(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114329358 A
(43)申请公布日 2022.04.12

(21)申请号 202111633858.8

(22)申请日 2021.12.28

(71)申请人 深圳市兆珑科技有限公司
地址 518000 广东省深圳市南山区粤海街道科技园社区琼宇路8号金科公司办公楼701

(72)发明人 王志浩

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
代理人 任敏

(51)Int.Cl.
G06F 21/12(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)
G06F 8/61(2018.01)

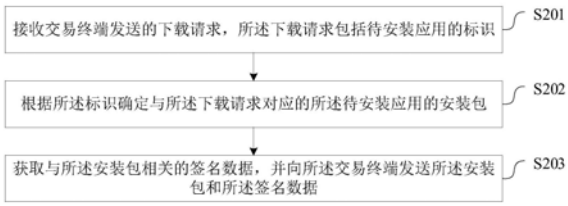
权利要求书2页 说明书11页 附图3页

(54)发明名称

应用签名方法、系统、交易终端及服务平台

(57)摘要

本申请适用于计算机应用技术领域，提供了一种应用签名方法、系统、服务平台及交易终端，该方法包括：交易终端向服务平台发送下载请求，该下载请求包括待安装应用的标识；服务平台接收下载请求，并根据标识确定与下载请求对应的待安装应用的安装包；服务平台获取与安装包关联的签名数据，并向交易终端发送安装包和签名数据；交易终端接收安装包和签名数据，对安装包和签名数据进行打包组合，得到签名应用包，并在对签名应用包验签通过后安装安装包。通过本申请，可以保证各个行业的应用被安全可靠地安装到交易终端上，提高交易终端安装应用的安全性及可靠性。



CN 114329358 A

1.一种应用签名方法,其特征在于,所述方法包括:

交易终端向服务平台发送下载请求,所述下载请求包括待安装应用的标识;

服务平台接收所述下载请求,并根据所述标识确定与所述下载请求对应的所述待安装应用的安装包;

服务平台获取与所述安装包关联的签名数据,并向所述交易终端发送所述安装包和所述签名数据;

交易终端接收所述安装包和所述签名数据,对所述安装包和所述签名数据进行打包组合,得到签名应用包,并在对所述签名应用包验签通过后安装所述安装包。

2.一种应用签名方法,其特征在于,应用于服务平台,所述方法包括:

接收交易终端发送的下载请求,所述下载请求包括待安装应用的标识;

根据所述标识确定与所述下载请求对应的所述待安装应用的安装包;

获取与所述安装包相关的签名数据,并向所述交易终端发送所述安装包和所述签名数据;

其中,所述签名数据和所述安装包用于指示所述交易终端对所述安装包和所述签名数据进行打包组合,得到签名应用包,并在对所述签名应用包验签通过后安装所述安装包。

3.如权利要求2所述的方法,其特征在于,所述下载请求还包括所述交易终端所属的代理商信息;在接收交易终端发送的下载请求之后,所述方法还包括:

根据所述代理商信息,向所述交易终端发送代理商证书;

其中,所述代理商证书为通过厂商私钥对代理商公钥进行签名得到的,所述代理商公钥为所述服务平台针对代理商生成的。

4.如权利要求2或3所述的方法,其特征在于,所述签名数据包括厂商签名文件和代理商签名文件;

在所述获取与所述安装包相关的签名数据之前,所述方法还包括:

基于所述待安装应用的标识,使用厂商私钥对所述待安装应用进行签名,生成与所述待安装应用相关联的所述厂商签名文件;

根据所述下载请求中的代理商信息,使用代理商私钥对所述待安装应用进行签名,生成与所述待安装应用相关联的所述代理商签名文件。

5.一种应用签名方法,其特征在于,应用于交易终端,所述方法包括:

向服务平台发送下载请求,所述下载请求包括待安装应用的标识;

接收所述服务平台基于所述标识发送的与所述下载请求对应的所述待安装包应用的安装包和签名数据;

对所述签名数据和所述安装包进行打包组合,得到签名应用包;

对所述签名应用包进行验签,并在验签通过后,安装所述安装包。

6.如权利要求5所述的方法,其特征在于,所述下载请求还包括所述交易终端所属的代理商信息;

在所述向服务平台发送下载请求之后,所述方法还包括:

接收所述服务平台基于所述代理商信息发送的代理商证书;

其中,所述代理商证书为通过厂商私钥对代理商公钥进行签名得到的,所述代理商公钥为所述服务平台针对代理商生成的。

7.如权利要求6所述的方法，其特征在于，所述签名数据包括厂商签名文件和代理商签名文件；

所述对所述签名应用包进行验签，包括：

使用厂商证书对所述厂商签名文件进行验签，验签通过，则确定所述安装包包含厂商签名；

使用验签通过的所述厂商证书对所述代理商证书进行验签，验签通过，则确定所述代理商证书为基于所述厂商私钥签名得到的；

使用验签通过的所述代理商证书对所述代理商签名文件进行验签，验签通过，则确定所述代理商签名文件为基于代理商私钥签名得到的。

8.一种应用签名系统，其特征在于，所述系统包括服务平台和交易终端；

所述交易终端，用于向服务平台发送下载请求，所述下载请求包括待安装应用的标识；

所述服务平台，用于接收所述下载请求，并根据所述标识确定与所述下载请求对应的所述待安装应用的安装包；

所述服务平台，还用于获取与所述安装包关联的签名数据，并向所述交易终端发送所述安装包和所述签名数据；

所述交易终端，还用于接收所述安装包和所述签名数据，对所述安装包和所述签名数据进行打包组合，得到签名应用包，并在对所述签名应用包验签通过后安装所述安装包。

9.一种服务平台，其特征在于，所述服务平台包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求2至4任一项所述方法的步骤。

10.一种交易终端，其特征在于，所述交易终端包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求5至7任一项所述方法的步骤。

应用签名方法、系统、交易终端及服务平台

技术领域

[0001] 本申请属于计算机应用技术领域，尤其涉及一种应用签名方法、系统、交易终端及电子设备。

背景技术

[0002] 随着互联网的发展，终端设备在各行各业的使用也越来越普及。在支付交易领域，为满足用户不同的需求，交易终端可以具有交易、支付、行业应用以及社交等多种功能，其应用软件的安全可信变得尤为重要，同时对交易终端的安全性管控的要求也越来越高。从而如何保证各个行业的应用被安全可靠地安装到交易终端上是极为重要的。

发明内容

[0003] 本申请实施例提供了一种应用签名方法、系统、服务平台及交易终端，可以保证各个行业的应用被安全可靠地安装到交易终端上，提高交易终端安装应用的安全性及可靠性。

[0004] 第一方面，本申请提供了一种应用签名方法，该方法可以包括：

[0005] 交易终端向服务平台发送下载请求，所述下载请求包括待安装应用的标识；

[0006] 服务平台接收所述下载请求，并根据所述标识确定与所述下载请求对应的所述待安装应用的安装包；

[0007] 服务平台获取与所述安装包关联的签名数据，并向所述交易终端发送所述安装包和所述签名数据；

[0008] 交易终端接收所述安装包和所述签名数据，对所述安装包和所述签名数据进行打包组合，得到签名应用包，并在对所述签名应用包验签通过后安装所述安装包。

[0009] 第二方面，本申请提供了一种应用签名方法，应用于服务平台，该方法可以包括：

[0010] 接收交易终端发送的下载请求，所述下载请求包括待安装应用的标识；

[0011] 根据所述标识确定与所述下载请求对应的所述待安装应用的安装包；

[0012] 获取与所述安装包相关的签名数据，并向所述交易终端发送所述安装包和所述签名数据；

[0013] 其中，所述签名数据和所述安装包用于指示所述交易终端对所述安装包和所述签名数据进行打包组合，得到签名应用包，并在对所述签名应用包验签通过后安装所述安装包。

[0014] 在第二方面的一种可能的实现方式中，所述下载请求还包括所述交易终端所属的代理商信息；在接收交易终端发送的下载请求之后，所述方法还包括：

[0015] 根据所述代理商信息，向所述交易终端发送代理商证书；

[0016] 其中，所述代理商证书为通过厂商私钥对代理商公钥进行签名得到的，所述代理商公钥为所述服务平台针对代理商生成的。

[0017] 在第二方面的一种可能的实现方式中，所述签名数据包括厂商签名文件和代理商

签名文件；

[0018] 在所述获取与所述安装包相关的签名数据之前，所述方法还包括：

[0019] 基于所述待安装应用的标识，使用厂商私钥对所述待安装应用进行签名，生成与所述待安装应用相关联的所述厂商签名文件；

[0020] 根据所述下载请求中的代理商信息，使用代理商私钥对所述待安装应用进行签名，生成与所述待安装应用相关联的所述代理商签名文件。

[0021] 第三方面，本申请提供了一种应用签名方法，应用于交易终端，该方法可以包括：

[0022] 向服务平台发送下载请求，所述下载请求包括待安装应用的标识；

[0023] 接收所述服务平台基于所述标识发送的与所述下载请求对应的所述待安装包应用的安装包和签名数据；

[0024] 对所述签名数据和所述安装包进行打包组合，得到签名应用包；

[0025] 对所述签名应用包进行验签，并在验签通过后，安装所述安装包。

[0026] 在第三方面的一种可能的实现方式中，所述下载请求还包括所述交易终端所属的代理商信息；

[0027] 在所述向服务平台发送下载请求之后，所述方法还包括：

[0028] 接收所述服务平台基于所述代理商信息发送的代理商证书；

[0029] 其中，所述代理商证书为通过厂商私钥对代理商公钥进行签名得到的，所述代理商公钥为所述服务平台针对代理商生成的。

[0030] 在第三方面的一种可能的实现方式中，所述签名数据包括厂商签名文件和代理商签名文件；

[0031] 所述对所述签名应用包进行验签，包括：

[0032] 使用厂商证书对所述厂商签名文件进行验签，验签通过，则确定所述安装包包含厂商签名；

[0033] 使用验签通过的所述厂商证书对所述代理商证书进行验签，验签通过，则确定所述代理商证书为基于所述厂商私钥签名得到的；

[0034] 使用验签通过的所述代理商证书对所述代理商签名文件进行验签，验签通过，则确定所述代理商签名文件为基于代理商私钥签名得到的。

[0035] 第四方面，本申请提供了一种应用签名系统，所述系统包括服务平台和交易终端；

[0036] 所述交易终端，用于向服务平台发送下载请求，所述下载请求包括待安装应用的标识；

[0037] 所述服务平台，用于接收所述下载请求，并根据所述标识确定与所述下载请求对应的所述待安装应用的安装包；

[0038] 所述服务平台，还用于获取与所述安装包关联的签名数据，并向所述交易终端发送所述安装包和所述签名数据；

[0039] 所述交易终端，还用于接收所述安装包和所述签名数据，对所述安装包和所述签名数据进行打包组合，得到签名应用包，并在对所述签名应用包验签通过后安装所述安装包。

[0040] 第五方面，本申请实施例提供了一种服务平台，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实

现第二方面所述的方法。

[0041] 第六方面，本申请实施例提供了一种交易终端，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现第三方面所述的方法。

[0042] 第七方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读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第一方面或第二方面所述的方法。

[0043] 第八方面，本申请实施例提供了一种计算机程序产品，当计算机程序产品在终端设备上运行时，使得终端设备执行上述第一方面或第二方面所述的方法。

[0044] 可以理解的是，上述第二方面至第八方面的有益效果可以参见第一方面中的相关描述，在此不再赘述。

[0045] 本申请与现有技术相比存在的有益效果是：本申请实施例中，交易终端向服务平台发送下载请求，该下载请求包括待安装应用的标识；服务平台接收下载请求，并根据标识确定与下载请求对应的待安装应用的安装包；服务平台获取与安装包关联的签名数据，并向交易终端发送安装包和签名数据；交易终端接收安装包和签名数据，对安装包和签名数据进行打包组合，得到签名应用包，并在对签名应用包验签通过后安装安装包；可以保证各个行业的应用被安全可靠地安装到交易终端上，提高交易终端安装应用的安全性及可靠性；具有较强的易用性与实用性。

附图说明

[0046] 为了更清楚地说明本申请实施例中的技术方案，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，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。

[0047] 图1是本申请实施例提供的系统应用场景的架构示意图；

[0048] 图2是本申请实施例提供的应用签名方法的实现流程示意图；

[0049] 图3是本申请实施例提供的服务平台生成签名数据的界面示意图；

[0050] 图4是本申请实施例提供的软件升级方法的实现流程示意图；

[0051] 图5是本申请实施例提供的软件升级方法的交互流程示意图；

[0052] 图6是本申请实施例提供的服务平台的结构示意图；

[0053] 图7是本申请实施例提供的交易终端的结构示意图。

具体实施方式

[0054] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0055] 应当理解，当在本申请说明书和所附权利要求书中使用时，术语“包括”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、

步骤、操作、元素、组件和/或其集合的存在或添加。

[0056] 还应当理解，在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这些组合。

[0057] 如在本申请说明书和所附权利要求书中所使用的那样，术语“如果”可以依据上下文被解释为“当...时”或“一旦”或“响应于确定”或“响应于检测到”。类似地，短语“如果确定”或“如果检测到[所描述条件或事件]”可以依据上下文被解释为意指“一旦确定”或“响应于确定”或“一旦检测到[所描述条件或事件]”或“响应于检测到[所描述条件或事件]”。

[0058] 另外，在本申请说明书和所附权利要求书的描述中，术语“第一”、“第二”、“第三”等仅用于区分描述，而不能理解为指示或暗示相对重要性。

[0059] 在本申请说明书中描述的参考“一个实施例”或“一些实施例”等意味着在本申请的一个或多个实施例中包括结合该实施例描述的特定特征、结构或特点。由此，在本说明书中的不同之处出现的语句“在一个实施例中”、“在一些实施例中”、“在其他一些实施例中”、“在另外一些实施例中”等不是必然都参考相同的实施例，而是意味着“一个或多个但不是所有的实施例”，除非是以其他方式另外特别强调。术语“包括”、“包含”、“具有”及它们的变形都意味着“包括但不限于”，除非是以其他方式另外特别强调。

[0060] 目前，基于网页Web技术的应用软件提供平台，在提供应用上传、测试、管理、认证以及下载等服务时，需要保证应用软件的安全性，以免应用软件遭受静态或动态的攻击，提高系统交互过程的安全性能。

[0061] 本申请实施例提供了一种应用签名方法，通过服务平台对应用进行在线签名，再由交易终端进一步对数据打包组合及验证，提高交易终端下载并安装应用软件时的安全性及可靠性。

[0062] 请参见图1，图1提供了系统应用场景的架构示意图。如图1所示，该系统可以包括服务平台10和交易终端20。其中，服务平台10可以获取应用开发者上传的应用软件，并对应用软件的类型及版本等属性进行管理；交易终端20可以从服务平台10下载并安装所需的应用软件；通过服务平台10与交易终端20之间的交互，实现对应用软件安全可靠的下载与安装。

[0063] 示例性的，该服务平台可以是PAXSTORE平台，交易终端可以是POS终端。

[0064] 在一些实施例中，交易终端20在接接收到用户输入的下载指令或更新指令后，则可以向服务平台10发送下载请求，该下载请求中包括待安装应用的标识。服务平台10在接收到下载请求后，根据该标识，确定下载请求对应的待安装应用的安装包；同时获取与该安装包关联的签名数据，将签名数据以及安装包发送给交易终端20。交易终端20在接收到安装包和签名数据后，对安装包再次进行组合打包，得到签名应用包，并对签名应用包验签通过后，安装该安装包。保证了应用的安全性以及与交易终端的对应性，可以避免其他终端的恶意下载与安装。

[0065] 基于以上的概述，下面对本申请提供的应用签名方法的流程进行详细说明。

[0066] 如图2所示，本申请实施例提供的应用签名方法的实现流程示意图。该方法执行主体可以是图1所示的系统中的服务平台10。该方法可以包括以下步骤：

[0067] S201，接收交易终端发送的下载请求，所述下载请求包括待安装应用的标识。

[0068] 在一些实施例中，服务平台可以向交易终端推送应用；当服务平台获取到第三方

开发人员上传的新应用或对已上传的应用的版本进行更新后，服务平台会将新应用或新版本的应用推送信息形式通知到交易终端。交易终端需要安装新的应用或者已安装的应用需要更新版本时，可以接收用户通过点击下载控件或升级控件输入的指令，基于该指令，交易终端向服务平台发送下载请求。

[0069] 示例性的，下载请求中可以包括待安装应用的标识，例如该标识可以为该应用的应用名称或者应用包的包名。

[0070] 在一些实施例中，所述下载请求还包括所述交易终端所属的代理商信息；在接收交易终端发送的下载请求之后，所述方法还包括：

[0071] 根据所述代理商信息，向所述交易终端发送代理商证书。

[0072] 其中，所述代理商证书为通过厂商私钥对代理商公钥进行签名得到的，所述代理商公钥为所述服务平台针对代理商生成的。

[0073] 示例性的，代理商为交易终端的拥有者，即代理出售交易终端的一方，服务平台接收代理商的注册。服务平台上注册新的代理商时，会针对该代理商生成应用的签名和验签公私钥。

[0074] 示例性的，服务平台为每一个注册的代理商生成一对公钥和私钥。其中，服务平台使用厂商私钥对代理商的公钥进行签名，组装成代理商证书，并发送到代理商所代理的交易终端；代理商的私钥则保存在服务平台。

[0075] 示例性的，服务平台可以针对不同的厂商的交易终端提供统一的应用签名标准，但是针对不同的厂商可以具有不同的签名数据。服务平台可以接入多个厂商生产的交易终端，可以针对多个厂商实现对应用的在线签名。针对不同的厂商，可以根据厂商上传的公钥和私钥对，获取厂商签名数据，以及获取厂商上传的个人身份识别码的解锁码(PIN(Personal Identification Number)Unlocking Key，PUK)。其中，不同的厂商可以对应不同的签名数据。

[0076] 示例性的，服务平台可以接收应用开发者上传的应用。通过数字证书认证中心(Certficate Authority，CA)服务，服务平台基于应用开发者的公钥生成应用开发者的CA证书。服务平台接收到应用开发者通过开发者中心上传的应用时，服务平台自动校验该应用的(Application package，APK)应用程序包中应用开发者的签名信息，以检查应用开发者的CA证书的有效性和合法性。

[0077] 示例性的，服务平台还可以提供基于应用市场级别的在线签名服务，可以生成应用市场中的应用程序的签名数据，例如该签名数据可以时代码签名证书PVK。服务平台可以向交易终端的客户端应用程序发送该签名数据。其中，该签名数据用于指示交易终端对应用的安装包与该签名数据进行组装。

[0078] S202，根据所述标识确定与所述下载请求对应的所述待安装应用的安装包。

[0079] 在一些实施例中，服务平台可以根据下载请求中的待安装应用的标识确定下载请求所对应的待安装应用的安装包。

[0080] 其中，其中该待安装应用可以为交易终端中没有安装过的应用或者已安装应用对应待更新后的新版本的应用。

[0081] 示例性的，服务平台包含第三方开发者开发的应用或者应用市场中的应用对应的安装包；该安装包可以是新开发的应用的安装包，还可以是已有应用更新版本后的安装包。

服务平台根据下载请求中的标识定位到待安装应用对应的安装包,即应用程序的原始包。

[0082] S203,获取与所述安装包相关的签名数据,并向所述交易终端发送所述安装包和所述签名数据。

[0083] 其中,所述签名数据和所述安装包用于指示所述交易终端对所述安装包和所述签名数据进行打包组合,得到签名应用包,并在对所述签名应用包验签通过后安装所述安装包。

[0084] 在一些实施例中,在该待安装应用上传到服务平台时,服务平台对该应用已生成相关的签名数据;交易终端需要下载该待安装应用时,服务平台基于请求下载的交易终端再生成该待安装应用的签名数据。因此服务平台会获取所有与该待安装应用相关的签名数据,并将所有的签名数据发送给请求下载的交易终端。

[0085] 在一些实施例中,所述签名数据包括厂商签名文件和代理商签名文件;在所述获取与所述安装包相关的签名数据之前,所述方法还包括:

[0086] 基于所述待安装应用的标识,使用厂商私钥对所述待安装应用进行签名,生成与所述待安装应用相关联的所述厂商签名文件;根据所述下载请求中的代理商信息,使用代理商私钥对所述待安装应用进行签名,生成与所述待安装应用相关联的所述代理商签名文件。

[0087] 示例性的,服务平台在接收到上传的应用之后,对该应用的应用包进行审核以及对该应用包中的应用开发者的签名信息进行校验;审核以及校验通过后,服务平台使用之前存储的厂商私钥对该应用包(或安装包)进行签名,生成厂商签名文件S1。该厂商签名文件是为了厂商的机器(交易终端)不能随意安装其他应用,应用必须包含厂商的私钥签名才能被安装,每个交易终端出厂的时候都自带厂商证书,用于验签厂商签名。

[0088] 示例性的,服务平台在接收到下载请求时,确定待安装应用的安装包后,还可以基于下载请求中的代理商信息确定该交易终端所属的代理商。服务平台根据存储的该代理商对应的代理商私钥对应用包进行在线签名,生成代理商签名文件S2。该代理商签名文件可以确保不同代理商之间的应用不能互相安装,若不同代理商使用的都是同一厂商的机器时,如果只有厂商签名文件,则无法保证不同代理商之间的应用不能互相安装。从而可以提高不同代理商之间安装应用的安全性与可靠性。

[0089] 在一些实施例中,服务平添需要维护每个待安装应用的原始安装包(或应用包),以及不同的签名数据,并且可以随时动态的切换签名数据。

[0090] 示例性的,服务平台可以接收网页Web端的管理员通过通用设置输入的自定义签名的签名数据,也可以通过全球Global的签名机制输入的签名数据。

[0091] 其中,基于自定义签名的签名机制,服务平台需要接收管理员上传的公钥加密标准(Public-Key Cryptography Standards12,P12)文件,如图3所示的服务平台的显示界面示意图。如图3所示,服务平台在开启自定义签名的模式后,可以选择签名机制,例如PAX对应的签名服务器等。在该自定义签名模式下,服务平台可以接收签名证书P12文件;由于该P12文件是个人密钥,打开该文件还需要输入密码,所以在该界面上还包括输入P12文件的密码的控件。

[0092] 示例性的,PAX对应的签名服务器在签名时调用的远程API的统一资源定位符(Uniform Resource Locator,URL);其中,签名服务器的公共证书文件可以用于认证签名

服务器，该证书可以选择性上传。

[0093] 示例性的，在服务平台的该显示界面还包括对应各个厂商对应的个人识别码的解锁密码PUK的上传控件，例如Yanghao、PAXBPS以及PAX等厂商所对用的PUK码。服务平台在接收到该厂商对应的PUK码后，验证该PUK码的合法性。

[0094] 需要说明的是，在服务平台批准或允许管理员订阅应用程序之前，需要先基于该服务平台的显示界面的提示控件进行签名服务的配置，服务平台在接收到上述配置信息后，基于该配置信息实现对上传的应用的在线签名机制。

[0095] 另外，服务平台在接收到管理员基于通用设置中输入的更改签名的指令(例如通过图3界面的重置控件接收到的更改指令)后，可以重新生成签名数据，对应的市场程序文件(例如安卓APK(AndroidPackage))则重新签名，异步进行对应用的在线签名。需要说明的是，服务平台针对上传的应用还设置有白名单机制；在更改签名数据时，不会对白名单中的应用进行签名。

[0096] 如图4所示，本申请实施例提供的应用签名方法的实现流程示意图。该方法执行主体可以是图1所示的系统中的交易终端20。该方法中与上述实施例实现原理相同的部分不再赘述，如图4所示该方法可以包括以下步骤：

[0097] S401，向服务平台发送下载请求，所述下载请求包括待安装应用的标识。

[0098] 在一些实施例中，交易终端需要安装新的应用或者已安装的应用需要更新版本时，可以接收用户通过点击下载控件或升级控件输入的指令，基于该指令，交易终端向服务平台发送下载请求。

[0099] 示例性的，交易终端可以提供用户登录的客户端应用程序，交易终端在接收到用户基于该客户端应用程序输入的安装或升级指令后，可以运行该客户端应用程序，对交易终端上的应用进行管理，例如与服务平台进行交互，下载待安装应用等。

[0100] 在一些实施例中，所述下载请求还包括所述交易终端所属的代理商信息；在所述向服务平台发送下载请求之后，所述方法还包括：接收所述服务平台基于所述代理商信息发送的代理商证书。

[0101] 其中，所述代理商证书为通过厂商私钥对代理商公钥进行签名得到的，所述代理商公钥为所述服务平台针对代理商生成的。

[0102] 示例性的，服务平台针对每个代理商生成一对与代理商对应的私钥和公钥，使用厂商私钥对公钥进行签名，得到代理商证书；交易终端接收服务平台发送的该代理商证书。

[0103] S402，接收所述服务平台基于所述标识发送的与所述下载请求对应的所述待安装包应用的安装包和签名数据。

[0104] 在一些实施例中，交易终端可以接收服务平台发送的与该待安装应用相关的所有签名数据。

[0105] S403，对所述签名数据和所述安装包进行打包组合，得到签名应用包。

[0106] S404，对所述签名应用包进行验签，并在验签通过后，安装所述安装包。

[0107] 在一些实施例中，所述签名数据包括厂商签名文件和代理商签名文件；所述对所述签名应用包进行验签，包括：

[0108] 使用厂商证书对所述厂商签名文件进行验签，验签通过，则确定所述安装包包含厂商签名；使用验签通过的所述厂商证书对所述代理商证书进行验签，验签通过，则确定所

述代理商证书为基于所述厂商私钥签名得到的;使用验签通过的所述代理商证书对所述代理商签名文件进行验签,验签通过,则确定所述代理商签名文件为基于代理商私钥签名得到的。

[0109] 示例性的,交易终端下载应用时会获取到服务平台提供的应用的原始包、厂商签名文件S1和代理商签名文件S2,交易终端获取到这三个文件后会将三个文件重新打包,生成一个签名应用包。然后,交易终端通过厂商证书对S1进行验签,确保应用包含厂商私钥的签名。交易终端自带厂商证书,通过厂商证书对代理商证书进行验签,确保代理商证书是厂商私钥签发的。交易终端使用代理商证书对S2进行验签,确保S2是代理商私钥签发的,全部完成验证后,则可以确保该待安装应用可以安装,并且无法安装到其他代理商的交易终端上去。

[0110] 如图5所示,本申请实施例提供的应用签名方法的交互流程示意图,该实现流程的原理与上述实施例相同,在此不再赘述。

[0111] 如图5所示,该交互流程示意图可以包括以下步骤:

[0112] 1、交易终端向服务平台发送下载请求;

[0113] 2、服务平台根据下载请求中的标识确定与下载请求对应的待安装应用的安装包;

[0114] 3、服务平台获取与安装包关联的签名数据;

[0115] 4、服务平台向交易终端发送安装包和签名数据;

[0116] 5、交易终端对安装包和签名数据进行打包组合,得到签名应用包,并在对签名应用包验签通过后安装所述安装包。

[0117] 通过本申请实施例,可以打破原有的交易状态只属于支付应用自身的业务逻辑,而其他应用不可见的束缚,让支付应用的交易状态在应用升级前对管理交易终端的客户端可知。而传统的应用管理平台对应用升级时并不会考虑应用自身是否处于空闲状态;从而可以避免由于升级导致交易数据的丢失。

[0118] 应理解,上述实施例中各步骤的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不应对本申请实施例的实施过程构成任何限定。

[0119] 对应于上文实施例所述的应用签名方法,本申请实施例提供了应用签名装置,为了便于说明,仅说明了与本申请实施例相关的部分。

[0120] 该装置包括:

[0121] 接收单元,用于接收交易终端发送的下载请求,所述下载请求包括待安装应用的标识;

[0122] 处理单元,用于根据所述标识确定与所述下载请求对应的所述待安装应用的安装包;

[0123] 签名单元,用于获取与所述安装包相关的签名数据,并向所述交易终端发送所述安装包和所述签名数据;

[0124] 其中,所述签名数据和所述安装包用于指示所述交易终端对所述安装包和所述签名数据进行打包组合,得到签名应用包,并在对所述签名应用包验签通过后安装所述安装包。

[0125] 对应于上文实施例所述的应用签名方法,本申请实施例提供的应用签名装置,为

了便于说明，仅说明了与本申请实施例相关的部分。

[0126] 该装置包括：

[0127] 发送单元，用于向服务平台发送下载请求，所述下载请求包括待安装应用的标识；

[0128] 接收单元，用于接收所述服务平台基于所述标识发送的与所述下载请求对应的所述待安装包应用的安装包和签名数据；

[0129] 处理单元，用于对所述签名数据和所述安装包进行打包组合，得到签名应用包；

[0130] 验证单元，用于对所述签名应用包进行验签，并在验签通过后，安装所述安装包。

[0131] 需要说明的是，上述装置/单元之间的信息交互、执行过程等内容，由于与本申请方法实施例基于同一构思，其具体功能及带来的技术效果，具体可参见方法实施例部分，此处不再赘述。

[0132] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0133] 本申请实施例还提供了一种应用签名系统，所述系统包括服务平台和交易终端；

[0134] 所述交易终端，用于向服务平台发送下载请求，所述下载请求包括待安装应用的标识；

[0135] 所述服务平台，用于接收所述下载请求，并根据所述标识确定与所述下载请求对应的所述待安装应用的安装包；

[0136] 所述服务平台，还用于获取与所述安装包关联的签名数据，并向所述交易终端发送所述安装包和所述签名数据；

[0137] 所述交易终端，还用于接收所述安装包和所述签名数据，对所述安装包和所述签名数据进行打包组合，得到签名应用包，并在对所述签名应用包验签通过后安装所述安装包。

[0138] 本申请实施例还提供了一种计算机可读存储介质，所述计算机可读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可实现上述各个方法实施例中的步骤。

[0139] 本申请实施例提供了一种计算机程序产品，当计算机程序产品在移动终端上运行时，使得移动终端执行时实现可实现上述各个方法实施例中的步骤。

[0140] 图6为本申请一实施例提供的服务平台6的结构示意图。如图6所示，该实施例的服务平台6包括：至少一个处理器60(图6中仅示出一个)、存储器61以及存储在所述存储器61中并可在所述至少一个处理器60上运行的计算机程序62，所述处理器60执行所述计算机程序62时实现上述实施例中的步骤。

[0141] 所述服务平台6可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。该服务平台6可包括，但不仅限于，处理器60、存储器61。本领域技术人员可以理解，图6

仅仅是服务平台6的举例，并不构成对服务平台6的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如还可以包括输入输出设备、网络接入设备等。

[0142] 所称处理器60可以是中央处理单元(Central Processing Unit，CPU)，该处理器60还可以是其他通用处理器、数字信号处理器(Digital Signal Processor，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现成可编程门阵列(Field-Programmable Gate Array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0143] 所述存储器61在一些实施例中可以是所述服务平台6的内部存储单元，例如服务平台6的硬盘或内存。所述存储器61在另一些实施例中也可以是所述服务平台6的外部存储设备，例如所述服务平台6上配备的插接式硬盘，智能存储卡(Smart Media Card，SMC)，安全数字(Secure Digital，SD)卡，闪存卡(Flash Card)等。进一步地，所述存储器61还可以既包括所述服务平台6的内部存储单元也包括外部存储设备。所述存储器61用于存储操作系统、应用程序、引导装载程序(BootLoader)、数据以及其他程序等，例如所述计算机程序的程序代码等。所述存储器61还可以用于暂时地存储已经输出或者将要输出的数据。

[0144] 图7为本申请一实施例提供的交易终端7的结构示意图。如图7所示，该实施例的交易终端7包括：至少一个处理器70(图7中仅示出一个)、存储器71以及存储在所述存储器71中并可在所述至少一个处理器70上运行的计算机程序72，所述处理器70执行所述计算机程序72时实现上述实施例中的步骤。

[0145] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，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计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质至少可以包括：能够将计算机程序代码携带到拍照装置/终端设备的任何实体或装置、记录介质、计算机存储器、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、电载波信号、电信信号以及软件分发介质。例如U盘、移动硬盘、磁碟或者光盘等。在某些司法管辖区，根据立法和专利实践，计算机可读介质不可以是电载波信号和电信信号。

[0146] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0147] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[0148] 在本申请所提供的实施例中，应该理解到，所揭露的装置/网络设备和方法，可以通过其它的方式实现。例如，以上所描述的装置/网络设备实施例仅仅是示意性的，例如，所

述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0149] 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单元来实现本实施例方案的目的。

[0150] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。


10
20

图1

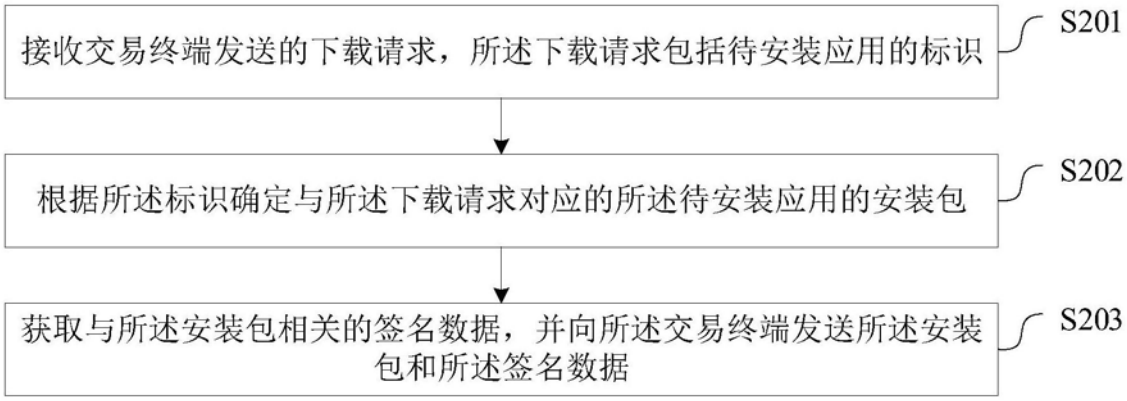

接收交易终端发送的下载请求，所述下载请求包括待安装应用的标识
S201
根据所述标识确定与所述下载请求对应的所述待安装应用的安装包
S202
获取与所述安装包相关的签名数据，并向所述交易终端发送所述安装包和所述签名数据
S203

图2

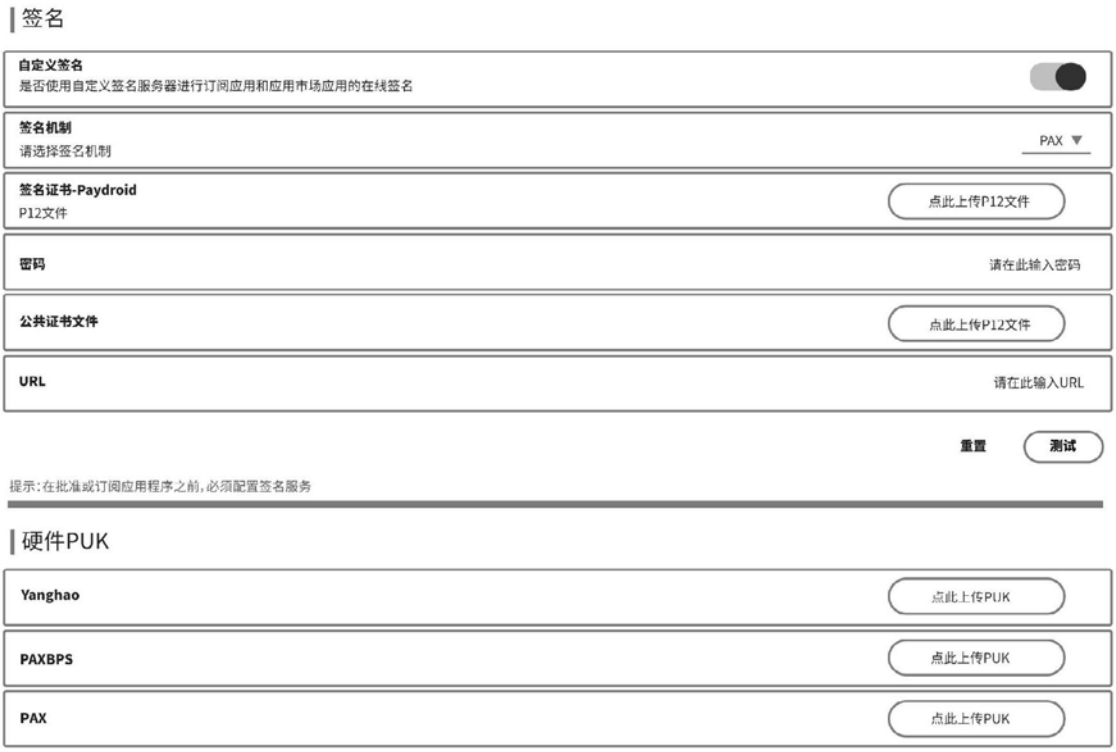

签名
自定义签名
是否使用自定义签名服务器进行订阅应用和应用市场应用的在线签名
签名机制
请选择签名机制
PAX
签名证书-Paydroid
P12文件
点此上传P12文件
密码
请在此输入密码
公共证书文件
点此上传P12文件
URL
请在此输入URL
重置
测试
提示:在批准或订阅应用程序之前,必须配置签名服务
硬件PUK
Yanghao
点此上传PUK
PAXBPS
点此上传PUK
PAX
点此上传PUK

图3

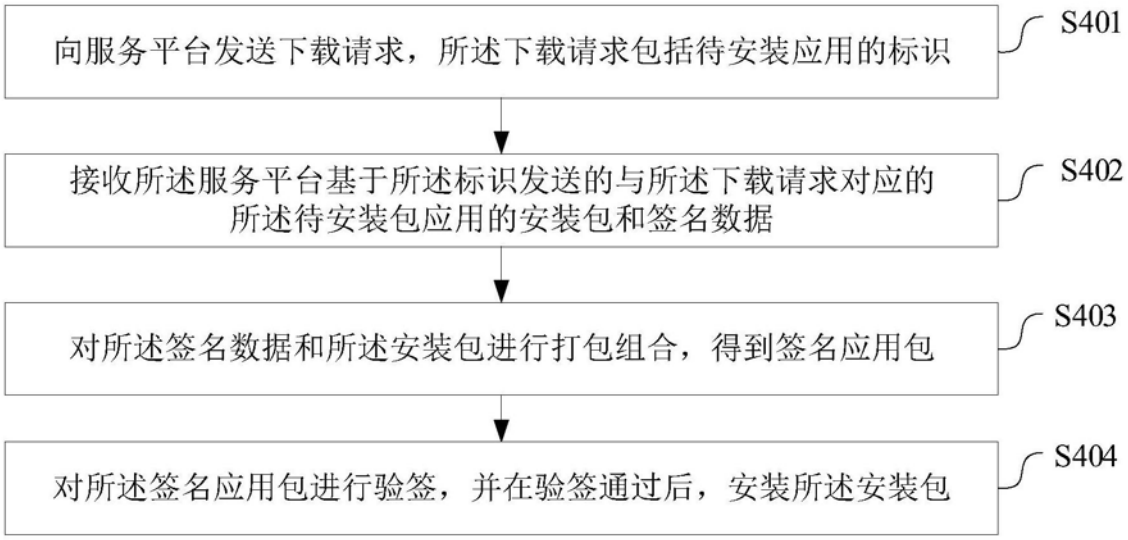

向服务平台发送下载请求，所述下载请求包括待安装应用的标识
S401
接收所述服务平台基于所述标识发送的与所述下载请求对应的所述待安装包应用的安装包和签名数据
S402
对所述签名数据和所述安装包进行打包组合，得到签名应用包
S403
对所述签名应用包进行验签，并在验签通过后，安装所述安装包
S404

图4

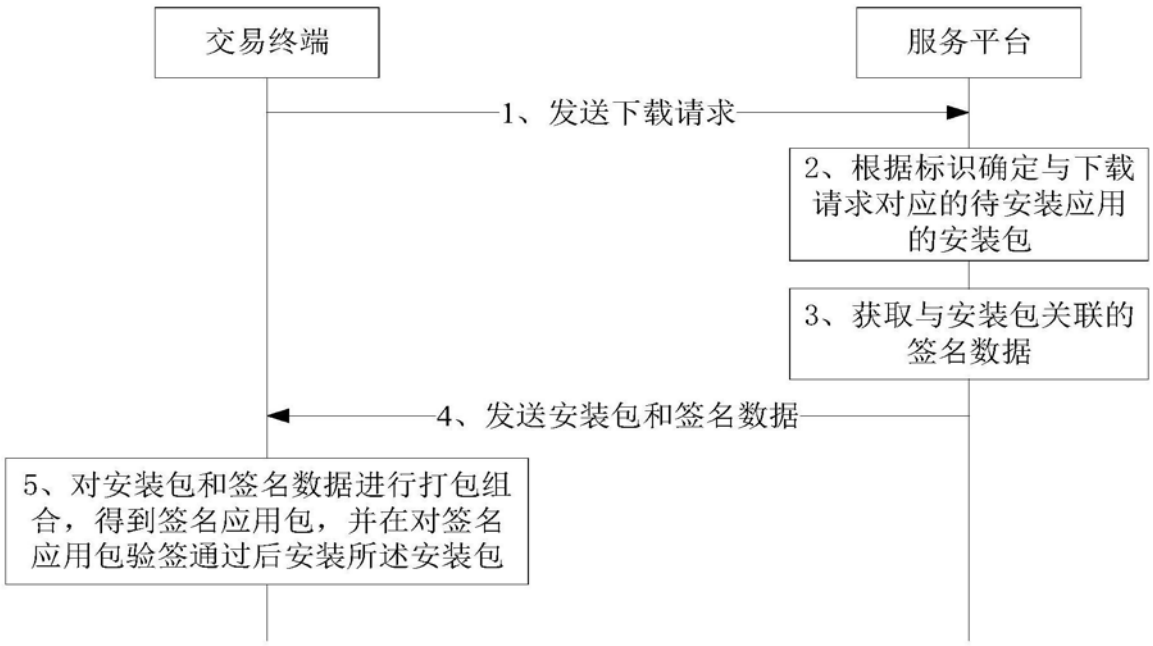

交易终端
服务平台
1、发送下载请求
2、根据标识确定与下载请求对应的待安装应用的安装包
3、获取与安装包关联的签名数据
4、发送安装包和签名数据
5、对安装包和签名数据进行打包组合，得到签名应用包，并在对签名应用包验签通过后安装所述安装包

图5

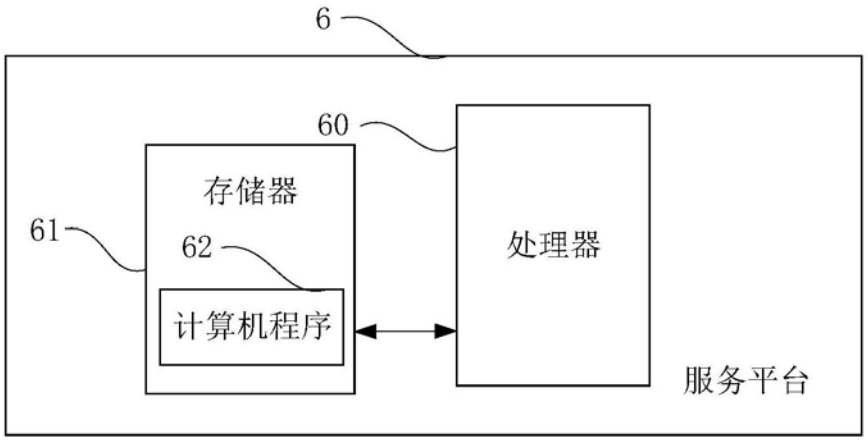


图6

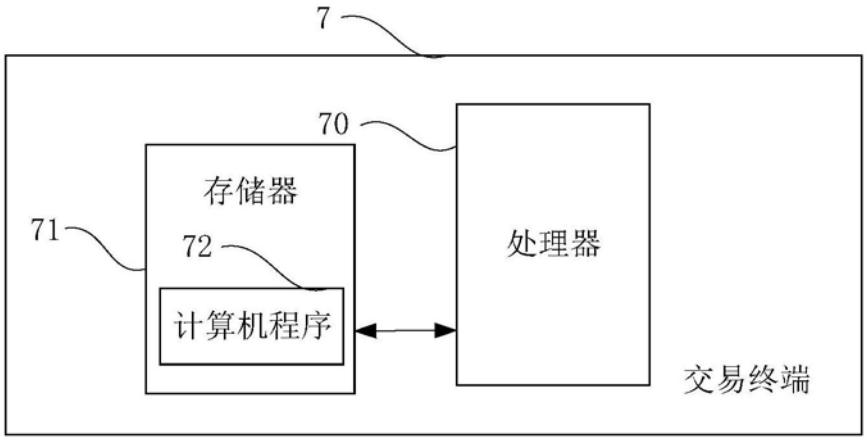


图7