

(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 11 月 23 日 (23.11.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/197974 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) G06Q 20/38 (2012.01)
H04L 9/32 (2006.01) G06Q 20/40 (2012.01)

(21) 国际申请号: PCT/CN2017/077512

(22) 国际申请日: 2017 年 3 月 21 日 (21.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610343447.8 2016年5月20日 (20.05.2016) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 丁林润 (DING, Linrun); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 李春欢 (LI, Chunhuan); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 回春野 (HUI, Chunye); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 彭蔚蔚 (PENG, Weiwei); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

(54) Title: BIOMETRIC CHARACTERISTIC-BASED SECURITY AUTHENTICATION METHOD, DEVICE AND ELECTRONIC EQUIPMENT

(54) 发明名称: 一种基于生物特征的安全认证方法、装置及电子设备

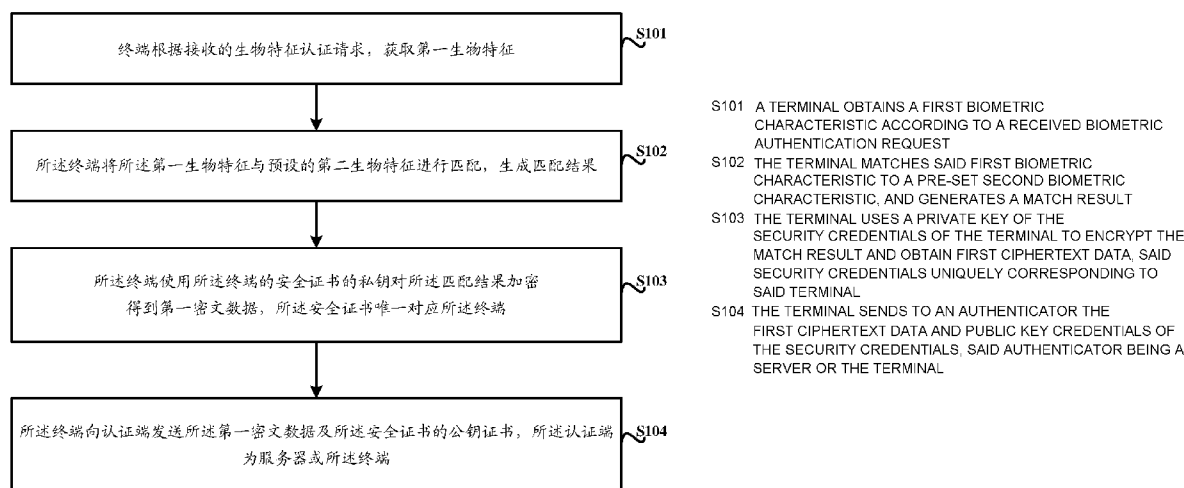


图 1

(57) Abstract: Disclosed in the present invention are a biometric characteristic-based security authentication method, device and electronic equipment, said method comprising: a terminal obtaining a first biometric characteristic according to a received biometric authentication request; the terminal matching said first biometric characteristic to a pre-set second biometric characteristic, generating a match result; the terminal using a private key of the security credentials of the terminal to encrypt the match result and obtain first ciphertext data, said security credentials uniquely corresponding to said terminal; the terminal sending to an authenticator the first ciphertext data and public key credentials of the security credentials, said authenticator being a server or the terminal. The present invention is used to solve the problem of security risks in current identity authentication.

JP, KE, KG, KH, KN, KP, KR, KW, 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))。

(57) 摘要: 本发明公开一种基于生物特征的安全认证方法、装置及电子设备, 该方法包括: 终端根据接收的生物特征认证请求, 获取第一生物特征; 所述终端将所述第一生物特征与预设的第二生物特征进行匹配, 生成匹配结果; 所述终端使用所述终端的安全证书的私钥对所述匹配结果加密得到第一密文数据, 所述安全证书唯一对应所述终端; 所述终端向认证端发送所述第一密文数据及所述安全证书的公钥证书, 所述认证端为服务器或所述终端, 用以解决现有身份认证存在安全隐患的问题。

一种基于生物特征的安全认证方法、装置及电子设备

本申请要求在 2016 年 5 月 20 日提交中华人民共和国知识产权局、申请号为 201610343447.8，发明名称为“一种基于生物特征的安全认证方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及电子通讯领域，尤其涉及一种基于生物特征的安全认证方法、装置及电子设备。

背景技术

随着诸如智能手机、平板电脑、智能电视等智能终端的不断发展和利用，人们利用智能终端设备越来越多地进行交易、获取服务，然而其中不可避免地会涉及到身份认证的问题。比如，用户在进行网上交易的过程中，需要将用户的支付信息提交给服务器端以实现支付功能，再比如，用户在网上获取某种服务时，需要将用户账户信息提交给服务器端以实现登录和服务获取。

关于身份认证的具体过程以现有的指纹认证技术举例来说：当用户需要进行认证时，首先客户端通过指纹传感器采集到用户指纹，然后提取指纹特征码，与指纹库中已保存的指纹特征识别样本进行特征匹配，该比对过程有两种模式：一种是在设备本地进行匹配，再将比对结果上传至服务器端；另一种是将指纹特征上传到服务器端，在服务器端进行匹配。最后如果匹配成功则认证通过。由于现有的指纹认证技术对于设备底层实现及传输过程的安全未做定义，所以就有可能导致匹配结果在设备上被第三方恶意软件等攻击者窃取或者篡改，或者在传输过程中被攻击者窃取或者篡改，一旦被篡改，假设一个本来认证失败应该被取消的交易，却因为认证通过导致交易成功，因此用户的账户安全就存在极大的安全隐患。

考虑金融领域对于支付交易的高安全性要求，目前的身份认证技术仍存在较大的安全隐患，因此亟需一种改进之后的身份认证方法可以避免现有的安全漏洞。

发明内容

本发明实施例提供一种基于生物特征的安全认证方法、装置及电子设备，用以解决现有身份认证存在安全隐患的问题。

第一方面，本发明实施例提供一种基于生物特征的安全认证方法，该方法包括：终端根据接收的生物特征认证请求，获取第一生物特征；所述终端将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果；所述终端使用所述终端的安全证书的私钥对所述匹配结果加密得到第一密文数据，所述安全证书唯一对应所述终端；

所述终端向认证端发送所述第一密文数据及所述安全证书的公钥证书，所述认证端为服务器或所述终端。

第二方面，本发明实施例进一步地提供一种基于生物特征的安全认证装置，该装置包括：收发单元，用于接收的生物特征认证请求；传感器，用于获取第一生物特征；匹配单元，用于将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果；

签名单元，用于使用所述终端的安全证书的私钥对所述匹配结果加密得到第一密文数据，所述安全证书唯一对应所述终端；

收发单元，还用于向认证端发送所述第一密文数据及所述安全证书的公钥证书，所述认证端为服务器或所述终端。

第三方面，本发明实施例提供一种电子设备，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所

述至少一个处理器执行，以使所述至少一个处理器能够执行上述本申请任意实施例提供的基于生物特征的安全认证方法。

第四方面，本发明实施例提供一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行上述任一项所述的基于生物特征的安全认证方法。

第五方面，本发明实施例提供一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述任一项所述的基于生物特征的安全认证方法。

本发明实施例一方面获取服务器端发送的关于生物特征的认证请求；根据所述认证请求获取第一认证信息集合，并将第一认证信息集合与安全存储区中第二认证信息集合进行匹配，所述第一认证信息集合至少包括采集的第一生物特征，所述第二认证信息集合至少包括预设的第二生物特征；另一方面利用预置的公私钥对匹配结果进行加密，并将签名后的匹配结果发送至服务器端，以便所述服务器端根据验签后匹配结果生成认证结果。可见，通过对匹配结果的签名保护，就可以保证匹配结果在传输过程中不被攻击者窃取或者篡改，进而得出正确的认证结果，保证了用户账户的安全。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图1为本发明实施例提供一种基于生物特征的安全认证方法流程示意图；

图2为本发明实施例提供一种安全证书分发架构；

图 3 为本发明实施例提供一种基于生物特征的安全认证系统;

图 4 为本发明实施例提供一种基于生物特征的联机安全认证方法流程示意图;

图 5 为本发明实施例提供一种基于生物特征的脱机安全认证方法流程示意图;

图 6 为本发明实施例提供一种认证端的解密过程;

图 7 为本发明实施例提供一种基于生物特征的纹认证的开通和绑定过程;

图 8 为本发明实施例提供一种基于生物特征的指纹认证替代密码的安全认证过程;

图 9 为本发明实施例提供一种基于生物特征的安全认证装置示意图;

图 10 为本发明实施例提供的一种电子设备的硬件结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明作进一步地详细描述,显然,所描述的实施例仅仅是本发明一部份实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

为了使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明作进一步地详细描述,显然,所描述的实施例仅仅是本发明一部份实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

本发明所涉及到的终端可以包括具有生物特征认证功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备,以及各种形式的用户设备(User Equipment,简称 UE),移动台(Mobile station,简称 MS),终端(terminal),终端设备(Terminal Equipment)等等。为方便

描述，本发明简称为终端。其中，所谓生物特征指的是指纹、虹膜、人脸、声纹等特征。

实施例一

参见图 1 所示，本发明实施例提供一种基于生物特征的安全认证方法流程示意图，具体地实现方法包括：

步骤 S101，终端根据接收的生物特征认证请求，获取第一生物特征。

步骤 S102，所述终端将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果。

步骤 S103，所述终端使用所述终端的安全证书的私钥对所述匹配结果加密得到第一密文数据，所述安全证书唯一对应所述终端。

步骤 S104，所述终端向认证端发送所述第一密文数据及所述安全证书的公钥证书，所述认证端为服务器或所述终端。

其中，生物特征认证请求中包含的要认证的生物特征是指纹、虹膜、声纹或者人脸等特征，所以当终端收到认证请求之后，向用户发出关于该生物特征采集的提示信息，用户输入该生物特征之后，传感器采集相应的生物特征，当然，该传感器可以集成在终端的内部，也可以作为单独的模块与终端通过接口连接，如下内容以传感器在终端内部的情景进行进一步地论述。

因为考虑到终端内部生成的匹配结果存在被篡改的风险，所以本发明实施例对匹配结果进行加密，具体做法是通过每个终端的安全证书对匹配结果进行数字签名，其中，终端的安全证书是通过证书系统按照设定规则分发得到的，例如图 2 所示，证书授权中心 (CA) 授权指纹服务证书注册系统 (RA)，由 RA 给终端制造商颁布证书。终端制造商负责自行颁发并管理终端的公钥证书，RA 不再参与颁发。当然若终端制造商不具备证书管理的能力，可由 RA 通过虚拟厂商的方式代替为每个终端颁发终端的安全证书。另外，终端制造商为终端颁发终端的公钥证书可以包含图中的三种类型：匹配单元证书、签名单元证书、传感器证书。其中：签名单元证书为必需，其作用是为了验证

后续验证匹配结果的真伪并将匹配结果进行签名后发送给认证端；而匹配单元证书和传感器证书为可选，其作用主要是为了建立第一安全通道和第二安全通道，保证安全通信，当然也可以采取其他不低于 TLS2.0 安全级别的认证方式进行替代。

当终端具有证书系统下发的安全证书时，利用匹配单元证书和传感器证书预先建立第一安全通道和第二安全通道，进一步地，所述终端将传感器采集的第一生物特征通过第一安全通道发送给所述终端的匹配单元；

所述匹配单元将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果，并将所述匹配结果通过第二安全通道发送给所述终端的签名单元，所述匹配单元中存储有所述第二生物特征；

所述签名单元使用先使用哈希函数对所述匹配结果生成匹配结果的摘要，再使用所述终端的安全证书对所述摘要加密，得到签名数据，所述签名单元中存储有所述终端的安全证书。

可见，传感器用于采集生物特征；匹配单元用于将采集到的生物特征与预先存储的生物特征进行匹配，生成匹配结果；签名单元用于对匹配结果进行数字签名，匹配单元和签名单元为集成在终端内部的单元，增加安全通道的目的是保证无论是指纹等生物特征的传输，还是匹配成功或者是失败的匹配结果均在安全通道中传输，保证这类敏感数据不会在传输过程中被窃取或篡改，进而保证通信安全。

其中，在终端启动时即建立第一安全通道和第二安全通道，所述传感器与所述匹配单元通过握手协议完成单向或者双向身份认证和会话密钥交换，从而建立所述第一安全通道；

所述匹配单元与所述签名单元通过握手协议完成单向或者双向身份认证和会话密钥交换，从而建立所述第二安全通道。

具体地，安全通道的建立协议由握手协议和记录协议两部分组成。其中握手协议用于完成匹配单元和签名单元之间的双向身份认证和会话密钥的交换过程，也用于完成匹配单元和传感器之间的双向身份认证和会话密钥交换

过程。记录协议用于完成应用数据的加密传输。另外，安全通道的建立协议遵循 TLS 1.2 及以上版本规范要求，或采取其他不低于 TLS1.2 安全级别的认证方式。

这样做的目的是限定终端应使用签名单元进行指纹的签名认证，以及保证用户标识代码（PIN）等敏感信息的安全输入和加密处理，并且支持传感器对采集后的指纹数据加密传输，支持指纹模板数据与终端绑定后加密存储。具有生物特征认证的终端能够安全地存储密钥，禁止外部对密钥的直接访问，并通过有效的安全机制防止密钥被非法注入、替换和使用，并保证用于安全认证的签名单元和匹配单元不被非法攻击。

因为认证端可以是服务器也可以是终端自身，所以就存在联机认证和脱机认证这样两种场景，当联机认证时，认证端就可以是应用 APP 对应的服务器；当脱机认证时，认证端就可以是终端内部的应用 APP，以生物特征认证是指纹认证为例，图 3 示例性地示出了联机认证和脱机认证对应的认证系统，其中，该系统中包括：指纹传感器、指纹匹配单元、指纹签名单元、终端收发单元、应用的 APP、应用的服务器、证书授权中心，具体地：

指纹传感器负责指纹采集，并将采集到的指纹模板信息加密传输给指纹服务；指纹匹配单元负责指纹模板信息加密存储、指纹运算、指纹比对等基础应用功能；指纹签名单元作为设备安全基础，提供安全认证服务，负责对指纹比对结果等关键数据进行数字签名；终端收发单元对指纹认证相关的接口调用进行封装，为上层应用程序调用底层功能提供统一的接口；应用 APP，比如 PC 端的支付网关页面或者时移动端的 APP，主要是提供用户交互界面，通过调用指纹服务的应用程序接口来调用设备的指纹功能。并且应用 APP 可以对签名后的第一密文数据进行脱机验签，并认证该笔交易和用户身份的合法性；应用的服务器，比如即支付应用后台业务系统，负责支付请求的发起和响应，预存储用户银行账户、终端标识及绑定关系等敏感数据，并且对签名后的第一数据进行联机验签，并认证该笔交易和用户身份的合法性。

基于图 3 所示的系统架构，如图 4 所示，本发明实施例提供了一种联机

认证场景下的安全认证方法，联机认证场景即终端联网状态下，通过后台业务系统服务器进行生物特征的认证，以指纹认证为例。该方法适用于线上支付场景，通过终端的通信接入互联网，系统中各单元的处理及交互过程如下：

步骤 S201，终端启动初始化工作，即建立第一安全通道和第二安全通道，即建立签名单和匹配单元之间的第二安全通道，并建立匹配单元和传感器之间的第一安全通道；

步骤 S202，当用户进行订单交易需要指纹认证时，交易对应的应用程序发出认证请求；

步骤 S203，传感器采集指纹信息，并通过第一安全通道，将指纹信息返回给匹配单元；

步骤 S204，匹配单元进行指纹比对、指纹存储等操作，得到指纹匹配的结果；

步骤 S205，匹配单元通过第二安全通道，将结果发送给签名单元，请求签名单元进行签名，签名单元对指纹匹配结果进行签名；

步骤 S206，签名单元将第一密文数据发送给应用程序；

步骤 S207，应用 APP 将终端的第一密文数据等发送给应用 APP 的后台服务器进行验证；

步骤 S208，应用 APP 的后台服务器对第一密文数据进行验证，以确认匹配结果是否可信；

步骤 S209，应用 APP 的后台服务器将认证结果返回给应用程序，应用程序根据认证结果继续后续的交易步骤。

当然，在进行安全认证之前，需要先开通身份认证，即用户在终端预先保存指纹模板，然后操作应用 APP，判断“生物识别类型”，若为“指纹认证”，则继续；判断“安全等级”，检验是否满足金融应用要求（等级 2 或 3），若满足，则继续；判断“后台业务随机因子”，校验是否与已存储的一致。若满足，则继续；如果所有的步骤都成功，认证通过，后台将卡号、设备、指纹绑定存储，开通成功。

另外，如图 5 所示，本发明实施例提供了一种脱机认证场景下的安全认证方法，脱机认证即终端不联网状态下，通过终端自身的应用程序进行指纹认证。适用于线下支付场景，通过终端的非接触式近场通信与 POS 终端进行信息交互，具体各单元的处理及交互过程如下：

步骤 S301~步骤 S306 同联机认证的步骤 S201~步骤 S206，不再赘述。

步骤 S307，应用程序直接验证第一密文数据，以确认匹配结果是否可信，并根据匹配结果进行后续操作。

为了进一步地保证安全认证的可靠性，所述匹配单元与所述签名单元在安全运行环境中运行，其中，所述安全运行环境包括可信执行环境 TEE 或者安全芯片，其中，所述安全运行环境中设置有满足不同交易权限的安全等级。当匹配单元在 TEE 中且签名单元在安全芯片中时，则安全级别属于较高级别，意味着对应业务范围为大额交易；当比对单元和签名单元都在 TEE 中时，则安全级别属于较低级别，意味着对应的业务范围为小额交易。

进一步地，所述终端将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果，还包括：

若所述第一生物特征与预设的第二生物特征匹配，则获取匹配的第二生物特征的权限；生成关于所述认证请求对应的待认证业务与所述第二生物特征的权限是否匹配的结果。

比如说，手机终端内部保存了多个指纹，其中，只有一个指纹是拥有付款的权限的，软件实现时，为具有付款权限的指纹增加一个设定的标识，这样，当指纹匹配完成时，再次判断该指纹是否拥有付款的权限，即判断该指纹是否有设定的标识，若有的话继续后面的步骤，否则，则提示没有权限，交易终止，又或者是，手机终端内部保存了一个用户的多个指纹，每个指纹用途不同，因为在软件实现时，为该用户的所以指纹设置对应的权限，即增加一个数组，数组中每个不同的枚举值代表不同的指纹的权限，当收到关于所述认证请求对应的待认证业务后，分析该业务对应的枚举值，然后当指纹匹配完成时，分析该指纹对应的枚举值与该业务对应的枚举值是否一致，进

而确定该指纹是否有处理该笔业务的权限，这样可以有效地避免误操作，比如家庭成员中孩子会经常使用父母的手机，有存在误交易的风险，所以此时可以为每个指纹设定交易权限，当然也可以是其它权限，如登录权限等。

进一步地，所述终端的安全证书的私钥包括所述终端的私钥、所述终端的安全证书的公钥证书包括所述终端的公钥证书、所述终端制造商的公钥证书，其中，所述终端的公钥证书为使用所述终端制造商的私钥签名所述终端的公钥得到，所述终端制造商的公钥证书为使用认证平台的私钥签名所述终端制造商的公钥得到。

如图 6 所示，在签名认证处理中，应用 APP 的服务器或者应用程序使用公钥验证技术验证终端的公钥证书，并且验证第一密文数据。具体地验签的步骤如下：

步骤一，检索 CA 根公钥：后台根据厂商公钥证书中的颁发机构密钥标识符确定使用哪一个 CA 根公钥；

步骤二，获取终端制造商公钥：后台使用 CA 根公钥验证终端制造商公钥证书，验证正确则取出证书中的终端制造商公钥；

步骤三，获取签名单元公钥：后台使用终端制造商公钥验证签名单元公钥证书，验证正确则取出证书中的签名单元公钥；

步骤四，验证签名的关键数据：后台使用签名单元公钥验证签名的第一密文数据。

步骤五，如果所有的步骤都成功，签名验证通过。

其中，签名单元需对匹配单元提供的指纹比对结果进行数字签名，即先使用哈希函数生成关键数据的摘要，再使用签名单元的私钥对摘要进行加密从而生成数字签名；匹配单元将签名数据和公钥证书一起发送给后台；后端业务平台（联机认证模式下）或应用程序（脱机认证模式下）使用公钥技术验证签名数据的合法性，从而保证被签名的第一密文数据是由终端上的签名单元创建的，即签名单元无法否认创建过该消息、该数据在传输过程中并未被第三方篡改过。

进一步地，所述终端发送所述安全证书的公钥证书给所述认证端；所述终端在收到所述认证端发送的设备认证通过后，发送所述第一密文数据给所述认证端。

所述发送所述第一密文数据给所述认证端之后，包括：

所述认证端通过以下方式解析密文数据：

所述认证端根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥；

所述认证端根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥；

若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过，并使用所述终端的公钥验证所述第一密文数据，得到所述匹配结果。

如图 6 所示，认证端利用公钥验证技术根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥 P_{MF} ，然后根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥 P_D ，当得到终端的公钥就可以认为该终端是合法终端，进一步地用终端的公钥对第一密文数据进行解密，得到解密之后的匹配结果，若为匹配成功，认证端可以后续的交易步骤，否则认证端就可以提示交易失败，终止交易。

进一步地，所述终端使用所述终端的安全证书的私钥对关键信息进行加密，得到第二密文数据；所述终端将所述第二密文数据发送给所述认证端。其中，所述关键信息至少包含终端标识、银行卡账号中的一种。

需要说明的是，上述步骤中终端使用所述终端的安全证书的私钥对关键信息进行加密与步骤 S103 中对所述匹配结果加密得到第一密文数据之间并没有严格的执行顺序，也就是说二者可以同时执行，即对匹配结果和关键信息作为整体一起进行加密，将加密之后得到的密文数据一起发送至认证端，当然也可以先执行步骤 S103，再对关键信息进行加密，又或者先对关键信息进行加密，再执行步骤 S103，具体的执行顺序根据实际需要确定。

进一步地，所述终端将所述第二密文数据发送给所述认证端之后，包括：

所述认证端通过以下方式解析密文数据:

所述认证端根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥, 根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥, 若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过;

使用所述终端的公钥验证所述第一密文数据, 得到所述匹配结果;

若所述匹配结果为匹配成功, 则使用所述终端的公钥验证所述第二密文数据, 得到所述关键信息;

确定所述关键信息是否符合预设的认证规则, 生成生物特征认证结果发送给所述终端。

例如关键信息是终端标识和银行卡账号, 则终端安全证书的私钥对终端标识和银行卡账号进行加密得到第二密文数据, 然后将第二密文数据连同第一密文数据发送给应用 APP 的服务器, 应用 APP 的服务器解密第一密文数据和第二密文数据后, 进一步判定解密得到的第二密文数据是否与预存的终端标识和银行卡账号一致, 若发现不一致, 同样认定该笔交易是不合法的, 认定交易失败, 之所以这样做是因为用终端标识和银行账号的绑定关系限定终端的交易, 因为这种绑定关系是用户常用交易, 若是来自其它终端, 则有可能存在因为用户敏感信息的泄露, 使得非法分子在其余终端非法使用敏感数据交易, 所以进一步地通过绑定关系进行限定。

为了更加系统地描述上述安全认证地过程, 本发明实施例仍然以指纹为例, 通过图 7 和图 8 所示的交互过程, 详细阐述这一过程, 其中图 7 阐述指纹认证的开通和绑定过程, 具体步骤如下:

步骤 S401, 应用程序调用接口获取终端关键信息, 包括: 终端标识、用户名、终端是否支持指纹认证功能、终端是否开启指纹、终端是否已录入指纹以及终端的安全等级。

步骤 S402, 应用程序将获取的终端关键信息传递给应用程序的服务器。

步骤 S403, 应用程序的服务器判断是否满足开通条件, 包括: 终端支持

指纹服务、设备满足安全等级、当前卡片/用户支持开通指纹支付、当前卡片/用户未在该终端上开通指纹功能（即不存在相应绑定关系）等。若满足，则进入下一步骤；

步骤 S404，应用程序的服务器发起引导开通请求；

步骤 S405，应用程序引导用户开通指纹认证，比如：在用户完成了一笔交易且判断该设备具备开通指纹认证的条件之后，可在交易成功页面提示用户开通指纹认证；

步骤 S406，用户选择开通指纹支付并同意协议后，若终端尚未录入指纹，则提示用户前往系统设置录入指纹，或者直接跳转至系统设置进行录入；若已录入，则应用程序将用户信息/卡号提供给后台（卡号可以根据当前已完成交易自动获取，否则需要持卡人输入）；

步骤 S407，后台生成业务随机因子，如：随机数、时间戳，并保存在数据库中；

步骤 S408，后台发起指纹认证请求，请求中包含业务随机因子；

步骤 S409，应用程序显示指纹验证界面；

步骤 S410，应用程序调用指纹服务接口进行指纹输入和验证，接口参数包含业务随机因子；

步骤 S411，指纹服务对用户输入的指纹进行验证，即：验证其是否与终端上已录入的指纹相匹配。若系统未录入指纹，还可跳转至系统指纹录入界面，录入成功后再返回并进行验证（取决于系统是否提供该功能以及用户体验评估）；

步骤 S412，指纹服务返回指纹验证结果等关键数据及签名、证书：如果验证失败，应用程序提示用户是否重试指纹验证功能，或者取消；如果验证成功，继续下一步；

步骤 S413，应用程序将返回的数据和用户信息/卡号发送给后台；

步骤 S414，后台验证指纹验证结果的签名数据是否正确，如果验签成功，则提取数据项并认证身份合法性，包括：判断指纹验证结果是否成功、生物

识别类型是否正确、安全等级是否满足要求、业务随机因子是否与后台存储一致等。若验签及认证均成功，则下一步；

步骤 S415，将用户信息/卡号与指纹 ID、用户 ID 和终端标识进行绑定并存储在后台；

步骤 S416，提示用户已成功开通指纹认证并绑定。

进一步地，当服务器完成指纹开通过程之后，图 8 示出了指纹认证替代密码的安全认证过程，具体步骤如下：

步骤 S501，用户操作应用程序，在应用程序发起订单支付请求；

步骤 S502，应用程序调用指纹服务的接口获取终端关键信息，包括：终端标识、用户 ID、终端是否支持指纹（即设备是否具备指纹传感器）、终端是否开启指纹、设备是否已录入指纹以及设备的安全等级。

步骤 S503，应用程序将返回的终端关键信息传递给应用程序的服务器。

步骤 S504，应用程序的服务器根据设备关键信息判断是否满足使用指纹认证来进行支付/登录的条件，包括：设备支持、开启并录入了指纹、设备满足安全等级、设备对应用户/卡号开通了指纹认证（即存在相应绑定关系）、订单金额满足限额条件等。若满足，则进入下一步；

步骤 S505，应用程序的服务器生成业务随机因子，如：随机数、时间戳，并保存在数据库中；

步骤 S506，应用程序的服务器发起指纹认证请求，请求中包含业务随机因子；

步骤 S507，应用程序显示指纹验证界面；

步骤 S508，应用程序调用指纹服务接口进行指纹输入和验证，接口参数包含业务随机因子；

步骤 S509，指纹服务对用户输入的指纹进行验证，即：验证其是否与设备上已录入的指纹相匹配；

步骤 S510，指纹服务返回指纹验证结果等关键数据及签名、证书：如果验证失败，应用程序提示用户是否重试指纹验证功能，或者放弃指纹验证转

为传统支付/登录方式；如果验证成功，继续下一步；

步骤 S511，应用程序将返回的数据和用户信息（如卡号）发送给后台；

步骤 S512，应用程序的服务器验证指纹验证结果的签名数据是否正确，如果验签成功，则提取数据项并认证身份及交易合法性，包括：判断指纹验证结果是否成功，生物识别类型是否正确，安全等级是否满足当前交易金额，业务随机因子是否与后台存储一致，指纹 ID、用户 ID 和设备 ID 以及卡号/用户信息是否与后台存储的绑定关系一致。若验签及认证均成功，则下一步；

步骤 S513，应用程序的服务器认证成功后向应用程序授权交易合法。

步骤 S514，应用程序完成指纹支付或者指纹登录等操作。

实施例二，本发明实施例还提供一种基于生物特征的安全认证装置，该装置可执行上述方法实施例。本发明实施例提供的装置如图 9 所示，包括：收发单元 401、传感器 402、匹配单元 403、签名单元 404，其中：

收发单元 401，用于接收生物特征认证请求；

传感器 402，用于获取第一生物特征；

匹配单元 403，用于将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果；

签名单元 404，用于使用所述终端的安全证书的私钥对所述匹配结果加密得到第一密文数据，所述安全证书唯一对应所述终端；

收发单元 401，还用于向认证端发送所述第一密文数据及所述安全证书的公钥证书，所述认证端为服务器或所述终端。

进一步地，所述传感器 402 具体用于：将采集的第一生物特征通过第一安全通道发送给所述匹配单元 403；

所述匹配单元 403 具体用于：将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果，并将所述匹配结果通过第二安全通道发送给所述签名单元 404，所述匹配单元中存储有所述第二生物特征；

所述签名单元 404 具体用于：先使用哈希函数对所述匹配结果生成匹配

结果的摘要，再使用所述终端的安全证书对所述摘要加密，得到签名数据，所述签名单元中存储有所述终端的安全证书。

进一步地，所述传感器 402 与所述匹配单元 403 通过握手协议完成单向或者双向身份认证和会话密钥交换，从而建立所述第一安全通道；

所述匹配单元 403 与所述签名单元 404 通过握手协议完成单向或者双向身份认证和会话密钥交换，从而建立所述第二安全通道。

进一步地，还包括：所述匹配单元与所述签名单元在安全运行环境中运行，其中，所述安全运行环境包括可信执行环境 TEE 或者安全芯片，其中，所述安全运行环境中设置有满足不同交易权限的安全等级。

进一步地，所述匹配单元 403 还用于：

若所述第一生物特征与预设的第二生物特征匹配，则获取匹配的第二生物特征的权限；生成关于所述认证请求对应的待认证业务与所述第二生物特征的权限是否匹配的结果。

其中，还包括：所述终端的安全证书的私钥包括所述终端的私钥、所述终端的安全证书的公钥证书包括所述终端的公钥证书、所述终端制造商的公钥证书，其中，所述终端的公钥证书为使用所述终端制造商的私钥签名所述终端的公钥得到，所述终端制造商的公钥证书为使用认证平台的私钥签名所述终端制造商的公钥得到。

进一步地，所述收发单元 401 具体用于：所述终端发送所述安全证书的公钥证书给所述认证端；

所述终端在收到所述认证端发送的设备认证通过后，发送所述第一密文数据给所述认证端；

或者，所述终端发送所述安全证书的公钥证书和第一密文数据给所述认证端，以使所述认证端根据安全证书的公钥证书认证所述终端是否为合法终端。

进一步地，还包括：认证端 405，用于通过以下方式解析密文数据：

根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述

终端制造商的公钥;

根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥;

若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过, 并使用所述终端的公钥验证所述第一密文数据, 得到所述匹配结果。

进一步地, 所述签名单元 404 还用于:

使用所述终端的安全证书的私钥对关键信息进行数字签名, 得到第二密文数据; 将所述第二密文数据发送给所述认证端。

当终端将所述第二密文数据发送给所述认证端之后, 所述认证端 405 还用于:

通过以下方式解析密文数据:

根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥, 根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥, 若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过;

使用所述终端的公钥验证所述第一密文数据, 得到所述匹配结果;

若所述匹配结果为匹配成功, 则使用所述终端的公钥验证所述第二密文数据, 得到所述关键信息;

确定所述关键信息是否符合预设的认证规则, 生成生物特征认证结果发送给所述终端。

其中, 所述关键信息至少包含终端标识、银行卡账号中的一种。

综上所述, 本发明实施例一方面获取服务器端发送的关于生物特征的认证请求; 根据所述认证请求获取第一认证信息集合, 并将第一认证信息集合与安全存储区中第二认证信息集合进行匹配, 所述第一认证信息集合至少包括采集的第一生物特征, 所述第二认证信息集合至少包括预设的第二生物特征; 另一方面利用预置的公钥证书对比对结果等关键信息进行数字签名, 并将签名数据发送至服务器端或者所述终端, 以便所述服务器端或者所述终端

验签后根据解密后匹配比对结果等关键信息生成认证结果。可见，通过公钥证书对匹配比对结果的数字签名保护，就可以认证发送方（终端）的合法性，保证被签名的关键信息是由合法终端创建的、防止交易抵赖发生、保证匹配比对结果在传输过程中不被攻击者窃取或者篡改的完整性，进而得出正确合法的认证结果，保证了用户账户的安全。

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、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。

实施例三

基于相同构思，参见图 10，为本发明实施例提供的一种电子设备 500 的硬件结构示意图，如图 10 所示，包括：

一个或多个处理器 510 以及存储器 520，图 8 中以一个处理器 510 为例。

执行基于生物特征的安全认证方法的电子设备还可以包括: 输入装置 530 和输出装置 540。

处理器 510、存储器 520、输入装置 530 和输出装置 540 可以通过总线或者其他方式连接, 图 5 中以通过总线连接为例。

存储器 520 作为一种非暂态计算机可读存储介质, 可用于存储非暂态软件程序、非暂态计算机可执行程序以及模块, 如本发明实施例中的具有生物特征认证方法的程序指令/模块(例如, 附图 9 所示的匹配单元 403、签名单元 404)。处理器 510 通过运行存储在存储器 520 中的非暂态软件程序、指令以及模块, 从而执行服务器的各种功能应用以及数据处理, 即实现上述方法实施例中的基于生物特征的安全认证方法。

存储器 520 可以包括存储程序区和存储数据区, 其中, 存储程序区可存储操作系统、至少一个功能所需要的应用程序; 存储数据区可存储根据列表项操作的处理装置的使用所创建的数据等。此外, 存储器 520 可以包括高速随机存取存储器, 还可以包括非暂态存储器, 例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施例中, 存储器 520 可选包括相对于处理器 510 远程设置的存储器, 这些远程存储器可以通过网络连接至列表项操作的处理装置。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

输入装置 530 可接收输入的数字或字符信息, 以及产生与电子设备的用户设置以及功能控制有关的键信号输入。输出装置 540 可包括显示屏等显示设备。

所述一个或者多个模块存储在所述存储器 520 中, 当被所述一个或者多个处理器 510 执行时, 执行上述任意方法实施例中的基于生物特征的安全认证方法。

上述产品可执行本发明实施例所提供的方法, 具备执行方法相应的功能模块和有益效果。未在本实施例中详尽描述的技术细节, 可参见本发明实施例所提供的方法。

本发明实施例的电子设备以多种形式存在，包括但不限于：

(1)移动通信设备：这类设备的特点是具备移动通信功能，并且以提供话音、数据通信为主要目标。这类终端包括：智能手机(例如 iPhone)、多媒体手机、功能性手机，以及低端手机等。

(2)超移动个人计算机设备：这类设备属于个人计算机的范畴，有计算和处理功能，一般也具备移动上网特性。这类终端包括：PDA、MID 和 UMPC 设备等，例如 iPad。

(3)便携式娱乐设备：这类设备可以显示和播放多媒体内容。该类设备包括：音频、视频播放器(例如 iPod)，掌上游戏机，电子书，以及智能玩具和便携式车载导航设备。

(4)服务器：提供计算服务的设备，服务器的构成包括处理器、硬盘、内存、系统总线等，服务器和通用的计算机架构类似，但是由于需要提供高可靠的服务，因此在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面要求较高。

(5)其他具有数据交互功能的电子装置。

实施例四

本发明实施例提供一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行上述任一项所述的基于生物特征的安全认证方法。

实施例五

本发明实施例提供一种计算机程序产品，所述计算机程序产品包括存储的非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述任一项所述的

基于生物特征的安全认证方法。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种基于生物特征的安全认证方法，其特征在于，该方法包括：

终端根据接收的生物特征认证请求，获取第一生物特征；

所述终端将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果；

所述终端使用所述终端的安全证书的私钥对所述匹配结果加密得到第一密文数据，所述安全证书唯一对应所述终端；

所述终端向认证端发送所述第一密文数据及所述安全证书的公钥证书，所述认证端为服务器或所述终端。

2、如权利要求1所述的方法，其特征在于，所述获取第一生物特征，包括：

所述终端将传感器采集的第一生物特征通过第一安全通道发送给所述终端的匹配单元；

所述终端将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果，包括

所述匹配单元将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果，并将所述匹配结果通过第二安全通道发送给所述终端的签名单元，所述匹配单元中加密存储有所述第二生物特征；

所述终端使用所述终端的安全证书对所述匹配结果加密得到第一密文数据，包括：

所述签名单元先使用哈希函数对所述匹配结果生成匹配结果的摘要，再使用所述终端的安全证书对所述摘要加密，得到签名数据，所述签名单元中存储有所述终端的安全证书。

3、如权利要求2所述的方法，其特征在于，所述获取第一生物特征之前，还包括：

所述传感器与所述匹配单元通过握手协议完成单向或者双向身份认证和

会话密钥交换，从而建立所述第一安全通道；

所述匹配单元与所述签名单元通过握手协议完成单向或者双向身份认证和会话密钥交换，从而建立所述第二安全通道。

4、如权利要求 2 所述的方法，其特征在于，还包括：

所述匹配单元与所述签名单元在安全运行环境中运行，其中，所述安全运行环境包括可信执行环境 TEE 或者安全芯片，其中，所述安全运行环境中设置有满足不同交易权限的安全等级。

5、如权利要求 1 所述的方法，其特征在于，所述终端将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果，还包括：

若所述第一生物特征与预设的第二生物特征匹配，则获取匹配的第二生物特征的权限；

生成关于所述认证请求对应的待认证业务与所述第二生物特征的权限是否匹配的结果。

6、如权利要求 1~5 任一所述的方法，其特征在于，还包括：

所述终端的安全证书的私钥包括所述终端的私钥、所述终端的安全证书的公钥证书包括所述终端的公钥证书、所述终端制造商的公钥证书，其中，所述终端的公钥证书为使用所述终端制造商的私钥签名所述终端的公钥得到，所述终端制造商的公钥证书为使用认证平台的私钥签名所述终端制造商的公钥得到。

7、如权利要求 6 所述的方法，其特征在于，所述终端发送所述第一密文数据及所述安全证书的公钥证书，包括：

所述终端发送所述安全证书的公钥证书给所述认证端；

所述终端在收到所述认证端发送的设备认证通过后，发送所述第一密文数据给所述认证端；

或者，所述终端发送所述安全证书的公钥证书和第一密文数据给所述认证端，以使所述认证端根据安全证书的公钥证书认证所述终端是否为合法终端。

8、如权利要求 6 所述的方法，其特征在于，所述发送所述第一密文数据给所述认证端之后，还包括：

所述认证端通过以下方式解析密文数据：

所述认证端根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥；

所述认证端根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥；

若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过，并使用所述终端的公钥验证所述第一密文数据，得到所述匹配结果。

9、如权利要求 6 所述的方法，其特征在于，还包括：

所述终端使用所述终端的安全证书的私钥对关键信息进行加密，得到第二密文数据；

所述终端将所述第二密文数据发送给所述认证端。

10、如权利要求 9 所述的方法，其特征在于，所述终端将所述第二密文数据发送给所述认证端之后，还包括：

所述认证端通过以下方式解析密文数据：

所述认证端根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥，根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥，若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过；

使用所述终端的公钥验证所述第一密文数据，得到所述匹配结果；

若所述匹配结果为匹配成功，则使用所述终端的公钥验证所述第二密文数据，得到所述关键信息；

确定所述关键信息是否符合预设的认证规则，生成生物特征认证结果发送给所述终端。

11、如权利要求 9~10 任一所述的方法，其特征在于，所述关键信息至少包含终端标识、银行卡账号中的一种。

12、一种基于生物特征的安全认证装置，其特征在于，该装置包括：

收发单元，用于接收的生物特征认证请求；

传感器，用于获取第一生物特征；

匹配单元，用于将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果；

签名单元，用于使用所述终端的安全证书的私钥对所述匹配结果加密得到第一密文数据，所述安全证书唯一对应所述终端；

收发单元，还用于向认证端发送所述第一密文数据及所述安全证书的公钥证书，所述认证端为服务器或所述终端。

13、如权利要求 12 所述的装置，其特征在于，所述传感器具体用于：将采集的第一生物特征通过第一安全通道发送给所述匹配单元；

所述匹配单元具体用于：将所述第一生物特征与预设的第二生物特征进行匹配，生成匹配结果，并将所述匹配结果通过第二安全通道发送给所述签名单元，所述匹配单元中存储有所述第二生物特征；

所述签名单元具体用于：先使用哈希函数对所述匹配结果生成匹配结果的摘要，再使用所述终端的安全证书对所述摘要加密，得到签名数据，所述签名单元中存储有所述终端的安全证书。

14、如权利要求 13 所述的装置，其特征在于，所述传感器与所述匹配单元通过握手协议完成单向或者双向身份认证和会话密钥交换，从而建立所述第一安全通道；

所述匹配单元与所述签名单元通过握手协议完成单向或者双向身份认证和会话密钥交换，从而建立所述第二安全通道。

15、如权利要求 13 所述的装置，其特征在于，还包括：

所述匹配单元与所述签名单元在安全运行环境中运行，其中，所述安全运行环境包括可信执行环境 TEE 或者安全芯片，其中，所述安全运行环境中设置有满足不同交易权限的安全等级。

16、如权利要求 12 所述的装置，其特征在于，所述匹配单元还用于：

若所述第一生物特征与预设的第二生物特征匹配，则获取匹配的第二生物特征的权限；

生成关于所述认证请求对应的待认证业务与所述第二生物特征的权限是否匹配的结果。

17、如权利要求 12~16 任一所述的装置，其特征在于，还包括：

所述终端的安全证书的私钥包括所述终端的私钥、所述终端的安全证书的公钥证书包括所述终端的公钥证书、所述终端制造商的公钥证书，其中，所述终端的公钥证书为使用所述终端制造商的私钥签名所述终端的公钥得到，所述终端制造商的公钥证书为使用认证平台的私钥签名所述终端制造商的公钥得到。

18、如权利要求 17 所述的装置，其特征在于，所述收发单元具体用于：

所述终端发送所述安全证书的公钥证书给所述认证端；

所述终端在收到所述认证端发送的设备认证通过后，发送所述第一密文数据给所述认证端；

或者，所述终端发送所述安全证书的公钥证书和第一密文数据给所述认证端，以使所述认证端根据安全证书的公钥证书认证所述终端是否为合法终端。

19、如权利要求 18 所述的装置，其特征在于，还包括：

认证端，用于通过以下方式解析密文数据：

根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥；

根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥；

若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过，并使用所述终端的公钥验证所述第一密文数据，得到所述匹配结果。

20、如权利要求 18 所述的装置，其特征在于，所述签名单元还用于：

使用所述终端的安全证书的私钥对关键信息进行加密，得到第二密文数

据；将所述第二密文数据发送给所述认证端。

21、如权利要求 20 所述的装置，其特征在于，终端将所述第二密文数据发送给所述认证端之后，所述认证端还用于：

通过以下方式解析密文数据：

根据所述终端制造商的公钥证书和预存的所述认证平台的公钥获得所述终端制造商的公钥，根据所述终端制造商的公钥和所述终端的公钥证书获得所述终端的公钥，若所述认证端获得所述终端的公钥则确定所述终端的设备认证通过；

使用所述终端的公钥验证所述第一密文数据，得到所述匹配结果；

若所述匹配结果为匹配成功，则使用所述终端的公钥验证所述第二密文数据，得到所述关键信息；

确定所述关键信息是否符合预设的认证规则，生成生物特征认证结果发送给所述终端。

22、如权利要求 20~21 任一所述的装置，其特征在于，所述关键信息至少包含终端标识、银行卡账号中的一种。

23、一种电子设备，其特征在于，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求 1 至 11 任一所述的方法。

24、一种非暂态计算机存储介质，其特征在于，所述非暂态计算机可读存储介质存储有计算机可执行指令，所述计算机可执行指令用于使所述计算机执行权利要求 1 至 11 任一项所述的方法。

25、一种计算机程序产品，其特征在于，所述计算机程序产品包括存储的非暂态计算机可读存储介质上的计算程序，所述计算机程序包括所述计算

机可执行指令，当所述计算机可执行指令被计算机执行时，使所述计算机执行权利要求 1 至 11 任一项所述的方法。

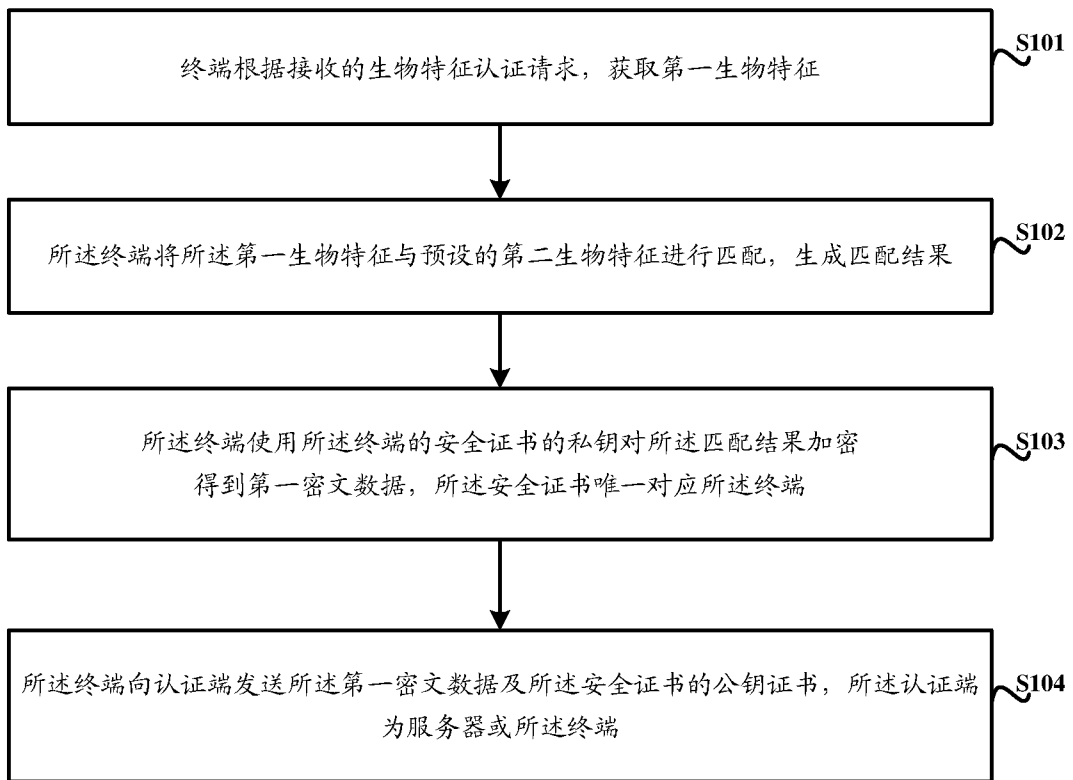


图 1

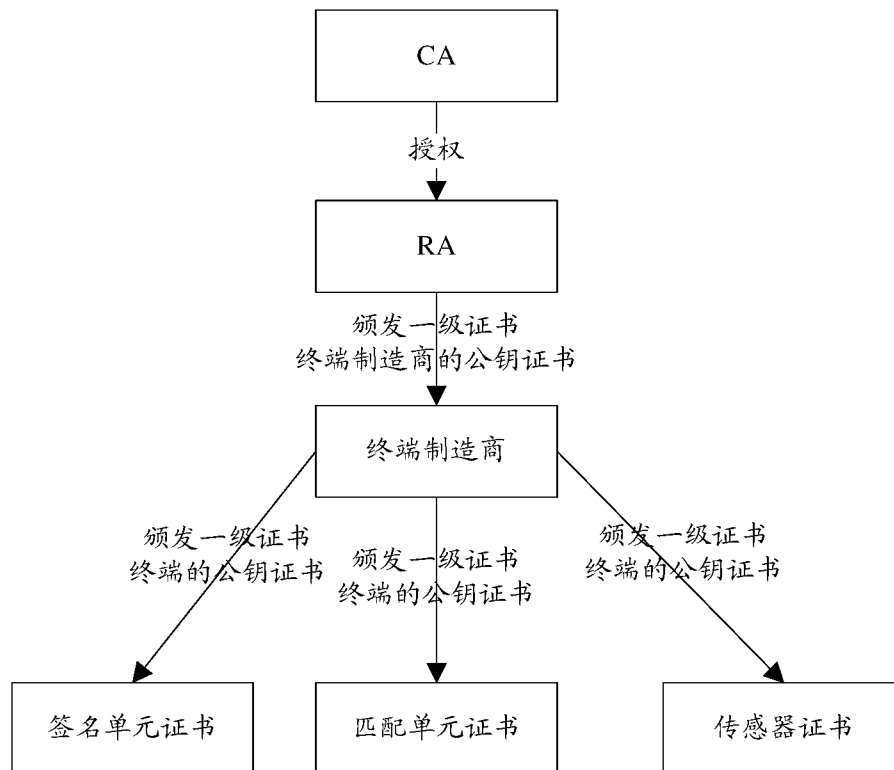


图 2

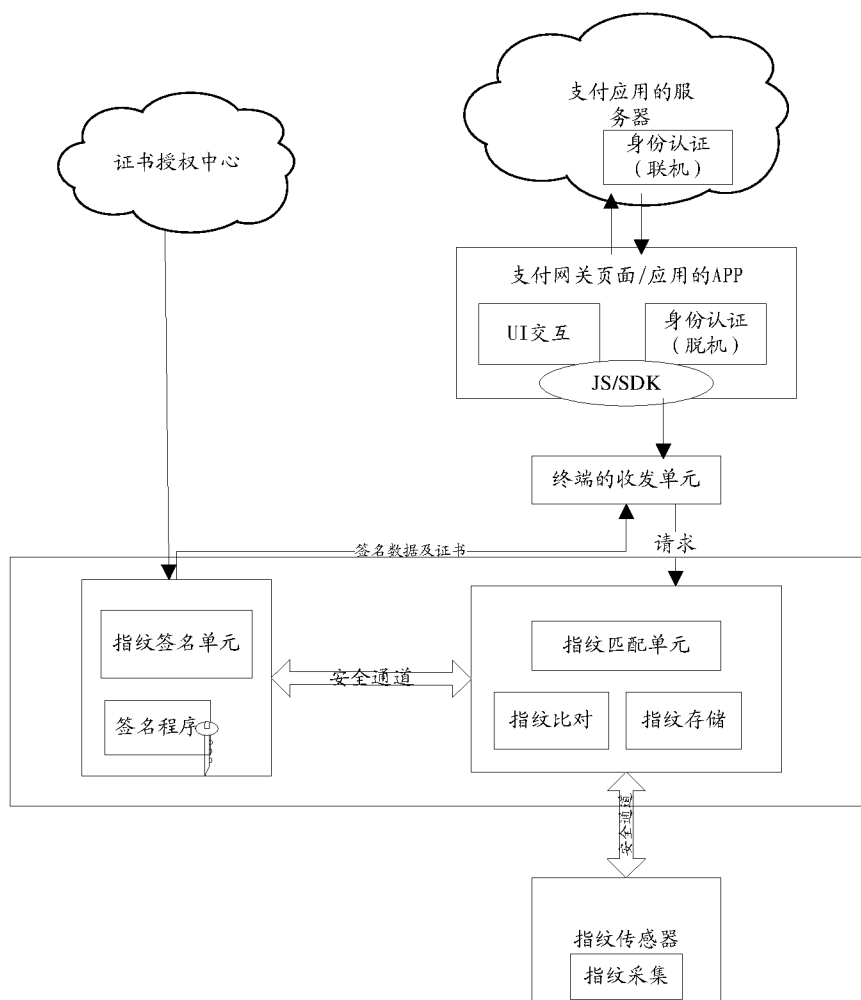


图 3

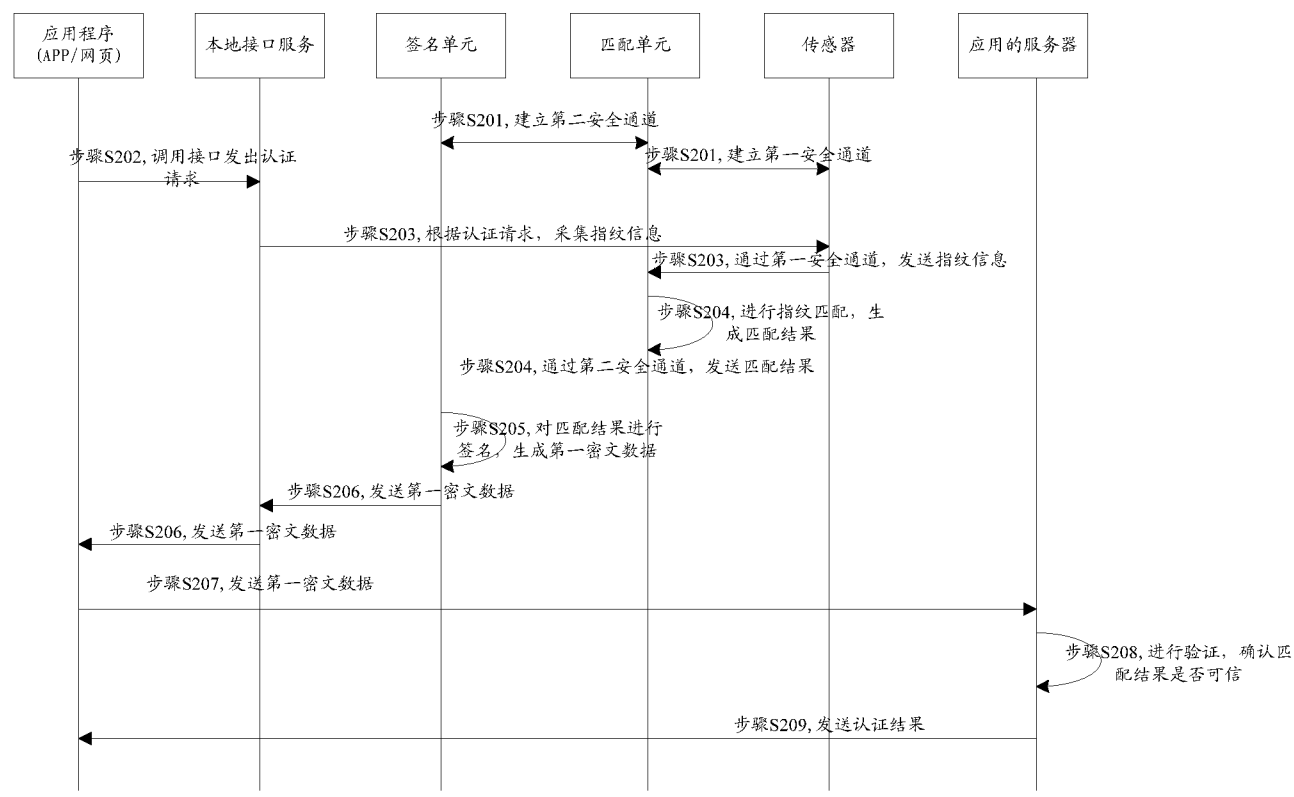


图 4

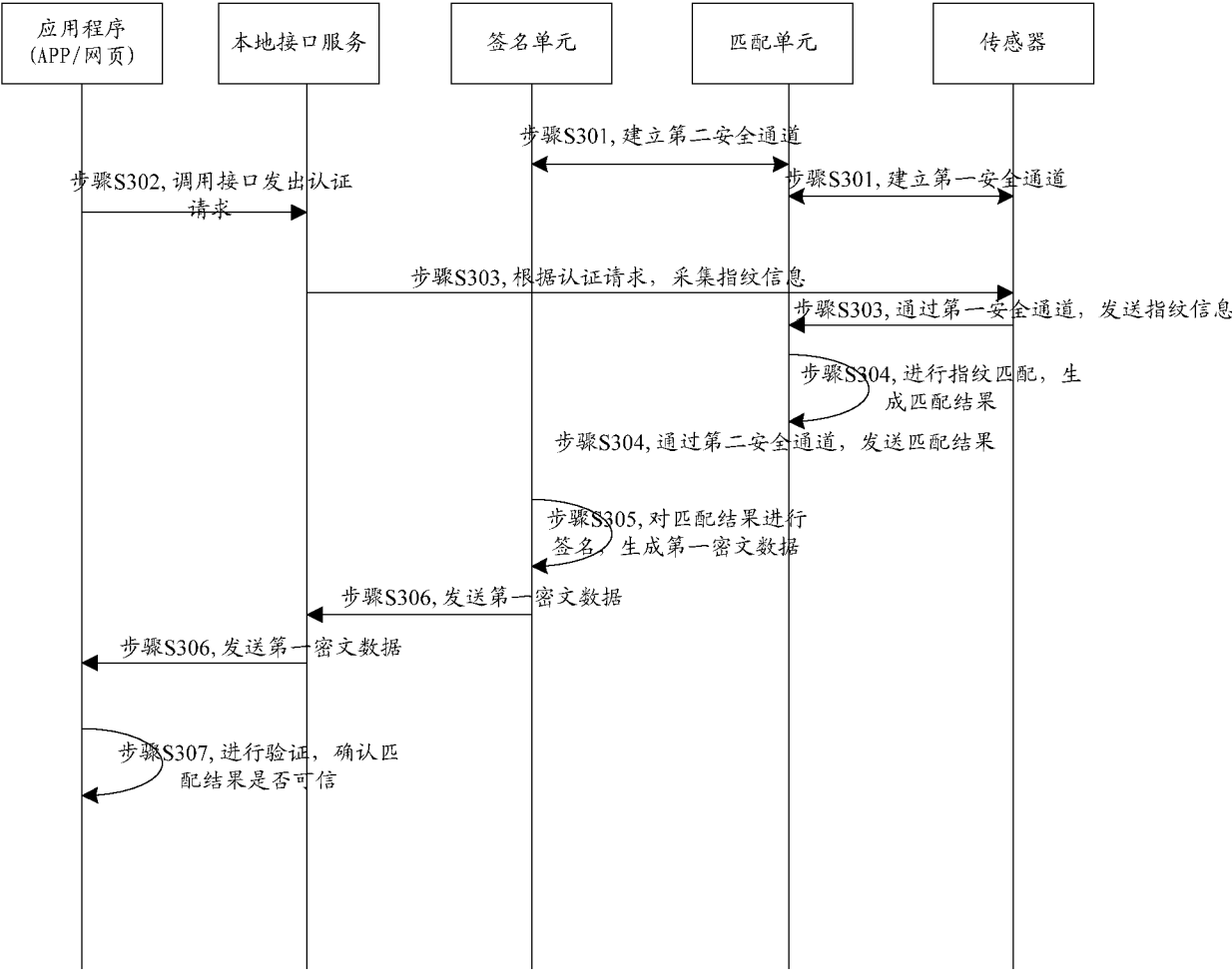


图 5

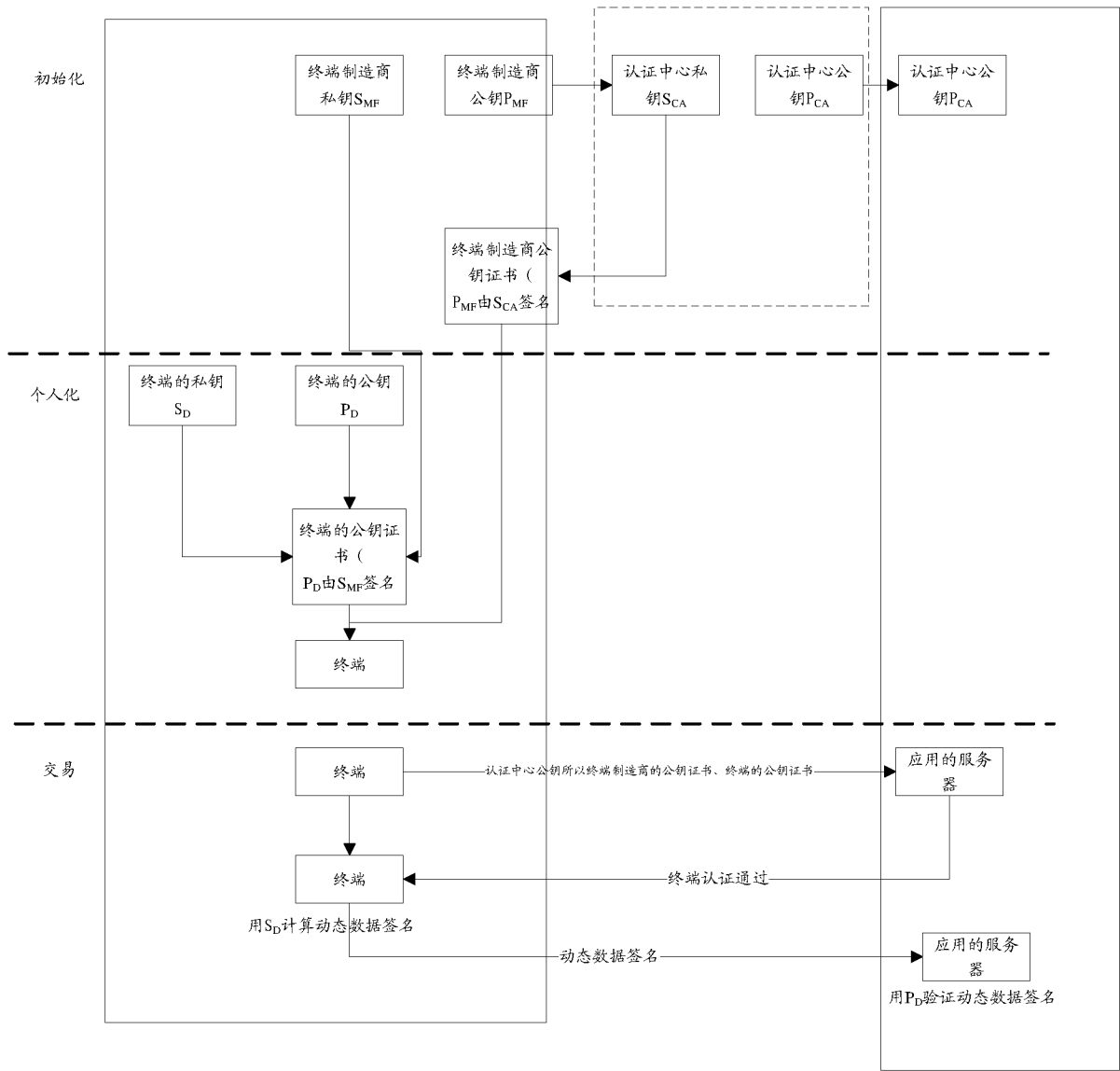


图 6

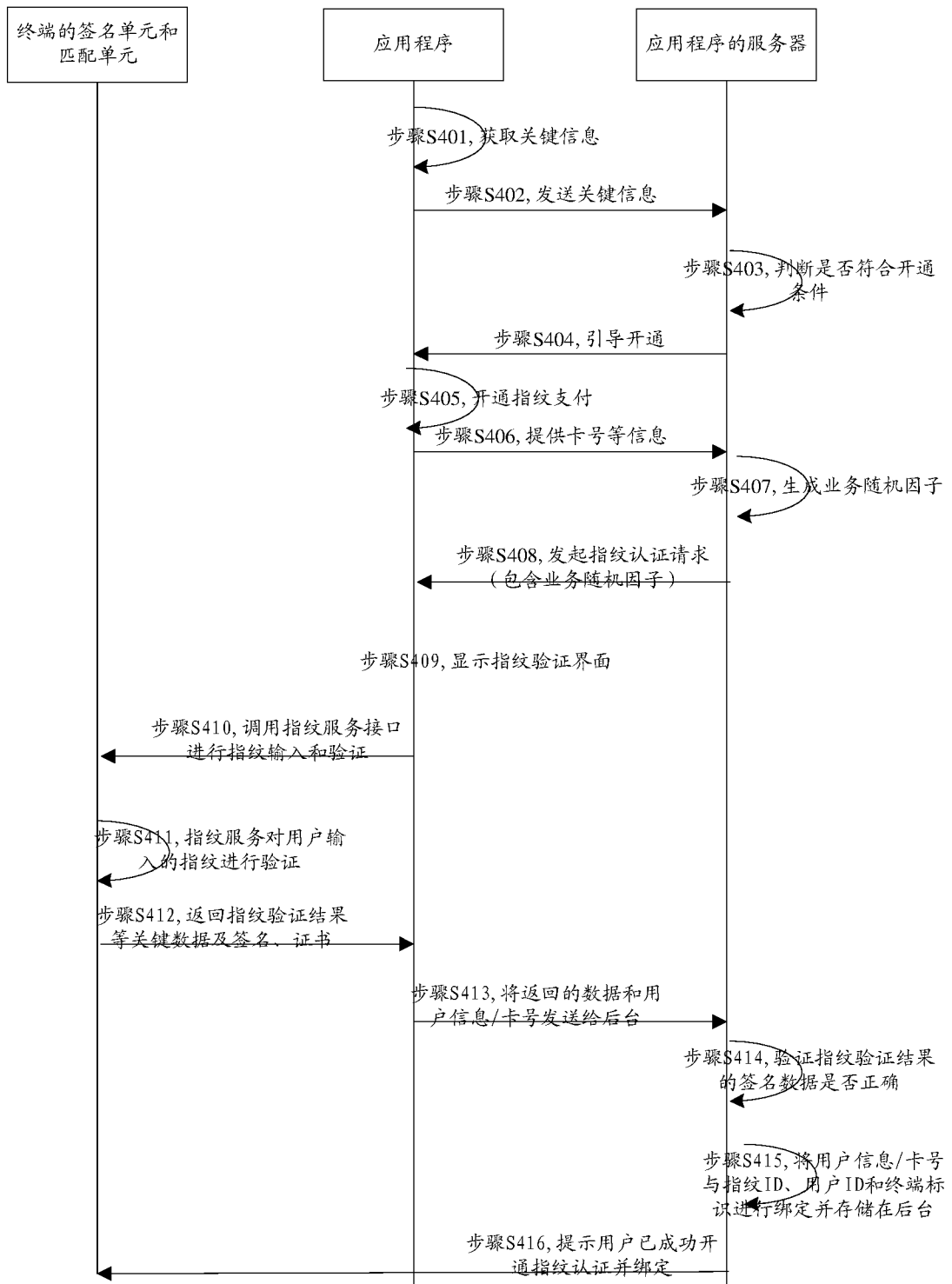


图 7

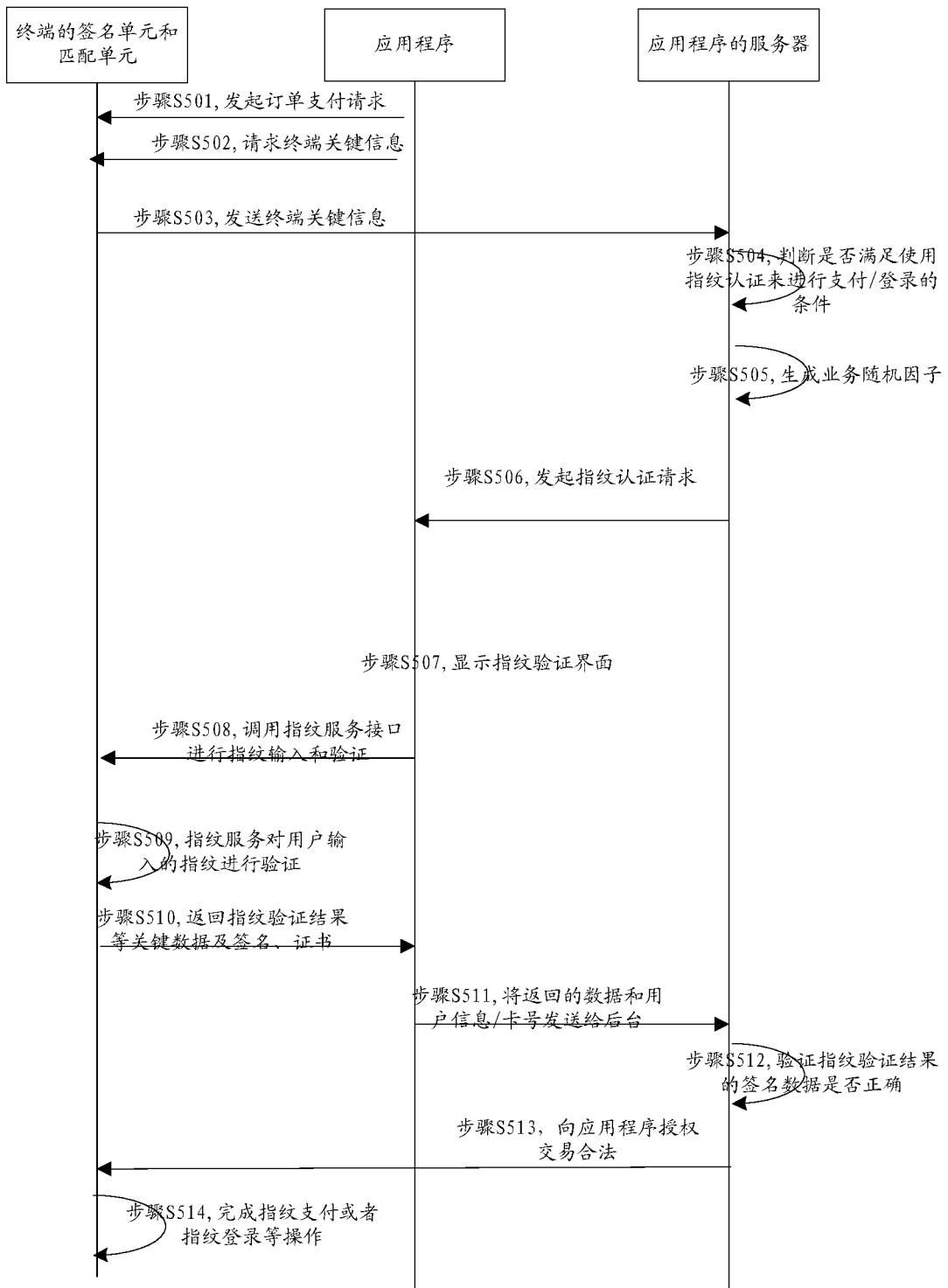


图 8

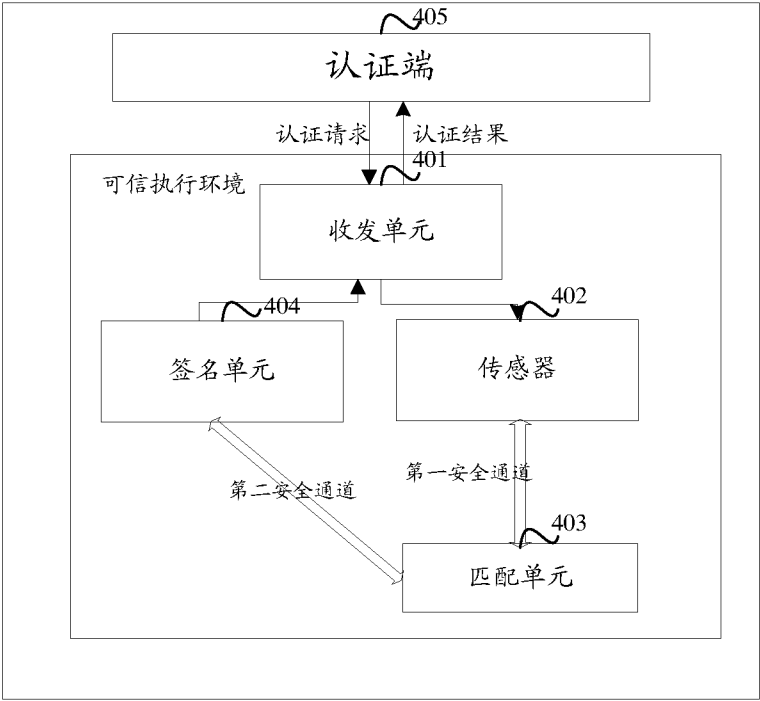


图 9

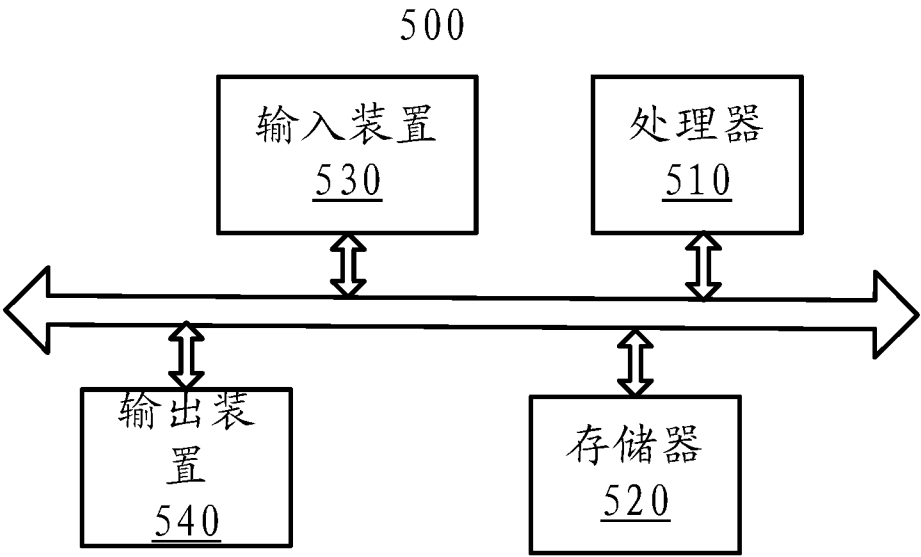


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/077512

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 9/32 (2006.01) i; G06Q 20/38 (2012.01) i; 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)

H04L; 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)

CNABS, CNTXT, CNKI, VEN, WOTXT: biology, result, biometrical, fingerprint, iris, match, compare, private key, public key, certificate, encrypt, signature, manufacturer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101741843 A (WATCHDATA SYSTEM CO., LTD.), 16 June 2010 (16.06.2010), description, paragraphs [0031]-[0038]	1-5, 12-16, 23-25
Y	CN 101741843 A (WATCHDATA SYSTEM CO., LTD.), 16 June 2010 (16.06.2010), description, paragraphs [0031]-[0038]	6-11, 17-22
Y	CN 104135368 A (HARBIN ENGINEERING UNIVERSITY), 05 November 2014 (05.11.2014), description, paragraphs [0013]-[0022] and [0102]	6-11, 17-22
PX	CN 105959287 A (CHINA UNIONPAY CO., LTD.), 21 September 2016 (21.09.2016), claims 1-22, and description, paragraphs [0147]-[0149]	1-25
A	US 2013308838 A1 (APPLE INC.), 21 November 2013 (21.11.2013), the whole document	1-25

☐ 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 02 June 2017 (02.06.2017)	Date of mailing of the international search report 09 June 2017 (09.03.2017)
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 LI, Qian Telephone No.: (86-10) 62089374

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2017/077512

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101741843 A	16 June 2010	CN 101741843 B	12 December 2012
CN 104135368 A	05 November 2014	None	
CN 105959287 A	21 September 2016	None	
US 2013308838 A1	21 November 2013	US 9135496 B2	15 September 2015
		US 2016012273 A1	14 January 2016

A. 主题的分类 H04L 29/06(2006.01)i; H04L 9/32(2006.01)i; G06Q 20/38(2012.01)i; 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) H04L; 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)) CNABS, CNTXT, CNKI, VEN, WOTXT: 生物, 指纹, 虹膜, 匹配, 对比, 私钥, 公钥, 证书, 加密, 签名, 结果, 制造商, biometrical, fingerprint, iris, match, compare, private key, public key, certificate, encrypt, signature, manufacturer																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 101741843 A (北京握奇数据系统有限公司) 2010年 6月 16日 (2010 - 06 - 16) 说明书[0031]-[0038]段</td> <td>1-5、12-16、23-25</td> </tr> <tr> <td>Y</td> <td>CN 101741843 A (北京握奇数据系统有限公司) 2010年 6月 16日 (2010 - 06 - 16) 说明书[0031]-[0038]段</td> <td>6-11、17-22</td> </tr> <tr> <td>Y</td> <td>CN 104135368 A (哈尔滨工程大学) 2014年 11月 5日 (2014 - 11 - 05) 说明书[0013]-[0022]、[0102]段</td> <td>6-11、17-22</td> </tr> <tr> <td>PX</td> <td>CN 105959287 A (中国银联股份有限公司) 2016年 9月 21日 (2016 - 09 - 21) 权利要求1-22、说明书[0147]-[0149]段</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>US 2013308838 A1 (APPLE INC.) 2013年 11月 21日 (2013 - 11 - 21) 全文</td> <td>1-25</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 101741843 A (北京握奇数据系统有限公司) 2010年 6月 16日 (2010 - 06 - 16) 说明书[0031]-[0038]段	1-5、12-16、23-25	Y	CN 101741843 A (北京握奇数据系统有限公司) 2010年 6月 16日 (2010 - 06 - 16) 说明书[0031]-[0038]段	6-11、17-22	Y	CN 104135368 A (哈尔滨工程大学) 2014年 11月 5日 (2014 - 11 - 05) 说明书[0013]-[0022]、[0102]段	6-11、17-22	PX	CN 105959287 A (中国银联股份有限公司) 2016年 9月 21日 (2016 - 09 - 21) 权利要求1-22、说明书[0147]-[0149]段	1-25	A	US 2013308838 A1 (APPLE INC.) 2013年 11月 21日 (2013 - 11 - 21) 全文	1-25
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
X	CN 101741843 A (北京握奇数据系统有限公司) 2010年 6月 16日 (2010 - 06 - 16) 说明书[0031]-[0038]段	1-5、12-16、23-25																		
Y	CN 101741843 A (北京握奇数据系统有限公司) 2010年 6月 16日 (2010 - 06 - 16) 说明书[0031]-[0038]段	6-11、17-22																		
Y	CN 104135368 A (哈尔滨工程大学) 2014年 11月 5日 (2014 - 11 - 05) 说明书[0013]-[0022]、[0102]段	6-11、17-22																		
PX	CN 105959287 A (中国银联股份有限公司) 2016年 9月 21日 (2016 - 09 - 21) 权利要求1-22、说明书[0147]-[0149]段	1-25																		
A	US 2013308838 A1 (APPLE INC.) 2013年 11月 21日 (2013 - 11 - 21) 全文	1-25																		
☐ 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 2017年 6月 2日		国际检索报告邮寄日期 2017年 6月 9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 李倩 电话号码 (86-10)62089374																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/077512

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	101741843	A	2010年 6月 16日	CN	101741843	B	2012年 12月 12日
CN	104135368	A	2014年 11月 5日	无			
CN	105959287	A	2016年 9月 21日	无			
US	2013308838	A1	2013年 11月 21日	US	9135496	B2	2015年 9月 15日
				US	2016012273	A1	2016年 1月 14日