

一种账户的开立方法、系统及装置

本申请要求于2021年07月16日提交中国国家知识产权局、申请号为202110808788.9、
5 申请名称为“一种账户的开立方法、系统及装置”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

本说明书涉及数据安全技术领域，尤其涉及一种账户的开立方法、系统及装置。

10

背景技术

离线场景下的创新支付，越来越受到国家的重视和各方机构的关注，进而硬件钱包受到更多关注。硬件钱包最大的特点就是数字资产从“云”到了“端”上，相应的，硬件钱包的开立环节即硬件钱包账户的开立成为非常关键的风险点。

15 那么，如何提供一种可信的硬件钱包账户的开立方法成为亟待解决的问题。

发明内容

本说明书一个或多个实施例提供了一种账户的开立方法、系统及装置，以实现提高账户开立可信度。

20 在本说明书第一方面，提供一种账户的开立方法，应用于终端设备，所述终端设备包含可信执行环境 TEE 和基于加密硬件的安全元件，所述方法包括：

在所述 TEE 中，获得当前用户的用户公钥；

在所述 TEE 中，利用预置的厂商私钥对所述用户公钥进行签名，得到用户证书；

在所述安全元件中，利用所述用户公钥对应的用户私钥，对开立信息进行签名，

25 其中，所述开立信息基于所述终端设备的设备信息生成；

在所述 TEE 中，至少基于所述用户证书以及签名后的开立信息，生成开立请求；

在所述 TEE 中，基于所述开立请求生成开立请求报文，并将所述开立请求报文发送至开立账户的服务器，以使所述服务器基于所述开立请求报文为所述当前用户开立账户。

30 在一种可实施方式中，所述获得当前用户的用户公钥，包括：

在所述 TEE 中，利用预先生成的设备公私钥对以及所述当前用户的用户标识，生成对应的用户公私钥对，包括所述用户公钥及其对应的用户私钥。

在一种可实施方式中，所述生成开立请求，包括：

获得厂商数字证书，其中包括所述厂商私钥对应的厂商公钥；

35 基于所述用户证书、所述厂商数字证书以及签名后的开立信息，生成开立请求。

- 在一种可实施方式中，所述基于所述开立请求生成开立请求报文，包括：
- 在所述 TEE 中，利用对称密钥，对所述开立请求加密，得到加密开立请求；
- 利用所述服务器的服务器公钥对所述对称密钥加密，得到加密后的第一加密密钥；
- 基于所述加密开立请求和所述第一加密密钥，生成开立请求报文。
- 5 在一种可实施方式中，还包括：
- 利用预设密钥随机生成方式，随机生成所述对称密钥。
- 在一种可实施方式中，还包括：
- 从所述 TEE 中获得预置的与服务器约定的服务器公钥；或
- 利用预设密钥协商算法，从服务器获得服务器公钥。
- 10 在一种可实施方式中，还包括：
- 获得所述服务器基于所述开立请求报文反馈的开立回复报文；
- 基于所述开立回复报文开立账户。
- 在一种可实施方式中，所述开立回复报文包括：利用所述对称密钥加密的开立回复密文，以及利用所述服务器公钥对应的服务器私钥对所述对称密钥加密所得的第二加密密钥；
- 15 所述基于所述开立回复报文开立账户，包括：
- 利用所述服务器公钥对所述第二加密密钥解密，得到对称密钥；
- 在确定解密所得的对称密钥与所述 TEE 中预先生成的对称密钥相同的情况下，利用所述对称密钥对所述开立回复密文进行解密，得到开立回复明文；
- 20 基于所述开立回复明文开立账户。
- 在本说明书第二方面，提供一种账户的开立方法，包括：应用于服务器，包括：
- 接收终端设备基于当前用户发送的开立请求报文，所述开立请求报文包括开立请求，所述开立请求包括用户证书以及签名后的开立信息，所述用户证书为，利用所述终端设备预置的厂商私钥对所述当前用户的用户公钥进行签名所得，所述签名后的开立信息为：利用所述当前用户对应的用户私钥对开立信息签名所得，所述开立信息基于所述终端设备的设备信息生成；
- 25 利用所述厂商私钥对应的厂商公钥，对所述用户证书进行第一验证；
- 若第一验证通过，利用所述用户证书中的所述用户公钥对所述签名后的开立信息进行第二验证；
- 30 若第二验证通过，利用所述开立信息中的设备信息确定开立回复报文，并发送至所述终端设备，以使所述终端设备基于所述开立回复报文开立账户。
- 在一种可实施方式中，所述开立请求还包括厂商数字证书，其中包括所述厂商私

钥对应的厂商公钥;

所述对所述用户证书进行第一验证, 包括:

利用所获得的厂商根公钥对所述厂商数字证书进行第三验证;

若第三验证通过, 利用所述厂商公钥, 对所述用户证书进行第一验证。

- 5 在一种可实施方式中, 所述开立请求为利用对称密钥加密所得的加密开立请求;
所述开立请求报文还包括: 利用服务器公钥对所述对称密钥加密所得的第一加密密钥;

在对所述用户证书进行第一验证之前, 还包括:

利用所述服务器公钥对应的服务器私钥, 解密所述第一加密密钥, 得到对称密钥;

利用所述对称密钥解密所述加密开立请求, 得到开立请求明文。

- 10 在一种可实施方式中, 所述利用所述开立信息中的设备信息确定开立回复报文,
包括:

利用所述设备信息, 确定开立回复;

利用所述对称密钥, 加密所述开立回复, 得到开立回复密文;

利用所述服务器私钥加密所述对称密钥, 得到加密后的第二加密密钥;

- 15 基于所述开立回复密文和所述第二加密密钥, 形成开立回复报文。

在本说明书第三方面, 提供一种账户的开立系统, 所述账户的开立系统包括终端设备和服务器; 所述终端设备, 配置为执行第一方面所述的方法; 所述服务器, 配置为执行第二方面所述的方法。

- 20 在本说明书第四方面, 提供一种账户的开立装置, 应用于终端设备, 所述终端设备包含可信执行环境 TEE 和基于加密硬件的安全元件, 所述装置包括:

第一获得模块, 配置为在所述 TEE 中, 获得当前用户的用户公钥;

第一签名模块, 配置为在所述 TEE 中, 利用预置的厂商私钥对所述用户公钥进行签名, 得到用户证书;

- 25 第二签名模块, 配置为在所述安全元件中, 利用所述用户公钥对应的用户私钥,
对开立信息进行签名, 其中, 所述开立信息基于所述终端设备的设备信息生成;

请求生成模块, 配置为在所述 TEE 中, 至少基于所述用户证书以及签名后的开立信息, 生成开立请求;

- 30 生成发送模块, 配置为在所述 TEE 中, 基于所述开立请求生成开立请求报文, 并将所述开立请求报文发送至开立账户的服务器, 以使所述服务器基于所述开立请求报文为所述当前用户开立账户。

在本说明书第五方面, 提供一种账户的开立装置, 应用于服务器, 包括:

报文接收模块, 配置为接收终端设备基于当前用户发送的开立请求报文, 所述开

立请求报文包括开立请求，所述开立请求包括用户证书以及签名后的开立信息，所述用户证书为，利用所述终端设备预置的厂商私钥对所述当前用户的用户公钥进行签名所得，所述签名后的开立信息为：利用所述当前用户对应的用户私钥对开立信息签名所得，所述开立信息基于所述终端设备的设备信息生成；

- 5 第一验证模块，配置为利用所述厂商私钥对应的厂商公钥，对所述用户证书进行第一验证；

第二验证模块，配置为若第一验证通过，利用所述用户证书中的所述用户公钥对所述签名后的开立信息进行第二验证；

- 10 确定发送模块，配置为若第二验证通过，利用所述开立信息中的设备信息确定开立回复报文，并发送至所述终端设备，以使所述终端设备基于所述开立回复报文开立账户。

在本说明书第六方面，提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书一个或多个实施例所提供的终端设备侧账户的开立方法。

- 15 在本说明书第七方面，提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书一个或多个实施例所提供的终端设备侧账户的开立方法。

- 20 在本说明书第八方面，提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书一个或多个实施例所提供的服务器侧账户的开立方法。

在本说明书第九方面，提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书一个或多个实施例所提供的服务器侧账户的开立方法。

- 25 根据本说明书实施例所提供的一种账号的开立方法及装置，在安全性相对最高的安全元件中，利用用户私钥对开立信息进行签名，保证开立信息的准确性、完整性以及避免其被窃取篡改。在终端设备的安全性较高的 TEE 中，利用预置的厂商私钥对用户公钥签名得到用户证书，并结合签名后的开立信息，生成开立请求报文，并在 TEE 中发送开立请求报文至开立账户的服务器。其中的用户证书可以表征该开立请求报文来自于设备厂商所生产的真实物理设备，并且开立请求报文的生成及发送过程在 TEE 及安全元件中完成，避免报文生成过程中相关信息的丢失，在一定程度上提高开立请求报文的可信度，进而提高对应账户开立可信度。
- 30

附图说明

- 35 为了更清楚地说明本说明书实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书的一些实施例，对于本领域普通技术人员来讲，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 为本说明书披露的一个实施例的实施框架示意图；
- 图 2 示出本说明书实施例提供的账户的开立方法的一种流程示意图；
- 图 3 示出本说明书实施例提供的账户的开立方法的另一流程示意图；
- 图 4 示出本说明书实施例提供的账户的开立系统的一种框架示意图；
- 5 图 5 示出本说明书实施例提供的账户的开立装置的一种框架示意图；
- 图 6 示出本说明书实施例提供的账户的开立装置的一种框架示意图。

具体实施方式

下面将结合附图详细描述本说明书实施例的技术方案。

- 10 本说明书实施例披露一种账户的开立方法及装置，下面对账户的开立的应用场景和发明构思进行介绍，具体如下：

硬件钱包一般依托于真实物理设备，其账户的开立也依托于真实物理设备，若账户开立设备为假手机、云手机等非真实物理设备，则很容易出现虚假硬件钱包，为开立账户的用户的资产安全带来危险。为了解决上述问题，目前账户开立过程中，从 APP 15 层面获取所在终端设备的设备信息，并利用设备信息组装账户开立请求报文，将该账户开立请求报文发送至开立账户的服务器，以进行账户开立申请。该过程中，APP 层面的信息获取易受到黑产攻击及模拟，服务器仍无法有效识别账户开立设备是否为真实的物理设备。

- 鉴于此，本说明书实施例提供了一种账户的开立方法，应用于终端设备。如图 1 20 所示，为本说明书披露的一个实施例的实施框架示意图，终端设备包含可信执行环境 TEE 和基于加密硬件的安全元件。终端设备在检测到当前用户发起账户开立申请的情况下，在 TEE 中，获得当前用户的用户公钥，并利用预置的厂商私钥对用户公钥进行签名，得到用户证书；在安全元件中，利用用户公钥对应的用户私钥，对基于终端设备的设备信息生成的开立信息进行签名；在 TEE 中，至少基于用户证书以及签名后的 25 开立信息，生成开立请求报文，并将其发送至开立账户的服务器，以使服务器基于开立请求报文为当前用户开立账户。一种可实施方式中，终端设备可以在 TEE 或安全元件中，基于设备信息生成开立信息。

该方案适用的账户可以是硬件钱包账户，也可以是其他依托于物理设备的、对安全性要求较高的账户，例如，身份认证账户，银行相关账户，等等。

- 30 其中，上述厂商私钥为终端设备的生产厂商在其生产线上存储于终端设备的私钥，该厂商私钥在一定程度上可以证明终端设备为厂商所生产的真实物理设备。

本实施例中，在安全性相对最高的安全元件中，利用用户私钥对开立信息进行签名，保证开立信息的准确性及完整性，并且避免其被窃取篡改。在终端设备的安全性较高的 TEE 中，利用预置的厂商私钥对用户公钥签名得到用户证书，并结合签名后的 35 开立信息，生成开立请求报文，并在 TEE 中发送开立请求报文至开立账户的服务器。

其中的用户证书可以表征该开立请求报文来自于设备厂商所生产的真实物理设备，并且开立请求报文的生成及发送过程在 TEE 及安全元件中完成，避免报文生成过程中相关信息的丢失，在一定程度上提高开立请求报文的可信度，进而提高对应账户开立可信度。

5 下面结合具体实施例，对本说明书提供的账户的开立方法进行详细阐述。

图 2 示出了本说明书提供的账户的开立方法的一种流程示意图。该方法应用于终端设备，该终端设备可以是任一具有数据计算、处理和存储的设备，例如可以为电脑、手机、平板电脑、智能手表和支付卡等。本说明书一个实施例中，该终端设备包含可信执行环境 TEE 以及基于加密硬件的安全元件，所述方法包括 S210-S250：

10 S210：在 TEE 中，获得当前用户的用户公钥。

其中，可信执行环境 TEE (Trusted Execution Environment)，是终端设备的处理器例如 CPU 上的一块区域。这块区域的作用是给数据和代码的执行提供一个更安全的空间，并保证它们的机密性和完整性。其通过创建一个独立运行的小型操作系统，实现安全存储、安全计算等涉及安全、隐私的数据处理。

15 基于加密硬件的安全元件可以包括但不限于 SE (Secure Element) 安全元件，其通常以芯片形式提供，在其中具有加密/解密逻辑电路，从而可以防止外部恶意解析攻击，保护数据安全。需要说明的是，安全元件是基于硬件对数据进行加密保护的环境，因此具有比 TEE 更高的安全级别。一种情况中，该安全元件可以是终端设备的内置安全元件，也可以是终端设备的外置安全元件，例如：终端设备为手机的情况下，外置的安全元件可以是 Sim 卡支持的安全元件。

20 在一种实现中，终端设备在检测到当前用户发起账户开立申请的情况下，在 TEE 中，获得当前用户的用户公钥。其中，该账户开立申请可以是当前用户基于账户开立相关应用发起的。账户开立相关应用可以提供有账户开立界面，该账户开立界面显示有账户开立按键，可以通过点击账户开立按键，触发账户开立申请。相应的，在一种情况中，终端设备还包括普通执行环境 REE，该账户开立相关应用可以运行于 REE 中。

25 在一个例子中，该账户开立相关应用可以为支付宝钱包，相应的，该当前用户可以为支付宝用户，该账户可以为：在支付宝钱包下针对支付宝用户所需开立的硬件钱包账户。

30 在另一例子中，该账户开立相关应用可以为 x 银行应用，该当前用户为该 x 银行用户，该账户可以为该 x 银行针对该当前用户所需开立的钱包账户。上述例子仅为本说明书的示例，该账户开立相关应用还可以是其他可开立账户的应用，该当前用户可以为该其他可开立账户的应用的用户，账户为该其他可开立账户的应用针对当前用户所需开立的账户。

35 在本说明书的一个实施例中，在 S210，可以包括：在 TEE 中，利用预先生成的设备公私钥对以及当前用户的用户标识，生成对应的用户公私钥对，包括用户公钥及其对应的用户私钥。

终端设备在检测到当前用户发起账户开立申请的情况下，在 TEE 中，获得预先生成的设备公私钥对以及当前用户的用户标识；利用例如国密算法的密钥生成算法，基于设备公私钥对以及用户标识，生成对应的用户公私钥对。其中，该用户标识可以为当前用户的用户 ID。该设备公私钥对可以是在首次启动账户开立相关应用时生成的一对公私钥对，并存储于 TEE 中。

一种实现中，在生成用户公私钥对之后，将其中的用户公钥存储于 TEE 中，将其中的用户私钥存储于安全元件中，以避免用户公私钥对被篡改。

S220：在 TEE 中，利用预置的厂商私钥对用户公钥进行签名，得到用户证书。其中，厂商私钥是：终端设备的厂商在终端设备生产线上存储于终端设备硬件中的密钥。该厂商私钥可以存储于终端设备的 TEE 中。由此，得到的用户证书中可以包括：用户公钥以及利用厂商私钥对用户公钥进行签名后所得的第一签名。

S230：在安全元件中，利用用户公钥对应的用户私钥，对开立信息进行签名。其中，开立信息基于终端设备的设备信息生成。

一种情况中，设备信息可以包括但不限于：终端设备的设备名称、设备标识、设备型号、制造商标识等。其中，设备标识用于唯一地标识出该终端设备，例如可以体现为 MAC 地址。设备型号可以指示出设备类型（电脑、智能手机、支付卡，或是智能手表），以及该类型下的具体机型。该设备信息预存于终端设备的 TEE 中，以避免设备信息被篡改。

一种可实施方式中，终端设备可以在 TEE 或安全元件中，基于设备信息生成开立信息。进而，在安全元件中，利用预设哈希算法对开立信息进行哈希值计算，得到开立信息对应的哈希值。利用安全元件中存储的用户私钥，对该哈希值进行加密，得到针对开立信息的数字签名。

S240：在 TEE 中，至少基于用户证书以及签名后的开立信息，生成开立请求。其中，开立请求用于向开立账户的服务器申请开立账户。该开立请求可以包括用户证书以及签名后的开立信息。该用户证书用于表征开立账户的终端设备为真实物理终端设备，签名后的开立信息用于辅助服务器验证开立信息是否准确、完整以及真实，在验证通过之后，服务器可利用开立信息生成开立回复，并反馈至终端设备，终端设备可以基于该开立回复开立账户。

在本说明书的一个实施例中，在 S240，可以包括如下步骤 11-12：

步骤 11：获得厂商数字证书，其中包括厂商私钥对应的厂商公钥。

步骤 12：基于用户证书、厂商数字证书以及签名后的开立信息，生成开立请求。

本实施例中，为了更好的提高账户开立可信度，在 S140 中，在 TEE 中获得厂商数字证书，其中包括厂商私钥对应的厂商公钥。该厂商数字证书是终端设备的厂商在终端设备生产线上，存储于终端设备的。一种情况中，该厂商数字证书存储于终端设备的 TEE 中。一种实现中，该厂商数字证书可以是证书颁发机构（CA, Certificate Authority）为终端设备的厂商颁发的证书。该厂商数字证书用于验证

用户证书的真实性。

得到用户证书、厂商数字证书以及签名后的开立信息之后，终端设备在 TEE 中，基于用户证书、厂商数字证书以及签名后的开立信息，生成开立请求。其中，开立请求包括用户证书、厂商数字证书以及签名后的开立信息。后续的，将开立请求发送至服务器之后，服务器可以首先验证厂商数字证书的真实性，在厂商数字证书的真实性验证通过之后，通过厂商数字证书中的厂商公钥，验证用户证书的真实性。相应的，该开立请求的可信度更好，进而账户开立可信度更高。其中，验证厂商数字证书的真实性可以是：基于服务器从终端设备的厂商处所获取的厂商根公钥，验证厂商数字证书的真实性。

10 S250: 在 TEE 中，基于开立请求生成开立请求报文，并将开立请求报文发送至开立账户的服务器，以使服务器基于开立请求报文为当前用户开立账户。

一种实现中，终端设备可以在 TEE 中，基于预设报文格式，基于开立请求生成开立请求报文，其中，该预设报文格式为基于终端设备与开立账户的服务器之间的数据传输协议所设置的格式。进而，将开立请求报文发送至开立账户的服务器。相应的，服务器基于开立请求报文为当前用户开立账户。

本实施例中，在安全性相对最高的安全元件中，利用用户私钥对开立信息进行签名，保证开立信息的准确性、完整性以及避免其被窃取篡改。在终端设备的安全性较高的 TEE 中，利用预置的厂商私钥对用户公钥签名得到用户证书，并结合签名后的开立信息，生成开立请求报文，并在 TEE 中发送开立请求报文至开立账户的服务器。其中的用户证书可以表征该开立请求报文来自于设备厂商所生产的真实物理设备，并且开立请求报文的生成及发送过程在 TEE 及安全元件中完成，避免报文生成过程中相关信息的丢失，在一定程度上提高开立请求报文的可信度，进而提高对应账户开立可信度。

20 为了避免开立请求报文传输过程中被截取，其中的设备信息被窃取，在本说明书的一个实施例中，可以对开立请求报文进行加密传输。相应的，在所述 S250，可以包括如下步骤 21-23:

步骤 21: 在 TEE 中，利用对称密钥，对开立请求加密，得到加密开立请求。

步骤 22: 利用服务器的服务器公钥对对称密钥加密，得到加密后的第一加密密钥。

30 步骤 23: 基于加密开立请求和第一加密密钥，生成开立请求报文。其中，开立请求报文中包括加密开立请求以及第一加密密钥。在一种情况中，第一加密密钥可以添加在开立请求报文的报文头处。

35 在一种可实施方式中，为了更好的提高对开立请求的保密性，在步骤 21 之前，还可以包括步骤: 在 TEE 中，利用预设密钥随机生成方式，随机生成前述对称密钥。在账户的开立流程，利用随机的对称密钥对开立请求加密，可在一定程度上增加开立请求报文中相关信息被窃取的难度，提高开立请求报文中相关信息的保密性以及安全性。其中，该预设密钥随机生成方式可以包括但不限于: DES (Data Encryption Standard,

数据加密算法)、3DES (Triple Data Encryption Algorithm, 三重数据加密算法) 以及 AES (Advanced Encryption Standard, 高级加密标准) 等对称加密算法。

- 服务器公钥可以是终端设备与服务器约定的密钥, 其可以预先预置于终端设备, 也可以在终端设备有需求时下发于终端设备。相应的, 在一种可实施方式中, 在步骤 5 22 之前, 还可以包括步骤: 从 TEE 中, 获得预置的与服务器约定的服务器公钥; 或利用预设密钥协商算法, 从开立账户的服务器获得服务器公钥。该预设密钥协商算法可以目前任一可协商密钥的算法, 本实施例中并不做限定。

- 利用该服务器公钥对对称密钥加密, 得到加密后的第一加密密钥。按照预设报文格式, 基于加密开立请求和第一加密密钥, 生成开立请求报文。并将开立请求报文发送至服务器。后续的, 服务器基于开立请求报文生成开立回复报文, 并反馈至终端设备。终端设备可基于开立回复报文开立账户。

本实施例基于终端设备厂商已有的通用能力和轻量级的数据处理方式, 实现了类似一设备一密钥的可靠性高的数据加密方案, 保障了数据传输过程中的机密性以及完整性。

- 15 在本说明书的一个实施例中, 在步骤 S250 之后, 还包括如下步骤 31-32:

步骤 31: 获得服务器基于开立请求报文反馈的开立回复报文。

步骤 32: 基于开立回复报文开立账户。其中, 该开立回复报文可包括指示终端设备开立账户的信息。相应的, 终端设备基于开立回复报文中的信息开立账户。

- 20 一种实现中, 终端设备可以通过 TEE 获得服务器基于开立请求报文反馈的开立回复报文, 进而, 在 TEE 中基于开立回复报文开立账户。

为了保证开立回复报文的安全性, 进而保证账户开立可信度, 服务器向终端设备反馈的开立回复报文包含的信息为加密之后的信息。在一种可实施方式中, 该开立回复报文包括: 利用对称密钥加密的开立回复密文以及利用服务器公钥对应的服务器私钥对对称密钥加密所得的第二加密密钥。

- 25 相应的, 前述步骤 32, 可以包括如下步骤 321-323:

步骤 321: 利用服务器公钥对第二加密密钥解密, 得到对称密钥。

步骤 322: 在确定解密所得的对称密钥与 TEE 中预先生成的对称密钥相同的情况下, 利用对称密钥对开立回复密文进行解密, 得到开立回复明文。

步骤 323: 基于开立回复明文开立账户。

- 30 本实现方式中, 终端设备通过 TEE 获得开立回复报文之后, 对开立回复报文进行解析, 得到其中的开立回复密文以及第二加密密钥; 利用服务器公钥对第二加密密钥解密, 得到对称密钥。判断解密所得的对称密钥与 TEE 中预先生成的对称密钥是否相同, 在确定解密所得的对称密钥与 TEE 中预先生成的对称密钥相同的情况下, 可以认为该开立回复报文为服务器真实下发的报文。相应的, 终端设备在 TEE 中, 利用对称
35 密钥对开立回复密文进行解密, 得到开立回复明文, 进而基于开立回复明文开立账户。

在上述账户的开立流程中，服务器与终端设备之间传输的数据，通过随机生成的对称密钥及服务器公私钥对进行加密解密，并且，在各方确认数据发送方的真实性以及数据本身的真实及完整性之后，执行后续步骤，以提高账户开立的可信度。

- 5 相应于上述方法实施例，图3示出了本说明书提供的账户的开立方法的另一种流程示意图。该方法应用于服务器，该服务器可以是由任何具有计算、处理能力的设备、装置、平台、服务器、设备集群来实现，该服务器用于：为发送开立请求报文的终端设备开立账户。本说明书一个实施例中，所述方法可以包括如下步骤 S310-S340：

- 10 S310：接收终端设备基于当前用户发送的开立请求报文。该开立请求报文包括开立请求，该开立请求包括用户证书以及签名后的开立信息，该用户证书为，利用终端设备预置的厂商私钥对当前用户的用户公钥进行签名所得，该签名后的开立信息为：利用当前用户对应的用户私钥对开立信息签名所得，开立信息基于终端设备的设备信息生成。

- 15 一种情况中，终端设备包含可信执行环境 TEE 以及基于加密硬件的安全元件。上述开立请求报文、开立请求以及用户证书可以是在终端设备的 TEE 中生成的，上述签名后的开立信息可以是在终端设备的安全元件中生成的。一种实现中，该开立请求报文为终端设备通过 TEE 向服务器发送的。

- 20 其中，上述当前用户为待开立账户的用户。一种情况中，该当前用户可以是设置于终端设备的账户开立相关应用的用户。终端设备还可以包括普通执行环境 REE，该账户开立相关应用可以运行于 REE 中。举例而言，该账户开立相关应用可以为支付宝钱包，相应的，该当前用户可以为支付宝用户，该账户可以为：在支付宝钱包下针对支付宝用户所需开立的硬件钱包账户。支付宝钱包可以在终端设备的 REE 中运行。

需要说明的，开立请求报文、开立请求、用户证书以及签名后的开立信息的生成过程，可以参见上述应用于终端设备的账户的开立方法实施例中所记载的生成过程，在此不再赘述。

- 25 一种实现中，服务器可以与若干个终端设备进行通信，接收若干个终端设备发送的开立请求报文，进而针对每一开立请求报文，执行本说明书实施例所提供的该账户的开立方法流程。服务器接收到开立请求报文之后，对开立请求报文进行解析，得到其中的用户证书以及签名后的开立信息。

- 30 S320：利用厂商私钥对应的厂商公钥，对用户证书进行第一验证。一种实现中，服务器可以预置有厂商私钥对应的厂商公钥。相应的，服务器接收到开立请求报文之后，针对该终端设备，从本地的预设存储区域，获得厂商私钥对应的厂商公钥；进而，利用厂商公钥，对用户证书进行第一验证。另一种实现中，服务器可以是在接收到开立请求报文之后，针对该终端设备，从该终端设备厂商对应的服务器下载得到该厂商公钥，进而，利用厂商公钥，对用户证书进行第一验证。

- 35 S330：若第一验证通过，利用用户证书中的用户公钥对签名后的开立信息进行第二验证。本步骤中，若第一验证通过，则可以表征用户证书中的用户公钥是真实完整的，且可以表征该终端设备为厂商生产的真实物理设备。相应的，可以确认该开立请

求报文为从真实物理终端所发送的。进而，服务器对用户证书进行解析，获得其中的用户公钥；并利用用户公钥对签名后的开立信息进行第二验证。

- 5 在一种实现中，若第一验证不通过，则可以认为用户证书中的用户公钥被篡改，或者该终端设备不是相应厂商所生产的真实终端设备。后续的，服务器可以不再执行后续步骤。一种情况中，服务器还可以向终端设备发送指示其不能开立账户的信息。

S340：若第二验证通过，利用开立信息中的设备信息确定开立回复报文，并发送

至终端设备，以使终端设备基于开立回复报文开立账户。本步骤中，若第二验证通过，则可以表征开立信息是真实完整的。相应的，服务器对开立信息进行解析，得到设备信息；进而，利用该设备信息确定开立回复报文，并发送至终端设备。

- 10 本实施例中，服务器对终端设备发送的开立请求报文进行两次验证，确定终端设备为真实物理终端设备，且开立请求报文为终端设备发送的真实的报文之后，向终端设备反馈开立回复报文，在一定程度上提高了终端设备账户开立的可信度。

在本说明书的一个实施例中，该开立请求还包括厂商数字证书，其中包括厂商私钥对应的厂商公钥；相应的，所述 S320，可以包括如下步骤 41-42：

- 15 步骤 41：利用所获得的厂商根公钥对厂商数字证书进行第三验证。其中，厂商根公钥可以是服务器预置于其本地的，也可以是在接收到终端设备发送的开立请求报文之后，从终端设备厂商对应的服务器处下载获得的，这都是可以的。

步骤 42：若第三验证通过，利用厂商公钥，对用户证书进行第一验证。

- 20 为了更好地证明终端设备为真实物理终端，保证账户开立可信度，该开立请求还可以包括厂商数字证书，其中包括厂商私钥对应的厂商公钥。相应的，服务器利用所获得的厂商根公钥对厂商数字证书进行第三验证。若第三验证通过，则表征厂商数字证书可信，即厂商可信，进而，解析厂商数字证书，得到其中的厂商公钥，利用厂商公钥对用户证书进行第一验证。

- 25 在本说明书的一个实施例中，该开立请求为利用对称密钥加密所得的加密开立请求；该开立请求报文还包括：利用服务器公钥对对称密钥加密所得的第一加密密钥；

相应的，在所述 S320 之前，还可以包括如下步骤 51-52：

步骤 51：利用服务器公钥对应的服务器私钥，解密第一加密密钥，得到对称密钥。

步骤 52：利用对称密钥解密加密开立请求，得到开立请求明文。

- 30 为了保证报文在传输过程中的安全性，该开立请求为利用对称密钥加密所得的加密开立请求；相应的，该开立请求报文还可以包括：利用服务器公钥对对称密钥加密所得的第一加密密钥。服务器对开立请求报文进行解析，得到其中的第一加密密钥以及加密开立请求。利用预置的服务器公钥对应的服务器私钥，解密第一加密密钥，得到对称密钥。进而利用对称密钥解密加密开立请求，得到开立请求明文。进而，基于开立请求明文中的设备信息，生成开立回复报文。

- 35 在本说明书的一个实施例中，所述 S340，可以包括如下步骤 61-64：

步骤 61: 利用设备信息, 确定开立回复。

步骤 62: 利用对称密钥, 加密开立回复, 得到开立回复密文。

步骤 63: 利用服务器私钥加密对称密钥, 得到加密后的第二加密密钥。

步骤 64: 基于开立回复密文和第二加密密钥, 形成开立回复报文。

- 5 为了保证报文在传输过程中的安全性, 服务器在步骤 S340, 首先利用设备信息, 确定开立回复, 利用从开立请求报文中解密所得的对称密钥, 加密开立回复, 得到开立回复密文。并利用服务器私钥加密对称密钥, 得到加密后的第二加密密钥。进而, 按照预设报文格式, 基于开立回复密文和第二加密密钥组装报文, 形成开立回复报文。将开立回复报文发送至终端设备, 以使终端设备基于该开立回复报文开立账户。利用
- 10 开立请求报文携带的对称密钥以及服务器私钥对报文进行加密, 进而传输加密后的开立回复报文, 保证报文在传输过程中的安全性, 提高账户开立可信度。

- 上述内容对本说明书的特定实施例进行了描述, 其他实施例在所附权利要求书的范围内。在一些情况下, 在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行, 并且仍然可以实现期望的结果。另外, 在附图中描绘的过程不一定要按照示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中, 多任务处理和并行处理也是可以的, 或者可能是有利的。
- 15 按照示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中, 多任务处理和并行处理也是可以的, 或者可能是有利的。

- 相应于上述方法实施例, 本说明书实施例提供了一种账户的开立系统 400, 其示意性框图如图 4 所示, 包括终端设备 410 和服务器 420; 终端设备 410, 配置为执行上述终端设备侧的账户的开立方法; 服务器 420, 配置为执行上述服务器侧的账户的开立方法。一种实现中, 服务器可为多个终端设备 410 开立账户。
- 20 相应于上述方法实施例, 本说明书实施例提供了一种账户的开立装置 500, 应用于终端设备, 所述终端设备包含可信执行环境 TEE 和基于加密硬件的安全元件, 其示意性框图如图 5 所示, 包括:

- 第一获得模块 510, 配置为在所述 TEE 中, 获得当前用户的用户公钥;
- 25 第一签名模块 520, 配置为在所述 TEE 中, 利用预置的厂商私钥对所述用户公钥进行签名, 得到用户证书;

 第二签名模块 530, 配置为在所述安全元件中, 利用所述用户公钥对应的用户私钥, 对开立信息进行签名, 其中, 所述开立信息基于所述终端设备的设备信息生成;

- 请求生成模块 540, 配置为在所述 TEE 中, 至少基于所述用户证书以及签名后的
- 30 开立信息, 生成开立请求;

 生成发送模块 550, 配置为在所述 TEE 中, 基于所述开立请求生成开立请求报文, 并将所述开立请求报文发送至开立账户的服务器, 以使所述服务器基于所述开立请求报文为所述当前用户开立账户。

- 在一种可实施方式中, 所述第一获得模块 510, 具体配置为在所述 TEE 中, 利用
- 35 预先生成的设备公私钥对以及所述当前用户的用户标识, 生成对应的用户公私钥对,

包括所述用户公钥及其对应的用户私钥。

在一种可实施方式中，所述请求生成模块 540，具体配置为获得厂商数字证书，其中包括所述厂商私钥对应的厂商公钥；

基于所述用户证书、所述厂商数字证书以及签名后的开立信息，生成开立请求。

- 5 在一种可实施方式中，所述生成发送模块 550，具体配置为在所述 TEE 中，利用对称密钥，对所述开立请求加密，得到加密开立请求；

利用所述服务器的服务器公钥对所述对称密钥加密，得到加密后的第一加密密钥；

基于所述加密开立请求和所述第一加密密钥，生成开立请求报文。

在一种可实施方式中，还包括：

- 10 密钥生成模块（图中未示出），配置为利用预设密钥随机生成方式，随机生成所述对称密钥。

在一种可实施方式中，还包括：

第二获得模块（图中未示出），配置为从所述 TEE 中获得预置的与服务器约定的服务器公钥；或

- 15 利用预设密钥协商算法，从服务器获得服务器公钥。

在一种可实施方式中，还包括：

第三获得模块（图中未示出），配置为获得所述服务器基于所述开立请求报文反馈的开立回复报文；

账户开立模块（图中未示出），配置为基于所述开立回复报文开立账户。

- 20 在一种可实施方式中，所述开立回复报文包括：利用所述对称密钥加密的开立回复密文，以及利用所述服务器公钥对应的服务器私钥对所述对称密钥加密所得的第二加密密钥；

所述账户开立模块，具体配置为利用所述服务器公钥对所述第二加密密钥解密，得到对称密钥；

- 25 在确定解密所得的对称密钥与所述 TEE 中预先生成的对称密钥相同的情况下，利用所述对称密钥对所述开立回复密文进行解密，得到开立回复明文；

基于所述开立回复明文开立账户。

相应于上述方法实施例，本说明书实施例提供了一种账户的开立装置 600，应用于服务器，该服务器用于为发送开立请求报文的终端设备开立账户，其示意性框图如图 6 所示，包括：

- 30 报文接收模块 610，配置为接收终端设备基于当前用户发送的开立请求报文，所述开立请求报文包括开立请求，所述开立请求包括用户证书以及签名后的开立信息，所述用户证书为，利用所述终端设备预置的厂商私钥对所述当前用户的用户公钥进行

签名所得，所述签名后的开立信息为：利用所述当前用户对应的用户私钥对开立信息签名所得，所述开立信息基于所述终端设备的设备信息生成；

第一验证模块 620，配置为利用所述厂商私钥对应的厂商公钥，对所述用户证书进行第一验证；

- 5 第二验证模块 630，配置为若第一验证通过，利用所述用户证书中的所述用户公钥对所述签名后的开立信息进行第二验证；

确定发送模块 640，配置为若第二验证通过，利用所述开立信息中的设备信息确定开立回复报文，并发送至所述终端设备，以使所述终端设备基于所述开立回复报文开立账户。

- 10 在一种可实施方式中，所述开立请求还包括厂商数字证书，其中包括所述厂商私钥对应的厂商公钥；

所述第一验证模块 620，具体配置为利用所获得的厂商根公钥对所述厂商数字证书进行第三验证；

若第三验证通过，利用所述厂商公钥，对所述用户证书进行第一验证。

- 15 在一种可实施方式中，所述开立请求为利用对称密钥加密所得的加密开立请求；所述开立请求报文还包括：利用服务器公钥对所述对称密钥加密所得的第一加密密钥；还包括：

第一解密模块（图中未示出），配置为在对所述用户证书进行第一验证之前，利用所述服务器公钥对应的服务器私钥，解密所述第一加密密钥，得到对称密钥；

- 20 第二解密模块（图中未示出），配置为利用所述对称密钥解密所述加密开立请求，得到开立请求明文。

在一种可实施方式中，所述确定发送模块 640，具体配置为利用所述设备信息，确定开立回复；

利用所述对称密钥，加密所述开立回复，得到开立回复密文；

- 25 利用所述服务器私钥加密所述对称密钥，得到加密后的第二加密密钥；

基于所述开立回复密文和所述第二加密密钥，形成开立回复报文。

上述装置实施例与方法实施例相对应，具体说明可以参见方法实施例部分的描述，此处不再赘述。装置实施例是基于对应的方法实施例得到，与对应的方法实施例具有同样的技术效果，具体说明可参见对应的方法实施例。

- 30 本说明书实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书所提供的所述终端设备侧账户的开立方法。

本说明书实施例还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书所提供的所述终

端设备侧账户的开立方法。

本说明书实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书所提供的所述服务器侧账户的开立方法。

5 本说明书实施例还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书所提供的所述服务器侧账户的开立方法。

10 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于存储介质和计算设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。

15 本领域技术人员应该可以意识到，在上述一个或多个示例中，本说明书实施例所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

 以上所述的具体实施方式，对本说明书实施例的目的、技术方案和有益效果进行了进一步的详细说明。所应理解的是，以上所述仅为本说明书实施例的具体实施方式而已，并不用于限定本说明书的保护范围，凡在本说明书的技术方案的基础之上所做的任何修改、等同替换、改进等，均应包括在本说明书的保护范围之内。

20

权 利 要 求 书

1、一种账户的开立方法，应用于终端设备，所述终端设备包含可信执行环境 TEE 和基于加密硬件的安全元件，所述方法包括：

在所述 TEE 中，获得当前用户的用户公钥；

在所述 TEE 中，利用预置的厂商私钥对所述用户公钥进行签名，得到用户证书；

在所述安全元件中，利用所述用户公钥对应的用户私钥，对开立信息进行签名，其中，所述开立信息基于所述终端设备的设备信息生成；

在所述 TEE 中，至少基于所述用户证书以及签名后的开立信息，生成开立请求；

在所述 TEE 中，基于所述开立请求生成开立请求报文，并将所述开立请求报文发送至开立账户的服务器，以使所述服务器基于所述开立请求报文为所述当前用户开立账户。

2、根据权利要求 1 所述的方法，所述获得当前用户的用户公钥，包括：

在所述 TEE 中，利用预先生成的设备公私钥对以及所述当前用户的用户标识，生成对应的用户公私钥对，包括所述用户公钥及其对应的用户私钥。

3、根据权利要求 1 所述的方法，所述生成开立请求，包括：

获得厂商数字证书，其中包括所述厂商私钥对应的厂商公钥；

基于所述用户证书、所述厂商数字证书以及签名后的开立信息，生成开立请求。

4、根据权利要求 1-3 任一项所述的方法，所述基于所述开立请求生成开立请求报文，包括：

在所述 TEE 中，利用对称密钥，对所述开立请求加密，得到加密开立请求；

利用所述服务器的服务器公钥对所述对称密钥加密，得到加密后的第一加密密钥；

基于所述加密开立请求和所述第一加密密钥，生成开立请求报文。

5、根据权利要求 4 所述的方法，还包括：

利用预设密钥随机生成方式，随机生成所述对称密钥。

6、根据权利要求 4 所述的方法，还包括：

从所述 TEE 中获得预置的与服务器约定的服务器公钥；或

利用预设密钥协商算法，从服务器获得服务器公钥。

7、根据权利要求 4 所述的方法，还包括：

获得所述服务器基于所述开立请求报文反馈的开立回复报文；

基于所述开立回复报文开立账户。

8、根据权利要求 7 所述的方法，所述开立回复报文包括：利用所述对称密钥加密的开立回复密文，以及利用所述服务器公钥对应的服务器私钥对所述对称密钥加密所得的第二加密密钥；

所述基于所述开立回复报文开立账户，包括：

利用所述服务器公钥对所述第二加密密钥解密，得到对称密钥；

在确定解密所得的对称密钥与所述 TEE 中预先生成的对称密钥相同的情况下，利用所述对称密钥对所述开立回复密文进行解密，得到开立回复明文；

基于所述开立回复明文开立账户。

9、一种账户的开立方法，应用于服务器，包括：

接收终端设备基于当前用户发送的开立请求报文，所述开立请求报文包括开立请求，所述开立请求包括用户证书以及签名后的开立信息，所述用户证书为，利用所述终端设备预置的厂商私钥对所述当前用户的用户公钥进行签名所得，所述签名后的开立信息为：利用所述当前用户对应的用户私钥对开立信息签名所得，所述开立信息基于所述终端设备的设备信息生成；

利用所述厂商私钥对应的厂商公钥，对所述用户证书进行第一验证；

若第一验证通过，利用所述用户证书中的所述用户公钥对所述签名后的开立信息进行第二验证；

若第二验证通过，利用所述开立信息中的设备信息确定开立回复报文，并发送至所述终端设备，以使所述终端设备基于所述开立回复报文开立账户。

10、如权利要求 9 所述的方法，所述开立请求还包括厂商数字证书，其中包括所述厂商私钥对应的厂商公钥；

所述对所述用户证书进行第一验证，包括：

利用所获得的厂商根公钥对所述厂商数字证书进行第三验证；

若第三验证通过，利用所述厂商公钥，对所述用户证书进行第一验证。

11、如权利要求 9 或 10 所述的方法，所述开立请求为利用对称密钥加密所得的加密开立请求；所述开立请求报文还包括：利用服务器公钥对所述对称密钥加密所得的第一加密密钥；

在对所述用户证书进行第一验证之前，还包括：

利用所述服务器公钥对应的服务器私钥，解密所述第一加密密钥，得到对称密钥；

利用所述对称密钥解密所述加密开立请求，得到开立请求明文。

12、如权利要求 11 所述的方法，所述利用所述开立信息中的设备信息确定开立回复报文，包括：

利用所述设备信息，确定开立回复；

- 利用所述对称密钥，加密所述开立回复，得到开立回复密文；
- 利用所述服务器私钥加密所述对称密钥，得到加密后的第二加密密钥；
- 基于所述开立回复密文和所述第二加密密钥，形成开立回复报文。
- 13、一种账户的开立系统，所述账户的开立系统包括终端设备和服务器；
- 所述终端设备，配置为执行权利要求 1-8 任一项所述的方法；
- 所述服务器，配置为执行权利要求 9-12 任一项所述的方法。
- 14、一种账户的开立装置，应用于终端设备，所述终端设备包含可信执行环境 TEE 和基于加密硬件的安全元件，所述装置包括：
- 第一获得模块，配置为在所述 TEE 中，获得当前用户的用户公钥；
- 第一签名模块，配置为在所述 TEE 中，利用预置的厂商私钥对所述用户公钥进行签名，得到用户证书；
- 第二签名模块，配置为在所述安全元件中，利用所述用户公钥对应的用户私钥，对开立信息进行签名，其中，所述开立信息基于所述终端设备的设备信息生成；
- 请求生成模块，配置为在所述 TEE 中，至少基于所述用户证书以及签名后的开立信息，生成开立请求；
- 生成发送模块，配置为在所述 TEE 中，基于所述开立请求生成开立请求报文，并将所述开立请求报文发送至开立账户的服务器，以使所述服务器基于所述开立请求报文为所述当前用户开立账户。
- 15、一种账户的开立装置，应用于服务器，包括：
- 报文接收模块，配置为接收终端设备基于当前用户发送的开立请求报文，所述开立请求报文包括开立请求，所述开立请求包括用户证书以及签名后的开立信息，所述用户证书为，利用所述终端设备预置的厂商私钥对所述当前用户的用户公钥进行签名所得，所述签名后的开立信息为：利用所述当前用户对应的用户私钥对开立信息签名所得，所述开立信息基于所述终端设备的设备信息生成；
- 第一验证模块，配置为利用所述厂商私钥对应的厂商公钥，对所述用户证书进行第一验证；
- 第二验证模块，配置为若第一验证通过，利用所述用户证书中的所述用户公钥对所述签名后的开立信息进行第二验证；
- 确定发送模块，配置为若第二验证通过，利用所述开立信息中的设备信息确定开立回复报文，并发送至所述终端设备，以使所述终端设备基于所述开立回复报文开立账户。
- 16、一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-8 任一项所述的方法。
- 17、一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所

述处理器执行所述可执行代码时，实现权利要求 9-12 任一项所述的方法。