

(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
2017年6月1日 (01.06.2017)



(10) 国际公布号
WO 2017/088261 A1

- (51) 国际专利分类号:
G06Q 20/02 (2012.01)
- (21) 国际申请号: PCT/CN2015/099616
- (22) 国际申请日: 2015年12月29日 (29.12.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510821881.8 2015年11月23日 (23.11.2015) CN
201510848445.X 2015年11月27日 (27.11.2015) CN
- (71) 申请人: 小米科技有限责任公司 (XIAOMI INC.)
[CN/CN]; 中国北京市海淀区清河中街68号华润五彩城购物中心二期13层, Beijing 100085 (CN)。
- (72) 发明人: 胡杨 (HU, Yang); 中国北京市海淀区清河中街68号华润五彩城购物中心二期13层由小米科技有限责任公司转交, Beijing 100085 (CN)。 黄媛媛 (HUANG, Yuanyuan); 中国北京市海淀区清河中街68号华润五彩城购物中心二期13层由小米科技有限责任公司转交, Beijing 100085 (CN)。
- (74) 代理人: 北京尚伦律师事务所 (SUNLAND LAW FIRM); 中国北京市朝阳区东三环北路2号南银大厦31层3108室, Beijing 100027 (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: BIOMETRIC TECHNOLOGY-BASED MOBILE PAYMENT METHOD, DEVICE AND APPARATUS

(54) 发明名称: 基于生物识别技术的移动支付设备、方法和装置

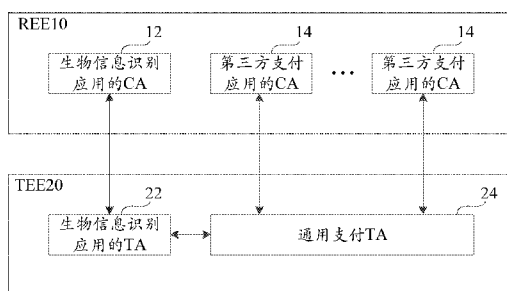


图 1

12 CA - BIOMETRIC INFORMATION IDENTIFICATION APPLICATION
14 CA - THIRD-PARTY PAYMENT APPLICATION
22 TA - BIOMETRIC INFORMATION IDENTIFICATION APPLICATION
24 UNIVERSAL PAYMENT TA

(57) Abstract: A biometric technology-based mobile payment method, device and apparatus. The mobile payment device comprises a biometric information identification application and a universal payment trusted application (TA) operating in a trusted execution environment (TEE). The universal payment TA (24) is configured to receive an invocation request from a third-party payment application, determine a target content requiring encryption and an encryption parameter required for encryption according to the invocation request, acquire a result of biometric information identification from the biometric information identification application, encrypt the target content according to the encryption parameter and the result of biometric information identification, and return the encryption result to the third-party payment application, such that the third-party payment application executes payment-related operations according to the encryption result. The present solution enables multiple third-party payment applications to share one universal payment TA (24), which is advantageous in reducing the cost of signature and prevents a malicious third-party payment application from being installed on a mobile terminal to reduce security risk in a TEE.

(57) 摘要:

[见续页]

WO 2017/088261 A1



一种基于生物识别技术的移动支付设备、方法和装置。移动支付设备包括生物信息识别应用和运行在 TEE 中的通用支付 TA (24)。通用支付 TA (24) 用于接收第三方支付应用的调用请求，根据调用请求确定需要加密的目标内容和执行加密所需的加密参数，从生物信息识别应用获取生物信息识别结果，根据加密参数和生物信息识别结果对目标内容进行加密，并向第三方支付应用返回加密结果。第三方支付应用根据加密结果执行支付相关操作。本方案可以实现多个第三方支付应用共用一个通用支付 TA (24)，有利于减少签名费用，避免移动终端安装到恶意的第三方支付应用，降低 TEE 的安全风险。

基于生物识别技术的移动支付设备、方法和装置

本申请基于申请号为 201510821881.8、申请日为 2015 年 11 月 23 日的中国专利申请、以及申请号为 201510848445.X、申请日为 2015 年 11 月 27 日的中国专利申请提出，并要求该两件中国专利申请的优先权，该两件中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本公开涉及移动支付技术领域，特别涉及一种基于生物识别技术的移动支付设备、方法和装置。

背景技术

移动支付是近年来发展和普及的在线支付方式。传统的移动支付方式，需要用户输入较多位数的支付密码以完成支付流程。为了简化用户操作，出现了基于生物识别技术的移动支付方式，如指纹支付。通过采集、识别和验证用户的生物信息，并在生物信息验证通过的情况下直接完成支付流程，从而使得用户免于输入支付密码。

由于涉及资金交易，移动支付对支付环境的安全性具有较高要求。目前而言，采用英国 ARM (Advanced RISC Machines) 公司提供的 TrustZone 技术，能够为移动支付的安全性提供较为可靠的解决方案。根据 TrustZone 技术的规定，移动终端分为 REE (Rich Execution Environment, 富执行环境) 和 TEE (Trusted Execution Environment, 可信执行环境)。其中，REE 是普通的非保密执行环境，移动终端的操作系统运行于 REE 中，TEE 是安全的保密执行环境。REE 中运行有 CA (Client Application, 客户应用)，而 TEE 中运行有 TA (Trusted Application, 可信应用)。与 REE 中的 CA 所不同的是，TEE 为 TA 提供一系列的安全服务，包括应用执行的完整性、安全存储、与输入输出设备的安全交互、密钥管理、加密算法以及

与 REE 中的 CA 进行安全通信等。以指纹支付为例，指纹识别应用包括 CA 和 TA 两部分，指纹识别应用的 TA 用于采集、识别和验证指纹信息，并将指纹信息的验证结果提供给指纹识别应用的 CA。如果第三方支付应用直接从指纹识别应用的 CA 获取验证结果，由于指纹识别应用的 CA 运行于 REE 中，第三方支付应用获取的验证结果是不可信的。因此，第三方支付应用也相应包括 CA 和 TA 两部分，第三方支付应用的 TA 直接从指纹识别应用的 TA 获取可信的验证结果，并提供给第三方支付应用的 CA，从而确保获取的验证结果真实可靠。

在实际应用中，用户有在一台移动终端中安装使用多款不同的第三方支付应用的需求。例如，一台移动终端同时支持支付宝和微信支付两款第三方支付应用。目前，移动终端中安装第三方支付应用的 TA 包括如下两种方式：第一，在移动终端出厂之前，即将第三方支付应用的 TA 预先安装在移动终端的 TEE 中；第二，第三方支付应用的 TA 以 SP (Service Provider, 服务提供商) TA 的形式进行开发和签名，后期通过下载的方式载入至移动终端的 TEE 中。然而，不论通过上述何种安装方式，若移动终端需要同时支持多款第三方支付应用，则会带

来如下问题：

第一，由于 TA 只有在被正式地数字签名过之后，才能顺利通过 TEE 中的 Trusted OS (Trusted Operating System, 可信的操作系统) 对其的身份验证，进而在 TEE 中正常运行，而对 TA 进行数字签名需要向提供 TrustZone 技术的公司支付一定的费用，因此若移动终端同时支持多款第三方支付应用，则需支付多项签名费用，造成成本增加；

第二，由于 TEE 中存储有诸如联系人信息、IMEI (International Mobile Equipment Identity, 移动设备国际身份码) 等重要私密信息，这些重要私密信息对于 TEE 中运行的 TA 来说是可见的，若移动终端安装了恶意的第三方支付应用，则 TEE 中存储的重要私密信息可能会被肆意读取，TEE 存在较高的安全风险。

发明内容

为了克服相关技术存在的问题，本公开实施例提供了一种基于生物识别技术的移动支付设备、方法和装置。所述技术方案如下：

根据本公开实施例的第一方面，提供了一种基于生物识别技术的移动支付设备，所述移动支付设备包括：

生物信息识别应用、以及运行在 TEE 中的通用支付 TA；

所述通用支付 TA，用于供多个第三方支付应用调用，接收第三方支付应用的调用请求，根据所述调用请求确定需要加密的目标内容和执行加密所需的加密参数，从所述生物信息识别应用获取生物信息识别结果，根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密，向所述第三方支付应用返回加密结果，使得所述第三方支付应用根据所述加密结果执行支付相关操作。

可选地，所述通用支付 TA，用于在第三方支付应用开通基于生物识别技术的支付功能时，在所述通用支付 TA 未存储有所述第三方支付应用所对应的应用密钥的情况下，采用第一密钥生成算法生成所述第三方支付应用的应用密钥，采用第一数据加密算法和设备密钥对所述应用密钥进行加密；

以及，所述通用支付 TA，还用于采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所述用户密钥进行加密；

其中，所述通用支付 TA 将加密后的应用密钥和用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

其中，所述加密参数包括所述第一密钥生成算法、所述第一数据加密算法、所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

可选地，所述通用支付 TA，用于在第三方支付应用开通基于生物识别技术的支付功能时，在所述通用支付 TA 已存储有所述第三方支付应用所对应的应用密钥的情况下，采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所

述用户密钥进行加密；

其中，所述通用支付 TA 将加密后的用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

其中，所述加密参数包括所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

可选地，所述通用支付 TA，用于在第三方支付应用针对目标用户帐号执行支付操作时，在所述生物信息识别结果指示所述生物信息验证通过的情况下，通过所述加密参数和所述目标用户帐号所对应的用户密钥对所述目标内容进行加密，得到加密结果；

其中，所述通用支付 TA 将所述加密结果返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器。

可选地，所述生物信息识别结果由所述生物信息识别应用在接收到所述第三方支付应用的调用请求之后，采集、识别和验证所述生物信息之后得到，并由所述生物信息识别应用发送给所述第三方支付应用；

所述第三方支付应用用于在确认从所述生物信息识别应用获取的所述生物信息识别结果指示所述生物信息验证通过的情况下，向所述通用支付 TA 发送所述调用请求。

可选地，所述通用支付 TA 包括：算法管理模块、密钥管理模块、数据加密模块、结果获取模块和密钥存储模块；

所述算法管理模块，用于管理基于生物识别技术的第三方支付应用所采用的算法；其中，所述算法包括：至少一种密钥生成算法和至少一种数据加密算法；

所述密钥管理模块，用于采用所述密钥生成算法生成执行支付相关操作所需的密钥；

所述数据加密模块，用于采用所述数据加密算法对需要加密的目标内容进行加密；

所述结果获取模块，用于从所述生物信息识别应用获取所述生物信息识别结果；

所述密钥存储模块，用于存储所述密钥管理模块生成的所述密钥。

可选地，所述第三方支付应用为运行在 REE 中的 CA。

根据本公开实施例的第二方面，提供了一种基于生物识别技术的移动支付方法，应用于运行在 TEE 中的通用支付 TA 中，所述通用支付 TA 用于供多个第三方支付应用调用；

所述方法包括：

接收第三方支付应用的调用请求；

根据所述调用请求确定需要加密的目标内容和执行加密所需的加密参数；

从所述生物信息识别应用获取生物信息识别结果；

根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密；

向所述第三方支付应用返回加密结果，使得所述第三方支付应用根据所述加密结果执行支付相关操作。

可选地，在第三方支付应用开通基于生物识别技术的支付功能时，所述方法还包括：

在所述通用支付 TA 未存储有所述第三方支付应用所对应的应用密钥的情况下，采用第一

密钥生成算法生成所述第三方支付应用的应用密钥，采用第一数据加密算法和设备密钥对所述应用密钥进行加密；

采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所述用户密钥进行加密；

5 将加密后的应用密钥和用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

其中，所述加密参数包括所述第一密钥生成算法、所述第一数据加密算法、所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

10 可选地，在第三方支付应用开通基于生物识别技术的支付功能时，所述方法还包括：

在所述通用支付 TA 已存储有所述第三方支付应用所对应的应用密钥的情况下，采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所述用户密钥进行加密；

15 将加密后的用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

其中，所述加密参数包括所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

可选地，在第三方支付应用针对目标用户帐号执行支付操作时，所述根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密，包括：

20 在所述生物信息识别结果指示所述生物信息验证通过的情况下，通过所述加密参数和所述目标用户帐号所对应的用户密钥对所述目标内容进行加密，得到加密结果，将所述加密结果返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器。

25 可选地，所述生物信息识别结果由所述生物信息识别应用在接收到所述第三方支付应用的调用请求之后，采集、识别和验证所述生物信息之后得到，并由所述生物信息识别应用发送给所述第三方支付应用；

所述第三方支付应用在确认从所述生物信息识别应用获取的所述生物信息识别结果指示所述生物信息验证通过的情况下，向所述通用支付 TA 发送所述调用请求。

可选地，所述第三方支付应用为运行在 REE 中的 CA。

30 根据本公开实施例的第三方面，提供了一种基于生物识别技术的移动支付装置，所述装置包括：

生物信息识别应用以及运行在可信执行环境 TEE 中的通用支付可信应用 TA；

所述装置还包括：处理器；

用于存储所述处理器的可执行指令的存储器；

其中，所述处理器被配置为：

35 接收第三方支付应用的调用请求；

根据所述调用请求确定需要加密的目标内容和执行加密所需的加密参数；

从所述生物信息识别应用获取生物信息识别结果；

根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密；

向所述第三方支付应用返回加密结果，使得所述第三方支付应用根据所述加密结果执行

5 支付相关操作。

本公开实施例提供的技术方案可以包括以下有益效果：

通过在 TEE 中安装运行可供多个第三方支付应用调用的通用支付 TA；解决了相关技术在移动终端需要支持多款第三方支付应用时，因在 TEE 中安装多个相应的 TA 而导致成本增加，且导致 TEE 存在较高的安全风险的问题；实现了多个第三方支付应用共用一个通用支付 TA，10 无需在 TEE 中安装多个 TA，一方面有助于减少签名费用，降低成本，另一方面能够有效避免移动终端安装到恶意的第三方支付应用的 TA，降低 TEE 的安全风险。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

15

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

图 1 是根据一示例性实施例示出的一种基于生物识别技术的移动支付设备的框图；

20 图 2 是根据另一示例性实施例示出的一种基于生物识别技术的移动支付设备的框图；

图 3 是根据一示例性实施例示出的一种基于生物识别技术的移动支付方法的流程图；

图 4 是根据另一示例性实施例示出的一种基于生物识别技术的移动支付方法的流程图；

图 5 是根据另一示例性实施例示出的一种基于生物识别技术的移动支付方法的流程图；

图 6 是根据另一示例性实施例示出的一种基于生物识别技术的移动支付方法的流程图；

25 图 7 是根据一示例性实施例示出的一种移动支付设备的框图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的30 实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

本公开涉及的移动支付设备，可以是手机、平板电脑、移动 PC (Personal Computer, 个人计算机)、PDA (Personal Digital Assistant, 个人数字助理) 等移动终端设备。移动支付设备配置有用于采集生物信息的传感器，具备基于生物识别技术的移动支付功能。其中，35

生物信息包括但不限于：指纹、虹膜、视网膜、基因、声音、人脸、手掌几何、静脉、步态和笔迹中的任意一项或者多项。例如，移动支付设备配置有指纹传感器，具备指纹支付功能。

本公开一示例性实施例提供了一种基于生物识别技术的移动支付设备，该移动支付设备
5 包括：生物信息识别应用、以及运行在 TEE 中的通用支付 TA。

通用支付 TA，用于供多个第三方支付应用调用，接收第三方支付应用的调用请求，根据该调用请求确定需要加密的目标内容和执行加密所需的加密参数，从生物信息识别应用获取生物信息识别结果，根据加密参数和生物信息识别结果对目标内容进行加密，向第三方支付应用返回加密结果，使得第三方支付应用根据加密结果执行支付相关操作。

10 通过在 TEE 中安装运行可供多个第三方支付应用调用的通用支付 TA；解决了相关技术在移动终端需要支持多款第三方支付应用时，因在 TEE 中安装多个相应的 TA 而导致成本增加，且导致 TEE 存在较高的安全风险的问题；实现了多个第三方支付应用共用一个通用支付 TA，无需在 TEE 中安装多个 TA，一方面有助于减少签名费用，降低成本，另一方面能够有效避免移动终端安装到恶意的第三方支付应用的 TA，降低 TEE 的安全风险。

15 可选地，在第三方支付应用开通基于生物识别技术的支付功能时，在通用支付 TA 未存储有第三方支付应用所对应的应用密钥的情况下，通用支付 TA 用于采用第一密钥生成算法生成第三方支付应用的应用密钥，采用第一数据加密算法和设备密钥对应用密钥进行加密；

以及，通用支付 TA 还用于采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和应用密钥对用户密钥进行加密；

20 其中，通用支付 TA 将加密后的应用密钥和用户密钥返回给第三方支付应用，以通过第三方支付应用提供给后台服务器；

其中，加密参数包括第一密钥生成算法、第一数据加密算法、第二密钥生成算法和第二数据加密算法，由第三方支付应用调用通用支付 TA 时通过调用请求指示。

25 可选地，在第三方支付应用开通基于生物识别技术的支付功能时，在通用支付 TA 已存储有第三方支付应用所对应的应用密钥的情况下，通用支付 TA，用于采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和应用密钥对用户密钥进行加密；

其中，通用支付 TA 将加密后的用户密钥返回给第三方支付应用，以通过第三方支付应用提供给后台服务器；

30 其中，加密参数包括第二密钥生成算法和第二数据加密算法，由第三方支付应用调用通用支付 TA 时通过调用请求指示。

通过上述方式，在基于生物识别技术的支付功能的开通阶段，通用支付 TA 生成目标用户帐号所对应的用户密钥，并将该用户密钥提供给后台服务器，以便后台服务器在后续支付阶段采用该用户密钥对用户身份的合法性进行校验，确保交易安全性。

35 可选地，在第三方支付应用针对目标用户帐号执行支付操作时，通用支付 TA，用于在生物信息识别结果指示生物信息验证通过的情况下，通过加密参数和目标用户帐号所对应的用

户密钥对目标内容进行加密，得到加密结果；

其中，通用支付 TA 将加密结果返回给第三方支付应用，以通过第三方支付应用提供给后台服务器。

通过上述方式，在目标用户帐号的支付阶段，通用支付 TA 采用目标用户帐号所对应的用户密钥对后台服务器所需校验的目标内容进行加密，并将加密结果反馈给后台服务器，以便后台服务器依据解密结果实现对用户身份的合法性进行校验，确保交易安全性。

可选地，生物信息识别结果由生物信息识别应用在接收到第三方支付应用的调用请求之后，采集、识别和验证生物信息之后得到，并由生物信息识别应用发送给第三方支付应用；

第三方支付应用用于在确认从生物信息识别应用获取的生物信息识别结果指示生物信息验证通过的情况下，向通用支付 TA 发送调用请求。

通过上述方式，第三方支付应用首先对生物信息识别结果进行分析，在确认生物信息验证通过的情况下，调用通用支付 TA 执行支付相关操作，避免进行无谓的调用，确保调用流程的合理化和规范化。

可选地，通用支付 TA 包括：算法管理模块、密钥管理模块、数据加密模块、结果获取模块和密钥存储模块；

算法管理模块，用于管理基于生物识别技术的第三方支付应用所采用的算法；其中，上述算法包括：至少一种密钥生成算法和至少一种数据加密算法；

密钥管理模块，用于采用密钥生成算法生成执行支付相关操作所需的密钥；

数据加密模块，用于采用数据加密算法对需要加密的目标内容进行加密；

结果获取模块，用于从生物信息识别应用获取生物信息识别结果；

密钥存储模块，用于存储密钥管理模块生成的密钥。

通过上述方式，将通用支付 TA 的功能实现地更为通用，以便通用支付 TA 能够支持多款用户常用的不同第三方支付应用。

可选地，第三方支付应用为运行在 REE 中的 CA。

图 1 是根据一示例性实施例示出的一种基于生物识别技术的移动支付设备的框图。如图 1 所示，该移动支付设备包括：REE10 和 TEE20。

REE10 中运行有生物信息识别应用的 CA12。

TEE20 中运行有通用支付 TA24 和生物信息识别应用的 TA22。

其中，通用支付 TA24 供多个第三方支付应用的 CA14 调用。在本公开实施例中，若移动支付设备需要同时支持多款第三方支付应用，仅需在移动终端设备中安装运行该多款第三方支付应用的 CA14 即可，该多款第三方支付应用的 CA14 共用一个通用支付 TA24。

生物信息识别应用的 CA12 用于在被第三方支付应用的 CA14 调用后，调用生物信息识别应用的 TA22，生物信息识别应用的 TA22 用于采集、识别和验证生物信息。通用支付 TA24 用于在被第三方支付应用的 CA14 调用后，根据调用请求确定需要加密的目标内容和执行加密所

需的加密参数，从生物信息识别应用的 TA24 获取生物信息识别结果，根据加密参数和生物信息识别结果对目标内容进行加密，向第三方支付应用的 CA14 返回加密结果，使得第三方支付应用的 CA14 根据加密结果执行支付相关操作。

综上所述，本实施例提供的移动支付设备，通过在 TEE 中安装运行可供多个第三方支付应用调用的通用支付 TA；解决了相关技术在移动终端需要支持多款第三方支付应用时，因在 TEE 中安装多个相应的 TA 而导致成本增加，且导致 TEE 存在较高的安全风险的问题；实现了多个第三方支付应用共用一个通用支付 TA，无需在 TEE 中安装多个 TA，一方面有助于减少签名费用，降低成本，另一方面能够有效避免移动终端安装到恶意的第三方支付应用的 TA，降低 TEE 的安全风险。

图 2 是根据另一示例性实施例示出的一种基于生物识别技术的移动支付设备的框图。如图 2 所示，该移动支付设备包括：REE10 和 TEE20。

REE10 中运行有生物信息识别应用的 CA12。

TEE20 中运行有通用支付 TA24 和生物信息识别应用的 TA22。

其中，通用支付 TA24 供多个第三方支付应用的 CA14 调用。

生物信息识别应用的 CA12 用于在被第三方支付应用的 CA14 调用后，调用生物信息识别应用的 TA22，生物信息识别应用的 TA22 用于采集、识别和验证生物信息。通用支付 TA24 用于在被第三方支付应用的 CA14 调用后，根据调用请求确定需要加密的目标内容和执行加密所需的加密参数，从生物信息识别应用的 TA24 获取生物信息识别结果，根据加密参数和生物信息识别结果对目标内容进行加密，向第三方支付应用的 CA14 返回加密结果，使得第三方支付应用的 CA14 根据加密结果执行支付相关操作。

在本实施例中，如图 2 所示，通用支付 TA24 包括：算法管理模块 241、密钥管理模块 242、数据加密模块 243、结果获取模块 244 和密钥存储模块 245。

算法管理模块 241，用于管理基于生物识别技术的第三方支付应用所采用的算法。上述算法包括：至少一种密钥生成算法和至少一种数据加密算法。其中，密钥生成算法是指用于生成执行支付相关操作所需的密钥的算法。在本实施例中，密钥生成算法用于生成第三方支付应用所对应的应用密钥，以及登录第三方支付应用的用户帐号所对应的用户密钥。数据加密算法是指用于对需要加密的目标内容进行加密的算法。在支付流程中，目标内容可包括由第三方支付应用的 CA14 与后台服务器协商确定的内容，如订单号。在开通流程（即指开通基于生物识别技术的支付功能的流程）中，目标内容可包括生成的应用密钥或者用户密钥。考虑到在本公开实施例中，通用支付 TA24 供多个第三方支付应用的 CA14 共用，而不同的第三方支付应用对于密钥生成算法和数据加密算法可能具有不同的要求，即使同一款第三方支付应用在生成不同的密钥时或者在对不同的内容进行加密时，也有可能采用不同的密钥生成算法或者采用不同的数据加密算法，因此算法管理模块 241 管理有至少一种密钥生成算法和至少一种数据加密算法，例如在算法管理模块 241 中预配置若干种常用的密钥生成算法和若干

种常用的数据加密算法。另外，数据加密算法可以是数字签名算法。

可选地，上述算法还包括：至少一种数据散列算法。其中，数据散列算法是指用于提取需要加密的目标内容的散列值的算法。采用数据加密算法对提取到的散列值进行加密。基于同样的理由，由于通用支付 TA24 供多个第三方支付应用的 CA14 共用，因此算法管理模块 241 管理有至少一种数据散列算法，例如在算法管理模块 241 中预配置若干种常用的数据散列算法。

密钥管理模块 242，用于采用密钥生成算法生成执行支付相关操作所需的密钥。其中，所采用的密钥生成算法由第三方支付应用的 CA14 在调用通用支付 TA24 时的调用请求中用参数进行指示。

数据加密模块 243，用于采用数据加密算法对需要加密的目标内容进行加密。其中，所采用的数据加密算法由第三方支付应用的 CA14 在调用通用支付 TA24 时的调用请求中用参数进行指示。可选地，当数据加密算法为数字签名算法时，数据加密模块 243 被配置为采用数字加密算法对目标内容进行数字签名。

结果获取模块 244，用于从生物信息识别应用的 TA22 获取生物信息识别结果。在本公开实施例中，生物信息识别应用用于对下列一项或者多项生物信息进行识别：指纹、虹膜、视网膜膜、基因、声音、人脸、手掌几何、静脉、步态和笔迹等。结合参考图 2，生物信息识别应用的 TA22 包括：采集模块 221、算法模块 222、识别模块 223 和存储模块 224。采集模块 221 被配置为获取用于采集生物信息的传感器采集得到的生物信息的原始数据。以指纹为例，当指纹传感器为摄像头时，采集模块 221 被配置为获取摄像头采集得到的指纹图像。算法模块 222 被配置为将生物信息的原始数据转换为数字数据。一方面，能够有效减少生物信息所需占用的存储空间；另一方面，由于直接存储生物信息的原始数据存在被复制的风险，将生物信息的原始数据转换为数字数据之后，能够提高生物信息的安全性。识别模块 223 被配置为将当前采集的生物信息与预先存储的生物信息进行匹配验证，得到识别结果。存储模块 224 被配置为存储生物信息和识别结果。

密钥存储模块 245，用于存储密钥管理模块 242 生成的密钥。在本公开实施例中，密钥存储模块 245 用于存储应用密钥和用户密钥。

可选地，密钥管理模块 242，还用于采用安全性保护算法对密钥进行处理，并将处理后的密钥存储至密钥存储模块 245 中。其中，安全性保护算法是指用于对密钥进行安全性保护的算法，包括但不限于数据加密算法、数据分割与拼装算法等。

下面，分别从开通流程（即指开通基于生物识别技术的支付功能的流程）和支付流程两个方面，对本实施例提供的系统进行介绍和说明。

1、开通流程（以第三方支付应用中的目标用户帐号为例）

第三方支付应用的 CA14，用于调用通用支付 TA24，请求通用支付 TA24 生成目标用户帐号所对应的用户密钥。

在密钥存储模块 245 中未存储有第三方支付应用所对应的应用密钥的情况下，通用支付

TA24, 用于采用第一密钥生成算法生成第三方支付应用的应用密钥; 通过数据加密模块 243 采用第一数据加密算法和设备密钥对应用密钥进行加密; 将加密后的应用密钥返回给第三方支付应用的 CA14, 以通过第三方支付应用的 CA14 提供给后台服务器; 以及, 通用支付 TA24, 还用于采用第二密钥生成算法生成目标用户帐号所对应的用户密钥; 通过数据加密模块 243 采用第二数据加密算法和应用密钥对用户密钥进行加密; 将加密后的用户密钥返回给第三方支付应用的 CA14, 以通过第三方支付应用的 CA14 提供给后台服务器。其中, 所采用的第一密钥生成算法、第一数据加密算法、第二密钥生成算法和第二数据加密算法, 由第三方支付应用的 CA14 调用通用支付 TA24 时通过调用请求指示。

在密钥存储模块 245 中已存储有第三方支付应用所对应的应用密钥的情况下, 通用支付 TA24, 用于采用第二密钥生成算法生成目标用户帐号所对应的用户密钥; 通过数据加密模块 243 采用第二数据加密算法和应用密钥对用户密钥进行加密; 将加密后的用户密钥返回给第三方支付应用的 CA14, 以通过第三方支付应用的 CA14 提供给后台服务器。其中, 所采用的第二密钥生成算法和第二数据加密算法, 由第三方支付应用的 CA14 调用通用支付 TA24 时通过调用请求指示。

可选地, 设备密钥、应用密钥和用户密钥中的任意一项或者多项为非对称密钥。

2、支付流程 (以第三方支付应用中的目标用户帐号为例)

第三方支付应用的 CA14, 用于调用生物信息识别应用的 CA12, 请求生物信息识别应用的 CA12 调用生物信息识别应用的 TA22 以采集、识别和验证生物信息。

第三方支付应用的 CA14, 还用于与后台服务器协商支付流程中所需校验的目标内容; 在生物信息识别应用的 CA12 获取到生物信息识别结果之后, 调用通用支付 TA24, 请求通用支付 TA24 对目标内容进行加密。

通用支付 TA24, 用于通过结果获取模块 244 从生物信息识别应用的 TA22 获取生物信息识别结果; 在生物信息识别结果指示生物信息验证通过的情况下, 通过数据加密模块 243 采用指定的数据加密算法和目标用户帐号所对应的用户密钥对目标内容进行加密, 得到加密结果。

第三方支付应用的 CA14, 还用于从通用支付 TA24 获取加密结果; 将加密结果发送给后台服务器; 其中, 后台服务器用于采用目标用户帐号所对应的用户密钥对加密结果进行解密, 得到解密内容, 并在解密内容与目标内容相符的情况下, 完成支付流程。

综上所述, 本实施例提供的移动支付设备, 通过在 TEE 中安装运行可供多个第三方支付应用调用的通用支付 TA; 解决了相关技术在移动终端需要支持多款第三方支付应用时, 因在 TEE 中安装多个相应的 TA 而导致成本增加, 且导致 TEE 存在较高的安全风险的问题; 实现了多个第三方支付应用共用一个通用支付 TA, 无需在 TEE 中安装多个 TA, 一方面有助于减少签名费用, 降低成本, 另一方面能够有效避免移动终端安装到恶意的第三方支付应用的 TA, 降低 TEE 的安全风险。

此外, 考虑到不同的第三方支付应用对密钥生成算法、数据加密算法等算法可能具有不

同的要求，通过在通用支付 TA 中预配置若干种常用的算法，使得通用支付 TA 能够支持多款用户常用的不同第三方支付应用。此外，由于通用支付 TA 中存储的算法是可以在后续设备升级的过程中进行更新的，因此通用支付 TA 有能力兼容更多的第三方支付应用。

需要说明的一点是，上述实施例中涉及的通用支付 TA 在实现其功能时，仅以上述各个功能模块的划分进行举例说明，实际应用中，可以根据实际需要而将上述功能分配由不同的功能模块完成，以完成以上描述的全部或者部分功能。

图 3 是本发明一个实施例提供的一种基于生物识别技术的移动支付方法的流程图。该方法可应用于上述图 1 或者图 2 所示实施例提供的移动支付设备中运行的通用支付 TA 中。该方法可包括如下步骤。

在步骤 302 中，接收第三方支付应用的调用请求。

在步骤 304 中，根据调用请求确定需要加密的目标内容和执行加密所需的加密参数。

在步骤 306 中，从生物信息识别应用获取生物信息识别结果。

在步骤 308 中，根据加密参数和生物信息识别结果对目标内容进行加密。

在步骤 310 中，向第三方支付应用返回加密结果，使得第三方支付应用根据加密结果执行支付相关操作。

综上所述，本实施例提供的移动支付方法，通过在 TEE 中安装运行可供多个第三方支付应用调用的通用支付 TA；解决了相关技术在移动终端需要支持多款第三方支付应用时，因在 TEE 中安装多个相应的 TA 而导致成本增加，且导致 TEE 存在较高的安全风险的问题；实现了多个第三方支付应用共用一个通用支付 TA，无需在 TEE 中安装多个 TA，一方面有助于减少签名费用，降低成本，另一方面能够有效避免移动终端安装到恶意的第三方支付应用的 TA，降低 TEE 的安全风险。

可选地，在第三方支付应用开通基于生物识别技术的支付功能时，所述方法还包括：

在所述通用支付 TA 未存储有所述第三方支付应用所对应的应用密钥的情况下，采用第一密钥生成算法生成所述第三方支付应用的应用密钥，采用第一数据加密算法和设备密钥对所述应用密钥进行加密；

采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所述用户密钥进行加密；

将加密后的应用密钥和用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

其中，所述加密参数包括所述第一密钥生成算法、所述第一数据加密算法、所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

可选地，在第三方支付应用开通基于生物识别技术的支付功能时，所述方法还包括：

在所述通用支付 TA 已存储有所述第三方支付应用所对应的应用密钥的情况下，采用第二

密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所述用户密钥进行加密；

将加密后的用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

5 其中，所述加密参数包括所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

可选地，在第三方支付应用针对目标用户帐号执行支付操作时，所述根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密，包括：

10 在所述生物信息识别结果指示所述生物信息验证通过的情况下，通过所述加密参数和所述目标用户帐号所对应的用户密钥对所述目标内容进行加密，得到加密结果，将所述加密结果返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器。

可选地，所述生物信息识别结果由所述生物信息识别应用在接收到所述第三方支付应用的调用请求之后，采集、识别和验证所述生物信息之后得到，并由所述生物信息识别应用发送给所述第三方支付应用；

15 所述第三方支付应用用于在确认从所述生物信息识别应用获取的所述生物信息识别结果指示所述生物信息验证通过的情况下，向所述通用支付 TA 发送所述调用请求。

可选地，所述第三方支付应用为运行在 REE 中的 CA。

20 图 4 是本发明另一实施例提供的一种基于生物识别技术的移动支付方法的流程图。该方法可包括如下步骤。

在步骤 402 中，第三方支付应用的 CA 调用生物信息识别应用的 CA，请求生物信息识别应用的 CA 调用生物信息识别应用的 TA 以采集、识别和验证生物信息。

在步骤 404 中，第三方支付应用的 CA 调用通用支付 TA。

25 在步骤 406 中，通用支付 TA 接收第三方支付应用的调用请求，根据调用请求确定需要加密的目标内容和执行加密所需的加密参数，从生物信息识别应用的 TA 获取生物信息识别结果，通用支付 TA 根据加密参数和生物信息识别结果对目标内容进行加密，向第三方支付应用的 CA 返回加密结果，使得第三方支付应用的 CA 根据加密结果执行支付相关操作。

30 综上所述，本实施例提供的移动支付方法，通过在 TEE 中安装运行可供多个第三方支付应用的 CA 调用的通用支付 TA；解决了相关技术在移动终端需要支持多款第三方支付应用时，因在 TEE 中安装多个相应的 TA 而导致成本增加，且导致 TEE 存在较高的安全风险的问题；实现了多个第三方支付应用的 CA 共用一个通用支付 TA，无需在 TEE 中安装多个 TA，一方面有助于减少签名费用，降低成本，另一方面能够有效避免移动终端安装到恶意的第三方支付应用的 TA，降低 TEE 的安全风险。

35 下面，通过图 5 和图 6 所示的两个方法实施例，分别从开通流程和支付流程两个方面进

行介绍和说明。

在图 5 所示实施例中，以第三方支付应用中的目标用户帐号的开通流程为例。如图 5 所示，该开通流程可包括如下几个步骤。

5 在步骤 501 中，第三方支付应用的 CA 调用通用支付 TA，请求通用支付 TA 生成第三方支付应用所对应的应用密钥。

其中，调用请求中携带有第一请求参数，该第一请求参数用于指示通用支付 TA 生成应用密钥的方式。依据 JCA (Java Cryptography Architecture, Java 加密体系结构) 的规定，在一种可能的实施方式中，第一请求参数包括 provider 参数、alias 参数和 algorithm 参数。其中，provider 参数用于指示调用通用支付 TA；alias 参数用于指示生成应用密钥的方式，
10 可以是第三方支付应用的标识，此时，通过第三方支付应用的标识，能够确定出生成密钥的方式；algorithm 参数用于指示生成应用密钥所采用的算法。

在步骤 502 中，通用支付 TA 检测是否已存储有第三方支付应用所对应的应用密钥。若否，则执行下述步骤 503；若是，则向第三方支付应用的 CA 反馈已经有应用密钥的指示信息。

在步骤 503 中，通用支付 TA 采用第一密钥生成算法生成应用密钥。

15 在步骤 504 中，通用支付 TA 采用第一数据加密算法和设备密钥对应用密钥进行加密，得到加密后的应用密钥。

可选地，若设备密钥为非对称密钥，通用支付 TA 采用第一数据加密算法和设备密钥的私钥对应用密钥进行加密，得到加密后的应用密钥。

可选地，当第一数据加密算法为数字签名算法时，通用支付 TA 采用数字签名算法和设备
20 密钥对应用密钥进行签名，得到应用密钥的签名结果。

在步骤 505 中，通用支付 TA 将加密后的应用密钥反馈给第三方支付应用的 CA。

在步骤 506 中，第三方支付应用的 CA 将加密后的应用密钥发送给后台服务器。

在步骤 507 中，后台服务器存储应用密钥。

后台服务器从第三方支付应用的 CA 接收加密后的应用密钥之后，采用设备密钥进行解
25 密，获取并存储应用密钥。

可选地，若设备密钥为非对称密钥，后台服务器采用设备密钥的公钥进行解密，获取并存储应用密钥。

此外，第三方支付应用的 CA 接收到通用支付 TA 反馈的应用密钥之后，还执行如下步骤
508。

30 在步骤 508 中，第三方支付应用的 CA 调用通用支付 TA，请求通用支付 TA 生成目标用户帐号所对应的用户密钥。

其中，调用请求中携带有第二请求参数，该第二请求参数用于指示通用支付 TA 生成用户密钥的方式。在一种可能的实施方式中，第二请求参数包括 provider 参数、alias 参数和 algorithm 参数。其中，provider 参数用于指示调用通用支付 TA；alias 参数用于指示生成
35 用户密钥的方式，例如可以是第三方支付应用的标识和目标用户帐号；algorithm 参数用于

指示生成用户密钥所采用的算法。

在步骤 509 中，通用支付 TA 采用第二密钥生成算法生成用户密钥。

在步骤 510 中，通用支付 TA 采用第二数据加密算法和应用密钥对用户密钥进行加密，得到加密后的用户密钥。

5 可选地，若应用密钥为非对称密钥，通用支付 TA 采用第二数据加密算法和应用密钥的私钥对用户密钥进行加密，得到加密后的用户密钥。

可选地，当第二数据加密算法为数字签名算法时，通用支付 TA 采用数字签名算法和应用密钥对用户密钥进行签名，得到用户密钥的签名结果。

在步骤 511 中，通用支付 TA 将加密后的用户密钥反馈给第三方支付应用的 CA。

10 在步骤 512 中，第三方支付应用的 CA 将加密后的用户密钥发送给后台服务器。

在步骤 513 中，后台服务器存储用户密钥。

后台服务器从第三方支付应用的 CA 接收加密后的用户密钥之后，采用应用密钥进行解密，获取并存储用户密钥。

15 可选地，若应用密钥为非对称密钥，后台服务器采用应用密钥的公钥进行解密，获取并存储用户密钥。

在图 6 所示实施例中，以第三方支付应用中的目标用户帐号的支付流程为例。如图 6 所示，该支付流程可包括如下几个步骤。

20 在步骤 601 中，第三方支付应用的 CA 调用生物信息识别应用的 CA，请求生物信息识别应用的 CA 调用生物信息识别应用的 TA。

在支付流程中，第三方支付应用的 CA 从后台服务器请求获取订单之后，调用生物信息识别应用的 CA，请求生物信息识别应用的 CA 调用生物信息识别应用的 TA，发起生物信息验证。

在步骤 602 中，生物信息识别应用的 CA 调用生物信息识别应用的 TA。

在步骤 603 中，生物信息识别应用的 TA 采集、识别和验证生物信息。

25 在步骤 604 中，生物信息识别应用的 TA 将生物信息识别结果反馈给生物信息识别应用的 CA。

在步骤 605 中，生物信息识别应用的 CA 将生物信息识别结果反馈给第三方支付应用的 CA。

30 在步骤 606 中，第三方支付应用的 CA 检测生物信息识别结果是否指示生物信息验证通过。若是，则执行下述步骤 607；若否，则结束流程。

在步骤 607 中，第三方支付应用的 CA 调用通用支付 TA，请求通用支付 TA 对目标内容进行加密。

35 其中，目标内容是第三方支付应用的 CA 与后台服务器协商的在支付流程中所需校验的内容。调用请求中携带有请求参数，该请求参数用于指示通用支付 TA 对目标内容进行加密的方式。在一种可能的实施方式中，请求参数包括 provider 参数、alias 参数和 algorithm 参数。

其中, provider 参数用于指示调用通用支付 TA; alias 参数可以是第三方支付应用的标识和目标用户帐号, alias 参数可作为密钥的索引, 用于指示加密所采用的用户密钥; algorithm 参数用于指示所采用的数据加密算法。

在步骤 608 中, 通用支付 TA 从生物信息识别应用的 TA 获取生物信息识别结果。

5 在步骤 609 中, 在生物信息识别结果指示生物信息验证通过的情况下, 通用支付 TA 采用指定的数据加密算法和登录第三方支付应用的目标用户帐号所对应的用户密钥对目标内容进行加密, 得到加密结果。

可选地, 若用户密钥为非对称密钥, 则通用支付 TA 采用预定的数据加密算法和用户密钥的私钥对目标内容进行加密, 得到加密结果。

10 可选地, 当数据加密算法为数字签名算法时, 通用支付 TA 采用数字签名算法和用户密钥对目标内容进行数字签名, 得到签名结果。

在步骤 610 中, 通用支付 TA 将加密结果提供给第三方支付应用的 CA。

在步骤 611 中, 第三方支付应用的 CA 将加密结果发送给后台服务器。

15 在步骤 612 中, 后台服务器采用目标用户帐号所对应的用户密钥对加密结果进行解密, 得到解密内容, 并在解密内容与目标内容相符的情况下, 完成支付流程。

可选地, 若用户密钥为非对称密钥, 后台服务器采用用户密钥的公钥对加密结果进行解密, 得到解密内容。

20 本公开一示例性实施例还提供了一种基于生物识别技术的移动支付装置, 能够实现本公开提供的移动支付方法。所述装置包括:

生物信息识别应用以及运行在可信执行环境 TEE 中的通用支付可信应用 TA;

所述装置还包括: 处理器;

用于存储所述处理器的可执行指令的存储器;

其中, 所述处理器被配置为:

25 接收第三方支付应用的调用请求;

根据所述调用请求确定需要加密的目标内容和执行加密所需的加密参数;

从所述生物信息识别应用获取生物信息识别结果;

根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密;

30 向所述第三方支付应用返回加密结果, 使得所述第三方支付应用根据所述加密结果执行支付相关操作。

图 7 是根据一示例性实施例示出的一种移动支付设备 700 的框图。例如, 移动支付设备 700 可以是手机、平板电脑、移动 PC 以及 PDA 等。如图 7 所示, 移动支付设备 700 包括: 系统级芯片 (System-on-a-Chip, SoC) 702、存储器 704、电源组件 706、输入/输出 (I/O) 接口 708 以及传感器组件 710。

35

系统级芯片 702 为移动支付设备 700 主要的处理部件，用于控制移动支付设备 700 的整体操作。在本实施例中，系统级芯片 702 包括 REE 和 TEE。REE 中运行有生物信息识别应用的 CA。TEE 中运行有通用支付 TA 和生物信息识别应用的 TA。其中，通用支付 TA 供多个第三方支付应用的 CA 调用。生物信息识别应用的 CA 用于在被第三方支付应用的 CA 调用后，调用生物信息识别应用的 TA，生物信息识别应用的 TA 用于采集、识别和验证生物信息。通用支付 TA 用于在被第三方支付应用的 CA 调用后，根据调用请求确定需要加密的目标内容和执行加密所需的加密参数，从生物信息识别应用的 TA 获取生物信息识别结果，根据加密参数和生物信息识别结果对目标内容进行加密，向第三方支付应用的 CA 返回加密结果，使得第三方支付应用的 CA 根据加密结果执行支付相关操作。系统级芯片 702 可以包括一个或多个处理器来执行指令，以完成上述方法的全部或部分步骤。

存储器 704 被配置为存储各种类型的数据以支持在移动支付设备 700 的操作。这些数据的示例包括用于在移动支付设备 700 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 704 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器 (SRAM)，电可擦除可编程只读存储器 (EEPROM)，可擦除可编程只读存储器 (EPROM)，可编程只读存储器 (PROM)，只读存储器 (ROM)，磁存储器，快闪存储器，磁盘或光盘。

电源组件 706 为移动支付设备 700 的各种组件提供电力。电源组件 706 可以包括电源管理系统，一个或多个电源，及其他与为移动支付设备 700 生成、管理和分配电力相关联的组件。

I/O 接口 708 为系统级芯片 702 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

传感器组件 710 包括一个或多个传感器，用于为移动支付设备 700 提供各个方面的状态评估。在本实施例中，传感器组件 710 至少包括用于采集生物信息的传感器。其中，生物信息包括但不限于：指纹、虹膜、视网膜、基因、声音、人脸、手掌几何、静脉、步态和笔迹中的任意一项或者多项。例如，传感器组件 710 包括指纹传感器，用于采集指纹信息。

在示例性实施例中，移动支付设备 700 还包括以下一个或多个组件：多媒体组件、音频组件和通信组件。

在示例性实施例中，移动支付设备 700 可以被一个或多个应用专用集成电路 (ASIC)、数字信号处理器 (DSP)、数字信号处理设备 (DSPD)、可编程逻辑器件 (PLD)、现场可编程门阵列 (FPGA)、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 704，上述指令可由移动支付设备 700 的处理器执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器 (RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动支付设备 700 的处理器执行时，使得移动支付设备 700 能够执行上述方法。

5 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

权利要求

1、一种基于生物识别技术的移动支付设备，其特征在于，所述移动支付设备包括：

生物信息识别应用、以及运行在可信执行环境 TEE 中的通用支付可信应用 TA；

5 所述通用支付 TA，用于供多个第三方支付应用调用，接收第三方支付应用的调用请求，根据所述调用请求确定需要加密的目标内容和执行加密所需的加密参数，从所述生物信息识别应用获取生物信息识别结果，根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密，向所述第三方支付应用返回加密结果，使得所述第三方支付应用根据所述加密结果执行支付相关操作。

10

2、根据权利要求 1 所述的移动支付设备，其特征在于，

所述通用支付 TA，用于在第三方支付应用开通基于生物识别技术的支付功能时，在所述通用支付 TA 未存储有所述第三方支付应用所对应的应用密钥的情况下，采用第一密钥生成算法生成所述第三方支付应用的应用密钥，采用第一数据加密算法和设备密钥对所述应用密钥进行加密；

15

以及，所述通用支付 TA，还用于采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所述用户密钥进行加密；

其中，所述通用支付 TA 将加密后的应用密钥和用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

20 其中，所述加密参数包括所述第一密钥生成算法、所述第一数据加密算法、所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

3、根据权利要求 1 所述的移动支付设备，其特征在于，

25 所述通用支付 TA，用于在第三方支付应用开通基于生物识别技术的支付功能时，在所述通用支付 TA 已存储有所述第三方支付应用所对应的应用密钥的情况下，采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥对所述用户密钥进行加密；

30 其中，所述通用支付 TA 将加密后的用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器；

其中，所述加密参数包括所述第二密钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

4、根据权利要求 1 所述的移动支付设备，其特征在于，

所述通用支付 TA，用于在第三方支付应用针对目标用户帐号执行支付操作时，在所述生物信息识别结果指示所述生物信息验证通过的情况下，通过所述加密参数和所述目标用户帐号所对应的用户密钥对所述目标内容进行加密，得到加密结果；

其中，所述通用支付 TA 将所述加密结果返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器。

5、根据权利要求 1 或 4 所述的移动支付设备，其特征在于，

所述生物信息识别结果由所述生物信息识别应用在接收到所述第三方支付应用的调用请求之后，采集、识别和验证所述生物信息之后得到，并由所述生物信息识别应用发送给所述第三方支付应用；

所述第三方支付应用用于在确认从所述生物信息识别应用获取的所述生物信息识别结果指示所述生物信息验证通过的情况下，向所述通用支付 TA 发送所述调用请求。

6、根据权利要求 1 所述的移动支付设备，其特征在于，所述通用支付 TA 包括：算法管理模块、密钥管理模块、数据加密模块、结果获取模块和密钥存储模块；

所述算法管理模块，用于管理基于生物识别技术的第三方支付应用所采用的算法；其中，所述算法包括：至少一种密钥生成算法和至少一种数据加密算法；

所述密钥管理模块，用于采用所述密钥生成算法生成执行支付相关操作所需的密钥；

所述数据加密模块，用于采用所述数据加密算法对需要加密的目标内容进行加密；

所述结果获取模块，用于从所述生物信息识别应用获取所述生物信息识别结果；

所述密钥存储模块，用于存储所述密钥管理模块生成的所述密钥。

7、根据权利要求 1 所述的移动支付设备，其特征在于，所述第三方支付应用为运行在富执行环境 REE 中的客户应用 CA。

8、一种基于生物识别技术的移动支付方法，其特征在于，应用于运行在可信执行环境 TEE 中的通用支付可信应用 TA 中，所述通用支付 TA 用于供多个第三方支付应用调用；

所述方法包括：

接收第三方支付应用的调用请求；

根据所述调用请求确定需要加密的目标内容和执行加密所需的加密参数；

从所述生物信息识别应用获取生物信息识别结果；

根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密；

向所述第三方支付应用返回加密结果，使得所述第三方支付应用根据所述加密结果执行支付相关操作。

9、根据权利要求 8 所述的方法，其特征在于，在第三方支付应用开通基于生物识别技术的支付功能时，所述方法还包括：

在所述通用支付 TA 未存储有所述第三方支付应用所对应的应用密钥的情况下，采用第一
5 密钥生成算法生成所述第三方支付应用的应用密钥，采用第一数据加密算法和设备密钥对所
述应用密钥进行加密；

采用第二密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和
所述应用密钥对所述用户密钥进行加密；

10 将加密后的应用密钥和用户密钥返回给所述第三方支付应用，以通过所述第三方支付应
用提供给后台服务器；

其中，所述加密参数包括所述第一密钥生成算法、所述第一数据加密算法、所述第二密
钥生成算法和所述第二数据加密算法，由所述第三方支付应用调用所述通用支付 TA 时通过所
述调用请求指示。

15 10、根据权利要求 8 所述的方法，其特征在于，在第三方支付应用开通基于生物识别技
术的支付功能时，所述方法还包括：

在所述通用支付 TA 已存储有所述第三方支付应用所对应的应用密钥的情况下，采用第二
密钥生成算法生成目标用户帐号所对应的用户密钥，采用第二数据加密算法和所述应用密钥
对所述用户密钥进行加密；

20 将加密后的用户密钥返回给所述第三方支付应用，以通过所述第三方支付应用提供给后
台服务器；

其中，所述加密参数包括所述第二密钥生成算法和所述第二数据加密算法，由所述第三
方支付应用调用所述通用支付 TA 时通过所述调用请求指示。

25 11、根据权利要求 8 所述的方法，其特征在于，在第三方支付应用针对目标用户帐号执
行支付操作时，所述根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密，
包括：

在所述生物信息识别结果指示所述生物信息验证通过的情况下，通过所述加密参数和所
述目标用户帐号所对应的用户密钥对所述目标内容进行加密，得到加密结果，将所述加密结
30 果返回给所述第三方支付应用，以通过所述第三方支付应用提供给后台服务器。

12、根据权利要求 8 或 11 所述的方法，其特征在于，

所述生物信息识别结果由所述生物信息识别应用在接收到所述第三方支付应用的调用请
求之后，采集、识别和验证所述生物信息之后得到，并由所述生物信息识别应用发送给所述

第三方支付应用；

所述第三方支付应用在确认从所述生物信息识别应用获取的所述生物信息识别结果指示所述生物信息验证通过的情况下，向所述通用支付 TA 发送所述调用请求。

- 5 13、根据权利要求 8 所述的方法，其特征在于，所述第三方支付应用为运行在富执行环境 REE 中的客户应用 CA。

14、一种基于生物识别技术的移动支付装置，其特征在于，所述装置包括：

生物信息识别应用以及运行在可信执行环境 TEE 中的通用支付可信应用 TA；

- 10 所述装置还包括：处理器；

用于存储所述处理器的可执行指令的存储器；

其中，所述处理器被配置为：

接收第三方支付应用的调用请求；

根据所述调用请求确定需要加密的目标内容和执行加密所需的加密参数；

- 15 从所述生物信息识别应用获取生物信息识别结果；

根据所述加密参数和所述生物信息识别结果对所述目标内容进行加密；

向所述第三方支付应用返回加密结果，使得所述第三方支付应用根据所述加密结果执行支付相关操作。

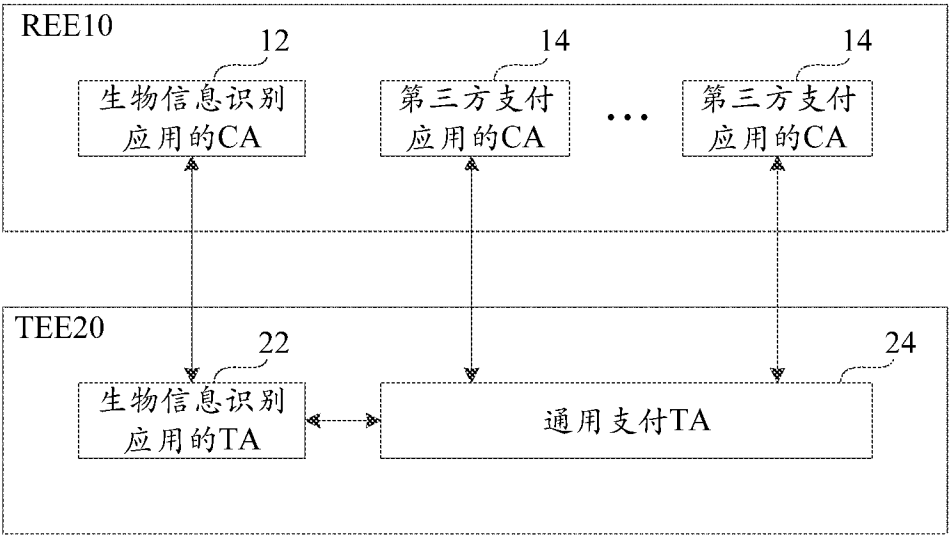


图 1

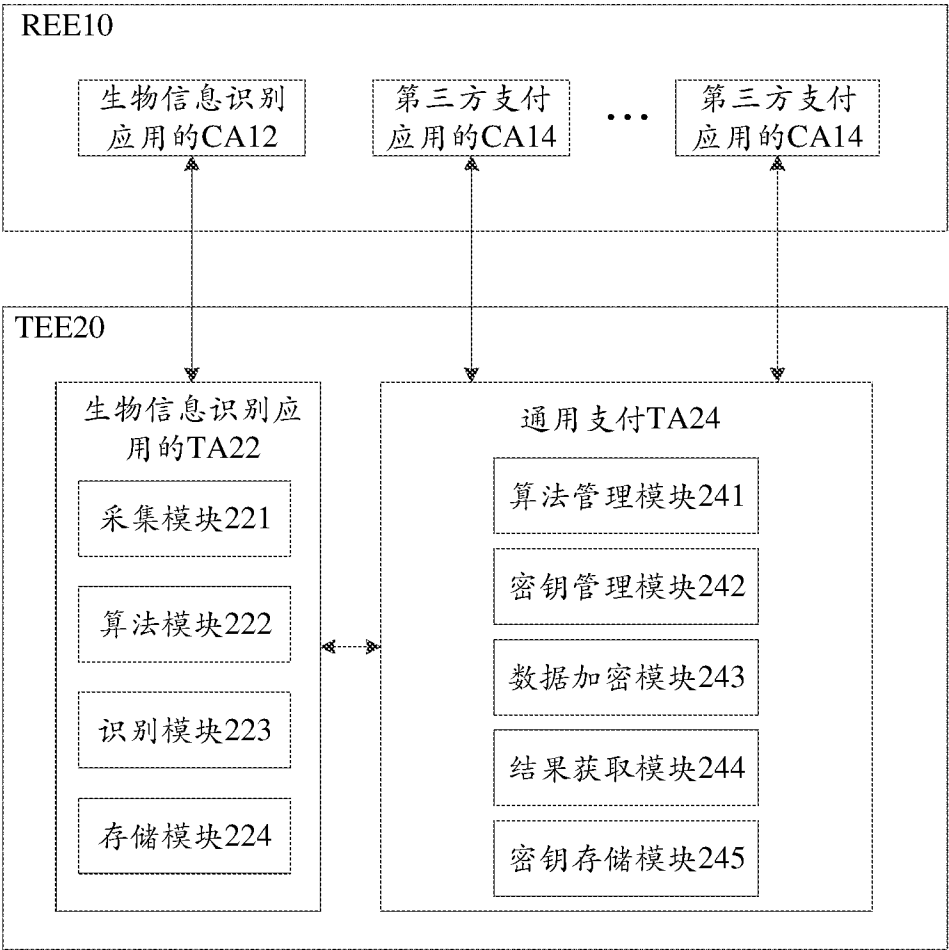


图 2

2/4

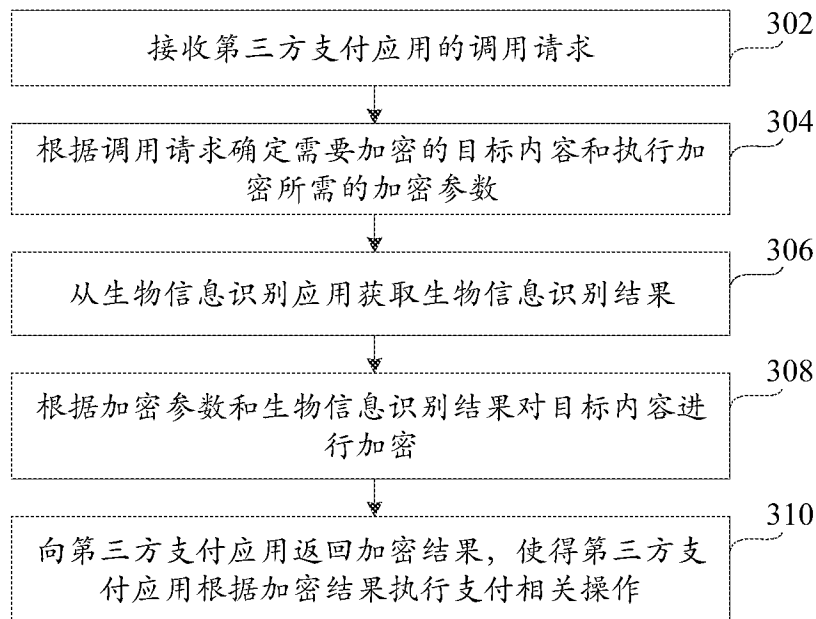


图 3

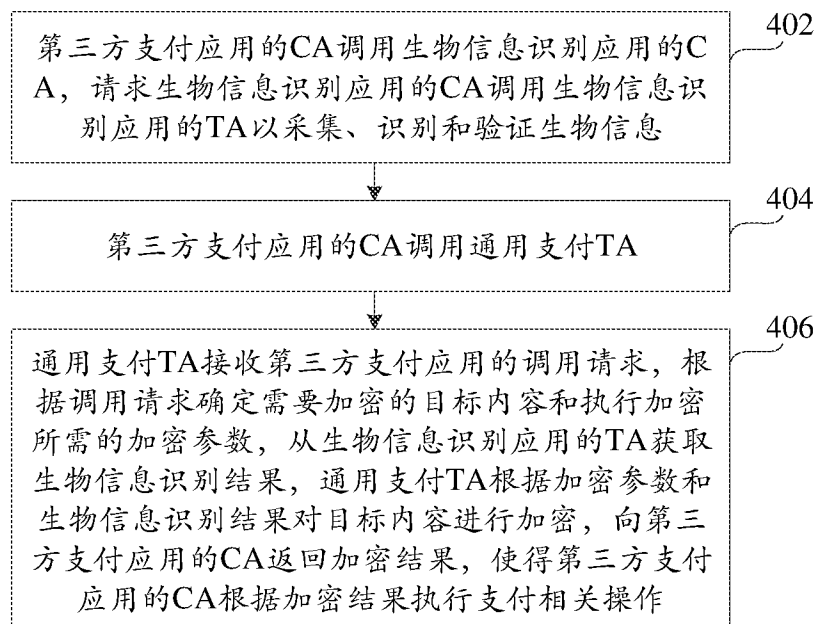


图 4

3/4

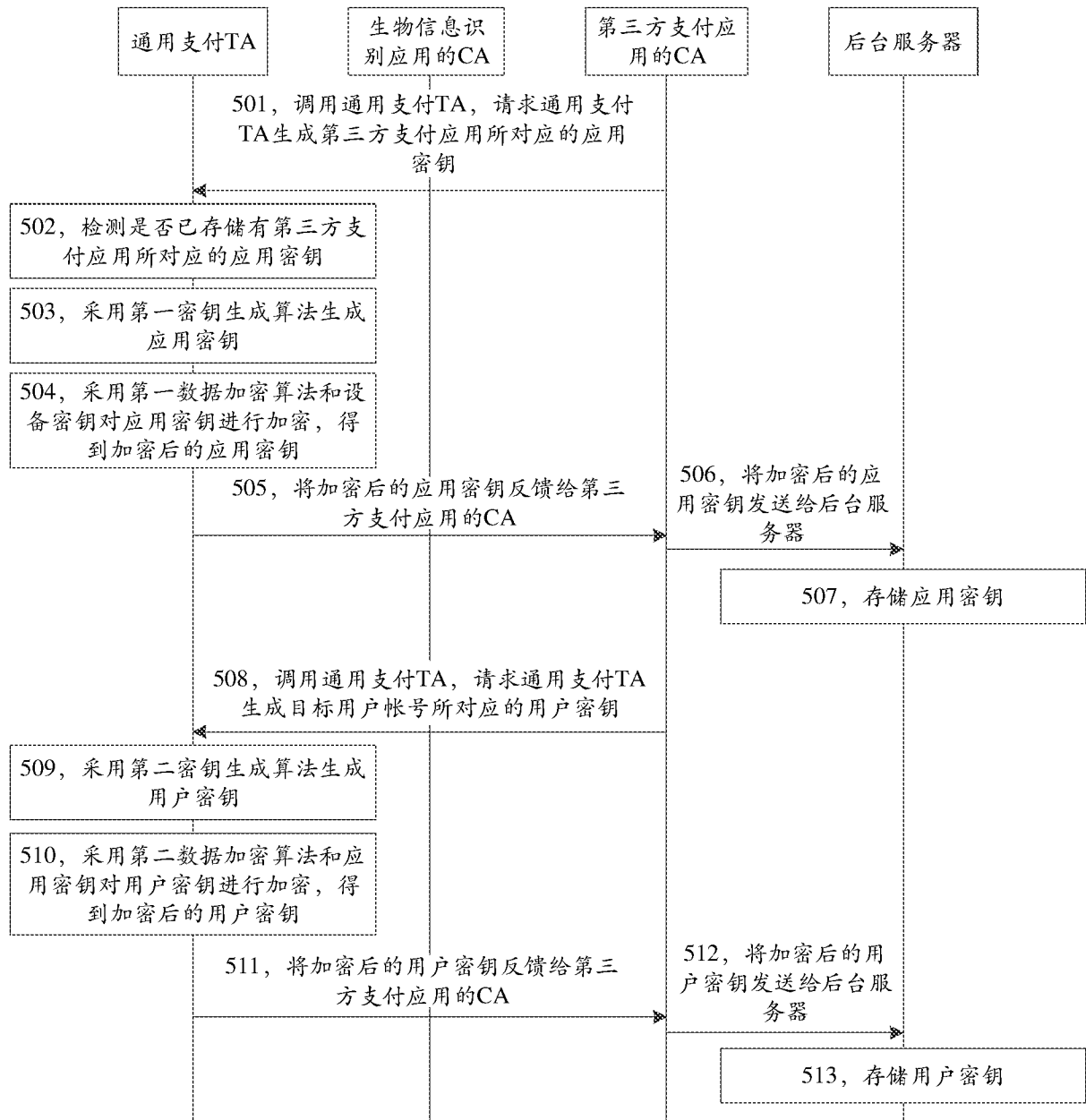


图 5

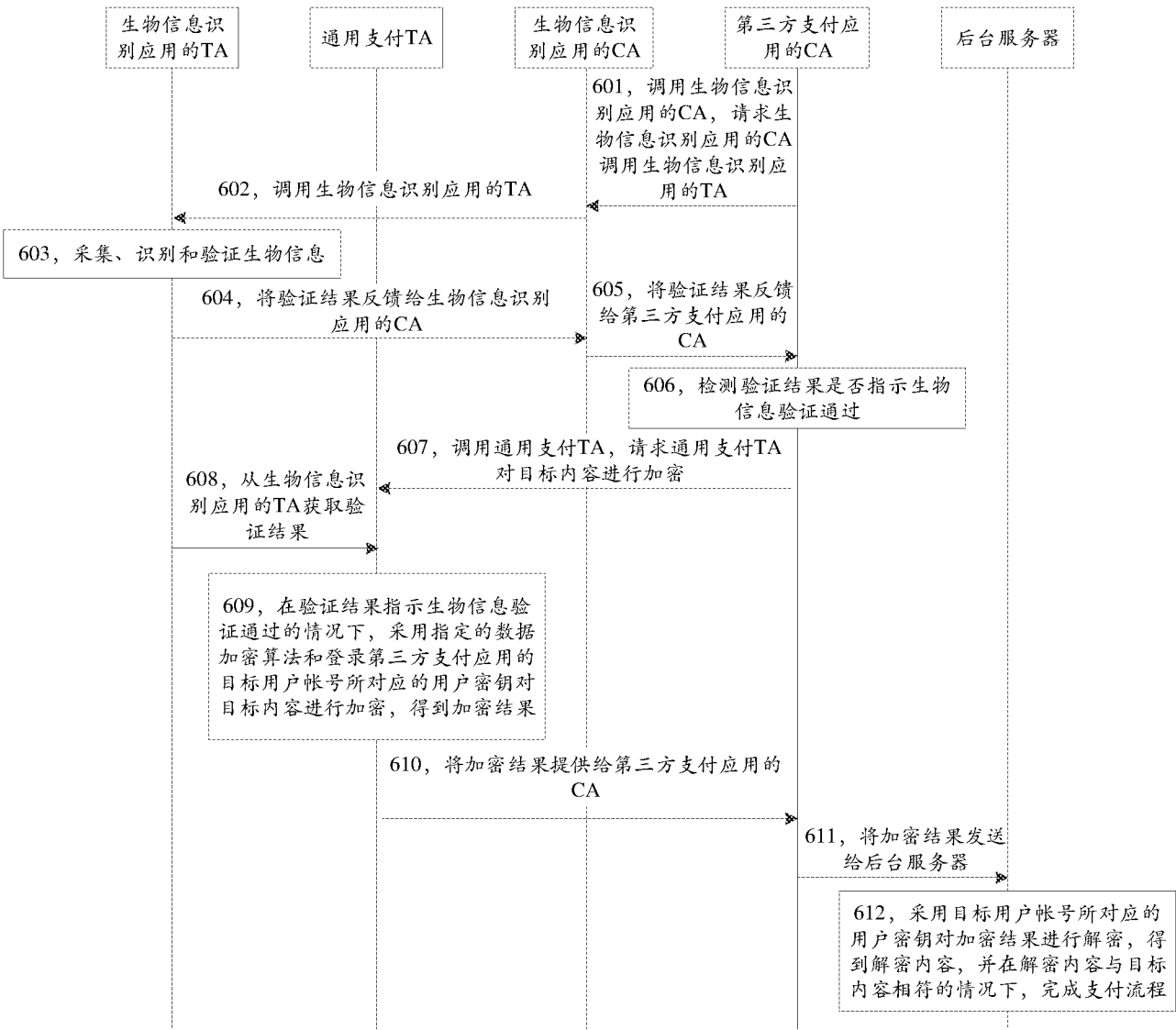


图 6

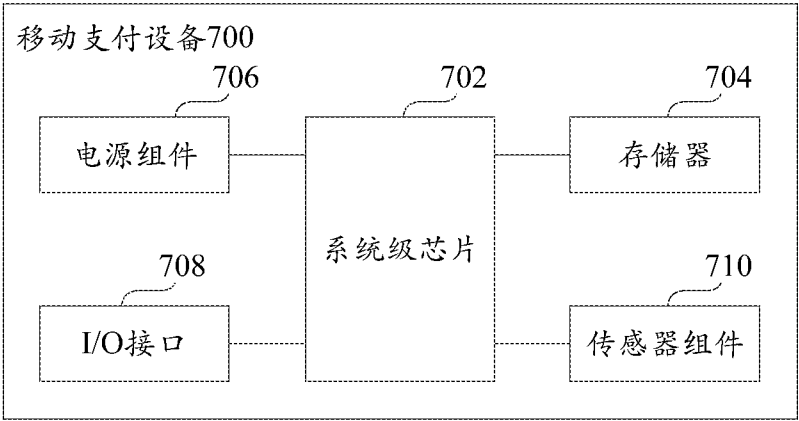


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/099616**A. CLASSIFICATION OF SUBJECT MATTER**

G06Q 20/02 (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, 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)

CNTXT; WOTXT: general, third party, call, finger print, trusted, application, TA, security, currency, third, party, pay+, transfer, request, encrypt+, biology, finger, mark, print

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104813349 A (GOOGLE INC.), 29 July 2015 (29.07.2015), the whole document	1-14
A	CN 103745155 A (EASTCOMPEACE TECHNOLOGY CO., LTD.), 23 April 2014 (23.04.2014), the whole document	1-14
A	CN 101986641 A (HANGZHOU SYNOCHIP TECHNOLOGIES CO., LTD.), 16 March 2011 (16.03.2011), the whole document	1-14
A	CN 103942880 A (SHANGHAI BOLU INFORMATION TECHNOLOGY CO. LTD.), 23 July 2014 (23.07.2014), the whole document	1-14

☐ 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 03 March 2016 (03.03.2016)	Date of mailing of the international search report 11 April 2016 (11.04.2016)
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 ZHAO, Weihua Telephone No.: (86-10) 62411830

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/099616

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104813349 A	29 July 2015	US 2014052637 A1	20 February 2014
		EP 2885753 A1	24 June 2015
		US 2014052532 A1	20 February 2014
		EP 2885753 A4	06 January 2016
		WO 2014028926 A1	20 February 2014
		US 2014052620 A1	20 February 2014
CN 103745155 A	23 April 2014	None	
CN 101986641 A	16 March 2011	None	
CN 103942880 A	23 July 2014	None	

A. 主题的分类 G06Q 20/02 (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, 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)) CNTXT: WOTXT: 可信, 应用, 安全, 通用, 第三方, 支付, 付款, 调用, 请求, 加密, 生物, 指纹, trusted, application, TA, security, currency, third, party, pay+, transfer, request, encrypt+, biology, finger, mark, print		
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	CN 104813349 A (谷歌公司) 2015年 7月 29日 (2015 - 07 - 29) 全文	1-14
A	CN 103745155 A (东信和平科技股份有限公司) 2014年 4月 23日 (2014 - 04 - 23) 全文	1-14
A	CN 101986641 A (杭州晟元芯片技术有限公司) 2011年 3月 16日 (2011 - 03 - 16) 全文	1-14
A	CN 103942880 A (上海博路信息技术有限公司) 2014年 7月 23日 (2014 - 07 - 23) 全文	1-14
☐ 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 3月 3日		国际检索报告邮寄日期 2016年 4月 11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		授权官员 赵伟华 电话号码 (86-10) 62411830

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/099616

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	104813349	A	2015年 7月 29日	US 2014052637 A1	2014年 2月 20日
				EP 2885753 A1	2015年 6月 24日
				US 2014052532 A1	2014年 2月 20日
				EP 2885753 A4	2016年 1月 6日
				WO 2014028926 A1	2014年 2月 20日
				US 2014052620 A1	2014年 2月 20日
CN	103745155	A	2014年 4月 23日	无	
CN	101986641	A	2011年 3月 16日	无	
CN	103942880	A	2014年 7月 23日	无	

表 PCT/ISA/210 (同族专利附件) (2009年7月)