

DATA MIGRATION METHOD, ELECTRONIC DEVICE, AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to a
5 data migration method, an electronic device, and a storage medium.

BACKGROUND

[0002] A device identifier (ID), also referred to as a device fingerprint, is a unique ID used to
identify a device. The device ID can be used to identify and distinguish different devices to ensure
device security and reliability. The device ID can be used in scenarios such as identity verification
10 and risk identification. For a service provider, device ID data may be deployed on a local private
server of the service provider in an on-premise deployment mode, or the device ID data may be
deployed on a central server in a central deployment mode, such as a software as a service (SaaS)
mode.

[0003] When the service provider performs an upgrade from the on-premise deployment mode
15 to the central deployment mode, how to smoothly migrate existing device ID data in the private
server in an upgrade process becomes a technical problem that needs to be urgently resolved at
present.

[0004] Content of the background part is merely information learned of by the inventor, and
neither means that the information has entered a public domain before an application date of this
20 disclosure, nor means that the information can become a conventional technology of this disclosure.

SUMMARY

[0005] This specification provides a data migration method, an electronic device, and a storage
medium, to smoothly migrate existing device ID data in a process in which a service provider
upgrades a data deployment mode, thereby reducing upgrade costs.

25 [0006] According to a first aspect, this specification provides a data migration method, used
to migrate device identifier data stored in a private server to a central server. The central server is
configured to provide data support for a client in place of the private server. The method is applied
to the central server and includes: receiving a verification request sent by a requesting device,

where the verification request is used to request to perform verification based on a target device identifier of a target client; sending a query request to the private server when the target device identifier is not found, where the query request is used to request to query the target device identifier; receiving a query result sent by the private server, and storing the target device identifier;
5 and sending a verification result in response to the verification request to the requesting device.

[0007] According to a second aspect, this specification further provides an electronic device, including: at least one storage medium, storing at least one instruction set used to perform data migration; and at least one processor, communicatively connected to the at least one storage medium. When the electronic device runs, the at least one processor reads the at least one
10 instruction set and performs the following operations based on an instruction of the at least one instruction set: receiving a verification request sent by a requesting device, where the verification request is used to request to perform verification based on a target device identifier of a target client; sending a query request to the private server when the target device identifier is not found, where the query request is used to request to query the target device identifier; receiving a query
15 result sent by the private server, and storing the target device identifier; and sending a verification result in response to the verification request to the requesting device.

[0008] According to a third aspect, this specification further provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set, and the at least one instruction set is executed by at least one processor to
20 implement the method according to the first aspect.

[0009] It can be learned from the above-mentioned technical solutions that, according to the data migration method, the electronic device, and the storage medium provided in this specification, device identifier data stored in the private server can be migrated to the central server. In a process of upgrading a data deployment mode of a service provider, to verify the target client
25 based on the target device identifier of the target client, the central server first locally queries the target device identifier. If the target device identifier is not found, the central server further queries the target device identifier by using the private server. In this way, if the private server stores the target device identifier, the central server can obtain the target device identifier and store the target device identifier in the central server. In this manner, in the process of upgrading the data
30 deployment mode of the service provider, the device identifier data previously stored in the private server can be retrieved, and the existing device identifier data in the private server is migrated to the central server. Therefore, it is ensured that device identifiers used before and after upgrade are consistent, and there is no need to regenerate device identifiers for all devices, thereby reducing upgrade costs. In addition, in this manner, the central server can be prevented from mistakenly
35 identifying an old device as a new device as far as possible, thereby avoiding unnecessary

disturbance to a target user and improving user experience.

[0010] Other functions of the data migration method, the electronic device, and the storage medium provided in this specification are listed in the following descriptions. Based on the descriptions, content described by using the following numbers and examples is clear to a person of ordinary skill in the art. Creative aspects of the data migration method, the electronic device, and the storage medium provided in this specification can be fully explained by practice or by using the method, apparatus, and combination described in the following detailed example.

BRIEF DESCRIPTION OF DRAWINGS

[0011] To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following description show merely some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0012] FIG. 1 is a schematic diagram of an application scenario of data migration according to some embodiments of this specification;

[0013] FIG. 2 is a diagram of a hardware structure of an electronic device according to some embodiments of this specification;

[0014] FIG. 3 is a flowchart of a data migration method according to some embodiments of this specification;

[0015] FIG. 4 is a flowchart of a data migration method according to some embodiments of this specification; and

[0016] FIG. 5 is a flowchart of a data migration method according to some embodiments of this specification.

DESCRIPTION OF EMBODIMENTS

[0017] Specific application scenarios and requirements of this specification are provided in the following descriptions, so that a person skilled in the art can manufacture and use content of this specification. For the person skilled in the art, various local modifications to the disclosed embodiments are apparent, and the general principles defined herein can be applied to other embodiments and applications without departing from the spirit and scope of this specification. Therefore, this specification is not limited to the shown embodiments, but has a widest scope consistent with that of the claims.

[0018] The terms used herein are only intended to describe a particular example embodiment,

but do not impose a limitation. For example, unless otherwise specified in the context, the singular forms "one", "a", and "the" used herein can also include a plural form. When used in this specification, the terms "include", "comprise", and/or "have" indicate/indicates existence of an associated integer, step, operation, element, and/or component, but does not exclude existence of one or more other features, integers, steps, operations, elements, components, and/or groups, or another feature, integer, step, operation, element, component, and/or group can be added to the system/method.

[0019] In consideration of the following descriptions, these and other features of this specification, operations and functions of related components of the structure, and economy of combination and manufacturing of components can be significantly improved. With reference to the accompanying drawings, all of these form a part of this specification. However, it should be clearly understood that the accompanying drawings are merely used for the purpose of illustration and description, and are not intended to limit the scope of this specification. It should be further understood that the accompanying drawings are not drawn to scale.

[0020] The flowchart used in this specification illustrates operations implemented by a system in some embodiments of this specification. It should be clearly understood that operations in the flowchart can be implemented out of sequence. On the contrary, operations can be implemented reversely or simultaneously. In addition, one or more other operations can be added to the flowchart. One or more operations can be removed from the flowchart.

[0021] For ease of description, this specification explains the terms that appear in the following descriptions:

[0022] 1. A device ID, also referred to as a device fingerprint, is a unique identifier used to identify and verify a device. A core principle of a fingerprint product of a device is to collect many data of the device (for example, hardware data and software data of the device), and generate, by using a built-in device ID retrieval algorithm, a unique ID used to identify the device. The unique ID is the device ID. The device ID is generated by the fingerprint product of the device. Device IDs generated by different service providers are different. The device ID can be used to distinguish different devices to ensure device security and reliability. Risk environment identification, risk detection, behavior risk analysis, etc. on a client can be implemented by using the device ID. For example, a service provider usually can identify, based on the device ID, whether a current client is a common device of a user account, to verify a device used by a user.

[0023] In some embodiments, in a process in which a user registers a user account by using an APP installed on a client, a server corresponding to the APP collects device data of the client, where the device data includes a plurality of software parameters and a plurality of hardware parameters; and processes the device data by using a specific tool to obtain a device ID that can

uniquely identify the client. The software parameters can include, for example, an APP name, an APP version, APP installation time, and a system version installed on a device. The hardware parameters can include, for example, a device manufacturer, a device brand, a device type and model, a device memory and storage size, baseband information, screen resolution, a media access control (MAC) address, an international mobile equipment identity (IMEI), an international mobile subscriber identity (IMSI), a network standard, and a baseband number. In addition, the device data can further include other parameters, such as a device serial number, a WiFi MAC, an operator name, power-on time, and a user-defined device name. The server corresponding to the APP can assign, to each device that uses the APP, a device ID that can uniquely identify the device.

10 The server corresponding to the APP can store a correspondence between a plurality of user accounts and a plurality of device IDs. When the user subsequently uses the APP again on the client or another device by using the user account, the server corresponding to the APP can determine, based on a device ID corresponding to the user account, whether a device that uses the APP this time is a common device of the user account. The above-mentioned specific tool is, for example, a device fingerprint software development kit (SDK).

15 **[0024]** 2. A device token is a token used to identify a user identity. Generally, when a user logs in to an APP on a client for the first time, a server corresponding to the APP generates a token for the user, and returns the token to the client. Subsequently, the client needs to bring only the token to request data from the server, and does not need to bring a user name and a password.

20 **[0025]** The server corresponding to the APP associates the device token with a device ID. The device ID can be found by using the device token. There is a many-to-one relationship between the device token and the device ID. In addition, the device token is temporary and has an expiration period. If the device token expires, the server corresponding to the APP generates a new device token for the user again.

25 **[0026]** 3. A device risk label is used to indicate whether a device has specific types of risks. For example, whether the device has risks such as firmware flashing, device modification, emulator installation, jailbreaking, hijacking injection, etc.

[0027] There is an association relationship between a device ID and a device risk label. A device risk label of a device corresponding to a device ID can be determined by using the device ID, so that risk identification can be performed on a related operation on the device by using the device risk label. It should be understood that the device ID does not change with the following operation: installing an emulator or a virtual machine on a device, flashing firmware, or modifying a device.

30

[0028] 3. On-premise deployment means deploying and managing an IT infrastructure in a physical facility owned by a service provider, which can include a data center, a server, network

35

hardware, a storage device, etc. For on-premise deployment, the service provider can have full control over all hardware, software, and data, and all data is stored in hardware owned by the service provider. Therefore, on-premise deployment can provide higher-level data security and privacy protection.

5 **[0029]** 4. SaaS is a service mode in which a software application is provided through the Internet. The software application program is provided as a service to a user through the Internet. In the SaaS mode, the software application program is hosted on a server of an SaaS service provider, and the user accesses and uses the program through the Internet. The user no longer needs to purchase and maintain an entire software infrastructure, and instead, the user gains permission
10 to access cloud software through subscription. The SaaS provider is responsible for software deployment, maintenance and security. The user can easily access and use software only through a web browser or a dedicated application program. The SaaS mode has advantages of flexibility, scalability, and low costs.

[0030] Before specific embodiments of this specification are described, an application
15 scenario of this specification is first described.

[0031] When a user uses an APP with a relatively high security requirement on a client, for example, when the user logs in to a payment APP or when the user initiates payment, the APP can be triggered to verify the client used by the user. Generally, a server corresponding to the APP verifies the client by using a device ID. Therefore, obtaining the device ID is extremely important.
20 Currently, there are two data deployment manners for data storage at a server end. One is an on-premise deployment mode, that is, device ID data is stored in a local private server of a service provider, and the service provider has full control over the device ID data. The other is a central deployment mode, that is, the device ID data is stored in a server (central server) of a service provider in the SaaS mode. When the service provider upgrades a data storage manner from the
25 on-premise deployment mode to the central deployment mode, to help obtain the device ID data, the device ID data needs to be migrated from the local private server to the central server, that is, updating from deploying the device ID data on the private server to deploying the device ID data on the central server, so that the central server provides data support for a client in place of the private server.

30 **[0032]** In the above-mentioned scenario, if the central server is directly used to replace the private server, the central server needs to regenerate new device IDs for all clients, which increases processing burden of the central server, resulting in relatively high upgrade costs.

[0033] In view of this, this specification provides a data migration method, an electronic device, and a storage medium, which can be applied to an upgrade scenario in which device ID data stored
35 in a private server is migrated to a central server. When a target device ID of a target client is not

found, the central server can query the target device ID by using the private server. In this way, if the private server stores the target device ID, the central server can obtain the target device ID and store the target device ID in the central server. In this manner, in a process of upgrading a data deployment mode of a service provider, the device ID data previously stored in the private server can be retrieved, and the existing device ID data in the private server is migrated to the central server. Therefore, it is ensured that device IDs used before and after upgrade are consistent, and there is no need to regenerate device IDs for all devices, thereby reducing upgrade costs. In addition, in this manner, the central server can be prevented from mistakenly identifying an old device as a new device as far as possible, thereby avoiding unnecessary disturbance to a target user and improving user experience.

[0034] FIG. 1 is a schematic diagram of an application scenario 001 of data migration according to some embodiments of this specification. As shown in FIG. 1, the application scenario can include a target user 100, a target client 200, and a serving end 300. The serving end 300 can include a first server 301 of a target service provider, a second server 302 of the target service provider, a central server 303, and a risk control system 304.

[0035] The target user 100 can perform a related event by using the target client 200. For example, the target client 200 is installed with one or more APPs, and the one or more APPs can provide a user with a capability to perform a related event. The APP includes but is not limited to a web browser APP, a search APP, a chat APP, a shopping APP, a service APP, a video APP, a financial APP, a payment APP, etc.

[0036] The target client 200 can be installed with a target APP, and the target APP provides a target service by using a target service provider. The target client 200 presents an interaction interface to the target user 100 by using the target APP, so that the target user 100 performs some events through the interaction interface. For example, the target service provider is a payment service provider, the target APP is an electronic wallet APP. In response to an operation of the target user 100, the target client 200 can present a login interface to the target user 100 by using the electronic wallet APP, the target user 100 can complete login in the login interface; or the target client 200 can present a payment interface to the target user 100 by using the electronic wallet APP, and the target user 100 can complete a payment event, etc. in the payment interface.

[0037] The target client 200 can include a mobile device, a tablet computer, a laptop computer, a device built in a motor vehicle or similar content, or any combination thereof. In some embodiments, the mobile device can include a smart home device, a smart mobile device, a virtual reality device, an augmented reality device or a similar device, or any combination thereof. In some embodiments, the smart home apparatus can include a smart television, a desktop computer, or any combination thereof. In some embodiments, the smart mobile device can include a

smartphone, a personal digital assistant, a game device, a navigation device, etc., or any combination thereof. In some embodiments, the virtual reality device or the augmented reality device can include a virtual reality helmet, virtual reality glasses, a virtual reality patch, an augmented reality helmet, augmented reality glasses, an augmented reality patch or similar content, or any combination thereof. For example, the virtual reality device or the augmented reality device can include AR glasses, a head-mounted display, and VR. In some embodiments, the apparatus built in the motor vehicle can include a vehicle-mounted computer, a vehicle-mounted television, etc. In some embodiments, the target client 200 can be a device with a positioning technology, and is configured to position a location of the target client 200.

10 **[0038]** As shown in FIG. 1, the target client 200 can be communicatively connected to the serving end 300. In some embodiments, the serving end 300 can be further communicatively connected to another client. A quantity of clients in the scenario is not limited in this specification. In some embodiments, the target client 200 can interact with the serving end 300 through a network to receive or send a message, etc.

15 **[0039]** The serving end 300 can include a server that provides various services. For example, the serving end 300 includes a background server that provides support for a page displayed by an APP on the target client 200. Specifically, the serving end 300 includes the first server 301 of the target service provider, the second server 302 of the target service provider, the central server 303, and the risk control system 304.

20 **[0040]** The first server 301 is a server of the target service provider, and is configured to provide support for a page displayed by a target APP installed on the target client 200, and provide a target service for the target user 100 in a process in which the target user 100 uses the target APP. The first server 301 can be communicatively connected to the target client 200. In a process in which the target user 100 uses the target service, the target client 200 can communicate with the first server 301 to exchange or transfer data. For example, when the target client 200 detects that the target user 100 performs some operations (for example, logging in to the target APP or performing a payment operation on an interaction page), the target client 200 sends user data and transaction data to the first server 301. The first server 301 sends the received user data and transaction data to the risk control system 304 for risk consultation, to obtain a risk result returned by the risk control system 304. Based on the risk result, the first server 301 can determine whether identity verification needs to be performed on the target user 100 by using the target client 200, or whether the current operation needs to be intercepted, to ensure security of the current operation.

25 **[0041]** The second server 302 is also referred to as a private server 302 and is also a server of the target service provider, and can be deployed locally in the target service provider. Therefore, the second server 302 can also be referred to as a local server of the target service provider. The

30

35

second server 302 is configured to store data of the target service provider and is independently managed and controlled by the target service provider. A mode of storing data by using the second server 302 is referred to as an on-premise deployment mode. In this specification, the second server 302 is configured to store device ID data of the target service provider. For ease of distinguishing from the central server 303, the second server 302 is subsequently referred to as a private server 302.

[0042] The central server 303 is deployed in a cloud, and can also be configured to store data. The target service provider can obtain, through the Internet, the data stored in the central server 303, and does not need to maintain local software and hardware facilities. A mode of storing data by using the central server 303 is referred to as a central deployment mode. In this specification, the central server 303 is configured to store the device ID data of the target service provider in place of the private server 302. The target client 200 can be communicatively connected to the central server 303. In the process in which the target user 100 uses the target service, the target client 200 can communicate with the central server 303 to exchange or transfer data. For example, when the target client 200 detects that the target user 100 performs some operations (for example, logging in to the target APP or performing a payment operation on an interaction page), the target client 200 can collect device data of the target client, and send the device data to the central server 303, so that the central server 303 queries a device ID of the target client 200 based on the device data, performs device verification based on the device ID, and returns a verification result to the target client 200.

[0043] In this specification, the central server 303 is communicatively connected to the private server 302, to obtain device ID data of the private server 302. In addition, a device ID retrieval algorithm is further built in the central server 303, and can be used to generate, based on hardware information and software information of the target client 200, a device ID used to identify the target client 200.

[0044] Actions related to the central server 303 in the data migration method provided in this specification can be performed on the central server 303. In this case, the central server 303 can store data or instructions corresponding to the central server 303 in the data migration method described in this specification, and can execute or be configured to execute the data or the instructions. In some embodiments, the central server 303 can include a hardware device with a data information processing function and a program needed for driving the hardware device to work.

[0045] The risk control system 304 can be deployed with a risk control policy, and is configured to perform risk detection on a target event generated in the process in which the target user 100 uses the target service. The risk control system 304 is communicatively connected to the

first server 301 and the central server 303 to transfer data. Specifically, the risk control system 304 can receive user data and transaction data that are sent by the first server 301, and receive device data (for example, a device ID and a device risk label) sent by the central server 303. The risk control system 304 can determine, based on the risk control policy with reference to the user data, the transaction data, and the device data, whether there is a risk in the current operation, to obtain a risk result. The risk result can be, for example, a risk level of the current operation. The risk control system 304 returns the risk result to the first server 301.

[0046] The risk control policy can include but is not limited to a risk control model obtained through pre-training by the target service provider, a risk control rule accumulated by the target service provider based on historical experience, etc. The target event can include but is not limited to the following: The target user 100 logs in to the target APP of the target client 200, and the target user 100 performs payment on the target APP of the target client 200.

[0047] FIG. 1 shows only a first server 301 of one target service provider and a private server 302 of the target service provider. However, it should be understood that the central server 303 can be further connected to a first server 301 and a private server 302 of another service provider, that is, the central server 303 can simultaneously provide data support for a plurality of different service providers. This is not limited in this specification.

[0048] It should be understood that quantities of target clients 200, serving ends 300, and networks 400 in FIG. 1 are merely examples. Depending on implementation needs, there may be any quantity of target clients 200, serving ends 300, and networks 400.

[0049] FIG. 2 is a diagram of a hardware structure of an electronic device 600 according to some embodiments of this specification. The electronic device 600 can perform the data migration method described in this specification. The data migration method is described in another part of this specification. When an action related to the central server 303 in the data migration method is performed on the central server 303, the electronic device 600 can be the central server 303.

[0050] As shown in FIG. 2, the electronic device 600 can include at least one storage medium 630 and at least one processor 620. In some embodiments, the electronic device 600 can further include a communication port 650 and an internal communication bus 610. In addition, the electronic device 600 can further include an I/O component 660.

[0051] The internal communication bus 610 can be connected to different system components, including the storage medium 630, the processor 620, and the communication port 650.

[0052] The I/O component 660 supports input/output between the electronic device 600 and another component.

[0053] The communication port 650 is used for data communication between the electronic device 600 and the outside. For example, the communication port 650 can be used for data

communication between the electronic device 600 and a network 400. The communication port 650 can be a wired communication port, or can be a wireless communication port.

[0054] The storage medium 630 can include a data storage apparatus. The data storage apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 632, a read-only storage medium (ROM) 634, or a random access storage medium (RAM) 636. The storage medium 630 further includes at least one instruction set stored in the data storage apparatus. The instruction set can be computer program code. When the electronic device 600 is the central server 303, the computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, etc. that correspond to the central server 303 that performs the data migration method provided in this specification.

[0055] The processor 620 can be communicatively connected to the storage medium 630 and the communication port 650 through the internal communication bus 610. The processor 620 is configured to execute the at least one instruction set. When the electronic device 600 runs as the central server 303, the processor 620 can read the at least one instruction set, and perform, based on an instruction of the at least one instruction set, the data migration method provided in this specification. The processor 620 can perform all steps of the central server 303 included in the method.

[0056] The processor 620 can be in a form of one or more processors. In some embodiments, the processor 620 can include one or more hardware processors, for example, a microcontroller, a microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit, processor, etc. that can perform one or more functions, or any combination thereof.

[0057] For only the purpose of description, only one processor 620 is described in the electronic device 600 in this specification. However, it should be noted that the electronic device 600 in this specification can further include a plurality of processors. Therefore, operations and/or method steps disclosed in this specification can be performed by one processor or can be performed jointly by a plurality of processors, as described in this specification. For example, if the processor 620 in the electronic device 600 in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or separately performed by two different processors 620 (for example, a first processor performs step A, and a second processor performs step B, or a first processor and a second processor jointly perform step A and step B).

[0058] For ease of understanding, the following describes the data migration method in this specification in an interactive manner.

[0059] FIG. 3 is a flowchart of a data migration method P100 according to some embodiments of this specification. As described above, the electronic device 600 can perform steps
5 corresponding to the central server 303 in the data migration method P100 described in this specification. Specifically, the processor 620 can read the instruction set stored in the local storage medium of the electronic device, and then perform, based on stipulation of the instruction set, the steps corresponding to the central server 303 in the data migration method P100 described in this specification.

10 [0060] As shown in FIG. 3, the method P100 can include the following steps.

[0061] S101: A requesting device sends a verification request to the central server 303, where the verification request is used to request to perform verification based on a target device ID of the target client 200.

[0062] The target client 200 is a client device used by the target user 100, and a target APP is
15 installed on the target client 200. If the target user 100 requests a specific service of the target APP in a process of using the target APP, for example, logging in to the target APP or requesting a payment service of the target APP, the target client 200 can trigger the requesting device to initiate verification, that is, send the verification request to the central server 303. The verification request can be device verification performed on the target client 200. The device verification can be
20 verification performed based on the target device ID of the target client 200 to verify whether the target client 200 is an allowed device.

[0063] The requesting device can be, for example, the target client 200 or the risk control system 304.

[0064] In a possible implementation, the requesting device is the target client 200, and the
25 verification request is a device identity verification request. If the target user 100 performs some operations (for example, logging in to the target APP or performing a payment operation on an interaction page) in the target APP by using the target client 200, in response to an operation of the target user 100, the target client 200 can send the verification request to the central server 303 to request to verify the target client 200.

30 [0065] In another possible implementation, the requesting device is the risk control system 304, and the verification request is a device risk verification request. If the target client 200 can request a target service from the first server 301, the target client 200 sends user data and transaction data to the first server 301, and the first server 301 sends the received user data and transaction data to the risk control system 304 for risk consultation. In response to the risk
35 consultation of the first server 301, the risk control system 304 can send the device risk verification

request to the central server 303 to request to obtain device data (for example, the target device ID and a device risk label) of the target client 200, to obtain a risk consultation result with reference to the user data, the transaction data, and the device data.

[0066] In some embodiments, the verification request carries a device token of the target client 200.

[0067] In some embodiments, the verification request further carries hardware information of the target client 200 and software information of the target client 200.

[0068] S102: The central server 303 queries the target device ID based on the verification request.

[0069] The central server 303 can first query whether the central server stores the target device ID. In some embodiments, the central server 303 can perform a query based on the device token of the target client 200. Because there is an association relationship between a device token and a device ID, when the target device ID of the target client 200 exists, the target device ID of the target client 200 can be found by using the device token of the target client 200.

[0070] If the central server 303 finds the target device ID, the central server 303 can directly perform verification by using the found target device ID, and return a verification result to the requesting device, so that the current procedure ends. This case indicates that the target device ID has previously been migrated from the private server 302 to the central server 303, or the target device ID is generated by the central server 303, and does not exist in the private server 302. Therefore, the target device ID does not need to be queried from the private server 302. If the central server 303 does not find the target device ID, subsequent steps continue to be performed.

[0071] S103: The central server 303 sends a query request to the private server 302 when the target device ID is not found, where the query request is used to request to query the target device ID.

[0072] When the central server 303 determines that the target device ID associated with the device token is not found, the central server 303 can send the query request to the private server 302 to request the private server 302 to query the target device ID of the target client 200. The query request carries the device token of the target client 200.

[0073] S104: The private server 302 queries the target device ID based on the query request.

[0074] In some embodiments, the private server 302 can perform a query based on the device token of the target client 200 carried in the query request.

[0075] S105: The private server 302 sends a query result to the central server 303.

[0076] S106: The central server 303 receives the query result, and stores the target device ID.

[0077] In some embodiments, if the private server 302 finds the target device ID, the query result carries the target device ID. The central server 303 can store the target device ID, and

associate the target device ID with the device token of the target client 200.

[0078] The above-mentioned case indicates that the private server 302 stores the target device ID of the target client 200, that is, the target client 200 is an old device. In the above-mentioned manner, the target device ID of the target client 200 can be retrieved from the private server 302 and migrated to the central server 303. Because the central server 303 associates the target device ID with the device token of the target client 200, if the requesting device subsequently initiates verification on the target client 200 again, the central server 303 can find the target device ID based on an association relationship stored in the central server, without requesting the private server 302 to provide a service again.

[0079] In some embodiments, if the private server 302 does not find the target device ID, the query result does not carry the target device ID. In this case, the target device ID of the target client 200 neither exists in the central server 303 nor exists in the private server 302, which represents that the target client 200 may be a new device, and the central server 303 needs to generate a device ID of the new device. The central server 303 can generate the target device ID based on the hardware information and the software information of the target client 200, and associate the target device ID with the device token of the target client 200.

[0080] The above-mentioned case indicates that neither the central server 303 nor the private server 302 stores the target device ID of the target client 200, that is, the target client 200 is a new device. In the above-mentioned manner, a new device ID can be generated for the target client 200. The central server 303 stores the newly generated target device ID, and associates the newly generated target device ID with the device token of the target client 200. If the requesting device subsequently initiates verification on the target client 200 again, the central server 303 can find the newly generated target device ID based on an association relationship stored in the central server, without requesting the private server 302 to provide a service again.

[0081] It should be understood that each time a device goes online, that is, the target user 100 logs in to the target APP on the target client 200, the verification procedure in the method P100 in this specification can be triggered. Operations of logging in to the target APP on different target clients 200 by different target users 100 enable target device IDs of different target clients 200 to be stored in the central server 303, thereby implementing migration of device ID data in the verification process.

[0082] It should also be understood that in actual applications, the data migration method in this specification is performed within a preset period. To be specific, within the preset period (for example, one year or two years), the private server 302 provides data support by using the central server 303, and the central server 303 queries the target device ID from the private server 303 when the central server does not find the target device ID, to ensure that a target device ID of a

target client 200 that goes online within the preset period is migrated to the central server 303. After the preset period, it is considered that data migration has been completed, and the private server 302 no longer provides a data support service, and only the central server 303 provides the data support service. In this case, if the central server 303 receives a verification request and does not find the target device ID of the target client 200 based on the verification request, the central server 303 can directly generate the target device ID for the target client 200, and bind the newly generated target device ID to the device token of the target client 200.

[0083] S107: The central server 303 sends a verification result in response to the verification request to the requesting device.

[0084] In some embodiments, the requesting device is the target client 200, and the verification request is a device identity verification request. FIG. 4 is a flowchart of a data migration method in this scenario. The target client 200 is installed with a target APP and a secure SDK, and the secure SDK is configured to collect device information and initiate verification. As shown in FIG. 4, before S101, the method P100 further includes the following steps.

[0085] S111: When the target user logs in to the target APP, the target APP sends an initialization message to the secure SDK.

[0086] S112: In response to the received initialization message, the secure SDK obtains device information of the target client 200, where the device information herein includes a device token of the target client 200, device hardware information of the target client 200, and device software information of the target client 200.

[0087] S101 can be specifically as follows: The secure SDK sends a device identity verification request to the central server 303, where the device identity verification request can include the device token of the target client 200, the device hardware information of the target client 200, and the device software information of the target client 200.

[0088] After S106, the method P100 further includes the following steps.

[0089] S113: The central server 303 performs device identity verification on the target client 200 based on the target device ID to generate a device identity verification result.

[0090] S107 can be specifically as follows: The central server 303 sends the device identity verification result to the secure SDK of the target client 200.

[0091] S114: The secure SDK returns the device token of the target client 200 to the target APP based on the device identity verification result.

[0092] It should be understood that the secure SDK is an SDK of a new version that can be connected to the central server 303. When the target client 200 integrates with the secure SDK of the new version, the central server 303 can perform device identity verification on the target client 200 according to the above-mentioned method, and stores the target device ID in the central server

303. If the target client 200 does not integrate with the secure SDK of the new version, that is, the target client 200 is installed with a secure SDK of an old version, device identity verification can be performed on the target client 200 only by using the private server 302, and data migration of the target device ID cannot be performed.

5 **[0093]** In some embodiments, the requesting device includes the risk control system 304, and the verification request is a device risk verification request. FIG. 5 is a flowchart of a data migration method in this scenario. As shown in FIG. 5, before S101, the method P100 further includes the following steps.

10 **[0094]** S121: The target client 200 reports an operation of the target user to the first server 301, where the operation can be, for example, a login or payment operation.

[0095] S122: The first server 301 sends a risk consultation request to the risk control system 304, where the risk consultation request is used to request to seek consultation on a risk of the current operation, and the risk consultation request carries user data and transaction data that are reported by the target client 200.

15 **[0096]** In some embodiments, the risk consultation request further carries the device token of the target client 200, which can be specifically a device token of the target client 200 at a risk control end (that is, the risk control system 204).

[0097] It should be understood that a device token of the target client 200 at a client may be different from the device token of the target client 200 at the risk control end. However, there is an association relationship between the two device tokens, and both are associated with the target device ID of the target client. In this specification, the device token of the target client 200 at the client and the device token of the target client 200 at the risk control end are collectively referred to as the device token of the target client 200, and the target device ID can be found by using the device token of the target client 200.

25 **[0098]** S101 can be specifically as follows: The risk control system 304 sends a device risk verification request to the central server 303.

[0099] In some embodiments, the device risk verification request carries the device token of the target client 200 at the risk control end. The central server 303 can determine and store the target device ID based on the device token of the target client 200 at the risk control end.

30 **[0100]** After S106, the method P100 further includes the following steps.

[0101] S123: The central server 303 determines, based on the target device ID, a device risk label associated with the target client 200.

[0102] In a possible implementation, the query result returned by the private server 302 to the central server 303 carries the target device ID and the device risk label of the target client 200.

35 **[0103]** In another possible implementation, the query result returned by the private server 302

to the central server 303 does not carry the target device ID and the device risk label of the target client 200. In this case, the central server 303 can generate the target device ID, and calculate the device risk label of the target client 200.

[0104] In some embodiments, the target device ID and the device risk label are obtained by the central server 303 through calculation based on the hardware information of the target client 200 and the software information of the target client 200.

[0105] The hardware information of the target client 200 and the software information of the target client 200 may be reported by the target client 200 to the central server 303, or may be sent by another server (for example, the first server 301) to the central server 303. This is not limited in this embodiment.

[0106] S107 can be specifically as follows: The central server 303 returns the target device ID to the risk control system 304. In some embodiments, the target device ID carries the device risk label associated with the target client 200.

[0107] S124: The risk control system 304 calculates a risk consultation result of the current operation with reference to the received target device ID, and the user data and the transaction data that are carried in the risk consultation request.

[0108] The risk control system 304 obtains the user data and the transaction data through S122, and obtains the device data (that is, the target device ID and the device risk label) through S107. With reference to the information, the risk control system 304 can obtain the risk consultation result of the current operation through calculation.

[0109] In some embodiments, the risk consultation result can be specifically a risk level of the current operation, for example, three levels: a high-level risk, a medium-level risk, and a low-level risk.

[0110] For example, if the target client 100 hits a device risk label of device modification when participating in a marketing activity, the risk consultation result of the current operation is the high risk; and if the target client 100 hits the device risk label of device modification during login, the risk consultation result of the current operation is the low risk.

[0111] For another example, if the target client 100 hits a device risk label indicating installation of high-risk software at a transaction stage, the risk consultation result of the current operation is the high risk; and if the target client 100 hits the device risk label indicating installation of high-risk software during login, the risk consultation result of the current operation is the low risk.

[0112] S125: The risk control system 304 returns the risk consultation result to the first server 301.

[0113] S126: The first server 301 sends indication information to the target client 200 based

on the risk consultation result, where the indication information is used to indicate the target client 200 to allow the current operation to proceed, perform user identity verification, or intercept the current operation.

[0114] For example, if the risk consultation result is the low risk, the first server 301 can indicate, by using the indication information, the target client 200 to allow the current operation to proceed; if the risk consultation result is the medium risk, the first server 301 can indicate, by using the indication information, the target client 200 to perform user identity verification, to determine, based on a verification result, whether the current operation is allowed to proceed; or if the risk consultation result is the high risk, the first server 301 can indicate, by using the indication information, the target client 200 to intercept the current operation.

[0115] In conclusion, according to the data migration method, the electronic device, and the storage medium provided in this specification, to verify the target client 200 based on the target device ID of the target client 200, the central server 303 first locally queries the target device ID. If the target device ID is not found, the central server 303 further queries the target device ID by using the private server 302. In this way, if the private server 302 stores the target device ID, the central server 303 can obtain the target device ID and store the target device ID in the central server 303. In this manner, in a process of upgrading a data deployment mode of a service provider, device ID data previously stored in the private server 302 can be retrieved, and the existing device ID data in the private server 302 is migrated to the central server 303. Therefore, it is ensured that device IDs used before and after upgrade are consistent, and there is no need to regenerate device IDs for all devices, thereby reducing upgrade costs. In addition, in this manner, the central server 303 can be prevented from mistakenly identifying an old device as a new device as far as possible, thereby avoiding unnecessary disturbance to the target user 100 and improving user experience.

[0116] Another aspect of this specification provides a non-transitory storage medium. The non-transitory storage medium stores at least one group of executable instructions used to perform data migration. When the executable instructions are executed by a processor, the executable instructions instruct the processor to implement the steps of the central server 303 in the data migration method P100 described in this specification. In some possible implementations, aspects of this specification can alternatively be implemented in a form of a program product, including program code. When the program product runs on the electronic device 600, the program code is used to enable the electronic device 600 to perform the steps of the central server 303 in the data migration method P100 described in this specification. The program product configured to implement the above-mentioned method can be a portable compact disc read-only memory (CD-ROM) that includes program code, and can run on the electronic device 600. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium

can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable medium can be a readable signal medium or a readable storage medium. For example, the readable storage medium can be but is not limited to an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus, or device, an infrared system, apparatus, or device, or a semiconductor system, apparatus, or device, or any combination thereof. More specific examples of the readable storage medium include: an electrical connection including one or more conducting wires, a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage component, a magnetic storage component, or any proper combination thereof. The computer-readable storage medium can include a data signal propagated in a baseband or as part of a carrier, and carries readable program code. The data signal propagated in such a way can be in a plurality of forms, and includes but is not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can further be any readable medium other than the readable storage medium, and the readable medium can be used to send, propagate, or transmit a program used by or in combination with an instruction execution system, apparatus, or component. The program code included in the readable storage medium can be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, an optical cable, an RF medium, etc., or any proper combination thereof. The program code for performing operations in this specification can be written in any combination of one or more program design languages. The program design language includes an object-oriented program design language, such as Java or C++, and further includes a conventional procedural program design language, such as a "C" language or a similar program design language. The program code can be completely executed on the electronic device 600, partially executed on the electronic device 600, executed as an independent software package, partially executed on the electronic device 600 and partially executed on a remote electronic device, or completely executed on a remote electronic device.

[0117] In the technical solutions provided in this specification, collection and use of the related hardware parameter of the device comply with related laws and regulations, and do not violate public order and good morals.

[0118] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results

can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

5 [0119] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the above-mentioned detailed disclosure can be presented only in an example manner, and can impose no limitation. Although it is not explicitly stated herein, a person skilled in the art can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be proposed in this specification, and fall within the spirit and scope
10 of the example embodiments of this specification.

[0120] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "one embodiment", "an embodiment", and/or "some embodiments" mean that particular features, structures, or characteristics described with reference to the embodiments can be included in at least one embodiment of this specification. Therefore, it
15 can be emphasized and understood that two or more of "an embodiment", "one embodiment", or "alternative embodiments" referred in parts of this specification do not necessarily indicate the same embodiment. In addition, particular features, structures, or characteristics can be properly combined in one or more embodiments of this specification.

[0121] It should be understood that in the above-mentioned descriptions of the embodiments of this specification, to help understand a feature, for the purpose of simplifying this specification, various features are combined in a single embodiment, accompanying drawing, or description thereof in this specification. However, this does not mean that the combination of these features is necessary. It is entirely possible for a person skilled in the art to mark some devices and understand the devices as separate embodiments when reading this specification. In other words, the
20 embodiments in this specification can also be understood as an integration of a plurality of secondary embodiments. Content of each secondary embodiment is also true when features are less than all features in one of the above-mentioned disclosed embodiments.

[0122] Each patent, patent application, publication of a patent application, and other materials, for example, articles, books, instructions, publications, documents, and products, that are cited in
30 this specification and that are other than any related historical litigation documents, any same historical litigation documents that may be inconsistent or conflict with this document, or any same historical litigation documents that may impose limiting impact on the widest scope of the claims can be incorporated herein by reference and used for all purposes now or later associated with this document. In addition, the terms in this document shall prevail if there is any inconsistency or
35 conflict between the descriptions, definitions, and/or use of the terms associated with any included

material and the descriptions, definitions, and/or use of the terms associated with this document.

[0123] Finally, it should be understood that the principles of the implementation solutions of this specification are described in the implementation solutions of the application disclosed in this specification. Other modified embodiments also fall within the scope of this specification.

- 5 Therefore, the embodiments disclosed in this specification are merely examples and not limitations. A person skilled in the art can use an alternative configuration according to the embodiments of this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

CLAIMS

What is claimed is:

1. A data migration method, used to migrate device identifier data stored in a private server to a central server, wherein the central server is configured to provide data support for a client in place of the private server, and the method is applied to the central server and comprises:
 - receiving a verification request sent by a requesting device, wherein the verification request is used to request to perform verification based on a target device identifier of a target client;
 - sending a query request to the private server when the target device identifier is not found, wherein the query request is used to request to query the target device identifier;
 - receiving a query result sent by the private server, and storing the target device identifier; and
 - sending a verification result in response to the verification request to the requesting device.
2. The method according to claim 1, wherein the verification request carries a device token of the target client.
3. The method according to claim 2, wherein the sending a query request to the private server when the target device identifier is not found comprises:
 - performing a query based on the device token, and determining that the target device identifier associated with the device token is not found; and
 - sending the query request to the private server, wherein the query request carries the device token.
4. The method according to claim 2, wherein the verification request further carries hardware information of the target client and software information of the target client.
5. The method according to claim 4, wherein the receiving a query result sent by the private server, and storing the target device identifier comprises:
 - determining that the query result carries the target device identifier, storing the target device identifier, and associating the target device identifier with the device token; or
 - determining that the query result does not carry the target device identifier, generating the target device identifier based on the hardware information and the software information, and associating the target device identifier with the device token.
6. The method according to claim 1, wherein the requesting device comprises the target client, and the verification request comprises a device identity verification request;
 - the receiving a verification request sent by a requesting device comprises:
 - receiving the device identity verification request sent by the target client; and
 - the sending a verification result in response to the verification request to the requesting device comprises:

performing the device identity verification on the target client based on the target device identifier to generate a device identity verification result; and

returning the device identity verification result to the target client.

7. The method according to claim 1, wherein the requesting device comprises a risk control system, and the verification request comprises a device risk verification request;

the receiving a verification request sent by a requesting device comprises:

receiving the device risk verification request sent by the risk control system; and

the sending a verification result in response to the verification request to the requesting device comprises:

determining, based on the target device identifier, a device risk label associated with the target client; and

returning the device risk label to the risk control system.

8. The method according to claim 7, wherein the target device identifier carries the device risk label associated with the target client.

9. The method according to claim 8, wherein the target device identifier and the device risk label are obtained through calculation based on hardware information of the target client and software information of the target client.

10. An electronic device, comprising:

at least one storage medium, storing at least one instruction set used to perform data migration;

and

at least one processor, communicatively connected to the at least one storage medium, wherein

when the electronic device runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an instruction of the at least one instruction set:

receiving a verification request sent by a requesting device, wherein the verification request is used to request to perform verification based on a target device identifier of a target client;

sending a query request to the private server when the target device identifier is not found, wherein the query request is used to request to query the target device identifier;

receiving a query result sent by the private server, and storing the target device identifier; and sending a verification result in response to the verification request to the requesting device.

11. The electronic device according to claim 10, wherein the verification request carries a device token of the target client.

12. The electronic device according to claim 11, wherein to send the query request to the private server when the target device identifier is not found, the at least one processor performs

the following operations:

performing a query based on the device token, and determining that the target device identifier associated with the device token is not found; and

5 sending the query request to the private server, wherein the query request carries the device token.

13. The electronic device according to claim 11, wherein the verification request further carries hardware information of the target client and software information of the target client.

14. The electronic device according to claim 13, wherein to receive the query result sent by the private server, and store the target device identifier, the at least one processor performs the
10 following operations:

determining that the query result carries the target device identifier, storing the target device identifier, and associating the target device identifier with the device token; or

determining that the query result does not carry the target device identifier, generating the target device identifier based on the hardware information and the software information, and
15 associating the target device identifier with the device token.

15. The electronic device according to claim 10, wherein the requesting device comprises the target client, and the verification request comprises a device identity verification request;

to receive the verification request sent by the requesting device, the at least one processor performs the following operation:

20 receiving the device identity verification request sent by the target client; and

to send the verification result in response to the verification request to the requesting device, the at least one processor performs the following operations:

performing the device identity verification on the target client based on the target device identifier to generate a device identity verification result; and

25 returning the device identity verification result to the target client.

16. The electronic device according to claim 10, wherein the requesting device comprises a risk control system, and the verification request comprises a device risk verification request;

to receive the verification request sent by the requesting device, the at least one processor performs the following operation:

30 receiving the device risk verification request sent by the risk control system; and

to send the verification result in response to the verification request to the requesting device, the at least one processor performs the following operations:

determining, based on the target device identifier, a device risk label associated with the target client; and

35 returning the device risk label to the risk control system.

17. The electronic device according to claim 16, wherein the target device identifier carries the device risk label associated with the target client.

18. The electronic device according to claim 17, wherein the target device identifier and the device risk label are obtained through calculation based on hardware information of the target client and software information of the target client.

19. A computer-readable non-transitory storage medium, wherein the computer-readable non-transitory storage medium stores at least one instruction set, and the at least one instruction set is executed by at least one processor to implement the method according to any one of claims 1 to 9.