

说明书

5

数据迁移方法、电子设备和存储介质

技术领域

本说明书涉及互联网技术领域，尤其涉及一种数据迁移方法、电子设备和存储介质。

10 背景技术

设备标识 (identifier, ID) 又称为设备指纹，是用来识别设备的唯一 ID。设备 ID 可以用于识别并区分不同的设备，以确保设备的安全性和可靠性。设备 ID 可用于身份验证、风险识别等场景。对于某一服务提供方来说，可以通过本地部署 (on-premise) 模式，将设备 ID 数据部署在该服务提供方的本地私有化服务器，也可以通过中心部署模式，
15 将设备 ID 数据部署在中心服务器上，例如，软件即服务 (software as a service, SaaS) 模式。

当服务提供方从本地部署模式升级为中心部署模式时，如何在升级过程中实现私有化服务器中设备 ID 数据的存量数据的平稳迁移，成为目前一项亟需解决的技术问题。

背景技术部分的内容仅仅是发明人个人所知晓的信息，并不代表上述信息在本公开
20 申请日之前已经进入公共领域，也不代表其可以成为本公开的现有技术。

发明内容

本说明书提供一种数据迁移方法、电子设备和存储介质，能够在服务提供方进行数据部署模式升级的过程中实现设备 ID 数据的存量数据的平稳迁移，以降低升级成本。

25 第一方面，本说明书提供一种数据迁移方法，用于将私有化服务器中存储的设备标识数据迁移至中心服务器，所述中心服务器用于替代所述私有化服务器为客户端提供数据支持，所述方法应用于所述中心服务器，包括：接收请求设备发送的验证请求，所述验证请求用于请求基于目标客户端的目标设备标识进行验证；在未查询到所述目标设备标识的情况下，向所述私有化服务器发送查询请求，所述查询请求用于请求查询所述目

标设备标识；接收所述私有化服务器发送的查询结果，并保存所述目标设备标识；以及向所述请求设备发送响应于所述验证请求的验证结果。

第二方面，本说明书还提供一种电子设备，包括：至少一个存储介质，存储有至少一个指令集，用于进行数据迁移；以及至少一个处理器，同所述至少一个存储介质通信连接，其中，当所述电子设备运行时，所述至少一个处理器读取所述至少一个指令集，并且根据所述至少一个指令集的指示：接收请求设备发送的验证请求，所述验证请求用于请求基于目标客户端的目标设备标识进行验证，在未查询到所述目标设备标识的情况下，向所述私有化服务器发送查询请求，所述查询请求用于请求查询所述目标设备标识，接收所述私有化服务器发送的查询结果，并保存所述目标设备标识，以及向所述请求设备发送响应于所述验证请求的验证结果。

第三方面，本说明书还提供一种计算机可读非暂时性存储介质，其中，所述计算机可读非暂时性存储介质中存储有至少一个指令集，所述至少一个指令集被至少一个处理器执行时，实现如第一方面所述的方法。

由以上技术方案可知，本说明书提供的数据迁移方法、电子设备和存储介质，能够将私有化服务器中存储的设备标识数据迁移至中心服务器。在服务提供方的数据部署模式升级过程中，为了基于目标客户端的目标设备标识对目标客户端进行验证，中心服务器先在本地查询目标设备标识，若未查询到，中心服务器再通过私有化服务器查询目标设备标识，这样，若私有化服务器存储有目标设备标识，中心服务器就能够获取该目标设备标识并将该目标设备标识保存在中心服务器上。通过这种方式，能够在服务提供方的数据部署模式升级过程中，找回原先已保存在私有化服务器的设备标识数据，将私有化服务器处设备标识数据的存量数据迁移至中心服务器，从而确保升级前后的设备标识保持一致，无需为所有设备重新生成设备标识，降低了升级成本。此外，这种方式能够尽可能地防止中心服务器把旧设备误识别成新设备，从而避免对目标用户不必要的打扰，能够提高用户体验。

本说明书提供的数据迁移方法、电子设备和存储介质的其他功能将在以下说明中部分列出。根据描述，以下数字和示例介绍的内容将对那些本领域的普通技术人员显而易见。本说明书提供的数据迁移方法、电子设备和存储介质的创造性方面可以通过实践或使用下面详细示例中所述的方法、装置和组合得到充分解释。

附图说明

为了更清楚地说明本说明书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他的附图。

- 5 图 1 示出了根据本说明书的一些实施例提供的一种数据迁移的应用场景示意图；
图 2 示出了根据本说明书的一些实施例提供的一种电子设备的硬件结构图；
图 3 示出了根据本说明书的一些实施例提供的一种数据迁移方法的流程图；
图 4 示出了根据本说明书的一些实施例提供的一种数据迁移方法的流程图；以及
图 5 示出了根据本说明书的一些实施例提供的一种数据迁移方法的流程图。

10

具体实施方式

- 以下描述提供了本说明书的特定应用场景和要求，目的是使本领域技术人员能够制造和使用本说明书中的内容。对于本领域技术人员来说，对所公开的实施例的各种局部修改是显而易见的，并且在不脱离本说明书的精神和范围的情况下，可以将这里定义的一般原理应用于其他实施例和应用。因此，本说明书不限于所示的实施例，而是与权利
- 15 要求一致的最宽范围。

- 这里使用的术语仅用于描述特定示例实施例的目的，而不是限制性的。比如，除非上下文另有明确说明，这里所使用的，单数形式“一”，“一个”和“该”也可以包括复数形式。当在本说明书中使用时，术语“包括”、“包含”和/或“含有”意思是指所关联的整数，步骤、操作、元素和/或组件存在，但不排除一个或多个其他特征、整数、步骤、操作、元素、组件和/或组的存在或在该系统/方法中可以添加其他特征、整数、步骤、操作、元素、组件和/或组。
- 20

- 考虑到以下描述，本说明书的这些特征和其他特征、以及结构的相关元件的操作和功能、以及部件的组合和制造的经济性可以得到明显提高。参考附图，所有这些形成本说明书的一部分。然而，应该清楚地理解，附图仅用于说明和描述的目的，并不旨在限制本说明书的范围。还应理解，附图未按比例绘制。
- 25

本说明书中使用的流程图示出了根据本说明书中的一些实施例的系统实现的操作。应该清楚地理解，流程图的操作可以不按顺序实现。相反，操作可以以反转顺序或同时实现。此外，可以向流程图添加一个或多个其他操作。可以从流程图中移除一个或多个

操作。

为了方便描述，本说明书对以下描述将会出现的术语进行解释：

1、设备 ID：又称为设备指纹，用于识别和验证设备的唯一标识。设备指纹产品的核心原理，是采集设备诸多的数据（比如设备的硬件数据和软件数据），通过内置的设备 ID 找回算法，生成一个用于标识这个设备的一个唯一 ID，这就是设备 ID。这个设备 ID 是设备指纹产品生成的，不同服务提供方所生成的设备 ID 不同。这个设备 ID 可以用于区分不同的设备，以确保设备的安全性和可靠性。利用设备 ID，可以实现对客户端上的风险环境识别、风险检测以及行为风险分析等，例如，服务提供方通常可以基于设备 ID 来识别当前客户端是否是用户账号的常用设备，以达到验证用户所使用的设备的目的。

在一些实施例中，在用户通过客户端安装的 APP 注册用户账号的过程中，APP 对应的服务器会采集所述客户端的设备数据，设备数据包括多个软件参数和多个硬件参数，并通过特定的工具将所述设备数据处理后得到一个可以唯一标识所述客户端的设备 ID。所述软件参数例如可以包括 APP 名称、APP 版本、APP 安装时间、设备安装的系统版本等。所述硬件参数例如可以包括设备制造商、设备品牌、设备类型及型号、设备内存及存储大小、基带信息、屏幕分辨率、媒体访问控制（media access control address, MAC）地址、国际移动设备识别码（international mobile equipment identity, IMEI）、国际移动用户识别码（international mobile subscriber identity, IMSI）、网络制式、基带编号等。另外，所述设备数据还可以包括其他参数，例如设备序列号、WiFi MAC、运营商名称、开机时间、用户自定义的设备名称等。APP 对应的服务器可以给每一个使用所述 APP 的设备赋予一个能够唯一标识所述设备的设备 ID。APP 对应的服务器可以存储多个用户账号和多个设备 ID 之间的对应关系。后续用户在所述客户端或者其他设备上通过所述用户账号再次使用所述 APP 时，APP 对应的服务器就可以基于所述用户账号对应的设备 ID 判断这次使用所述 APP 的设备是否是所述用户账号的常用设备。上述特定的工具比如设备指纹软件开发工具包（software development kit, SDK）。

2、设备令牌（token）：是一种用于标识用户身份的令牌。通常，当用户在客户端上第一次登录 APP 时，APP 对应的服务器会为该用户生成一个 token，并将该 token 返回给客户端，以后客户端只需要带上这个 token 向服务器请求数据即可，无需带上用户名和密码。

APP 对应的服务器会将设备 token 与设备 ID 进行关联，通过设备 token 可以找到设

备 ID。设备 token 与设备 ID 之间是多对一的关系。此外，设备 token 是临时的，存在有效期。若设备 token 失效了，APP 对应的服务器会再次为用户生成新的设备 token。

3、设备风险标签：用于表示设备是否具有某些类别的风险，例如，设备是否具有刷机、改机、装模拟器、越狱、劫持注入等风险。

5 设备 ID 与设备风险标签之间具备关联关系，通过设备 ID 可以确定该设备 ID 所对应的设备的设备风险标签，从而可以利用该设备风险标签对该设备上的相关操作进行风险识别。应理解，设备 ID 不会随着设备装模拟器、装虚拟机、刷机、改机等操作而改变。

3、本地部署（on-premise）：指的是在服务提供方自有的物理设施内部署和管理 IT
10 基础设施，可能包括数据中心、服务器、网络硬件、存储设备等等。对于本地部署，服务提供方可以享有对所有硬件、软件和数据完全控制权，所有数据都存储在服务提供方自有的硬件中，因此，本地部署可以提供更高的数据安全性和隐私保护。

4、SaaS：是一种通过互联网提供软件应用的服务模式。将软件应用程序作为服务通过互联网提供给用户。在 SaaS 模式下，软件应用程序托管在 SaaS 的服务提供商的服务器
15 上，用户通过互联网访问并使用程序。用户不再需要购买和维护软件的整个基础架构，而是通过订阅的方式获得对云端软件的访问权限。SaaS 提供商负责软件的部署、维护和安全性等方面的工作，用户只需要通过网络浏览器或专用应用程序就可以方便地访问和使用软件。SaaS 模式具备灵活性、可扩展性和成本低等优势。

在对本说明书具体实施例说明之前，先对本说明书的应用场景进行介绍。

20 用户在客户端上使用安全性要求较高的 APP 时，例如用户登录支付类 APP，或者用户在 APP 发起支付时，可能会触发 APP 对用户所使用的客户端进行验证。一般情况下，APP 对应的服务器会采用设备 ID 对客户端进行验证，因此，设备 ID 的获取至关重要。目前，服务器端的数据存储存在两种数据部署方式。一种是本地部署模式，即将设备 ID 数据保存在服务提供方的本地的私有化服务器中，由服务提供方享有对设备 ID 数
25 据的完全控制权。另一种是中心部署模式，即将设备 ID 数据保存在 SaaS 模式的服务提供商的服务器（中心服务器）中。当服务提供方将数据存储方式从本地部署模式升级为中心部署模式时，为了便于获取设备 ID 数据，需要将设备 ID 数据从本地私有化服务器中迁移至中心服务器中，即将设备 ID 数据部署在私有化服务器升级为将设备 ID 数据部署在中心服务器，由中心服务器替代私有化服务器为客户端提供数据支持。

在上述场景中，若直接使用中心服务器替代私有化服务器，需要中心服务器为所有客户端重新生成新的设备 ID，这样会加重中心服务器的处理负担，造成较高的升级成本。

有鉴于此，本说明书提供一种数据迁移方法、电子设备和存储介质，可以应用于将私有化服务器中已保存的设备 ID 数据迁移至中心服务器的升级场景中。其中，中心服务器可以在未查询到目标客户端的目标设备 ID 的情况下，通过私有化服务器查询目标设备 ID，这样，若私有化服务器存储有目标设备 ID，中心服务器就能够获取该目标设备 ID 并将该目标设备 ID 保存在中心服务器上。通过这种方式，能够在服务提供方的数据部署模式升级过程中，找回原先已保存在私有化服务器的设备 ID 数据，将私有化服务器处设备 ID 数据的存量数据迁移至中心服务器，从而确保升级前后的设备 ID 保持一致，无需为所有设备重新生成设备 ID，降低了升级成本。此外，这种方式能够尽可能地防止中心服务器把旧设备误识别成新设备，从而避免对目标用户不必要的打扰，能够提高用户体验。

图 1 示出了根据本说明书的一些实施例提供的一种数据迁移的应用场景 001 的应用场景示意图。如图 1 所示，所述应用场景可以包括目标用户 100、目标客户端 200 以及服务端 300。其中，服务端 300 可以包括目标服务提供方的第一服务器 301、目标服务提供方的第二服务器 302、中心服务器 303 以及风控系统 304。

其中，目标用户 100 可以通过目标客户端 200 执行相关事件。例如，目标客户端 200 安装有一个或多个 APP，所述一个或多个 APP 能够为用户提供执行相关事件的能力。所述 APP 包括但不限于：网页浏览器类 APP、搜索类 APP、聊天类 APP、购物类 APP、服务类 APP、视频类 APP、理财类 APP、支付类 APP 等等。

目标客户端 200 可以安装有目标 APP，该目标 APP 由目标服务提供方提供目标服务。目标客户端 200 通过目标 APP 向目标用户 100 呈现交互界面，以便目标用户 100 通过该交互界面执行一些事件。例如，上述目标服务提供方为支付服务提供方，目标 APP 为电子钱包 APP，响应于目标用户 100 的操作，目标客户端 200 可以通过电子钱包 APP 为目标用户 100 呈现登录界面，目标用户 100 可以在登录界面完成登录，或者目标客户端 200 可以通过电子钱包 APP 向目标用户 100 呈现支付界面，目标用户 100 可以在支付界面完成支付事件等。

目标客户端 200 可以包括移动设备、平板电脑、笔记本电脑、机动车辆的内置设备

或类似内容，或其任意组合。在一些实施例中，所述移动设备可包括智能家居设备、智能移动设备、虚拟现实设备、增强现实设备或类似设备，或其任意组合。在一些实施例中，所述智能家居装置可包括智能电视、台式电脑等，或任意组合。在一些实施例中，所述智能移动设备可包括智能手机、个人数字辅助、游戏设备、导航设备等，或其任意组合。在一些实施例中，所述虚拟现实设备或增强现实设备可能包括虚拟现实头盔、虚拟现实眼镜、虚拟现实补丁、增强现实头盔、增强现实眼镜、增强现实补丁或类似内容，或其中的任何组合。例如，所述虚拟现实设备或所述增强现实设备可能包括 AR 眼镜、头戴式显示器、VR 等。在一些实施例中，所述机动车中的内置装置可包括车载计算机、车载电视等。在一些实施例中，目标客户端 200 可以是具有定位技术的设备，用于定位目标客户端 200 的位置。

如图 1 所示，目标客户端 200 可以与服务端 300 进行通信连接。在一些实施例中，服务端 300 还可以与其他客户端进行通信连接。本说明书对该场景中客户端的数量不作限定。在一些实施例中，目标客户端 200 可以通过网络与服务端 300 交互，以接收或发送消息等。

服务端 300 可以包括提供各种服务的服务器，例如，服务端 300 包括对目标客户端 200 上的 APP 显示的页面提供支持的后台服务器。具体地，服务端 300 包括目标服务提供方的第一服务器 301、目标服务提供方的第二服务器 302、中心服务器 303 以及风控系统 304。

其中，第一服务器 301 是目标服务提供方的服务器，用于对目标客户端 200 上所安装的目标 APP 显示的页面提供支持，并在目标用户 100 使用目标 APP 的过程中为目标用户 100 提供目标服务。第一服务器 301 可以与目标客户端 200 通信连接，在目标用户 100 使用目标服务的过程中，目标客户端 200 可以与第一服务器 301 进行通信以便交换或者传递数据。例如，在目标客户端 200 检测到目标用户 100 在目标 APP 中执行某些操作（例如登录目标 APP，或者在交互页面中执行支付操作）时，目标客户端 200 将用户数据和交易数据发送给第一服务器 301。第一服务器 301 会将收到的用户数据和交易数据发送给风控系统 304 进行风险咨询，获得风控系统 304 返回的风险结果。根据风险结果，第一服务器 301 可以确定是否需要通过目标客户端 200 对目标用户 100 进行身份认证，或者是否需要对本次操作进行拦截，从而确保本次操作的安全性。

第二服务器 302 也称为私有化服务器 302，也是目标服务提供方的服务器，可以部署在目标服务提供方的本地，因此第二服务器 302 还可以称为目标服务提供方的本地服

务器。第二服务器 302 用于存储目标服务提供方的数据，由目标服务提供方独立管理控制。通过第二服务器 302 存储数据的模式称为本地部署模式。在本说明书中，第二服务器 302 用于存储目标服务提供方的设备 ID 数据。为了便于与中心服务器 303 区分，后续将第二服务器 302 称为私有化服务器 302。

5 中心服务器 303 部署在云端，也可以用于存储数据，目标服务提供方通过互联网即可获取存储在中心服务器 303 的数据，无需维护本地软硬件设施。通过中心服务器 303 存储数据的模式称为中心部署模式。在本说明书中，中心服务器 303 用于替代私有化服务器 302 存储目标服务提供方的设备 ID 数据。目标客户端 200 可以与中心服务器 303 通信连接，在目标用户 100 使用目标服务的过程中，目标客户端 200 可以与中心服务器
10 303 进行通信以便交换或者传递数据。例如，在目标客户端 200 检测到目标用户 100 在目标 APP 中执行某些操作（例如登录目标 APP，或者在交互页面中执行支付操作）时，目标客户端 200 可以采集自身的设备数据，并将设备数据发送给中心服务器 303，以便中心服务器 303 根据设备数据查询目标客户端 200 的设备 ID，基于设备 ID 进行设备验证，并向目标客户端 200 返回验证结果。

15 本说明书的中心服务器 303 与私有化服务器 302 通信连接，能够获取私有化服务器 302 的设备 ID 数据。此外，中心服务器 303 还内置有设备 ID 找回算法，能够基于目标客户端 200 的硬件信息和软件信息，生成一个用于标识目标客户端 200 的设备 ID。

 本说明书提供的数据迁移方法中的中心服务器 303 的相关动作可以在中心服务器 303 上执行。此时，中心服务器 303 可以存储有执行本说明书描述的数据迁移方法中的
20 中心服务器 303 对应的数据或指令，并可以执行或用于执行所述数据或指令。在一些实施例中，中心服务器 303 可以包括具有数据信息处理功能的硬件设备和驱动该硬件设备工作所需必要的程序。

 风控系统 304 可以部署有风控策略，用于对目标用户 100 在使用目标服务过程中产生的目标事件进行风险检测。风控系统 304 与第一服务器 301 和中心服务器 303 通信连
25 接，能够进行数据传递。具体地，风控系统 304 可以接收第一服务器 301 发送的用户数据和交易数据，并接收中心服务器 303 发送的设备数据（例如，设备 ID 和设备风险标签等），风控系统 304 可以结合用户数据、交易数据和设备数据，基于风控策略判断当前操作是否存在风险，从而得到风险结果。该风险结果例如可以是当前操作的风险等级。风控系统 304 向第一服务器 301 返回风险结果。

上述风控策略可以包括但不限于：由目标服务提供方预先训练得到的风控模型，由目标服务提供方基于历史经验积累的风控规则等。上述目标事件可以包括但不限于：目标用户 100 在目标客户端 200 的目标 APP 上登录，目标用户 100 在目标客户端 200 的目标 APP 上支付等。

5 图 1 仅示出了一个目标服务提供方的第一服务器 301 和目标服务提供方的私有化服务器 302。但应理解，上述中心服务器 303 还可以连接有其他服务提供方的第一服务器 301 和私有化服务器 302，即中心服务器 303 可以同时为多个不同的服务提供方提供数据支持，本说明书对此不作限定。

应该理解，图 1 中的目标客户端 200、服务端 300 和网络 400 的数目仅仅是示意性的。
10 根据实现需要，可以具有任意数目的目标客户端 200、服务端 300 和网络 400。

图 2 示出了根据本说明书的一些实施例提供的一种电子设备 600 的硬件结构图。电子设备 600 可以执行本说明书描述的数据迁移方法。所述数据迁移方法在本说明书中的其他部分介绍。当所述数据迁移方法中的中心服务器 303 相关的动作在中心服务器 303 上执行时，电子设备 600 可以是中心服务器 303。

15 如图 2 所示，电子设备 600 可以包括至少一个存储介质 630 和至少一个处理器 620。在一些实施例中，电子设备 600 还可以包括通信端口 650 和内部通信总线 610。同时，电子设备 600 还可以包括 I/O 组件 660。

内部通信总线 610 可以连接不同的系统组件，包括存储介质 630、处理器 620 和通信端口 650。

20 I/O 组件 660 支持电子设备 600 和其他组件之间的输入/输出。

通信端口 650 用于电子设备 600 同外界的数据通信，比如，通信端口 650 可以用于电子设备 600 同网络 400 之间的数据通信。通信端口 650 可以是有线通信端口也可以是无线通信端口。

存储介质 630 可以包括数据存储装置。所述数据存储装置可以是非暂时性存储介质，
25 也可以是暂时性存储介质。比如，所述数据存储装置可以包括磁盘 632、只读存储介质（ROM）634 或随机存取存储介质（RAM）636 中的一种或多种。存储介质 630 还包括存储在所述数据存储装置中的至少一个指令集。所述指令集可以是计算机程序代码。当电子设备 600 为中心服务器 303 时，所述计算机程序代码可以包括执行本说明书提供的数据迁移方法中的中心服务器 303 对应的程序、例程、对象、组件、数据结构、过程、

模块等等。

处理器 620 可以同存储介质 630 以及通信端口 650 通过内部通信总线 610 通信连接。处理器 620 用以执行上述至少一个指令集。当电子设备 600 作为中心服务器 303 运行时,处理器 620 可以读取所述至少一个指令集,并且根据所述至少一个指令集的指示,
5 执行本说明书提供的数据迁移方法。处理器 620 可以执行该方法包含的中心服务器 303 的所有步骤。

处理器 620 可以是一个或多个处理器的形式,在一些实施例中,处理器 620 可以包括一个或多个硬件处理器,例如微控制器,微处理器,精简指令集计算机(RISC),专用集成电路(ASIC),特定于应用的指令集处理器(ASIP),中心处理单元(CPU),图
10 形处理单元(GPU),物理处理单元(PPU),微控制器单元,数字信号处理器(DSP),现场可编程门阵列(FPGA),高级 RISC 机器(ARM),可编程逻辑器件(PLD),能够执行一个或多个功能的任何电路或处理器等,或其任何组合。

仅仅为了说明问题,在本说明书中电子设备 600 中仅描述了一个处理器 620。然而,应当注意,本说明书中电子设备 600 还可以包括多个处理器,因此,本说明书中披露的
15 操作和/或方法步骤可以如本说明书所述的由一个处理器执行,也可以由多个处理器联合执行。例如,如果在本说明书中电子设备 600 的处理器 620 执行步骤 A 和步骤 B,则应该理解,步骤 A 和步骤 B 也可以由两个不同处理器 620 联合或分开执行(例如,第一处理器执行步骤 A,第二处理器执行步骤 B,或者第一处理器和第二处理器共同执行步骤 A 和 B)。

20 为了便于理解,下面以交互的方式描述本说明书的数据迁移方法。

图 3 示出了根据本说明书的一些实施例提供的一种数据迁移方法 P100 的流程图。如前所述,电子设备 600 可以执行本说明书所述的数据迁移方法 P100 中的中心服务器 303 对应的步骤。具体地,处理器 620 可以读取存储在其本地存储介质中的指令集,然后根据所述指令集的规定,执行本说明书所述的数据迁移方法 P100 中的中心服务器 303
25 对应的步骤。

如图 3 所示,所述方法 P100 可以包括:

S101: 请求设备向中心服务器 303 发送验证请求,所述验证请求用于请求基于目标客户端 200 的目标设备 ID 进行验证。

其中，目标客户端 200 是目标用户 100 所使用的客户端设备，目标客户端 200 上安装有目标 APP。若目标用户 100 在使用目标 APP 的过程中，请求目标 APP 的某项服务，例如登录目标 APP、或者请求目标 APP 的支付服务，目标客户端 200 可以触发请求设备发起验证，即向中心服务器 303 发送验证请求。验证请求可以是对目标客户端 200 进行的设备验证。所述设备验证可以是基于目标客户端 200 的目标设备 ID 所进行的验证，以验证目标客户端 200 是否为允许的设备。

所述请求设备例如可以为目标客户端 200 或者风控系统 304。

在一种可能的实现方式中，所述请求设备为目标客户端 200，所述验证请求为设备身份验证请求。若目标用户 100 通过目标客户端 200 在目标 APP 中执行某些操作（例如登录目标 APP，或者在交互页面中执行支付操作），响应于目标用户 100 的操作，目标客户端 200 可以向中心服务器 303 发送验证请求，请求对目标客户端 200 进行验证。

在另一种可能的实现方式中，所述请求设备为风控系统 304，所述验证请求为设备风险验证请求。若目标客户端 200 可以向第一服务器 301 请求目标服务，目标客户端 200 会将用户数据和交易数据发送给第一服务器 301，第一服务器 301 会将收到的用户数据和交易数据发送给风控系统 304 进行风险咨询。响应于第一服务器 301 的风险咨询，风控系统 304 可以向中心服务器 303 发送设备风险验证请求，请求获取目标客户端 200 的设备数据（例如，目标设备 ID 和设备风险标签等），以便于结合用户数据、交易数据和设备数据得到风险咨询结果。

在一些实施例中，所述验证请求携带目标客户端 200 的设备令牌。

在一些实施例中，所述验证请求还携带目标客户端 200 的硬件信息以及目标客户端 200 的软件信息。

S102：中心服务器 303 基于验证请求，查询目标设备 ID。

中心服务器 303 可以先查询自身是否保存有目标设备 ID。在一些实施例中，中心服务器 303 可以基于目标客户端 200 的设备令牌进行查询。由于设备令牌与设备 ID 具有关联关系，在目标客户端 200 的目标设备 ID 存在的情况下，通过目标客户端 200 的设备令牌，即可查询到目标客户端 200 的目标设备 ID。

若中心服务器 303 查询到目标设备 ID，中心服务器 303 可以直接利用查询到的目标设备 ID 进行验证，并向请求设备返回验证结果，本流程结束。这种情况说明目标设备 ID 之前已经从私有化服务器 302 迁移至了中心服务器 303，或者目标设备 ID 就是中

心服务器 303 生成的，不存在于私有化服务器 302 中，那么无需再到私有化服务器 302 查询。若中心服务器 303 未查询到目标设备 ID，则继续执行后续步骤。

S103：在未查询到目标设备 ID 的情况下，中心服务器 303 向私有化服务器 302 发送查询请求，所述查询请求用于请求查询所述目标设备 ID。

5 中心服务器 303 确定未查询到与所述设备令牌关联的所述目标设备 ID 时，中心服务器 303 可以向私有化服务器 302 发送所述查询请求，以请求私有化服务器 302 查询目标客户端 200 的目标设备 ID。所述查询请求中携带有目标客户端 200 的所述设备令牌。

S104：私有化服务器 302 基于查询请求，查询目标设备 ID。

10 在一些实施例中，私有化服务器 302 可以基于查询请求中携带的目标客户端 200 的设备令牌进行查询。

S105：私有化服务器 302 向中心服务器 303 发送查询结果。

S106：中心服务器 303 接收查询结果，并保存所述目标设备 ID。

15 在一些实施例中，私有化服务器 302 查询到了目标设备 ID，则所述查询结果中携带有所述目标设备 ID。中心服务器 303 可以保存所述目标设备 ID，并将所述目标设备 ID 与目标客户端 200 的所述设备令牌关联。

20 上述情况说明私有化服务器 302 存储有目标客户端 200 的目标设备 ID，即目标客户端 200 为旧设备。通过上述方式，能够将目标客户端 200 的目标设备 ID 从私有化服务器 302 找回并迁移至中心服务器 303。由于中心服务器 303 将目标设备 ID 与目标客户端 200 的设备令牌进行了关联，若后续请求设备再次发起对目标客户端 200 的验证，中心服务器 303 可以基于自身保存的关联关系查找到目标设备 ID，无需私有化服务器 302 再提供服务。

25 在一些实施例中，私有化服务器 302 未查询到目标设备 ID，则所述查询结果中没有携带有所述目标设备 ID。此时，目标客户端 200 的目标设备 ID 既不存在于中心服务器 303 中，也不存在于私有化服务器 302 中，代表目标客户端 200 可能是新的设备，中心服务器 303 需生成新设备的设备 ID。中心服务器 303 可以基于所述目标客户端 200 的所述硬件信息以及所述软件信息生成所述目标设备 ID，并将所述目标设备 ID 与目标客户端 200 的所述设备令牌关联。

30 上述情况说明中心服务器 303 和私有化服务器 302 均没有存储目标客户端 200 的目标设备 ID，即目标客户端 200 为新设备。通过上述方式，能够为目标客户端 200 生成新的设备 ID。中心服务器 303 保存该新生成的目标设备 ID，并将新生成的目标设备 ID 与

目标客户端 200 的设备令牌进行了关联,若后续请求设备再次发起对目标客户端 200 的验证,中心服务器 303 可以基于自身保存的关联关系查找到该新生成的目标设备 ID,无需私有化服务器 302 再提供服务。

5 应理解,每次设备上线,即目标用户 100 在目标客户端 200 上登录目标 APP,都可以触发本说明书的方法 P100 的验证流程。不同的目标用户 100 在不同的目标客户端 200 上的登录目标 APP 操作,可以使得不同的目标客户端 200 的目标设备 ID 均保存在中心服务器 303 上,从而实现验证过程中的设备 ID 数据的迁移。

还应理解,在实际应用中,本说明书的数据迁移方法会在预设期限内执行,即在预设期限内(例如,1 年、或者 2 年),私有化服务器 302 会通过中心服务器 303 提供数据
10 支持,中心服务器 303 会在自身未查询到目标设备 ID 的情况下向私有化服务器 303 查询,从而确保预设期限内上线的目标客户端 200 的目标设备 ID 迁移至中心服务器 303。在预设期限之后,认为已经完成了数据迁移,私有化服务器 302 不再提供数据支持服务,只由中心服务器 303 提供数据支持服务。若此时中心服务器 303 接收到验证请求,并且基于该验证请求未查询到目标客户端 200 的目标设备 ID,中心服务器 303 可以直接为
15 该目标客户端 200 生成目标设备 ID,并将新生成的目标设备 ID 与目标客户端 200 的设备令牌绑定。

S107: 中心服务器 303 向请求设备发送响应于所述验证请求的验证结果。

在一些实施例中,所述请求设备为目标客户端 200,所述验证请求为设备身份验证请求。图 4 示出了这种场景下的数据迁移方法的流程图。其中,目标客户端 200 安装有
20 目标 APP 和安全 SDK,安全 SDK 用于采集设备信息并发起验证。如图 4 所示,在 S101 之前,方法 P100 还包括:

S111: 当目标用户登录目标 APP 时,目标 APP 向安全 SDK 发送初始化消息。

S112: 响应于接收到的初始化消息,安全 SDK 获取目标客户端 200 的设备信息,这里的设备信息包括目标客户端 200 的设备令牌、目标客户端 200 的设备硬件信息以及
25 目标客户端 200 的设备软件信息。

S101 具体可以为:安全 SDK 向中心服务器 303 发送设备身份验证请求,该设备身份验证请求中可以包括目标客户端 200 的设备令牌、目标客户端 200 的设备硬件信息以及目标客户端 200 的设备软件信息。

在 S106 之后,方法 P100 还包括:

S113: 中心服务器 303 基于所述目标设备 ID 对目标客户端 200 进行设备身份验证, 生成设备身份验证结果。

S107 具体可以为: 中心服务器 303 向目标客户端 200 的安全 SDK 发送设备身份验证结果。

5 S114: 安全 SDK 基于设备身份验证结果, 向目标 APP 返回目标客户端 200 的设备令牌。

应理解, 上述安全 SDK 为能够连接到中心服务器 303 的新版本 SDK, 在目标客户端 200 集成了新版本的安全 SDK 的情况下, 可以按照上述方法由中心服务器 303 进行目标客户端 200 的设备身份验证, 同时将目标设备 ID 保存至中心服务器 303。若目标
10 客户端 200 未集成新版本的安全 SDK, 即目标客户端 200 安装的是旧版本的安全 SDK, 那么只能通过私有化服务器 302 进行目标客户端 200 的设备身份验证, 且无法进行目标设备 ID 的数据迁移。

在一些实施例中, 所述请求设备包括风控系统 304, 所述验证请求为设备风险验证请求。图 5 示出了这种场景下的数据迁移方法的流程图。如图 5 所示, 在 S101 之前,
15 方法 P100 还包括:

S121: 目标客户端 200 向第一服务器 301 上报目标用户的操作, 该操作例如可以为登录或支付操作。

S122: 第一服务器 301 向风控系统 304 发送风险咨询请求, 所述风险咨询请求用于请求咨询本次操作的风险, 风险咨询请求携带有目标客户端 200 上报的用户数据和交易
20 数据。

在一些实施例中, 风险咨询请求还携带有目标客户端 200 的设备令牌, 具体可以为目标客户端 200 在风控端 (即风控系统 204) 的设备令牌。

应理解, 目标客户端 200 在客户端的设备令牌和目标客户端 200 在风控端的设备令牌可以不同, 但二者之间存在关联关系, 且均与目标客户端的目标设备 ID 关联。本说明书将目标客户端 200 在客户端的设备令牌和目标客户端 200 在风控端的设备令牌统称为目标客户端 200 的设备令牌, 通过目标客户端 200 设备令牌, 就可以查找到目标设备
25 ID。

S101 具体可以为: 风控系统 304 向中心服务器 303 发送设备风险验证请求。

在一些实施例中，所述设备风险验证请求中携带目标客户端 200 在风控端的设备令牌。中心服务器 303 基于目标客户端 200 在风控端的设备令牌，可以确定并保存目标设备 ID。

在 S106 之后，方法 P100 还包括：

- 5 S123：中心服务器 303 基于目标设备 ID，确定与目标客户端 200 关联的设备风险标签。

在一种可能的实现方式中，私有化服务器 302 返回给中心服务器 303 的查询结果携带有目标设备 ID 和目标客户端 200 的设备风险标签。

- 10 在另一种可能的实现方式中，私有化服务器 302 返回给中心服务器 303 的查询结果未携带目标设备 ID 和目标客户端 200 的设备风险标签。此时，中心服务器 303 可以自己生成目标设备 ID，并计算目标客户端 200 的设备风险标签。

在一些实施例中，所述目标设备 ID 以及所述设备风险标签是中心服务器 303 基于目标客户端 200 的硬件信息以及目标客户端 200 的软件信息计算得到的。

- 15 其中，目标客户端 200 的硬件信息和目标客户端 200 的软件信息可以是目标客户端 200 上报给中心服务器 303 的，也可以是其他服务器（例如第一服务器 301）发送给中心服务器 303 的，本实施例对此不作限定。

S107 具体可以为：中心服务器 303 向风控系统 304 返回目标设备 ID。在一些实施例中，所述目标设备 ID 中携带有与目标客户端 200 关联的设备风险标签。

- 20 S124：风控系统 304 结合接收到的目标设备 ID 以及风险咨询请求中携带的用户数据和交易数据，计算本次操作的风险咨询结果。

风控系统 304 通过 S122 获取到了用户数据和交易数据，通过 S107 获取到了设备数据（即上述目标设备 ID 和设备风险标签），结合这些信息，风控系统 304 可以计算得到本次操作的风险咨询结果。

- 25 在一些实施例中，所述风险咨询结果具体可以为本次操作的风险等级，例如，高危、中危、低危三个等级。

例如，若目标客户端 100 在参加营销活动的情况下命中了改机的设备风险标签，那么本次操作的风险咨询结果就是高危。若目标客户端 100 在登录的情况下命中了改机的设备风险标签，那本次操作的风险咨询结果是低危。

又例如，若目标客户端 100 在交易环节命中了安装高危软件的设备风险标签，那么本次操作的风险咨询结果就是高危。若目标客户端 100 在登录的情况下命中了安装高危软件的设备风险标签，那么本次操作的风险咨询结果就是低危。

S125：风控系统 304 向第一服务器 301 返回所述风险咨询结果。

5 S126：第一服务器 301 根据所述风险咨询结果，向目标客户端 200 发送指示信息，该指示信息用于指示目标客户端 200 通过本次操作，或者进行用户身份验证，或者拦截本次操作。

例如，若风险咨询结果为低危，则第一服务器 301 可以通过指示信息指示目标客户端 200 通过本次操作；若风险咨询结果为中危，则第一服务器 301 可以通过指示信息指示目标客户端 200 进行用户身份验证，从而根据验证结果决定是否通过本次操作；若风险咨询结果为高危，则第一服务器 301 可以通过指示信息指示目标客户端 200 对本次操作进行拦截。

综上所述，本说明书提供的数据迁移方法、电子设备和存储介质，为了基于目标客户端 200 的目标设备 ID 对目标客户端 200 进行验证，中心服务器 303 先在本地查询目标设备 ID，若未查询到，中心服务器 303 再通过私有化服务器 302 查询目标设备 ID，这样，若私有化服务器 302 存储有目标设备 ID，中心服务器 303 就能够获取该目标设备 ID 并将该目标设备 ID 保存在中心服务器 303 上。通过这种方式，能够在服务提供方的数据部署模式升级过程中，找回原先已保存在私有化服务器 302 的设备 ID 数据，将私有化服务器 302 处设备 ID 数据的存量数据迁移至中心服务器 303，从而确保升级前后的设备 ID 保持一致，无需为所有设备重新生成设备 ID，降低了升级成本。此外，这种方式能够尽可能地防止中心服务器 303 把旧设备误识别成新设备，从而避免对目标用户 100 不必要的打扰，能够提高用户体验。

本说明书另一方面提供一种非暂时性存储介质，存储有至少一组用来进行数据迁移的可执行指令。当所述可执行指令被处理器执行时，所述可执行指令指导所述处理器实施本说明书所述的数据迁移方法 P100 中的中心服务器 303 的步骤。在一些可能的实施方式中，本说明书的各个方面还可以实现为一种程序产品的形式，其包括程序代码。当所述程序产品在电子设备 600 上运行时，所述程序代码用于使电子设备 600 执行本说明书描述的数据迁移方法 P100 中的中心服务器 303 的步骤。用于实现上述方法的程序产品可以采用便携式紧凑盘只读存储器 (CD-ROM) 包括程序代码，并可以在电子设备 600 上运行。然而，本说明书的程序产品不限于此，在本说明书中，可读存储介质可以是任

何包含或存储程序的有形介质，该程序可以被指令执行系统使用或者与其结合使用。所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子包括：

5 具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑盘只读存储器（CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。所述计算机可读存储介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或

10 上述的任意合适的组合。可读存储介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。可读存储介质上包含的程序代码可以用任何适当的介质传输，包括但不限于无线、有线、光缆、RF 等等，或者上述的任意合适的组合。可以以一种或多种程序设计语言的任意组合来编写用于执行本说明书操作的程序代码，所述程序设计语言包括

15 面向对象的程序设计语言—诸如 Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在电子设备 600 上执行、部分地在电子设备 600 上执行、作为一个独立的软件包执行、部分在电子设备 600 上部分在远程电子设备上执行、或者完全在远程电子设备上执行。

本说明提供的技术方案中，所涉及的对设备的硬件参数的采集以及使用，均符合相关

20 法律法规的规定，且不违背公序良俗。

上述对本说明书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求示出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

25 以的或者是可能有利的。

综上所述，在阅读本详细公开内容之后，本领域技术人员可以明白，前述详细公开内容可以仅以示例的方式呈现，并且可以不是限制性的。尽管这里没有明确说明，本领域技术人员可以理解本说明书需求囊括对实施例的各种合理改变，改进和修改。这些改变，改进和修改旨在由本说明书提出，并且在本说明书的示例性实施例的精神和范围内。

30 此外，本说明书中的某些术语已被用于描述本说明书的实施例。例如，“一个实施

例”，“实施例”和/或“一些实施例”意味着结合该实施例描述的特定特征，结构或特性可以包括在本说明书的至少一个实施例中。因此，可以强调并且应当理解，在本说明书的各个部分中对“实施例”或“一个实施例”或“替代实施例”的两个或更多个引用不一定都指代相同的实施例。此外，特定特征，结构或特性可以在本说明书的一个或多个实施例中适当地组合。

应当理解，在本说明书的实施例的前述描述中，为了帮助理解一个特征，出于简化本说明书的目的，本说明书将各种特征组合在单个实施例、附图或其描述中。然而，这并不是说这些特征的组合是必须的，本领域技术人员在阅读本说明书的时候完全有可能将其中一部分设备标注出来作为单独的实施例来理解。也就是说，本说明书中的实施例也可以理解为多个次级实施例的整合。而每个次级实施例的内容在于少于单个前述公开实施例的所有特征的时候也是成立的。

本文引用的每个专利，专利申请，专利申请的出版物和其他材料，例如文章、书籍、说明书、出版物、文件、物品等，除了与其相关的任何历史起诉文件、可能与本文件不一致或相冲突的任何相同的、或者任何可能对权利要求的最宽范围具有限制性影响的任何相同的历史起诉文件，均可以通过引用结合于此，并用于现在或以后与本文件相关联的所有目的。此外，如果在与任何所包含的材料相关联的术语的描述、定义和/或使用与本文档相关的术语、描述、定义和/或之间存在任何不一致或冲突时，使用本文件中的术语为准。

最后，应理解，本文公开的申请的实施方案是对本说明书的实施方案的原理的说明。其他修改后的实施例也在本说明书的范围内。因此，本说明书披露的实施例仅作为示例而非限制。本领域技术人员可以根据本说明书中的实施例采取替代配置来实现本说明书中的申请。因此，本说明书的实施例不限于申请中被精确地描述过的实施例。

权 利 要 求 书

1. 一种数据迁移方法,用于将私有化服务器中存储的设备标识数据迁移至中心服务器,所述中心服务器用于替代所述私有化服务器为客户端提供数据支持,所述方法应用于所述中心服务器,包括:

5 接收请求设备发送的验证请求,所述验证请求用于请求基于目标客户端的目标设备标识进行验证;

 在未查询到所述目标设备标识的情况下,向所述私有化服务器发送查询请求,所述查询请求用于请求查询所述目标设备标识;

 接收所述私有化服务器发送的查询结果,并保存所述目标设备标识;以及

10 向所述请求设备发送响应于所述验证请求的验证结果。

2. 如权利要求 1 所述的方法,其中,所述验证请求携带所述目标客户端的设备令牌。

15 3. 如权利要求 2 所述的方法,其中,所述在未查询到所述目标设备标识的情况下,向所述私有化服务器发送查询请求,包括:

 基于所述设备令牌进行查询,确定未查询到与所述设备令牌关联的所述目标设备标识;以及

 向所述私有化服务器发送所述查询请求,所述查询请求中携带有所述设备令牌。

20

4. 如权利要求 2 所述的方法,其中,所述验证请求还携带所述目标客户端的硬件信息以及所述目标客户端的软件信息。

25 5. 如权利要求 4 所述的方法,其中,所述接收所述私有化服务器发送的查询结果,并保存所述目标设备标识,包括:

 确定所述查询结果中携带有所述目标设备标识,保存所述目标设备标识,并将所述目标设备标识与所述设备令牌关联;或者

 确定所述查询结果中没有携带有所述目标设备标识,基于所述硬件信息以及所述软件信息生成所述目标设备标识,并将所述目标设备标识与所述设备令牌关联。

6. 如权利要求 1 所述的方法，其中，所述请求设备包括所述目标客户端，所述验证请求包括设备身份验证请求；
- 所述接收请求设备发送的验证请求，包括：
- 5 接收所述目标客户端发送的所述设备身份验证请求；
- 所述向所述请求设备发送响应于所述验证请求的验证结果，包括：
- 基于所述目标设备标识对所述目标客户端进行所述设备身份验证，生成设备身份验证结果；以及
- 向所述目标客户端返回所述设备身份验证结果。
- 10
7. 如权利要求 1 所述的方法，其中，所述请求设备包括风控系统，所述验证请求包括设备风险验证请求；
- 所述接收请求设备发送的验证请求，包括：
- 接收所述风控系统发送的所述设备风险验证请求；
- 15 所述向所述请求设备发送响应于所述验证请求的验证结果，包括：
- 基于所述目标设备标识，确定与所述目标客户端关联的设备风险标签；以及
- 向所述风控系统返回所述设备风险标签。
8. 如权利要求 7 所述的方法，其中，所述目标设备标识中携带有与所述目标客户端
- 20 关联的所述设备风险标签。
9. 如权利要求 8 所述的方法，其中，所述目标设备标识以及所述设备风险标签是基于所述目标客户端的硬件信息以及所述目标客户端的软件信息计算得到的。
- 25
10. 一种电子设备，包括：
- 至少一个存储介质，存储有至少一个指令集，用于进行数据迁移；以及
- 至少一个处理器，同所述至少一个存储介质通信连接，
- 其中，当所述电子设备运行时，所述至少一个处理器读取所述至少一个指令集，并且根据所述至少一个指令集的指示：

- 接收请求设备发送的验证请求，所述验证请求用于请求基于目标客户端的目标设备标识进行验证，
- 在未查询到所述目标设备标识的情况下，向所述私有化服务器发送查询请求，所述查询请求用于请求查询所述目标设备标识，
- 5 接收所述私有化服务器发送的查询结果，并保存所述目标设备标识，以及
 向所述请求设备发送响应于所述验证请求的验证结果。
11. 如权利要求 10 所述的电子设备，其中，所述验证请求携带所述目标客户端的设备令牌。
- 10
12. 如权利要求 11 所述的电子设备，其中，为了在未查询到所述目标设备标识的情况下，向所述私有化服务器发送查询请求，所述至少一个处理器：
- 基于所述设备令牌进行查询，确定未查询到与所述设备令牌关联的所述目标设备标识；以及
- 15 向所述私有化服务器发送所述查询请求，所述查询请求中携带有所述设备令牌。
13. 如权利要求 11 所述的电子设备，其中，所述验证请求还携带所述目标客户端的硬件信息以及所述目标客户端的软件信息。
- 20
14. 如权利要求 13 所述的电子设备，其中，为了接收所述私有化服务器发送的查询结果，并保存所述目标设备标识，所述至少一个处理器：
- 确定所述查询结果中携带有所述目标设备标识，保存所述目标设备标识，并将所述目标设备标识与所述设备令牌关联；或者
- 确定所述查询结果中没有携带有所述目标设备标识，基于所述硬件信息以及所述软件信息生成所述目标设备标识，并将所述目标设备标识与所述设备令牌关联。
- 25
15. 如权利要求 10 所述的电子设备，其中，所述请求设备包括所述目标客户端，所述验证请求包括设备身份验证请求；
- 为了接收请求设备发送的验证请求，所述至少一个处理器：
- 30 接收所述目标客户端发送的所述设备身份验证请求；

为了向所述请求设备发送响应于所述验证请求的验证结果，所述至少一个处理器：
基于所述目标设备标识对所述目标客户端进行所述设备身份验证，生成设备身份验证结果；以及
向所述目标客户端返回所述设备身份验证结果。

5

16. 如权利要求 10 所述的电子设备，其中，所述请求设备包括风控系统，所述验证请求包括设备风险验证请求；

为了接收请求设备发送的验证请求，所述至少一个处理器：

接收所述风控系统发送的所述设备风险验证请求；

10 为了向所述请求设备发送响应于所述验证请求的验证结果，所述至少一个处理器：
基于所述目标设备标识，确定与所述目标客户端关联的设备风险标签；以及
向所述风控系统返回所述设备风险标签。

17. 如权利要求 16 所述的电子设备，其中，所述目标设备标识中携带有与所述目标
15 客户端关联的所述设备风险标签。

18. 如权利要求 17 所述的电子设备，其中，所述目标设备标识以及所述设备风险标签是基于所述目标客户端的硬件信息以及所述目标客户端的软件信息计算得到的。

20 19. 一种计算机可读非暂时性存储介质，其中，所述计算机可读非暂时性存储介质中存储有至少一个指令集，所述至少一个指令集被至少一个处理器执行时，实现如权利要求 1 至 9 中任一项所述的方法。

25