Identity Verification Method and Device and Electronic Device

Technical Field

[01] Embodiments of the present specification relate to the technical field of the Internet, and in particular, to a method and an apparatus for identity verification and an electronic device.

Background

[02] Along with the continuous development of the Internet, there are more and more scenarios in which electronic passes or electronic keys are realized through mobile terminals, such as mobile payment, hotel check-in, punch-in at work, smart locks, and the like.

[03] Taking a smart lock as an example, a user may use a mobile terminal to open the smart lock. For example, the smart lock needs to verify the identity of the user. Only after the identity verification is successful, can the mobile terminal obtain an electronic pass or an electronic key. In other words, before the mobile terminal obtains an electronic pass or an electronic key, a device needs to verify the identity of the user. It can be seen that, since the device needs to perform identity verification, the device needs to have some software and/or hardware requirements. For example, when face recognition is used to perform identity verification, the device needs to have some computation capabilities in the software aspect and have a camera in the hardware aspect.

[04] An identity verification solution applicable to a device that does not have high performance requirements needs to be provided.

Summary

[05] Embodiments of the present specification provide a method and an apparatus for identity verification and an electronic device.

[06] According to a first aspect of the embodiments of the present specification, a method for identity verification is provided, comprising:

[07] a mobile terminal obtaining a device identifier of a device, and uploading the obtained device identifier to a server;

[08] the server performing validity verification on the device identifier, and returning a result of the validity verification to the mobile terminal;

[09] in the situation where the received result of the validity verification returned by the server is valid, the mobile terminal collecting identity feature information of a user, and uploading the collected identity feature information to the server; and

[10] the server performing identity verification on the identity feature information, and in the situation where the identity verification is successful, issuing an electronic pass to the mobile terminal, wherein the electronic pass is used to obtain a service provided by the device.

[11] According to a second aspect of the embodiments of the present specification, a method for identity verification is provided, the method applied on a mobile terminal and comprising:

[12] obtaining a device identifier of a device;

[13] uploading the device identifier to a server, causing the server to perform validity verification on the device identifier;

[14] in the situation where a received result of the validity verification returned by the server is valid, collecting identity feature information of a user;

[15] uploading the identity feature information to the server, causing the server to perform identity verification on the identity feature information; and

[16] obtaining an electronic pass issued by the server when the identity verification is successful, wherein the electronic pass is used to obtain a service provided by the device.

[17] According to a third aspect of the embodiments of the present specification, an apparatus for identity verification is provided, the apparatus applied on a mobile terminal and comprising:

[18] a first obtaining unit configured to obtain a device identifier of a device;

[19] a first uploading unit configured to upload the device identifier to a server, causing the server to perform validity verification on the device identifier;

[20] a collecting unit configured to collect, in the situation where a received result of the validity verification returned by the server is valid, identity feature information of a user;

[21] a second uploading unit configured to upload the identity feature information to the server, causing the server to perform identity verification on the identity feature information; and

[22] a second obtaining unit configured to obtain an electronic pass issued by the server when the identity verification is successful, wherein the electronic pass is used to obtain a service provided by the device.

[23] According to a fourth aspect of the embodiments of the present specification, an electronic device is provided, comprising:

[24] a processor; and

[25] a memory configured to store instructions executable by the processor,

[26] wherein the processor is configured to implement the method for identity verification according to any one of the above.

[27] According to the embodiments of the present specification, identity verification that has been originally performed by a device is now performed by a server, which may lower software and hardware requirements of the device, and the embodiments may then also be applicable to a device that does not have high performance.

Brief Description of the Drawings

[28] FIG. 1 is a concept diagram of a system architecture for realizing identity verification according to some embodiments of the present specification;

[29] FIG. 2 is a flow chart of a method for identity verification according to some embodiments of the present specification;

[30] FIG. 3 is a flow chart of a method for identity verification according to some embodiments of the present specification;

[31] FIG. 4 is a hardware structural diagram of an apparatus for identity verification according to some embodiments of the present specification; and

[32] FIG. 5 is a schematic diagram of modules of an apparatus for identity verification according to some embodiments of the present specification.

Detailed Description

[33] Example embodiments will be described in detail below, and the examples of the embodiments are illustrated in the accompanying drawings. When the description below involves the accompanying drawings, identical numbers in different drawings represent identical or similar elements, unless otherwise indicated. The implementation manners described in the following example embodiments do not represent all implementation manners consistent with the present specification. Conversely, they are merely examples of apparatuses and methods consistent with some aspects of the present specification as described in detail in the appended claims.

[34] Terms used in the present specification are only for the purpose of describing particular embodiments, rather than limiting the present specification. “A,” “the,” and “said” in the singular form used in the present specification and the appended claims are intended to include the plural forms as well, unless clearly indicated in the context to have other meanings. It should also be understood that the term “and/or” used herein refers to and includes any or all possible combinations of one or more associated listed items.

[35] It should be understood that terms such as first, second, third, etc. may be used in the present specification to describe various information, but the information shall not be limited to these terms. These terms are only used to differentiate information of the same type from another. For example, without departing from the scope of the present specification, first

information may also be referred to as second information, and similarly, second information may also be referred to as first information. Depending on the context, the term “if” used herein may be construed as “when…” or “at the time of…” or “in response to determining.”

[36] As described above, on the one hand, since the device needs to perform identity verification, the device needs to have some software and/or hardware requirements. For example, when face recognition is used to perform identity verification, the device needs to have some computation capabilities in the software aspect and have a camera in the hardware aspect. On the other hand, there are strict energy consumption requirements when some devices are designed, such as low power devices powered by batteries. These devices generally adopt low power modules, and thus cannot meet the demand for long-term complex computation. Taking smart locks as an example again, smart locks are generally powered by batteries, and low power modules are adopted to achieve long-term use.

[37] The present specification may involve one or more systems. FIG. 1 is referenced in the following. A concept diagram of an example architecture of a system applicable in the present specification is illustrated, and the concept diagram of the architecture of the system may comprise a device 11, a mobile terminal 12, and a server 13.

[38] The device 11 may refer to a device for which an electronic pass or an electronic key is required. The device corresponds to various devices in various scenarios. For example, in the scenario of hotel check-in, the device may be a self-service terminal for check-in, and in the scenario of opening a lock, the device may be a smart lock.

[39] The mobile terminal 11 may refer to a client used by a user. The client may refer to a terminal device installed with an application, such as a mobile phone installed with an application APP.

[40] The server 13 may refer to an application server, a server cluster, or a cloud platform constructed based on a server cluster, in communication with the device 11 and the mobile terminal 12. The server 13 may be used for identity verification.

[41] In example applications, when a user needs to obtain a service provided by the device 11, the mobile terminal 12 may obtain a device identifier of the device 11 and collect identity feature information of the user, which are verified by the server 13, and ultimately, an electronic pass issued by the server 13 is obtained. Then, the mobile terminal 12 may obtain the service provided by the device 11 based on the electronic pass.

[42] Embodiments of a method for identity verification according to the present specification will be described below with reference to the example shown in FIG. 2. As shown in FIG. 2, the method may comprise the following steps.

[43] In Step 110, a mobile terminal obtains a device identifier of a device, and uploads the obtained device identifier to a server.

[44] In some embodiments, the device identifier comprises a static device identifier and/or a dynamic device identifier.

[45] Taking a static device identifier as an example, the device identifier is unique, i.e., each device may correspond to one unique device identifier, such as a device serial number, an ID, and the like when the device leaves the factory.

[46] Taking a dynamic device identifier as an example, the device identifier may comprise a dynamic token, such as token. The dynamic token may refer to an encrypted character string, which may be generated by a preset algorithm. Generally, the dynamic token changes dynamically. For example, the dynamic token obtained by the mobile terminal each time is different, or the device periodically generates a new token.

[47] In some embodiments, the mobile terminal obtaining a device identifier of a device comprises:

[48] the mobile terminal obtaining, by establishing short-range wireless communication with the device, a device identifier transmitted by the device.

[49] For example, the short-range wireless communication comprises one of Bluetooth communication, infrared communication, wireless local area network, WI-FI, Ultra-Wide Band communication, Zigbee communication, and near-field communication.

[50] In some embodiments, a module applicable for short-range wireless communication may be integrated in the device, for example, a Bluetooth module, an infrared (IrDA) module, a wireless local area network (WI-FI or WLAN, mostly adopting the 802.11-series protocols) module, a WI-FI Direct module, a Ultra-Wide Band module, a Zigbee module, and a near-field communication (NFC) module, so as to achieve short-range receiving and transmitting of wireless signals. Similarly, the same module applicable for short-range wireless communication may also be integrated in the mobile terminal.

[51] In some embodiments, the Bluetooth technology is taken as an example for description.

[52] As a short-range wireless communication technology for replacing data cables, the Bluetooth technology can support point to point and point to multi-point communications, thereby achieving fast and convenient information exchange between devices.

[53] A device may transmit, via a Bluetooth module, a broadcasting signal containing its own identifier (UUID). According to the Bluetooth technology, the Bluetooth module may be identified through a Universally Unique Identifier (UUID). Each UUID temporally and spatially ensures the uniqueness of a Bluetooth service. A UUID may be, for example, in a

short form (16 or 32 bits) or a long form (128 bits). A UUID may be transmitted via a Bluetooth broadcasting signal.

[54] Preferably, the Bluetooth Low Energy (BLE) technology may be adopted as the Bluetooth technology. More preferably, the iBeacon technology may be adopted. The iBeacon technology is a technology developed based on BLE with characteristics of low cost, extensive expansion, and flexible customization. The iBeacon technology may enable a smart phone or other apparatuses to execute corresponding commands within a sensing range of an iBeacon base station. For example, in the embodiments, a payment collection device may be an iBeacon base station. iBeacon has been provided on the OS for mobile devices (iOS7) released by Apple, Inc. in September 2013.

[55] Typically, there are two BLE communication manners: advertising and connecting. Advertising is a one-way sending mechanism and one of the broadcasting modes. A device to be searched (e.g., an iBeacon base station, a payment collection device) may send a data packet at a time interval of 20 ms to 10 s. A battery is consumed faster when a shorter time interval is used, and it is faster to find the device. The data packet length is at most 47 bytes, which may typically consist of the following parts:

[56] 1 byte: preamble (1 byte for the preamble)

[57] 4 bytes: access address (4 bytes for address)

[58] 39 bytes: advertising channel PDU (39 bytes for PDU data packet)

[59] 3 bytes: CRC (3 bytes for CRC data check)

[60] A BLE device may operate in a single and non-connectable advertising mode (in this mode, all information is included in an advertising data packet); in addition, a BLE device may also operate in a connectable mode (i.e., the connecting mode).

[61] The device in the embodiments may operate in a single and non-connectable advertising mode. In this way, the device mainly sends out its own device identifier in the advertising mode. For example, the device identifier of the device may be carried in the above-described PDU data packet.

[62] The mobile terminal may find the UUID of the device by scanning Bluetooth signals being broadcast. For example, an application installed on the mobile terminal may drive the mobile terminal to scan wireless signals by calling a low level Application Programming Interface (API). Then, a wireless signal sent by the device, e.g., a Bluetooth signal sent in the advertising mode, may be scanned. Since the Bluetooth signal sent by the device includes its own device identifier information UUID, the mobile terminal may find this UUID from the scanned Bluetooth broadcasting signal.

[63] In some embodiments, the mobile terminal obtaining a device identifier of a device, for example, comprises:

[64] the mobile terminal obtaining, by scanning a graphic code provided by the device, a device identifier of the device.

[65] In the embodiments, the device may display a graphic code including a device identifier. A module for scanning graphic codes, such as a camera, a code scanner, and the like, may be integrated in the mobile terminal, so as to scan the graphic code to obtain the device identifier.

[66] In some embodiments, the camera is taken as an example for description.

[67] The mobile terminal may turn on the camera. When the camera collects an image of the graphic code, the device identifier included in the graphic code may be obtained through analysis by local analysis software on the mobile terminal or a remote server.

[68] In some embodiments, the graphic code may comprise a QR code, a barcode, and the like.

[69] In Step 120, the server performs validity verification on the device identifier, and returns a result of the verification to the mobile terminal.

[70] In some embodiments, the server performing validity verification on the device identifier may, for example, comprise:

[71] determining whether the device corresponding to the device identifier has been registered on the server;

[72] in the situation where the device corresponding to the device identifier has been registered on the server, determining that the result of the verification is valid.

[73] Typically, the manufacturer of the device may complete the registration on the server when the device leaves the factory. As a result, the server may store a correspondence relationship between the device identifier and the device and also have a record of registration.

[74] In some embodiments, for a dynamic device identifier, the server may have the same algorithm as the algorithm on the device for generating a dynamic token. Through the algorithm, the server may verify whether a dynamic token uploaded by the mobile terminal is correct. In the situation where the dynamic token is correct, the server determines that the result of the verification is valid.

[75] After the server determines the result of the verification, the server may return the result of the verification to the mobile terminal.

[76] In Step 130, in the situation where the received result of the verification returned by the server is valid, the mobile terminal collects identity feature information of a user, and uploads the collected identity feature information to the server.

[77] In some embodiments, the identity feature information may comprise biometric information.

[78] The biometric information comprises at least one of a fingerprint, a palmprint, an iris, an eyeprint, a face, a sound wave, and a brain wave. Correspondingly, a module for collecting biometric information needs to be integrated in the mobile terminal. For example, a user's face image may be collected through a camera, a user's fingerprint may be collected through a fingerprint module, a user's sound wave information may be collected through a sound wave module, and the like.

[79] In some embodiments, the identity feature information may also comprise password information input by a user.

[80] In Step 140, the server performs identity verification on the identity feature information, and in the situation where the verification is successful, issues an electronic pass to the mobile terminal, wherein the electronic pass is used to obtain a service provided by the device.

[81] In the present embodiment, the server may store identity feature information pre-stored by the user. Upon receiving the identity feature information uploaded by the mobile terminal, the server may compare the identity feature information with the pre-stored identity feature information. If the identity feature information is consistent with the pre-stored identity feature information, it indicates that the current user is the user himself or herself; otherwise, it indicates that the current user is not the user himself or herself.

[82] In the situation where the verification is successful, the server may issue an electronic pass to the mobile terminal. The electronic pass may be approved by the device, and the mobile terminal may use the electronic pass to obtain a service provided by the device.

[83] Taking a smart lock scenario as an example, after the mobile terminal obtains the electronic pass, the mobile terminal may open the smart lock by using the electronic pass.

[84] Taking a hotel check-in scenario as an example, after the mobile terminal obtains the electronic pass, the mobile terminal may complete check-in by using the electronic pass.

[85] According to the embodiments of the present specification, identity verification that has been originally performed by a device is now performed by a server, which may lower software and hardware requirements of the device and the embodiments may then also be applicable to a device that does not have high performance. On the other hand, whether the

current user is the user himself or herself may be determined through the identity verification, which prevents impersonation and improves the reliability.

[86] In some embodiments, the mobile terminal using the electronic pass may be as follows.

[87] The mobile terminal sends the electronic pass to the device, which may, referring to Step 110, be implemented based on short-range wireless communication. Then, the device may locally perform validation on the electronic pass and provide services only after the validation is successful. Alternatively, the device may upload the electronic pass to the server for the server to validate the electronic pass, and the services may be provided when a result of the validation returned by the server is valid.

[88] Method embodiments with a mobile terminal as the main body according to the present specification are described below with reference to FIG. 3. The embodiments may correspond to FIG. 2.

[89] In Step 210, obtain a device identifier of a device;

[90] In Step 220, upload the device identifier to a server, causing the server to perform validity verification on the device identifier;

[91] In Step 230, in the situation where a received result of the verification returned by the server is valid, collect identity feature information of a user;

[92] In Step 240, upload the identity feature information to the server, causing the server to perform identity verification on the identity feature information; and

[93] In Step 250, obtain an electronic pass issued by the server when the identity verification is successful, wherein the electronic pass is used to obtain a service provided by the device.

[94] In some embodiments, the obtaining a device identifier of a device may, for example, comprise:

[95] obtaining, by establishing short-range wireless communication with the device, the device identifier transmitted by the device;

[96] or,

[97] obtaining, by scanning a graphic code provided by the device, the device identifier of the device.

[98] In some embodiments, the short-range wireless communication comprises one of Bluetooth communication, infrared communication, wireless local area network, WI-FI, UltraWide Band communication, Zigbee communication, and near-field communication.

[99] In some embodiments, the identity feature information comprises biometric information.

[100] In some embodiments, the biometric information comprises at least one of a fingerprint, a palmprint, an iris, an eyeprint, a face, a sound wave, and a brain wave.

[101] In some embodiments, the device identifier comprises a static device identifier and/or a dynamic device identifier.

[102] In some embodiments, the dynamic device identifier comprises a dynamic token.

[103] Corresponding to the above-described method embodiments for identity verification, the present specification further provides embodiments of an apparatus for identity verification. The apparatus embodiment may be implemented through software, hardware, or a combination of software and hardware. Take software implementation as an example, an apparatus in the sense of logics is formed by a processor of a device where the apparatus is located reading corresponding computer program instructions from a non-volatile storage into the memory. From the perspective of the hardware layer, a hardware structure of a device where the apparatus for identity verification is located according to the present specification may, as shown in FIG. 4, comprise a processor, a network interface, a memory, and a non-volatile storage. In addition, the device where the apparatus is located in the embodiment may further comprise other hardware typically according to actual functions of the identity verification, which will not be elaborated herein.

[104] FIG. 5 is a schematic diagram of modules of an apparatus for identity verification according to some embodiments of the present specification. The apparatus comprises:

[105] a first obtaining unit 310 configured to obtain a device identifier of a device;

[106] a first uploading unit 320 configured to upload the device identifier to a server, causing the server to perform validity verification on the device identifier;

[107] a collecting unit 330 configured to collect, in the situation where a received result of the validity verification returned by the server is valid, identity feature information of a user;

[108] a second uploading unit 340 configured to upload the identity feature information to the server, causing the server to perform identity verification on the identity feature information; and

[109] a second obtaining unit 350 configured to obtain an electronic pass issued by the server when the identity verification is successful, wherein the electronic pass is used to obtain a service provided by the device.

[110] In an optional embodiment,

[111] the first obtaining unit 310 may, for example, comprise

[112] a first obtaining sub-unit configured to obtain, by establishing short-range wireless communication with the device, a device identifier transmitted by the device;

[113] alternatively,

[114] a second obtaining sub-unit configured to obtain, by scanning a graphic code provided by the device, a device identifier of the device.

[115] In an optional embodiment,

[116] the short-range wireless communication comprises one of Bluetooth communication, infrared communication, wireless local area network, WI-FI, Ultra Wide Band communication, Zigbee communication, and near-field communication.

[117] In an optional embodiment,

[118] the identity feature information comprises biometric information.

[119] In an optional embodiment,

[120] the biometric information comprises at least one of a fingerprint, a palmprint, an iris, an eyeprint, a face, a sound wave, and a brain wave.

[121] In an optional embodiment,

[122] the device identifier comprises a static device identifier and/or a dynamic device identifier.

[123] In an optional embodiment,

[124] In some embodiments, the dynamic device identifier comprises a dynamic token.

[125] The system, apparatus, module, or unit elaborated in the embodiments can, for example, be achieved by a computer chip or entity or by a product having a function. One typical implementation device is a computer, and an exemplary form of the computer can be a personal computer, a laptop computer, a cellular telephone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email receiving and transmitting device, a game console, a tablet computer, a wearable device, or a combination of any of the above devices.

[126] For detailed implementation processes of functions and roles of the units in the above-described apparatus, the implementation processes of corresponding steps in the above-described method may be referenced, which will not be elaborated again herein.

[127] Since the apparatus embodiments substantially correspond to the method embodiments, the description of relevant parts of the method embodiments may be referenced for related parts. The above-described apparatus embodiments are merely examples, wherein the units described as separate parts may or may not be physically separated. Parts displayed as units may or may not be physical units, i.e., may be located at one place or may be distributed over a plurality of network units. Some or all of the modules can be selected according to actual needs to achieve the objectives of the solutions of the present specification. One of ordinary

skill in the art can understand and implement the solutions of the present specification without creative effort.

[128] FIG. 5 schematically describes internal functional modules and structure of the apparatus for identity verification above, and the essential executing entity of the apparatus may be an electronic device, comprising:

[129] a processor; and

[130] a memory configured to store instructions executable by the processor,

[131] obtaining a device identifier of a device;

[132] uploading the device identifier to a server, causing the server to perform validity verification on the device identifier;

[133] in the situation where a received result of the validity verification returned by the server is valid, collecting identity feature information of a user;

[134] uploading the identity feature information to the server, causing the server to perform identity verification on the identity feature information; and

[135] obtaining an electronic pass issued by the server when the identity verification is successful, wherein the electronic pass is used to obtain a service provided by the device.

[136] Optionally, the obtaining a device identifier of a device may, for example, comprise:

[137] obtaining, by establishing short-range wireless communication with the device, the device identifier transmitted by the device;

[138] or,

[139] obtaining, by scanning a graphic code provided by the device, the device identifier of the device.

[140] Optionally, the short-range wireless communication comprises one of Bluetooth communication, infrared communication, wireless local area network, WI-FI, Ultra-Wide Band communication, Zigbee communication, and near-field communication.

[141] Optionally, the identity feature information comprises biometric information.

[142] Optionally, the biometric information comprises at least one of a fingerprint, a palmprint, an iris, an eyeprint, a face, a sound wave, and a brain wave.

[143] Optionally, the device identifier comprises a static device identifier and/or a dynamic device identifier.

[144] Optionally, the dynamic device identifier comprises a dynamic token.

[145] In the above-described embodiments of the electronic device, it should be understood that the processor may be a Central Processing Unit (English: Central Processing Unit, or CPU in short), or may be other general-purpose processors, digital signal processors (English:

Digital Signal Processor, or DSP in short), Application Specific Integrated Circuits (English: Application Specific Integrated Circuit, or ASIC in short), and the like. The general-purpose processor may be a micro-processor, or the processor may be any conventional processor, while the above-described memory may be a read-only memory (English: read-only memory, or ROM in abbreviation), a random access memory (English: random access memory, or RAM in short), a flash memory, a hard drive, or a solid-state drive. Steps of the methods disclosed in combination with the embodiments of the present specification may be directly embodied as being executed by a hardware processor or executed by a combination of hardware and software modules in the processor.

[146] All the embodiments in the present specification are described in a progressive manner, the same or similar parts between the various embodiments may refer to each other, and each embodiment focuses on the differences from the other embodiments. In particular, since the electronic device embodiments are substantially similar to the method embodiments, the electronic device embodiments are described in a relatively simple manner, and the description of relevant parts of the method embodiments may be referenced for related parts.

[147] It will be easy for those skilled in the art to conceive, after considering the present specification and practicing the inventions disclosed here, of other implementation solutions of the present specification. The present specification intends to cover any modifications, uses, or adaptive variations of the present specification. These modifications, uses, or adaptive variations comply with the general principles of the present specification, and comprise common general knowledge or conventional technical means in the art that are not disclosed in the present specification. The present specification and embodiments may be only deemed to be exemplary, and the true scope and spirit are pointed out in the claims below.

[148] It should be understood that the present specification is not limited to the accurate structure described above and illustrated in the accompanying drawings, and the present specification may be subject to various modifications and variations without departing from the scope of the present specification. The scope of the present specification shall be limited only by the appended claims.

What is claimed is:

1. A method for identity verification, comprising:

a mobile terminal obtaining a device identifier of a device, and uploading the obtained device identifier to a server;

the server performing validity verification on the device identifier, and returning a result of the validity verification to the mobile terminal;

in the situation where the received result of the validity verification returned by the server is valid, the mobile terminal collecting identity feature information of a user, and uploading the collected identity feature information to the server; and

the server performing identity verification on the identity feature information, and in the situation where the identity verification is successful, issuing an electronic pass to the mobile terminal, wherein the electronic pass is used to obtain a service provided by the device.

2. A method for identity verification, the method applied on a mobile terminal and comprising:

obtaining a device identifier of a device;

uploading the device identifier to a server, causing the server to perform validity verification on the device identifier;

in the situation where a received result of the validity verification returned by the server is valid, collecting identity feature information of a user;

uploading the identity feature information to the server, causing the server to perform identity verification on the identity feature information; and

obtaining an electronic pass issued by the server when the identity verification is successful, wherein the electronic pass is used to obtain a service provided by the device.

3. The method according to claim 2, wherein the obtaining a device identifier of a device comprises:

obtaining, by establishing short-range wireless communication with the device, the device identifier transmitted by the device;

or,

obtaining, by scanning a graphic code provided by the device, the device identifier of the device.

4. The method according to claim 3, wherein the short-range wireless communication comprises one of Bluetooth communication, infrared communication, wireless local area network, WI-FI, Ultra-Wide Band communication, Zigbee communication, and near-field communication.

5. The method according to claim 2, wherein the identity feature information comprises biometric information.

6. The method according to claim 5, wherein the biometric information comprises at least one of a fingerprint, a palmprint, an iris, an eyeprint, a face, a sound wave, and a brain wave.

7. The method according to claim 2, wherein the device identifier comprises a static device identifier and/or a dynamic device identifier.

8. The method according to claim 7, wherein the dynamic device identifier comprises a dynamic token.

9. An apparatus for identity verification, comprising:

a first obtaining unit configured to obtain a device identifier of a device;

a first uploading unit configured to upload the device identifier to a server, causing the server to perform validity verification on the device identifier;

a collecting unit configured to collect, in the situation where a received result of the validity verification returned by the server is valid, identity feature information of a user;

a second uploading unit configured to upload the identity feature information to the server, causing the server to perform identity verification on the identity feature information; and

a second obtaining unit configured to obtain an electronic pass issued by the server when the identity verification is successful, wherein the electronic pass is used to obtain a service provided by the device.

10. An electronic device, comprising:

a processor; and

a memory configured to store instructions executable by the processor,

wherein the processor is configured to implement the method according to any one of claims 1-8.