

说明书

发明名称：生物支付设备的认证方法、装置、计算机设备和存储介质

本申请要求于 2020 年 03 月 23 日提交中国专利局，申请号为 202010208265.6，发明名称为“生物支付设备的认证方法、装置、计算机设备和存储介质”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。

5

技术领域

本申请涉及互联网通信技术领域，特别是涉及一种生物支付设备的认证方法、装置、计算机设备和存储介质。

10 背景技术

随着生物支付技术的发展，生物支付被广泛应用在多种商业场景。以生物支付场景中的刷脸支付为例，一个具体的应用场景为：收银终端获取到收款金额后，调用摄像头采集用户的人脸图像并向支付系统发送，在支付系统对用户的人脸图像识别通过后，返回付款码至收银终端，收银终端根据付款
15 码向支付系统发起支付请求，完成支付。

刷脸支付无需用户在终端上操作付款码，而是由支付系统根据收银终端采集的人脸图像生成，因此，需要对接入的收银设备进行认证，以确保用户资金账户的安全。传统的人脸支付设备的认证是简单的映射关系认证，将设备的签名字符串和设备编号保存在系统属性中，调用设备认证接口进行设备
20 认证。支付认证服务器用对设备编号进行验证，从而实现设备端与支付系统双向认证，互相信任身份，建立双向的安全链路。

在实际应用中，利用签名和设备编码映射关系进行认证的方式较为简单，另一台设备通过迁移设备编码与设备签名即可冒充设备进行设备认证，从而影响生物支付的安全性能。

发明内容

根据本申请的各种实施例，提供一种生物支付设备的认证方法、装置、计算机设备和存储介质。

5 一种生物支付设备的认证方法，所述方法包括：

获取设备的密钥，其中，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

根据所述密钥和设备信息生成签名；

10 基于所述设备信息和所述签名向支付认证服务器发送认证请求，所述认证请求指示所述支付认证服务器根据所述设备信息对所述签名进行验证，并根据验证结果生成对所述生物支付设备的认证结果；及

接收所述支付认证服务器返回认证结果，所述认证结果使所述支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

15 一种生物支付设备的认证方法，包括：

接收生物支付设备基于签名和设备信息发送的认证请求，其中，所述签名由所述生物支付设备根据密钥和设备信息生成，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

根据所述设备信息对所述签名进行验证；

20 根据验证结果生成对所述生物支付设备的认证结果；及

向所述生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。

一种生物支付设备的认证装置，所述装置包括：

25 密钥获取模块，用于获取设备的密钥，其中，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

签名模块，用于根据所述密钥和设备信息生成签名；

认证模块，用于基于所述设备信息和所述签名向支付认证服务器发送认证请求，所述认证请求指示所述支付认证服务器根据所述设备信息对所述签名进行验证，并根据验证结果生成对所述生物支付设备的认证结果；

接收模块，用于接收所述支付认证服务器返回认证结果，所述认证结果
5 使所述支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

一种生物支付设备的认证装置，包括：

认证获取模块，用于接收生物支付设备基于签名设备信息发送的认证请
10 求，其中，所述签名由所述生物支付设备根据密钥和设备信息生成，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

验证模块，用于根据所述设备信息对所述签名进行验证；

认证模块，用于根据验证结果生成对所述生物支付设备的认证结果；

15 发送模块，用于向所述生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。

一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现以下步骤：

20 获取设备的密钥，其中，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

根据所述密钥和设备信息生成签名；

基于所述设备信息和所述签名向支付认证服务器发送认证请求，所述认证请求指示所述支付认证服务器根据所述设备信息对所述签名进行验证，并
25 根据验证结果生成对所述生物支付设备的认证结果；

接收所述支付认证服务器返回认证结果，所述认证结果使所述支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现以下步骤：

- 接收生物支付设备基于签名和设备信息发送的认证请求，其中，所述签名由所述生物支付设备根据密钥和设备信息生成，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；
- 根据所述设备信息对所述签名进行验证；
- 根据验证结果生成对所述生物支付设备的认证结果；及
- 向所述生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。

一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现以下步骤：

- 获取设备的密钥，其中，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；
- 根据所述密钥和设备信息生成签名，并基于所述签名向支付认证服务器发送认证请求，所述认证请求携带有设备标识，所述认证请求指示所述支付认证服务器根据所述设备标识对所述签名进行验证，并根据验证结果生成对所述生物支付设备的认证结果；
- 接收所述支付认证服务器返回认证结果，所述认证结果使所述支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现以下步骤：

- 接收生物支付设备基于签名和设备信息发送的认证请求，其中，所述签名由所述生物支付设备根据密钥和设备信息生成，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

根据所述设备信息对所述签名进行验证；

根据验证结果生成对所述生物支付设备的认证结果；及

向所述生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。

5

一种计算机程序，该计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述各方法实施例中的步骤。

10

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，

15 在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

图 1 为一个实施例中生物支付设备的认证方法的应用环境图；

图 2 为一个实施例中生物支付设备的认证方法的流程示意图；

图 3 为一个实施例中生物支付设备的生产环境示意图；

图 4 为一个实施例中具有 SE 的生物支付设备的认证过程的流程示意图；

20 图 5 为一个实施例中具有 TEE 的生物支付设备的认证过程的流程示意图；

图 6 为一个实施例中无 SE、TEE 的生物支付设备的认证过程的流程示意图；

图 7 为另一个实施例中生物支付设备的认证方法的流程示意图；

25 图 8 为一个实施例中生物支付设备的认证装置的结构框图；

图 9 为另一个实施例中生物支付设备的认证装置的结构框图；

图 10 为一个实施例中计算机设备的内部结构图；

图 11 为另一个实施例中计算机设备的内部结构图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及
5 实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例
仅仅用以解释本申请，并不用于限定本申请。

本申请提供的人脸支付设备的认证方法，可以应用于如图 1 所示的应用
环境中。其中，生物支付设备 102 通过网络与支付认证服务器 104 通过网络
进行通信，生物支付设备获取设备的密钥，其中，密钥是生产阶段通过生产
10 商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；根据
密钥和设备信息生成签名；基于签名向支付认证服务器发送认证请求，认证
请求携带有设备标识，认证请求指示支付认证服务器根据设备标识对签名进
行验证，并根据验证结果生成对生物支付设备的认证结果；接收支付认证服
务器返回认证结果，认证结果使支付认证服务器基于已认证的生物支付设备
15 发送的生物数据实现生物支付。其中，生物支付设备 102 可以是具有人体生
物数据采集器件的收银终端，包括有指纹采集器件、图像采集器件等硬件设
备，支付认证服务器 104 可以用独立的服务器或者是多个服务器组成的服务
器集群来实现。

在一个实施例中，如图 2 所示，提供了一种生物支付设备的认证方法，
20 以该方法应用于图 1 中的生物支付设备为例进行说明，包括以下步骤：

步骤 202，获取设备的密钥，其中，密钥是生产阶段通过生产商设备与
支付认证服务器通信而获得的被支付认证服务器认可的密钥。

生物支付是指采集人体生物数据作为支付凭证的一种支付手段，人体生
物数据包括指纹、人脸、笔迹、声音和步态等。不同于扫码支付由用户通过
25 操作个人手机生成私密性强的付款码，人体生物数据是一种能够通过公开手
段获得的数据，如通过摄像头采集人脸，通过麦克风采集声音，通过摄像头
采集步态等。因此，从某种手段来说，人体特征数据是一种公开数据，这就

需要生物支付设备是被认证通过的，以保障支付通信链路的安全。

为确保生物支付的安全性，一方面，从源头确保生物支付设备是通过支付平台资质认证的生产商所生产的合格设备，获得用于认证的密钥，另一方面，生物支付设备作为商家的收银终端被使用时，与支付认证服务器通信，

5 根据密钥生成签名，在支付认证服务器对签名验证通过后，建立生物支付设备与支付认证服务器的安全链路。

其中，生产商是指生物支付设备的生产商，生产商通过入驻支付平台的商户平台，作为支付平台的商户而获得生产能够被支付平台认证的生物支付设备的资质，生产商生产完成的生物支付设备需要通过支付平台的验收，进

10 而被售卖给商家，作为商家的收银终端。

生产商设备是生产商与支付认证服务器通信工具，是设备生产的辅助工具。生物支付设备生产完成后，通过生产商设备与支付认证服务器通信获得被支付认证服务器认可的密钥。

一种实施方式的设备密钥的获取方式为生产阶段在生物支付设备生成公

15 私钥，将公钥导出至生产商设备，由于生产商通过了支付平台的资质认证，可通过生产商设备将公钥上传至支付认证服务器。即私钥生成和保存在生物支付设备本地，公钥上传至支付认证服务器，由于公钥是被具有资质的生产商设备所上传的，且支付认证服务器具有与生物支付设备匹配公钥，因而，生物支付设备本地的私钥是被支付认证服务器认可的密钥。

20 一种实施方式的设备密钥的获取方式是生产阶段将生物支付设备导出设备信息至生产商设备，由于生产商通过了支付平台的资质认证，可通过生产商设备将设备信息上传至支付认证服务器，由支付认证服务器根据设备信息生成密钥，并返回至生产商设备，由生产商设备将密钥烧录至生物支付设备。由于密钥是支付认证服务器根据设备信息生成的，因此，密钥是被支付认证

25 服务器认可的。

步骤 204，根据密钥和设备信息生成签名。

具体地，生物支付设备根据密钥对设备信息生成签名，即使用密钥对设

备信息进行加密，得到的密文即此次传输过程的签名。设备信息是指能够标识生物支付设备身份的信息，可以为设备 ID，设备 MAC 地址等。

步骤 206，基于设备信息和签名向支付认证服务器发送认证请求，认证请求指示支付认证服务器根据设备信息对签名进行验证，并根据验证结果生成对生物支付设备的认证结果。

生物支付设备基于设备信息和签名向支付认证服务器发送认证请求。向支付认证服务器发送的设备信息与生物支付设备用于生成签名的设备信息相同。支付认证服务器接收到认证请求后，根据设备标识获取生物支付设备对应的解密方式，如获取该设备信息对应的公钥或解密规则，根据公钥和密钥规则解密签名得到设备信息，验证解密得到的设备信息与接收到的设备信息是否一致，根据验证结果生成对生物支付设备的认证结果。

若解密得到的设备信息与接收到的设备信息一致则验签通过，得到签名验证通过的验证结果，进一步得到生物支付设备认证通过的认证结果。若解密得到的设备信息与接收到的设备信息不一致，则验签不通过，得到签名验证失败的验证结果，进一步得到生物支付设备认证失败的认证结果。

步骤 208，接收支付认证服务器返回认证结果，认证结果使支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

具体地，在支付认证服务器认证通过后，支付认证服务器登记认证通过的生物支付设备，建立生物支付设备与支付认证服务器的安全链路。生物支付设备采集生物数据，将采集的生物数据和设备标识发送至支付认证服务器。支付认证服务器根据设备标识判断生物支付设备是否为认证通过的设备，若是，则对采集的生物数据与数据库中存储的用户的特征数据进行匹配，根据匹配的用户账户信息生成付款码，将付款码返回至生物支付设备，由生物支付设备根据付款码向支付认证服务器发起付款，支付认证服务器从对应账号进行扣款。而若认证服务器根据设备标识判断生物支付设备为非认证通过的设备，则将该生物支付设备的付款请求不作处理，认定为非法设备以保障用户支付账户安全。

上述的生物支付设备的认证方法，生物支付设备的密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥，进而利用密钥生成签名信息，发送给支付认证服务器验签，而签名是在生物支付设备端根据密钥生成的，密钥具有较高的安全等级，其它终端不能获得
5 密钥生成签名冒充设备进行设备认证。支付验证服务器根据认证结果能够确定发送生物数据的设备是哪一台设备，是否为支付平台所认证过的设备，只有通过支付验证服务器认证的生物支付设备采集的生物数据，在支付验证服务器侧才能获得付款码，从而确保生物支付的安全性能。

在另一个实施例中，生产阶段通过生产商设备与支付认证服务器通信而
10 获得被支付认证服务器认可的密钥的方式，包括：根据密钥生产指令生成公钥和私钥；导出公钥至生产商设备，由生产商设备上传公钥至支付认证服务器。

具体地，生物支付设备在完成硬件生产后，出厂前需要配置好设备密钥。如图 3 所示的生产环境示意图。生物支付设备 302 与生产商设备 304 连接，
15 生产商设备 304 与支付认证服务器 306 通信连接。

其中，密钥生产指令是指生物支付设备生产过程中用于启动产生公钥和私钥的指令。具体为在生物支付设备硬件生产完成后，为生物支付设备搭载操作系统，运行操作系统，根据密钥生产指令生成公钥和私钥。

公钥和私钥是使用非对称加密算法得到的一个密钥对中，将其中的一个
20 向外界公开，称为公钥，另一个自己保留，称为私钥。通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用密钥对的时候，如果用其中一个密钥加密一段数据，必须用另一个密钥解密。比如用私钥加密必须用公钥解密，否则解密将不会成功。

本申请中，私钥是密钥对所有者持有，即私钥是生物支付设备所持有，
25 不可公布，公钥由密钥对所有者公布支付验证服务器。具体地，通过被支付认证服务器认可的生产商设备公布给支付认证服务器，由于支付认证服务器获得了生物支付设备私钥对应的公钥，能够对私钥的加密文件进行解密，从

而使得生物支付设备中的私钥被支付认证服务器认可，通过支付认证服务器中的公钥能够对生物支付设备使用私钥加密的数据进行解密。

本实施例中，通过在生物支付设备生成公钥和私钥，私钥不导出，仅将公钥导出至支付认证服务器，使得生物支付设备的密钥无法被复制，避免生物支付设备被冒充，确保生物支付的安全性能。

一个实施例中，生物支付设备安装有安全芯片（Secure Element, SE）。安全芯片是一颗独立于生物支付设备主芯片的硬件芯片，能够防止外部恶意解析攻击，保护核心敏感数据安全，在芯片中具有密码算法逻辑电路，可以向外部提供安全的密码学算法服务。安全芯片不仅能防止来自软件层的逻辑攻击，还能抵抗物理攻击，即使其物理破坏拆解，也能够保护其中存储数据的安全。

如图 4 所示，利用安全芯片实现生物支付设备的认证，包括两个阶段：

第一阶段为生产阶段：生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥。

具体地，生物支付设备接入安全芯片，根据密钥生产指令控制生物支付设备的安全芯片生成公钥和私钥。

具体地，生物支付设备的主芯片利用安全芯片的密钥生成方法，控制安全芯片生成公钥和私钥。安全芯片相对于生物支付的主芯片是一个单独的硬件环境，其生成的公钥和私钥从硬件上与主芯片隔离，即使主芯片受到攻击，仍能确保密钥的安全。因此，利用安全芯片生成公钥和私钥的安全级别高。

生物支付设备将公钥导出至生产商设备，生产商设备通过安全接口将公钥上传至支付认证服务器。

具体地，根据安全芯片国密标准，只有加密密钥的公钥才可以导出，私钥不可以导出，利用生产商设备将公钥上传至支付认证服务器，从而使支付认证服务器持有该生物支付设备的公钥，使支付认证服务器具有能够对利用生物支付设备的私钥加密的数据进行解密的能力。在实际的应用中，生产商设备将设备标识和公钥一同上传至支付认证服务器，支付认证服务器建立设

备标识和公钥的对应关系，便于后续快速查找匹配到生物支付设备对应的公钥。

其中，生产商是通过支付平台认证，具有生产资质，因而对于生产商上传的公钥支付认证服务器认可，进而支付认证服务器认可该公钥对应的私钥。

- 5 支付认证服务器建立设备标识和公钥的对应关系，并向生产商设备返回上传结果。至此，认证的第一阶段完成，公钥上传至支付认证服务器，私钥存储在生物支付设备的安全芯片。

- 第二阶段为商家认证阶段，对位于商家侧的生物支付设备，利用被支付认证服务器认可的私钥向支付认证服务器认证，以建立生物支付设备与支付
10 认证服务器的安全链路。

其中，当商家侧的生物支付设备需要与支付认证服务器建立通信连接时，均需向支付认证服务器认证，以建立与支付认证服务器的安全通信链路。

首先，位于商家侧的生物支付设备控制安全芯片根据私钥和设备信息生成签名。

- 15 本实施例中，签名是在安全芯片中生成的，能够避免签名被迁移。根据私钥对设备信息生成签名，避免设备信息在传输过程中被篡改。为提高签名的时效性，还可进一步地，利用私钥对设备信息和时间戳进行签名。从而使支付验证服务器验证设备信息是否被篡改的同时，还对时间有效性进行验证，进一步提高支付安全。其次，通过将签名发送至支付认证服务器，支付认证
20 服务器获取私钥对应的公钥对签名进行验证。具体地，支付认证服务器接收到认证请求后，根据设备信息，获取对应的公钥，利用公钥对签名进行验签，根据公钥解密签名得到设备信息，验证解密得到的设备信息与接收到的设备信息是否一致，得到对签名的验证结果。

- 同时，还对签名的时间戳进行验证，根据当前时间与签名信息中的时间
25 戳验证签名的有效性期，进一步提高支付安全。若解密得到的设备信息与接收到的设备信息一致且时间有效，则验签通过，得到生物支付设备认证通过结果。若验证解密得到的设备信息与接收到的设备信息不一致，或时间超出

有效性期，则验签失败，得到生物支付设备认证失败结果。

再次，支付认证服务器向生物支付设备返回认证结果，认证结果使支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

具体地，在支付认证服务器认证通过后，支付认证服务器登记认证通过的生物支付设备，建立生物支付设备与支付认证服务器的安全链路。生物支付设备采集生物数据，将采集的生物数据和设备标识发送至支付认证服务器。支付认证服务器根据设备标识判断生物支付设备是否为认证通过的设备，若是，则对采集的生物数据与数据库中存储的用户的特征数据进行匹配，根据匹配的用户账户信息生成付款码，将付款码返回至生物支付设备，由生物支付设备根据付款码向支付认证服务器发起付款，支付认证服务器从对应账号进行扣款。而若认证服务器根据设备标识判断生物支付设备为非认证通过的设备，则将该生物支付设备的付款请求不作处理，认为为非法设备以保障用户支付账户安全。

本实施例中通过利用安全芯片，从隔离的硬件上产生公私钥和生成签名，且公钥只导出一次，私钥无法导出，使得生物支付设备的密钥无法复制，避免生物支付设备被冒充，从硬件上隔离使认证方法具有最高安全等级。

一个实施例中，生物支付设备搭载有可执行环境（Trusted Execution Environment, TEE），可执行环境借鉴于可信计算技术思想，旨在保护安全敏感的代码执行和相关数据信息免受恶意敌手的攻击和破坏，是建立可信移动终端平台的基础。TEE 主要是微内核操作系统组成，隔离于普通终端操作系统组成的富执行环境。TEE 能够抵御来自软件层的攻击，安全防护能力低于 SE。

如图 5 所示，利用可执行环境实现生物支付设备的认证，包括两个阶段：

第一阶段为生产阶段：生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥。

具体地，生物支付设备搭载可执行环境，基于可执行环境生成公钥和私钥。由于可执行环境是微内核操作系统组成，隔离于普通终端操作系统组成

的富执行环境，能够在软件上隔离生成密钥，提高密钥的安全等级。

生物支付设备将公钥导出至生产商设备，生产商设备通过安全接口将公钥上传至支付认证服务器。

本实施例中，私钥产生于可执行环境中，私钥无法导出，公钥只导出一次上传至支付认证服务器。从而使支付认证服务器持有该生物支付设备的公钥，使支付认证服务器具有能够对利用生物支付设备的私钥加密的数据进行解密的能力。在实际的应用中，生产商设备将设备标识和公钥一同上传至支付认证服务器，支付认证服务器建立设备标识和公钥的对应关系，便于后续快速查找匹配到生物支付设备对应的公钥。

其中，生产商是通过支付平台认证，具有生产资质，因而对于生产商上传的公钥支付认证服务器认可，进而支付认证服务器认可该公钥对应的私钥。支付认证服务器建立设备标识和公钥的对应关系，并向生产商设备返回上传结果。至此，认证的第一阶段完成，公钥上传至支付认证服务器，私钥存储在生物支付设备。

第二阶段为商家认证阶段，对位于商家侧的生物支付设备，利用被支付认证服务器认可的私钥向支付认证服务器认证，以建立生物支付设备与支付认证服务器的安全链路。

其中，当商家侧的生物支付设备需要与支付认证服务器建立通信连接时，均需向支付认证服务器认证，以建立与支付认证服务器的安全通信链路。

首先，位于商家侧的生物支付设备基于可执行环境根据私钥和设备信息生成签名。

其次，将签名发送至支付认证服务器，支付认证服务器获取私钥对应的公钥对签名进行验证。

再次，支付认证服务器向生物支付设备返回认证结果，认证结果使支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

认证的过程与基于安全芯片的认证过程相同，此处不再赘述。

本实施例中通过利用可执行环境，从软件上产生公私钥和生成签名，且

公钥只导出一次，私钥无法导出，使得生物支付设备的密钥无法复制，避免生物支付设备被冒充，从软件隔离使认证方法具有较高安全等级。

另一个实施例中，对于不支持 TEE 也没有 SE 的生物支付设备，如图 6 所示，实现生物支付设备的认证，包括两个阶段：

- 5 第一阶段为生产阶段，生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥。

具体地，生物支付设备将多因子设备信息导出至生产商设备，通过生产商设备将多因子设备信息上传至支付认证服务器，由支付认证服务器根据多因子设备信息生成存放该生物支付设备的密钥的动态链接库文件。

- 10 其中，多因子设备信息包括设备相关的多因子信息，即多重设备信息，如，包括但不限于品牌名称、设备名称、制造商名称、产品名称设备 MAC 地址，设备 ID，UUID(Unique Device Identifier)，设备序列号等等。

- 支付认证服务器根据多因子设备信息生成密钥，同时利用动态链接库存储密钥。动态链接库文件（SO 文件）就是一个黑盒子，支付认证服务器利用
15 黑盒子的加密规则将密钥存储在动态链接库文件中。由于黑盒规则是加密的，因而 SO 文件产生密钥的规则是加密的，无法进行设备的密钥复制。

- 支付认证服务器将存储有密钥的动态链接库文件发送至生产商设备，生产商设备将动态链接库文件烧录至生物支付设备。具体地，生物支付设备根据生产商设备的烧录指令，将生产商设备接收的支付认证服务器返回的动态
20 链接库文件烧录至生物支付设备。

本实施例中，对于生物支付设备不具有安全芯片和可执行环境，通过利用支付认证服务器生成密钥，利用外部导入的手段将密钥烧录至生物支付设备。时间为了避免外部导入时密钥被窃取，可采用加固手段，将密钥存储至 SO 文件中，将对 SO 文件进行混淆和加固处理。

- 25 具体地，烧录至生物支付设备的动态链接库文件不随设备恢复出厂设备而丢失，确保生密钥永久性存储在生物支付设备。

第二阶段商家认证阶段，对位于商家侧的生物支付设备，利用被支付认

证服务器认可的密钥向支付认证服务器认证，以建立生物支付设备与支付认证服务器的安全链路。

首先，利用动态链接库文件存放的密钥对设备信息进行加密，生成签名。

其次，将签名发送至支付认证服务器，支付认证服务器。获取对应的动态链接库文件对应的解密规则，对签名验签，得到解密的设备信息，验证解密的设备信息与接收到的设备信息是否一致。

再次，支付认证服务器向生物支付设备返回认证结果，认证结果使支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

本实施例中，对于无 SE 芯片和 TEE 的生物支付设备，通过由支付认证服务器根据生物支付设备的多因子设备信息生成用于存储密钥的动态链接库文件，进而通过生产商设备将存储有密钥的动态链接库文件导入至生物支付设备，由于密钥存放在 SO 文件中，加密和解密操作都在 SO 文件里，而通过黑盒的 SO 文件产生密钥，黑盒的规则是加密的，无法进行设备密钥的复制，从而提高了密钥的安全性。

进一步地，支付验证服务器对于存储了密钥的 SO 文件还采用混淆和加固的方式提高 SO 文件的安全等级，使 SO 文件不能轻易地被反向编译。SO 文件是二进制文件，通过利用混淆工具将二进制文件的代码混淆，将 SO 文件的代码顺序打乱，进行防逆向保护，利用加固程序加密 SO 文件使之无法被反向编译，进一步提高密钥的安全性。

上述的生物支付设备的认证方法，考虑了具有安全芯片、具有可执行环境以及非 SE、非 TEE 的生物支付设备的安全认证，几乎兼容了所有生物支付设备的认证，具有广泛的可适用性。

本申请的生物支付设备的认证方法，考虑了生物支付的特殊性，通过利用具有较高安全等级的密钥生成签名信息，发送给支付认证服务器验签，其它终端不能获得密钥生成签名冒充设备进行设备认证。支付验证服务器根据认证结果能够确定发送生物数据的设备是哪一台设备，是否为支付平台所认证过的设备，只有通过支付验证服务器认证的生物支付设备采集的生物数据，

在支付验证服务器侧才能获得付款码，从而确保生物支付的安全性能。

本申请的生物支付设备的认证方法，可应用于人脸支付、指纹支付、声纹支付等等。

如图 7 所示，提供一种生物支付设备的认证方法，以该方法应用于图 1 中的支付认证服务器为例进行说明，包括：

步骤 702，接收生物支付设备基于签名和设备信息发送的认证请求，其中，签名由生物支付设备根据密钥和设备信息生成，密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥。

生物支付是指采集人体生物数据作为支付凭证的一种支付手段，人体生物数据包括指纹、人脸、笔迹、声音和步态等。不同于扫码支付由用户通过操作个人手机生成私密性强的付款码，人体生物数据是一种能够通过公开手段获得的数据，如通过摄像头采集人脸，通过麦克风采集声音，通过摄像头采集步态等。因此，从某种手段来说，人体特征数据是一种公开数据，这就需要生物支付设备是被认证通过的，以保障支付通信链路的安全。

为确保生物支付的安全性，一方面，从源头确保生物支付设备是通过支付平台资质认证的生产商所生产的合格设备，获得用于认证的密钥，另一方面，生物支付设备作为商家的收银终端被使用时，与支付认证服务器通信，根据密钥生成签名，在支付认证服务器对签名验证通过后，建立生物支付设备与支付认证服务器的安全链路。

一种实施方式的设备密钥的获取方式为生产阶段在生物支付设备生成公私钥，将公钥导出至生产商设备，由于生产商通过了支付平台的资质认证，可通过生产商设备将公钥上传至支付认证服务器。即私钥生成和保存在生物支付设备本地，公钥上传至支付认证服务器，由于公钥是被具有资质的生产商设备所上传的，且支付认证服务器具有与生物支付设备匹配公钥，因而，生物支付设备本地的私钥是被支付认证服务器认可的密钥。

一种实施方式的设备密钥的获取方式是生产阶段将生物支付设备导出设备信息至生产商设备，由于生产商通过了支付平台的资质认证，可通过生产

商设备将设备信息上传至支付认证服务器，由支付认证服务器根据设备信息生成密钥，并返回至生产商设备，由生产商设备将密钥烧录至生物支付设备。由于密钥是支付认证服务器根据设备信息生成的，因此，密钥是被支付认证服务器认可的。

5 步骤 704，根据设备信息对签名进行验证。

具体地，生物支付设备根据密钥对设备信息生成签名，即使用密钥对设备信息进行加密，得到的密文即此次传输过程的签名。设备信息是指能够标识生物支付设备身份的信息，可以为设备 ID，设备 MAC 地址等。

生物支付设备基于设备信息和签名向支付认证服务器发送认证请求。向
10 支付认证服务器发送的设备信息与生物支付设备用于生成签名的设备信息相同。支付认证服务器接收到认证请求后，根据设备标识获取生物支付设备对应的解密方式，如获取该设备信息对应的公钥或解密规则，根据公钥和密钥规则解密签名得到设备信息，验证解密得到的设备信息与接收到的设备信息是否一致，根据验证结果生成对生物支付设备的认证结果。

15 步骤 706，根据验证结果生成对生物支付设备的认证结果。

若解密得到的设备信息与接收到的设备信息一致则验签通过，得到签名验证通过的验证结果，进一步得到生物支付设备认证通过的认证结果。若解密得到的设备信息与接收到的设备信息不一致，则验签不通过，得到签名验证失败的验证结果，进一步得到生物支付设备认证失败的认证结果。

20 步骤 708，向生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。

具体地，在支付认证服务器认证通过后，支付认证服务器登记认证通过的生物支付设备，建立生物支付设备与支付认证服务器的安全链路。生物支付设备采集生物数据，将采集的生物数据和设备标识发送至支付认证服务器。

25 支付认证服务器根据设备标识判断生物支付设备是否为认证通过的设备，若是，则对采集的生物数据与数据库中存储的用户的特征数据进行匹配，根据匹配的用户账户信息生成付款码，将付款码返回至生物支付设备，由生物支

付设备根据付款码向支付认证服务器发起付款，支付认证服务器从对应账号进行扣款。而若认证服务器根据设备标识判断生物支付设备为非认证通过的设备，则将该生物支付设备的付款请求不作处理，认定为非法设备以保障用户支付账户安全。

- 5 上述的生物支付设备的认证方法，生物支付设备的密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥，进而利用密钥生成签名信息，发送给支付认证服务器验签，而签名是在生物支付设备端根据密钥生成的，密钥具有较高的安全等级，其它终端不能获得密钥生成签名冒充设备进行设备认证。支付验证服务器根据认证结果能够确定发送生物数据的设备是哪一台设备，是否为支付平台所认证过的设备，只有通过支付验证服务器认证的生物支付设备采集的生物数据，在支付验证服务器侧才能获得付款码，从而确保生物支付的安全性能。
- 10

- 在另一个实施例中，生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥的方式，包括：获取生产商设备上传的生物支付设备的公钥，其中，公钥以及公钥对应的私钥根据密钥生产指令生成，公钥被导出至生产商设备。具体地，生物支付设备在完成硬件生产后，出厂前需要配置好设备密钥。如图 3 所示的生产环境示意图。生物支付设备 302 与生产商设备 304 连接，生产商设备 304 与支付认证服务器 306 通信连接。
- 15

- 其中，密钥生产指令是指生物支付设备生产过程中用于启动产生公钥和私钥的指令。具体为在生物支付设备硬件生产完成后，为生物支付设备搭载操作系统，运行操作系统，根据密钥生产指令生成公钥和私钥。
- 20

- 本申请中，私钥是密钥对所有者持有，即私钥是生物支付设备所持有，不可公布，公钥是密钥对持有者公布支付验证服务器，具体地，通过被支付认证服务器认可的生产商设备公布给支付认证服务器，由于支付认证服务器获得了生物支付设备私钥对应的公钥，能够对私钥的加密文件进行解密，从而使得生物支付设备中的私钥被支付认证服务器认可，通过支付认证服务器中的公钥能够对生物支付设备使用私钥加密的数据进行解密。
- 25

本实施例中，通过在生物支付设备生成公钥和私钥，私钥不导出，仅将公钥导出至支付认证服务器，使得生物支付设备的密钥无法被复制，避免生物支付设备被冒充，确保生物支付的安全性能。

一个实施例中，生物支付设备接入安全芯片，根据密钥生产指令控制生物支付设备的安全芯片生成公钥和私钥。生物支付设备将公钥导出至生产商设备，生产商设备通过安全接口将公钥和设备标识上传至支付认证服务器。位于商家侧的生物支付设备控制安全芯片根据私钥和设备信息生成签名。

另一个实施中，生物支付设备搭载可执行环境，基于可执行环境生成公钥和私钥。生物支付设备将公钥导出至生产商设备，生产商设备通过安全接口将公钥和设备标识上传至支付认证服务器。位于商家侧的生物支付设备基于可执行环境根据私钥和设备信息生成签名。

进一步地，支付认证服务器获取对应的公钥，根据设备信息和公钥对签名进行验证。

在另一个实施例中，生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥的方式，包括：获取生产商设备上传的生物支付设备的多因子信息；根据多因子信息生成存储生物支付设备的密钥的动态链接库文件；将动态链接库文件发送至生产商设备，动态链接库文件指示生产商设备将动态链接库文件烧录至生物支付设备。

其中，多因子设备信息包括设备相关的多因子信息，即多重设备信息，如，包括但不限于品牌名称、设备名称、制造商名称、产品名称设备 MAC 地址，设备 ID，UUID(Unique Device Identifier)，设备序列号等等。

支付认证服务器根据多因子设备信息生成与密钥，建立密钥与多因子设备信息的对应关系，同时利用动态链接库存储密钥，将其传输至生产商设备，使密钥被导入至生物支付设备。动态链接库文件(SO 文件)就是一个黑盒子，支付认证服务器利用黑盒子的加密规则将密钥存储在动态链接库文件中。由于黑盒规则是加密的，因而 SO 文件产生密钥的规则是加密的，无法进行设备的密钥复制。

具体地，生物支付设备根据生产商设备的烧录指令，将生产商设备接收的支付认证服务器返回的动态链接库文件烧录至生物支付设备。烧录至生物支付设备的动态链接库文件不随设备恢复出厂设备而丢失，确保生物密钥永久性存储在生物支付设备。

- 5 本实施例中，对于无 SE 芯片和 TEE 的生物支付设备，通过由支付认证服务器根据生物支付设备的多因子设备信息生成用于存储密钥的动态链接库文件，进而通过生产商设备将存储有密钥的动态链接库文件导入至生物支付设备，由于密钥存放在 SO 文件中，加密和解密操作都在 SO 文件里，而通过黑盒的 SO 文件产生密钥，黑盒的规则是加密的，无法进行设备密钥的复制，
10 从而提高了密钥的安全性。

进一步地，支付验证服务器对存储有密钥的动态链接库文件进行混淆和加固处理。通过利用混淆工具将二进制文件的代码混淆，将 SO 文件的代码顺序打乱，进行防逆向保护，利用加固程序加密 SO 文件使之无法被反向编译，进一步提高密钥的安全性。

15

- 应该理解的是，虽然图 2、4-7 的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图 2、4-7 中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

- 25 在一个实施例中，如图 8 所示，提供了一种生物支付设备的认证装置，该装置可以采用软件模块或硬件模块，或者是二者的结合成为计算机设备的一部分，该装置具体包括：

密钥获取模块 802，用于获取设备的密钥，其中，密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

签名模块 804，用于根据密钥和设备信息生成签名。

认证模块 806，用于基于设备信息和签名向支付认证服务器发送认证请求，认证请求指示支付认证服务器根据设备信息对签名进行验证，并根据验证结果生成对生物支付设备的认证结果；

接收模块 808，用于接收支付认证服务器返回认证结果，认证结果使支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。

在另一个实施例中，密钥获取模块，包括：密钥生成模块，用于根据密钥生产指令生成公钥和私钥。

密钥导出模块，用于导出公钥至生产商设备，由生产商设备上传公钥至支付认证服务器。

其中，密钥生成模块，用于据密钥生产指令控制生物支付设备的安全芯片生成公钥和私钥。

签名模块，用于控制安全芯片根据私钥和设备信息生成签名。

其中，密钥生成模块，用于根据密钥生产指令，基于可执行环境生成公钥和私钥。

签名模块，用于基于可执行环境根据私钥和设备信息生成签名。

在另一个实施例中，密钥获取模块，包括：

设备信息导出模块，用于将多因子设备信息导出至生产商设备，通过生产商设备将多因子设备信息发送至支付认证服务器，由支付认证服务器根据多因子信息生成存储生物支付设备的密钥的动态链接库文件；

密钥导入模块，用于响应生产商设备的烧录指令，将支付认证服务器返回的动态链接库文件烧录至本地。

在另一个实施例中，动态链接库文件为混淆和加固的动态链接库文件，签名模块，用于根据混淆和加固的动态链接库文件所存储的密钥对设备信息进行加密生成签名。

一种生物支付设备的认证装置，如图 9 所示，包括：

认证获取模块 902，用于接收生物支付设备基于签名设备信息发送的认证请求，其中，签名由生物支付设备根据密钥和设备信息生成，密钥是生产
5 阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

验证模块 904，用于根据设备信息对签名进行验证；

认证模块 906，用于根据验证结果生成对生物支付设备的认证结果；

发送模块 908，用于向生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。
10

在另一个实施例中，还包括密钥获取模块，用于获取生产商设备上传的生物支付设备的设备标识和公钥，其中，公钥以及公钥对应的私钥根据密钥生产指令生成，公钥被导出至生产商设备。

在另一个实施例中，密钥获取模块，包括：

15 设备信息获取模块，用于获取生产商设备上传的生物支付设备的多因子信息；

密钥生成模块，用于根据多因子信息生成存储生物支付设备的密钥的动态链接库文件；

密钥发送模块，用于将动态链接库文件发送至生产商设备，动态链接库
20 文件指示生产商设备将动态链接库文件烧录至生物支付设备。

在另一个实施列中，还包括密钥处理模块，用于对存储有密钥的动态链接库文件进行混淆和加固处理。

关于生物支付设备的认证装置的具体限定可以参见上文中对于生物支付设备的认证方法的限定，在此不再赘述。上述生物支付设备的认证装置中的
25 各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图 10 所示。该计算机设备包括通过系统总线连接的处理器、存储器和网络接口。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储生物支付设备数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种生物支付设备的认证方法。

10 在一个实施例中，提供了一种计算机设备，该计算机设备可以是终端，其内部结构图可以如图 11 所示。该计算机设备包括通过系统总线连接的处理器、存储器、通信接口、显示屏和生物数据采集装置。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机程序。该
15 内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的通信接口用于与外部的终端进行有线或无线方式的通信，无线方式可通过 WIFI、运营商网络、NFC（近场通信）或其他技术实现。该计算机程序被处理器执行时以实现一种生物支付设备的认证方法。该计算机设备的显示屏可以是液晶显示屏或者电子墨水显示屏，该计算机设备的生物数
20 据采集装置可以是图像采集装置，也可以为指纹采集装置和/或声音采集装置。

本领域技术人员可以理解，图 10 和图 11 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，
25 或者组合某些部件，或者具有不同的部件布置。

在一个实施例中，还提供了一种计算机设备，包括存储器和处理器，存

存储器中存储有计算机程序，该处理器执行计算机程序时实现上述各方法实施例中的步骤。

在一个实施例中，提供了一种计算机可读存储介质，存储有计算机程序，该计算机程序被处理器执行时实现上述各方法实施例中的步骤。

- 5 在一个实施例中，提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述各方法实施例中的步骤。

10

- 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的
- 15 的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器（Read-Only Memory, ROM）、磁带、软盘、闪存或光存储器等。易失性存储器可包括随机存取存储器（Random Access Memory, RAM）或外部高速缓冲存储器。作为说明而非局限，RAM 可以是多种形式，比如静态随机存取存储器（Static
- 20 Random Access Memory, SRAM）或动态随机存取存储器（Dynamic Random Access Memory, DRAM）等。

以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

- 25 以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对申请专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干

变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。