路（英文：application-specific integrated circuit，缩写：ASIC），可编程逻辑器件（英文：programmable logic device，缩写：PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（英文：complex programmable logic device，缩写：CPLD），现场可编程逻辑门阵列（英文：field-programmable gate array，缩写：FPGA），通用阵列逻辑（英文：generic array logic，缩写：GAL）或其任意组

合。存储器 703 可以包括易失性存储器（英文：volatile memory），例如随机存取存储器（英文：random-access memory，缩写：RAM）；存储器 703 也可以包括非易失性存储器（英文：non-volatile memory），例如只读存储器（英文：read-only memory，缩写：ROM），快闪存储器（英文：flash memory），硬盘（英文：hard disk drive，缩写：HDD）或固态硬盘（英文：solid-state drive，缩写：SSD）；存储器 703 还可以包括上述种类的存储器的组合。

所述存储器 703 可以用来存储计算机指令。

所述处理器 701，用于若检测到所述支付终端的安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区；

所述 NFC 模块 702，用于通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

可选的，所述支付终端中还包括收发机 706 和 Wi-Fi 模块 707；

所述处理器 701 还用于：

若检测到所述安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求；

所述收发机 706 或所述 Wi-Fi 模块 707，还用于接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

可选的，所述支付终端中还包括收发机 706 和 Wi-Fi 模块 707：

所述收发机 706 或所述 Wi-Fi 模块 707，用于接收第一身份验证数据；

所述处理器 701，用于确定所述第一身份验证数据与所述安全存储中保存的第二身份验证数据匹配。

可选的，所述验证信息包含有效期参数；

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在

所述预设有效时间内有效;

所述处理器 701 具体用于:

检测到所述安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

可选的，所述验证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效;

所述处理器 701 具体用于:

检测到所述安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

可选的，所述 NFC 模块 702 还用于:

获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法;

所述处理器 701 还用于：根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证方法 CD-CVM。

可选的，所述支付终端中还包括蓝牙模块 704 以及图像采集模块 705:

所述支付终端通过所述 NFC 模块 702 向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述支付终端在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的；或者

所述支付终端通过所述图像采集模块 705 扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

所述支付终端通过所述蓝牙模块 704 接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

可选的，所述支付终端中还包括收发机 706 和 Wi-Fi 模块 707；所述收发机 706 或所述 Wi-Fi 模块 707 用于:

接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易；

将所述交易日志同步到云验证服务器。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请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信道（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的方法、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、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指令，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。

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。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要

求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1、一种支付验证方法，其特征在于，该方法包括:

支付终端若检测到所述支付终端的安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区;

所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

2、根据权利要求 1 所述的方法，其特征在于，所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM 之前，还包括:

所述支付终端若检测到所述支付终端的安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求;

所述支付终端接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述支付终端检测到所述支付终端的安全存储中存在有效的验证信息之前，还包括:

所述支付终端接收第一身份验证数据，并确定所述第一身份验证数据与所述支付终端的安全存储中保存的第二身份验证数据匹配。

4、根据权利要求 1 至 3 任一所述的方法，其特征在于，所述验证信息包含有效期参数;

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在所述预设有效时间内有效;

所述支付终端检测到所述支付终端的安全存储中存在有效的验证信息，包括:

所述支付终端检测到所述支付终端的安全存储中存在所述验证信息且确

定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

5、根据权利要求 1 至 3 任一所述的方法，其特征在于，所述验证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效；

所述支付终端检测到所述支付终端的安全存储中存在有效的验证信息，包括:

所述支付终端检测到所述支付终端的安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

6、根据权利要求 1 至 5 任一所述的方法，其特征在于，所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM 之前，还包括:

所述支付终端获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法;

所述支付终端根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证方法 CD-CVM。

7、根据权利要求 6 所述的方法，其特征在于，所述支付终端获取所述结算终端的终端交易属性，包括:

所述支付终端向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述支付终端在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的；或者

所述支付终端通过扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

所述支付终端通过接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

8、根据权利要求 1 至 7 任一所述的方法，其特征在于，所述支付终端通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM 之后，还包括:

所述支付终端接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易;

所述支付终端将所述交易日志同步到云验证服务器。

9、一种支付验证装置，其特征在于，该装置包括:

处理单元，用于若检测到安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区;

收发单元，用于通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

10、根据权利要求 9 所述的装置，其特征在于，所述处理单元还用于:

若检测到所述安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求;

所述收发单元，还用于接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

11、根据权利要求 9 或 10 所述的装置，其特征在于，所述收发单元还用于:

接收第一身份验证数据，并确定所述第一身份验证数据与所述安全存储中保存的第二身份验证数据匹配。

12、根据权利要求 9 至 11 任一所述的装置，其特征在于，所述验证信息包含有效期参数;

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在所述预设有效时间内有效;

所述处理单元具体用于:

检测到所述安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

13、根据权利要求 9 至 11 任一所述的装置，其特征在于，所述验证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效；

所述处理单元具体用于：

检测到所述安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

14、根据权利要求 9 至 13 任一所述的装置，其特征在于，所述收发单元还用于：

获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法；

根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证方法 CD-CVM。

15、根据权利要求 14 所述的装置，其特征在于，所述收发单元具体用于：

向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述装置在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的；或者

通过扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

通过接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

16、根据权利要求 9 至 15 任一所述的装置，其特征在于，所述收发单元还用于：

接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易；

将所述交易日志同步到云验证服务器。

17、一种支付终端，其特征在于，包括：处理器、近场通信 NFC 模块；

所述处理器，用于若检测到所述支付终端的安全存储中存在有效的验证

信息，则将当前使用的支付卡片的持卡人验证方法 CVM 变更为无需 CVM，所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境 TEE 中的可信存储区或富执行环境 REE 中的安全存储区；

所述 NFC 模块，用于通知所述结算终端所述支付卡片支持的 CVM 为无需 CVM，以便所述结算终端按照所述无需 CVM 对所述用户进行验证并完成交易。

18、根据权利要求 17 所述的支付终端，其特征在于，所述支付终端中还包括收发机和 Wi-Fi 模块；

所述处理器还用于：

若检测到所述安全存储中不存在有效的验证信息，则向云验证服务器发送包括验证参数的验证请求；

所述收发机或所述 Wi-Fi 模块，还用于接收所述云验证服务器返回的验证信息；所述验证信息为所述云验证服务器核实所述验证参数通过后生成并发送的。

19、根据权利要求 17 或 18 所述的支付终端，其特征在于，所述支付终端中还包括收发机和 Wi-Fi 模块；

所述收发机或所述 Wi-Fi 模块，用于接收第一身份验证数据；

所述处理器，用于确定所述第一身份验证数据与所述安全存储中保存的第二身份验证数据匹配。

20、根据权利要求 17 至 19 任一所述的支付终端，其特征在于，所述验证信息包含有效期参数；

所述有效期参数为云验证服务器设置的预设有效时间，所述验证信息在所述预设有效时间内有效；

所述处理器具体用于：

检测到所述安全存储中存在所述验证信息且确定所述验证信息对应的预设有效时间未超期，则确定安全存储中存在有效的验证信息。

21、根据权利要求 17 至 20 任一所述的支付终端，其特征在于，所述验

证信息为云验证服务器设置的支付交易次数；其中，所述支付终端每次使用所述支付卡片支付交易成功则所述支付交易次数减一，所述支付交易次数不为 0 时有效；

所述处理器具体用于：

检测到所述安全存储中存在所述支付交易次数且确定所述支付交易次数不为 0，则确定安全存储中存在有效的验证信息。

22、根据权利要求 17 至 21 任一所述的支付终端，其特征在于，所述 NFC 模块还用于：

获取所述结算终端的终端交易属性；所述终端交易属性指示所述结算终端支持的 CVM 方法；

所述处理器还用于：根据所述终端交易属性确定所述结算终端不支持消费者设备持卡人验证方法 CD-CVM。

23、根据权利要求 22 所述的支付终端，其特征在于，所述支付终端中还包括蓝牙模块以及图像采集模块：

所述支付终端通过所述 NFC 模块向所述结算终端发送处理选项数据对象列表 PDOL 以获取所述结算终端的终端交易属性；所述 PDOL 为所述支付终端在接收到结算终端发送的选择应用程序标识 SELECT AID 命令后发送的；或者

所述支付终端通过所述图像采集模块扫描包含获取所述结算终端的终端交易属性的统一资源定位符 URL 的二维码，获取所述结算终端的终端交易属性；或者

所述支付终端通过所述蓝牙模块接收蓝牙低功耗 BLE 广播消息获取所述结算终端的终端交易属性。

24、根据权利要求 17 至 23 任一所述的支付终端，其特征在于，所述支付终端中还包括收发机和 Wi-Fi 模块：所述收发机或所述 Wi-Fi 模块用于：

接收云验证服务器推送的交易成功通知，并在交易日志中将所述支付交易的类型标记为 CVM 降级交易；

将所述交易日志同步到云验证服务器。

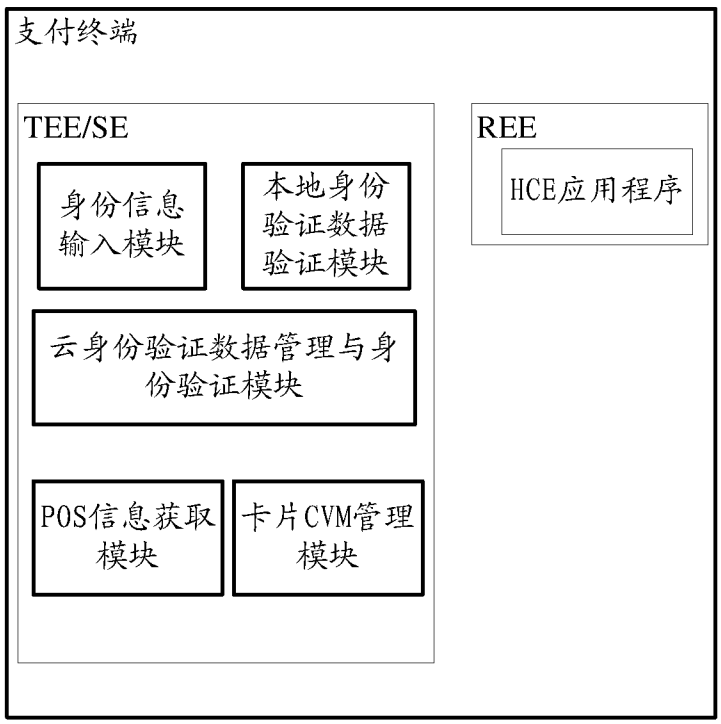

支付终端
TEE/SE
身份信息输入模块
本地身份验证数据验证模块
云身份验证数据管理与身份验证模块
POS信息获取模块
卡片CVM管理模块
REE
HCE应用程序

图 1

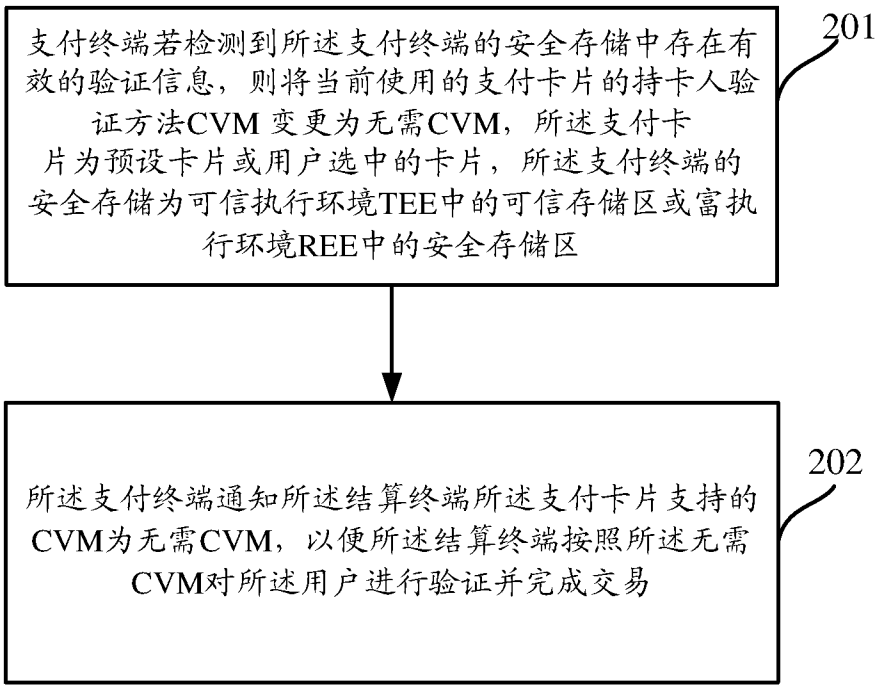

支付终端若检测到所述支付终端的安全存储中存在有效的验证信息，则将当前使用的支付卡片的持卡人验证方法CVM 变更为无需CVM，所述支付卡片为预设卡片或用户选中的卡片，所述支付终端的安全存储为可信执行环境TEE中的可信存储区或富执行环境REE中的安全存储区
201
所述支付终端通知所述结算终端所述支付卡片支持的CVM为无需CVM，以便所述结算终端按照所述无需CVM对所述用户进行验证并完成交易
202

图 2

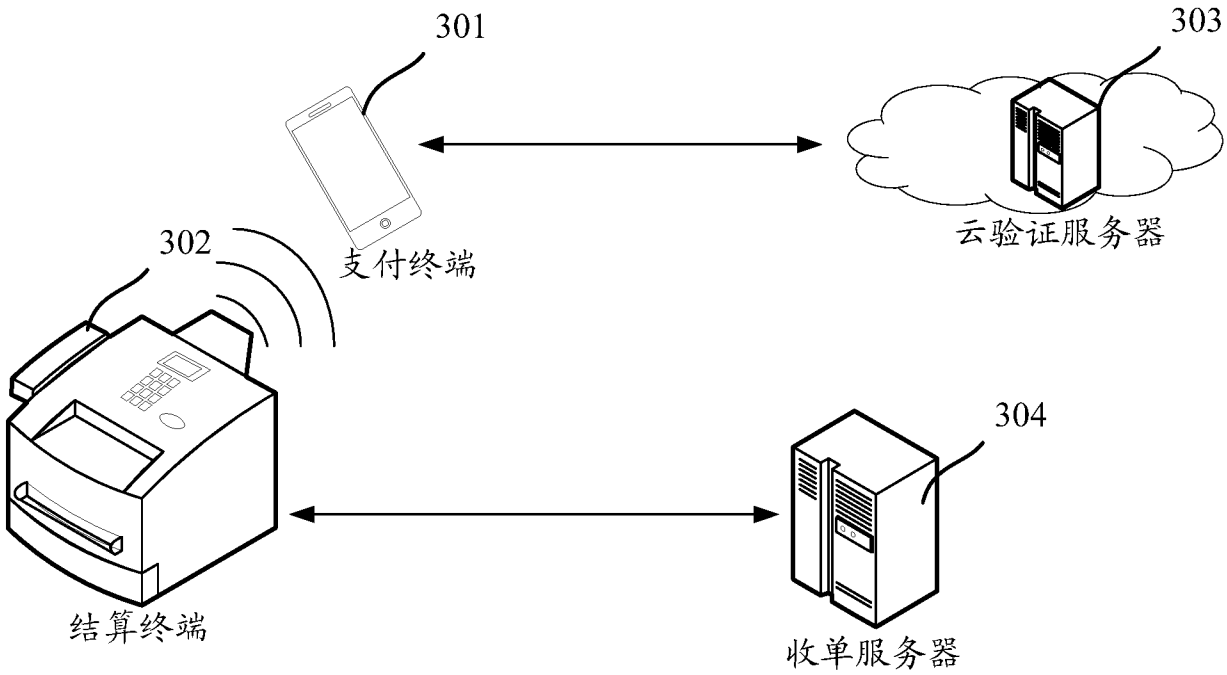


图 3

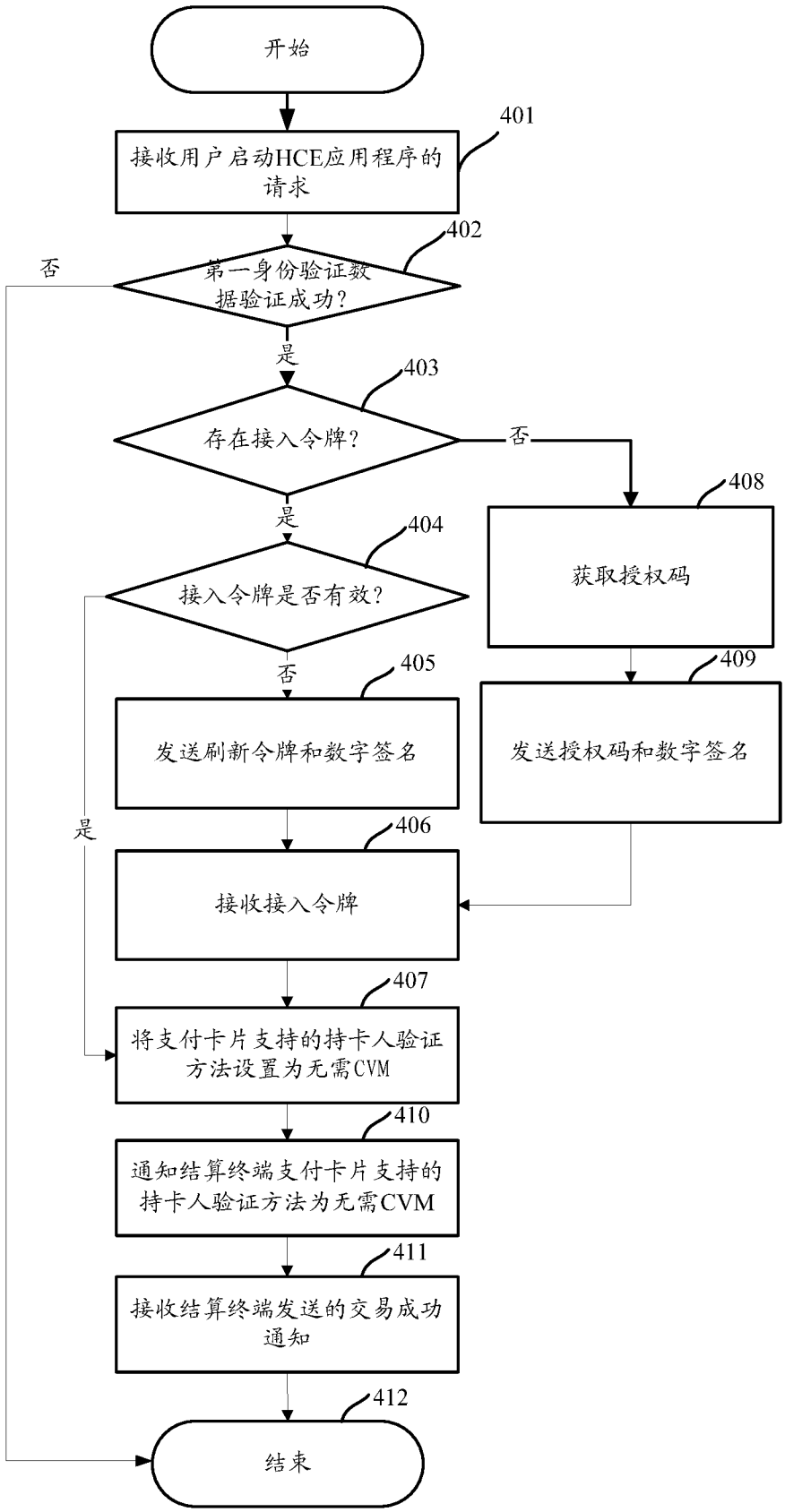

开始
401
接收用户启动HCE应用程序的请求
402
第一身份验证数据验证成功?
否
是
403
存在接入令牌?
否
是
404
接入令牌是否有效?
否
是
405
发送刷新令牌和数字签名
406
接收接入令牌
407
将支付卡片支持的持卡人验证方法设置为无需CVM
410
通知结算终端支付卡片支持的持卡人验证方法为无需CVM
411
接收结算终端发送的交易成功通知
412
结束
408
获取授权码
409
发送授权码和数字签名

图 4

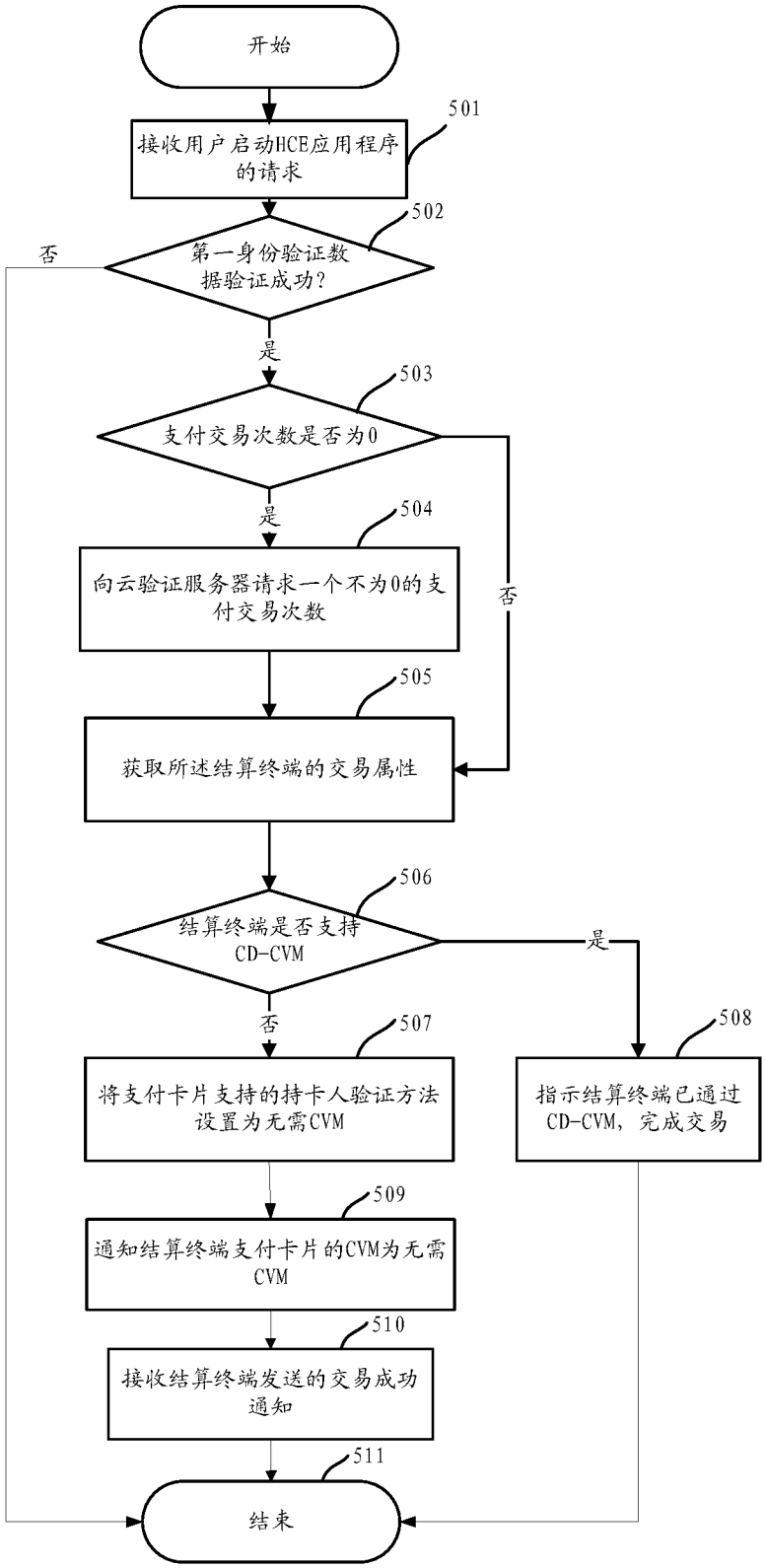

开始
501
接收用户启动HCE应用程序的请求
502
第一身份验证数据验证成功?
否
是
503
支付交易次数是否为0
是
否
504
向云验证服务器请求一个不为0的支付交易次数
505
获取所述结算终端的交易属性
506
结算终端是否支持CD-CVM
是
否
507
将支付卡片支持的持卡人验证方法设置为无需CVM
508
指示结算终端已通过CD-CVM，完成交易
509
通知结算终端支付卡片的CVM为无需CVM
510
接收结算终端发送的交易成功通知
511
结束

图 5

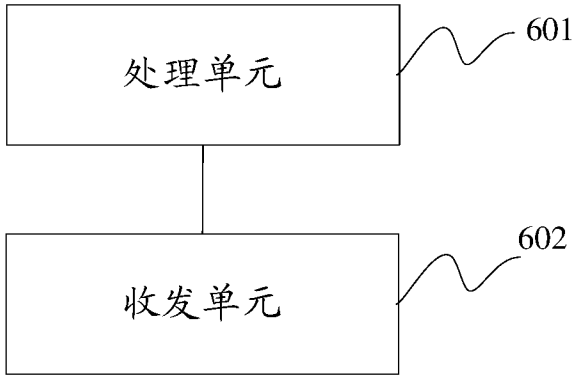

处理单元
601
收发单元
602

图 6

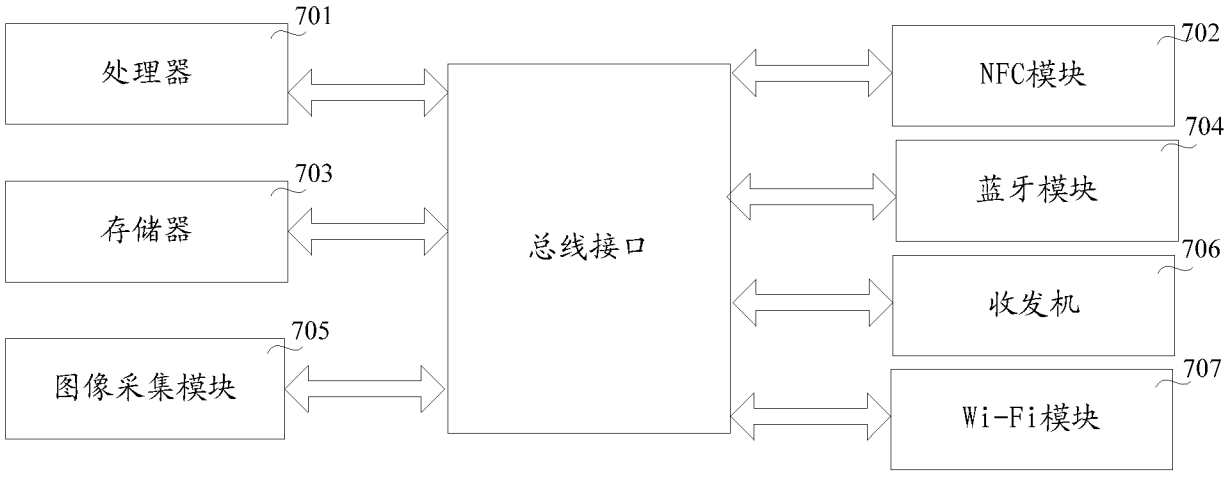

处理器
701
存储器
703
图像采集模块
705
总线接口
NFC模块
702
蓝牙模块
704
收发机
706
Wi-Fi模块
707

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/087763

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38 (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; H04L; G06F

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)

CNKI, CNPAT, WPI, EPODOC, IEEE: wallet, trade, pay, mobile, cellphone, portable, TEE, REE, authentication, verify, CVM, CD?CVM, passcode, PIN, cardholder, trade, quick pass, move, omit, automation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2015095771 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 25 June 2015 (25.06.2015) description, paragraphs [0036], [0052], [0080], [0085], [0109]-[0119] and [0309]-[0316], and figures 1-3	1-24
A	CN 105518732 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 20 April 2016 (20.04.2016) the whole document	1-24
A	CN 104517211 A (INVENTEC SHANGHAI TECHNOLOGY CO., LTD.; INVENTEC (SHANGHAI) APPLIANCES CO., LTD.; INVENTEC APPLIANCE CORP.) 15 April 2015 (15.04.2015) the whole document	1-24
A	CN 102054316 A (CHINA UNIONPAY CO., LTD.) 11 May 2011 (11.05.2011) the whole document	1-24
A	WO 2015179637 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 26 November 2015 (26.11.2015) the whole document	1-24

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 March 2017	31 March 2017
Name and mailing address of the ISA 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 DONG, Hongmei Telephone No. (86-10) 62413677

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/087763

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2015095771 A1	25 June 2015	US 2015178724 A1	25 June 2015
		CA 2931093 A1	25 June 2015
		AU 2014368949 A1	09 June 2016
		US 2016217452 A1	28 July 2016
		SG 11201604906Q A	28 July 2016
		US 2015180836 A1	25 June 2015
		KR 20160101117 A	24 August 2016
		CN 105830107 A	03 August 2016
		US 2016140545 A1	19 May 2016
CN 105518732 A	20 April 2016	EP 3017413 A1	11 May 2016
		AU 2014285774 A1	07 January 2016
		KR 20160015375 A	12 February 2016
		US 2016132880 A1	12 May 2016
		WO 2015001473 A1	08 January 2015
CN 104517211 A	15 April 2015	TW 201624371 A	01 July 2016
CN 102054316 A	11 May 2011	None	
WO 2015179637 A1	26 November 2015	US 2015339664 A1	26 November 2015

国际检索报告

国际申请号
PCT/CN2016/087763

A. 主题的分类

G06Q 20/38(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; H04L; G06F

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））

CNKI, CNPAT, WPI, EPODOC, IEEE: 支付，交易，付款，闪付，钱包，移动，手机，支付，验证，认证，鉴权，授权，无需，不需，省略，密码，身份，免密，自动; wallet, trade, pay, mobile, cellphone, portable, TEE, REE, authentication, verify, CVM, CD?CVM, passcode, PIN, cardholder

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
A	WO 2015095771 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 2015年 6月 25日 (2015-06-25) 说明书第0036、0052、0080、0085、0109-0119、0309-316段、附图1-3	1-24
A	CN 105518732 A (维萨国际服务协会) 2016年 4月 20日 (2016-04-20) 全文	1-24
A	CN 104517211 A (英华达上海科技有限公司 英华达上海电子有限公司 英华达股份有限公司) 2015年 4月 15日 (2015-04-15) 全文	1-24
A	CN 102054316 A (中国银联股份有限公司) 2011年 5月 11日 (2011-05-11) 全文	1-24
A	WO 2015179637 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 2015年 11月 26日 (2015-11-26) 全文	1-24

☐ 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	国际检索报告邮寄日期
2017年 3月 15日	2017年 3月 31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 传真号 (86-10)62019451	受权官员 董洪梅 电话号码 (86-10)62413677

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/087763

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)
WO	2015095771	A1	2015年 6月 25日	US	2015178724	A1	2015年 6月 25日
				CA	2931093	A1	2015年 6月 25日
				AU	2014368949	A1	2016年 6月 9日
				US	2016217452	A1	2016年 7月 28日
				SG	11201604906Q	A	2016年 7月 28日
				US	2015180836	A1	2015年 6月 25日
				KR	20160101117	A	2016年 8月 24日
				CN	105830107	A	2016年 8月 3日
				US	2016140545	A1	2016年 5月 19日
CN	105518732	A	2016年 4月 20日	EP	3017413	A1	2016年 5月 11日
				AU	2014285774	A1	2016年 1月 7日
				KR	20160015375	A	2016年 2月 12日
				US	2016132880	A1	2016年 5月 12日
				WO	2015001473	A1	2015年 1月 8日
CN	104517211	A	2015年 4月 15日	TW	201624371	A	2016年 7月 1日
CN	102054316	A	2011年 5月 11日		无		
WO	2015179637	A1	2015年 11月 26日	US	2015339664	A1	2015年 11月 26日