

一种离线身份验证的方法、装置、存储介质及电子设备

技术领域

[01]本说明书涉及计算机技术领域，尤其涉及一种离线身份验证的方法、装置、存储介质及电子设备。

背景技术

[02]随着互联网的快速发展,私有的隐私数据越来越受到大众的关注。而为了保证用户数据的安全性,在执行业务时,可以通过采集到的用户指纹、人脸或者虹膜等生物特征对用户进行身份验证。具体过程为:终端设备将采集的生物特征发送至服务器,服务器将终端设备发送的生物特征与之前保存用户录入的生物特征进行比对,比对通过后,即确定用户通过身份验证。

[03]但是，目前的身份验证方式并不能对用户进行有效地身份验证。

发明内容

[04]本说明书提供一种离线身份验证的方法、装置、存储介质及电子设备，以解决相关技术存在的在无法对用户进行有效地安全身份验证的问题。

[05] 本说明书采用下述技术方案：本说明书提供了一种离线身份验证的方法，所述方法应用于终端设备，所述终端设备中设有安全环境，所述安全环境和所述终端设备中的其他系统环境相互数据隔离，包括：响应于用户的离线支付请求，获取所述终端设备在离线状态下采集到的所述用户的待验证身份信息；对所述待验证身份信息进行签名，得到签名后的待验证身份信息；将所述签名后的待验证身份信息发送到所述安全环境中，以在所述安全环境中，对所述签名后的待验证身份信息进行验签，并在所述签名后的待验证身份信息通过验签后，将所述待验证身份信息与所述安全环境中保存的标准身份信息进行比对，得到第一比对结果；根据所述第一比对结果，对所述用户进行离线身份验证。

[06]可选地，响应于用户的离线支付请求，获取所述终端设备在离线状态下采集到的所述用户的待验证身份信息，具体包括：响应于用户的离线支付请求，监测所述用户是否开通使用离线身份验证的方式进行离线支付的权限；若确定所述用户开通所述权限，则获取所述终端设备在离线状态下采集到的所述用户的待验证身份信息。

[07]可选地,所述方法还包括:响应于所述用户在线状态下针对所述权限发送的权限开通请求,采集所述用户录入的标准身份信息;将所述标准身份信息发送给服务器,以使所述服务器对所述标准身份信息进行保存。

[08]可选地,对所述待验证身份信息进行签名,具体包括:通过业务私钥,对所述待验证身份信息进行数字签名。

[09]可选地,对所述签名后的待验证身份信息进行验签,具体包括:通过存储在安全环境中的业务公钥,在所述安全环境中对所述签名后的待验证身份信息进行验签。

[10]可选地,对所述待验证身份信息进行签名,得到签名后的待验证身份信息,具体包括:对所述待验证身份信息进行加密,得到加密后待验证身份信息;对所述加密后待验证身份信息进行签名,得到签名后的待验证身份信息;将所述待验证身份信息与所述安全环境中保存的标准身份信息进行比对,得到第一比对结果,具体包括:将所述加密后待验证身份信息和所述安全环境中保存的加密后的标准身份信息进行比对,得到第一比对结果。

[11]可选地,将所述标准身份信息发送给服务器,以使所述服务器对所述标准身份信息进行保存,具体包括:将所述标准身份信息以及预先生成的业务公钥发送给服务器,以使所述服务器对所述标准身份信息和所述业务公钥进行保存;所述方法还包括:响应于所述用户在线状态下发送的支付请求,获取所述终端设备在线状态下采集到的所述用户的第二待验证身份信息;通过业务私钥,对所述第二待验证身份信息进行签名,得到签名后的第二待验证身份信息;将所述签名后的第二待验证身份信息发送给所述服务器,以使所述服务器通过所述业务公钥对所述签名后的第二待验证身份信息进行验签,并在所述签名后的第二待验证身份信息通过验签后,将所述第二待验证身份信息与所述服务器中保存的标准身份信息进行比对,得到第二比对结果,以根据所述第二比对结果,对所述用户进行在线身份验证。

[12]本说明书提供了一种离线身份验证装置,所述装置中设有安全环境,所述安全环境和所述装置中的其他系统环境相互数据隔离,包括:获取模块,用于响应于用户的离线支付请求,获取所述装置在离线状态下采集到的所述用户的待验证身份信息;签名模块,用于对所述待验证身份信息进行签名,得到签名后的待验证身份信息;比对模块,用于将所述签名后的待验证身份信息发送到所述安全环境中,以在所述安全环境中,对所述签名后的待验证身份信息进行验签,并在所述签名后的待验证身份信息通过验签后,将所述待验证身份信息与所述安全环境中保存的标准身份信息进行比对,得到第一比对结

果；验证模块，用于根据所述第一比对结果，对所述用户进行离线身份验证。

[13]本说明书提供了一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述离线身份验证的方法。

[14]本说明书提供了一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述离线身份验证的方法。

[15]本说明书采用的上述至少一个技术方案能够达到以下有益效果：在本说明书提供的离线身份验证方法，获取终端设备在离线状态下采集到的用户的待验证身份信息，对待验证身份信息进行签名，得到签名后的待验证身份信息，将签名后的待验证身份信息发送到安全环境中，以在安全环境中，对签名后的待验证身份信息进行验签，并在签名后的待验证身份信息通过验签后，将待验证身份信息与安全环境中保存的标准身份信息进行比较，得到第一比对结果，根据第一比对结果，对用户进行离线身份验证。

[16]从上述方法中可以看出，在离线状态下，由于预先在本地的安全环境中保存了用户用于身份验证的标准身份信息，使得用户处于离线状态时，依然可以采集用户的待验证身份信息，通过在本地安全环境内比对用户的待验证身份信息和标准身份信息，完成对用户的离线身份验证，保证了用户在离线状态下依然能够进行身份验证，从而提高执行业务的效率，给用户带来便利。并且，由于标准身份信息保存在安全环境内，且，用户的待验证身份信息和标准身份信息的比对也是在安全环境内完成，这样能够保证用户的隐私数据不被泄露，进一步保证了用户的信息安全。

附图说明

[17]此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。

[18]图 1 为本说明书中提供的一种离线身份验证方法的流程示意图。

[19]图 2 为本说明书中一种离线身份验证方法的终端设备运行方式示意图。

[20]图 3 为本说明书提供的一种离线身份验证方法的装置的示意图。

[21]图 4 为本说明书提供的一种对应于图 1 的电子设备的示意图。

具体实施方式

[22]为使本说明书的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，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他实施例，都属于本说明书保护的范围。

[23]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[24]图 1 为本说明书中提供一种离线身份验证的方法的流程示意图，包括步骤 S100 至步骤 S106。

[25]S100：响应于用户的离线支付请求，获取终端设备在离线状态下采集到的用户的待验证身份信息。

[26]在现实生活中，用户可能会面临在不同环境下执行业务的场景，例如，在处于网络不佳或者无网环境时，用户和商家进行面对面支付，或用户在购物软件上完成支付操作。在执行支付业务的过程中，为了保证用户账户及用户隐私数据的安全性，需要对用户进行身份验证，基于此，本申请应用于离线环境，使用户在离线状态下依然能够完成身份验证。

[27]例如，用户在执行支付业务环节时通过客户端发起了支付请求，此时客户端若监测到用户当前处于离线状态，则可以通过本申请提供的离线身份验证方式对用户进行身份验证。以用户通过指纹信息进行离线身份验证为例，具体地，在进行身份验证的过程中，客户端可以弹出一个身份验证界面，该界面向用户展示录入指纹的文字或者图像提示，用于引导用户根据提示录入指纹信息。其中，客户端采集到的指纹信息即为终端设备在离线状态下采集到的用户的待验证身份信息。

[28]在本说明书中，终端设备可以包括诸如手机、平板电脑等移动设备，待验证身份信息是指生物特征信息，包括指纹、人脸和虹膜数据等等。本说明书中提供的离线验证方法对任何一种生物特征信息均适用，为了便于描述，下面仅以用户的指纹信息为例作为用户的待验证身份信息进行阐述，但用户的待验证身份信息不仅仅限于指纹信息。

[29]需要说明的是，在实际应用中，用户想要在离线状态下进行身份验证以执行支付业务，需要先开通使用离线身份验证的方式进行离线支付的权限。因此，在监测到用户发送的离线支付请求后，需要先判断用户是否开通使用离线身份验证的方式进行离线支付

的权限，若用户并未开通，则需要用户授权进行开通该权限。而若客户端确定用户开通了使用离线身份验证的方式进行离线支付的权限后，则可以通过本申请提供的离线身份验证的方式，对用户进行身份验证。

[30]S102：对所述待验证身份信息进行签名，得到签名后的待验证身份信息。

[31]在执行支付业务的过程中，用户输入指纹信息后，客户端将获取终端设备在离线状态下采集到的用户的指纹信息，而为了保证业务执行过程中的安全性，在后续对待验证指纹信息进行验证之前，需要对此待验证指纹信息进行签名，具体地，可以通过预先生成的业务私钥对待验证指纹信息进行数字签名。

[32]通过预先生成的业务私钥对待验证指纹信息进行数字签名后，在后续离线身份验证过程中，也需要通过预先生成的该业务公钥来验签。其中，所述业务公钥和业务私钥，是在客户端监测到用户开通了使用离线身份验证的方式进行离线支付的权限后，由客户端在安全环境中生成，并将其保存在安全环境中。

[33]为了进一步地保证信息的安全性，在本申请提供的离线身份验证方法中，还可以先将待验证指纹信息进行加密，得到待验证指纹信息的密文信息，再通过预先生成的业务私钥对该密文信息进行数字签名。这样能够保证在后续的验签过程中，待验证指纹信息是以密文的形式来验签，由于对待验证指纹信息进行了加密，即使待验证指纹信息泄露，也不会造成用户隐私的外泄，进一步地保证了用户隐私数据的安全性。

[34]S104：将所述签名后的待验证身份信息发送到所述安全环境中，以在安全环境中，对所述签名后的待验证身份信息进行验签，并在所述签名后的待验证身份信息通过验签后，将所述待验证身份信息与所述安全环境中保存的标准身份信息进行比对，得到第一比对结果。

[35]客户端可以将签名后的待验证指纹信息发送到安全环境中，并在安全环境中，对签名后的待验证指纹信息进行验签。其中，该安全环境是由终端设备划分的一个安全区域，且安全环境和终端设备中的其他系统环境相互数据隔离，验签的过程都是在安全环境中进行，进一步保证了数据的安全性。

[36]其中，本说明书中提到的安全环境可以是指可信执行环境（Trusted Execution Environment, TEE）。

[37]在安全环境中，通过预先生成的业务公钥对待验证指纹信息进行验签，若验签不通过，则身份验证失败，在签名后的待验证指纹信息通过验签后，则可以将待验证指纹信

息与安全环境中保存的之前用户录入的用于进行身份验证的标准指纹信息进行比对。其中，客户端监测到用户开通使用离线身份验证的方式进行离线支付的权限后，会采集用户录入的标准指纹信息保存至安全环境内。

[38]从上述的内容可以看出，由终端设备采集的待验证指纹信息可以有两种不同情况，即，对待验证指纹信息进行加密，或者不对其进行加密。在不对待验证指纹信息进行加密的情况下，安全环境中预先保存的用于进行身份验证的标准指纹信息是明文形式的标准指纹信息。所以，在签名后的待验证指纹信息通过验签后，可以直接将待验证指纹信息与标准指纹信息进行比对，得到第一比对结果。若对待验证指纹信息进行加密，用户在录入标准指纹信息时，客户端需要对录入的标准指纹信息进行加密，并将密文信息保存至安全环境中，后续进行身份验证时，则可以将待验证指纹的密文信息和标准指纹的密文信息进行比对，得到第一比对结果。

[39]S106：根据所述第一比对结果，对所述用户进行离线身份验证。

[40]在安全环境中，将待验证指纹信息与安全环境中保存的标准指纹信息进行比对后，得到了第一比对结果，若第一比对结果为不同，即，待验证指纹信息与安全环境中保存的标准指纹信息不相同，则用户身份验证失败，若第一比对结果为相同，即，待验证指纹信息与安全环境中保存的标准指纹信息相同，则用户通过身份验证，继续执行业务。

[41]需要说明的是，客户端监测到用户开通了使用离线身份验证的方式进行离线支付的权限后，在安全环境中生成的业务公钥和业务私钥，不仅能够应用于离线的身份验证过程中，还可以应用于在线的身份验证过程中。

[42]具体地，当用户执行在线支付业务时，客户端获取终端设备在在线状态下采集到的用户的第二待验证指纹信息，将第二待验证指纹信息签名后发送至服务器。其中，用户在之前开通使用离线身份验证的方式进行离线支付的权限时，客户端将用户录入的标准指纹信息以发送给服务器保存。同时，也可以将在安全环境内预先生成的业务公钥发给服务器保存。所以，客户端将第二待验证指纹信息通过业务私钥进行数字签名后发送给服务器，服务器可以通过保存的业务公钥对其进行验签，并在验签通过后，将第二待验证指纹信息与服务器中保存的标准指纹信息进行比对，得到第二比对结果，根据第二比对结果，确定用户是否继续执行业务。若第二比对结果为相同，即，第二待验证指纹信息与服务器中保存的标准指纹信息相同，则用户通过身份验证，支付成功。

[43]进一步地，由终端设备采集的第二待验证指纹信息可分为两种不同情况。第一种情

况是需要先对第二待验证指纹信息进行加密，具体地，在用户录入标准指纹信息时，服务器通过加密算法对用户的标准指纹信息进行加密，并将密文信息保存至服务器，同时服务器将此加密算法数据发给客户端。当然，该加密算法数据也可以在用户开通上述权限时，由服务器发送给客户端并进行保存。需要说明的是，本说明书中提到的加密算法数据实际上就是指加密算法，具体可以理解为服务器是以数据的形式将所采用的加密算法给到客户端中的。

[44]那么，在对用户进行身份验证的过程中，客户端在获取终端设备采集的第二待验证指纹信息时，将需要采用同样的加密算法对其进行加密，并将加密后的第二待验证指纹信息发送至服务器。服务器将加密后第二待验证指纹的密文信息与预先保存的标准指纹的密文信息进行比对，若比对通过，用户支付成功。

[45]另一种情况为，不对第二待验证指纹信息加密，在身份验证过程中，直接将客户端获取的第二待验证指纹的明文信息发送至服务器中，与服务器中预先保存的用户标准指纹的明文信息进行比对，根据比对结果确定用户是否继续执行业务，比对结果不相同，则身份验证失败，比对结果相同，身份验证通过，则用户支付成功。

[46]其中，加密算法可以包括：哈希加密算法 Hash、消息摘要算法（Message-Digest Algorithm MD5，MD5）等。本说明书不对具体的所采用的加密算法进行限定。

[47]从上述内容中可以看出，在离线状态下，由于预先在本地的安全环境中保存了用户用于身份验证的标准身份信息，使得用户处于离线状态时，依然可以采集用户的待验证身份信息，通过在本地安全环境内比对用户的待验证身份信息和标准身份信息，完成对用户的离线身份验证，保证了用户在离线状态下依然能够进行身份验证，从而提高用户执行支付业务的效率，给用户带来便利。并且，由于标准身份信息保存在安全环境内，且，用户的待验证身份信息和标准身份信息的比对也是在安全环境内完成，这样能够保证用户的隐私数据不被泄露，进一步保证了用户的信息安全。

[48]为了便于理解，图 2 为本说明书中一种离线身份验证方法的终端设备运行方式示意图。

[49]图 2 为本说明书中一种离线身份验证方法的终端设备运行方式示意图，具体包括以下内容：在用户处于在线情况时，客户端监测用户是否开通离线执行所述业务请求对应业务的权限，若监测到用户没有开通，则弹出提示信息提醒用户授权该权限。在用户开通离线执行业务权限时，客户端在安全环境中生成相应的业务公钥和业务私钥，将其保

存在安全环境中，并将业务公钥发送给服务器保存。与此同时，客户端采集用户录入的标准身份信息，将标准身份信息分别发送至安全环境和服务器保存。

[illegible]

[51]当用户执行在线支付业务时，客户端获取终端设备在在线状态下采集到的用户的第二待验证指纹信息，并将第二待验证指纹信息签名后发送至服务器。其中，由于用户在此之前开通离线执行业务的权限时，客户端已经将用户的标准指纹信息以及安全环境内生成的业务公钥发送给服务器保存，所以由服务器通过业务公钥对其进行验签，并在验签通过后，将第二待验证指纹信息与标准指纹信息进行比对，得到第二比对结果，根据第二比对结果，确定用户是否成功支付。

[52]以上为本说明书的一个或多个实施例提供的离线身份验证方法，基于同样的思路，本说明书还提供了相应的离线身份验证装置，如图3所示。

[illegible]

[54]可选地, 所述获取模块 300 用于, 响应于用户的离线支付请求, 监测所述用户是否开通使用离线身份验证的方式进行离线支付的权限; 若确定所述用户开通所述权限, 则获取所述装置在离线状态下采集到的所述用户的待验证身份信息。

[55]可选地,所述装置还包括:第一发送模块 308,用于响应于所述用户在线状态下针对所述权限发送的权限开通请求,采集所述用户录入的标准身份信息;将所述标准身份信息发送给服务器,以使所述服务器对所述标准身份信息进行保存。

[56]可选地,所述签名模块 302 用于,通过业务私钥,对所述待验证身份信息进行数字签名。

[57]可选地,所述比对模块 304 用于,通过存储在安全环境中的业务公钥,在所述安全环境中对所述签名后的待验证身份信息进行验签。

[58]可选地,所述签名模块 302 用于,对所述待验证身份信息进行加密,得到加密后待验证身份信息;对所述加密后待验证身份信息进行签名,得到签名后的待验证身份信息。

[59]可选地,所述比对模块 304 用于,将所述加密后待验证身份信息和所述安全环境中保存的加密后的标准身份信息进行比对,得到第一比对结果。

[60]可选地,所述第一发送模块 308 还用于,将所述标准身份信息以及预先生成的业务公钥发送给服务器,以使所述服务器对所述标准身份信息和所述业务公钥进行保存;

[61]所述装置还包括:第二发送模块 310,用于响应于所述用户在线状态下发送的支付请求,获取所述装置在线状态下采集到的所述用户的第二待验证身份信息;通过业务私钥,对所述第二待验证身份信息进行签名,得到签名后的第二待验证身份信息;将所述签名后的第二待验证身份信息发送给所述服务器,以使所述服务器通过所述业务公钥对所述签名后的第二待验证身份信息进行验签,并在所述签名后的第二待验证身份信息通过验签后,将所述第二待验证身份信息与所述服务器中保存的标准身份信息进行比对,得到第二比对结果,以根据所述第二比对结果,对所述用户进行在线身份验证。

[62]本说明书还提供了一种计算机可读存储介质,该存储介质存储有计算机程序,计算机程序可用于执行上述图 1 提供的一种离线身份验证方法。

[63]本说明书还提供了图 4 所示的一种对应于图 1 的电子设备的示意结构图。如图 4,在硬件层面,该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器,当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,以实现上述图 1 的离线身份验证方法。当然,除了软件实现方式之外,本说明书并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限于各个逻辑单元,也可以是硬件或逻辑器件。

[64]在 20 世纪 90 年代,对于一个技术的改进可以很明显地区分是硬件上的改进(例如,

对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而,随着技术的发展,当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此,不能说一个方法流程的改进就不能用硬件实体模块来实现。例如,可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array, FPGA))就是这样一种集成电路,其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上,而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且,如今,取代手工地制作集成电路芯片,这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现,它与程序开发撰写时所用的软件编译器相类似,而要编译之前的原始代码也得用特定的编程语言来撰写,此称之为硬件描述语言(Hardware Description Language, HDL),而HDL也并非仅有一种,而是有许多种,如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等,目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚,只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中,就可以很容易得到实现该逻辑方法流程的硬件电路。

[65]控制器可以按任何适当的方式实现,例如,控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit, ASIC)、可编程逻辑控制器和嵌入微控制器的形式,控制器的例子包括但不限于以下微控制器:ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及Silicone Labs C8051F320,存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道,除了以纯计算机可读程序代码方式实现控制器以外,完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件,而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至,可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[66]上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的,计算机例

如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[67]为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[68]本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[69]本说明书是参照根据本说明书实施例的方法、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。

[70]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。

[71]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。

[72]在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[73]内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的

示例。

[74]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

[75]还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括要素的过程、方法、商品或者设备中还存在另外的相同要素。

[76]本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[77]本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[78]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，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

权利要求书

1、一种离线身份验证的方法，所述方法应用于终端设备，所述终端设备中设有安全环境，所述安全环境和所述终端设备中的其他系统环境相互数据隔离，包括：

响应于用户的离线支付请求，获取所述终端设备在离线状态下采集到的所述用户的待验证身份信息；

对所述待验证身份信息进行签名，得到签名后的待验证身份信息；

将所述签名后的待验证身份信息发送到所述安全环境中，以在所述安全环境中，对所述签名后的待验证身份信息进行验签，并在所述签名后的待验证身份信息通过验签后，将所述待验证身份信息与所述安全环境中保存的标准身份信息进行比对，得到第一比对结果；

根据所述第一比对结果，对所述用户进行离线身份验证。

2、如权利要求 1 所述的方法，响应于用户的离线支付请求，获取所述终端设备在离线状态下采集到的所述用户的待验证身份信息，包括：

响应于用户的离线支付请求，监测所述用户是否开通使用离线身份验证的方式进行离线支付的权限；

若确定所述用户开通所述权限，则获取所述终端设备在离线状态下采集到的所述用户的待验证身份信息。

3、如权利要求 2 所述的方法，所述方法还包括：

响应于所述用户在线状态下针对所述权限发送的权限开通请求，采集所述用户录入的标准身份信息；

将所述标准身份信息发送给服务器，以使所述服务器对所述标准身份信息进行保存。

4、如权利要求 1 所述的方法，对所述待验证身份信息进行签名，包括：

通过业务私钥，对所述待验证身份信息进行数字签名。

5、如权利要求 4 所述的方法，对所述签名后的待验证身份信息进行验签，包括：

通过存储在安全环境中的业务公钥，在所述安全环境中对所述签名后的待验证身份信息进行验签。

6、如权利要求 1 所述的方法，对所述待验证身份信息进行签名，得到签名后的待验证身份信息，包括：

对所述待验证身份信息进行加密，得到加密后待验证身份信息；

对所述加密后待验证身份信息进行签名，得到签名后的待验证身份信息；

将所述待验证身份信息与所述安全环境中保存的标准身份信息进行比对，得到第一

比对结果, 包括:

将所述加密后待验证身份信息和所述安全环境中保存的加密后的标准身份信息进行比较, 得到第一比对结果。

7、如权利要求 3 所述的方法, 将所述标准身份信息发送给服务器, 以使所述服务器对所述标准身份信息进行保存, 包括:

将所述标准身份信息以及预先生成的业务公钥发送给服务器, 以使所述服务器对所述标准身份信息和所述业务公钥进行保存;

所述方法还包括:

响应于所述用户在线状态下发送的支付请求, 获取所述终端设备在线状态下采集到的所述用户的第二待验证身份信息;

通过业务私钥, 对所述第二待验证身份信息进行签名, 得到签名后的第二待验证身份信息;

将所述签名后的第二待验证身份信息发送给所述服务器, 以使所述服务器通过所述业务公钥对所述签名后的第二待验证身份信息进行验签, 并在所述签名后的第二待验证身份信息通过验签后, 将所述第二待验证身份信息与所述服务器中保存的标准身份信息进行比对, 得到第二比对结果, 以根据所述第二比对结果, 对所述用户进行在线身份验证。

8、一种离线身份验证装置, 所述装置中设有安全环境, 所述安全环境和所述装置中的其他系统环境相互数据隔离, 包括:

获取模块, 用于响应于用户的离线支付请求, 获取所述装置在离线状态下采集到的所述用户的待验证身份信息;

签名模块, 用于对所述待验证身份信息进行签名, 得到签名后的待验证身份信息;

比对模块, 用于将所述签名后的待验证身份信息发送到所述安全环境中, 以在所述安全环境中, 对所述签名后的待验证身份信息进行验签, 并在所述签名后的待验证身份信息通过验签后, 将所述待验证身份信息与所述安全环境中保存的标准身份信息进行比对, 得到第一比对结果;

验证模块, 用于根据所述第一比对结果, 对所述用户进行离线身份验证。

9、一种计算机可读存储介质, 所述存储介质存储有计算机程序, 所述计算机程序被处理器执行时实现上述权利要求 1~7 任一项所述的方法。