DEVICE CONFIGURATION METHOD, APPARATUS AND SYSTEM

The present application claims priority to Chinese Patent Application No. 201710039829.6, filed on January 19, 2017 and entitled "DEVICE CONFIGURATION METHOD, APPARATUS AND SYSTEM," which is incorporated herein by reference in its entirety.

Technical Field

The present application relates to the field of intelligent device technology, and, more particularly, to a device configuration method, a device configuration apparatus, and a device configuration system.

Background

Intelligent devices are applied more and more frequently in the related art. For example, in an enterprise scenario, an intelligent entrance guard, an intelligent attendance machine, an intelligent conference terminal and so on are widely used to improve the work efficiency within an enterprise. By taking the intelligent attendance machine as an example, attendance data of enterprise members within the enterprise is involved and financial management, personnel control and so on need to be performed according to the attendance data. Thus, only an administrative user within the enterprise has an administrative permission of the intelligent attendance machine, and may configure a wireless network used by the intelligent attendance machine, a bound enterprise or department, attendance rules and so on.

However, as the intelligent attendance machine in the related art is provided with a physical key such as "RESET," the intelligent attendance machine will be reset no matter who triggers the physical key, thereby resulting in extremely high hidden security dangers.

Summary

In view of the foregoing, a device configuration method, a device configuration apparatus, and a device configuration system are provided in the present application, which may configure a device based on software, thus eliminating hidden security dangers of a physical key while simplifying configuration operations.

To achieve the foregoing objective, the following technical solutions are provided in the present application.

According to a first aspect of the present application, a device configuration system is provided, including: a user device of a preset administrative user, a server, and an intelligent device, wherein:

the user device is configured to send a binding request for the intelligent device to the server, the binding request being used for instructing the server to bind the intelligent device;

the server is configured to record an administrative permission for the administrative user to the intelligent device in the process of binding; and

the intelligent device is configured to, when a near-field communication signal from any user is received, identify the identity of the user; and when the user is determined as the administrative user, establish a near-field communication connection with an electronic device of the user to allow the user to configure the intelligent device.

According to a second aspect of the present application, a device configuration method is provided, including:

sending, by a user device, a near-field communication signal including identity information of a logged-in user to an intelligent device to instruct the intelligent device to identify the identity of the logged-in user; and

determining, by the user device, according to a response of the intelligent device to the near-field communication signal, that the intelligent device determines the logged-in user as an administrative user corresponding to the intelligent device, and establishing a near-field communication connection with the intelligent device to configure the intelligent device.

According to a third aspect of the present application, a device configuration method is provided, including:

acquiring, by a server, identity authentication information of an administrative user corresponding to a preset intelligent device when a configuration request sent by a preset user for the intelligent device is received; and

returning, by the server, the identity authentication information to the preset user such that the preset user sends a near-field communication signal including the identity authentication information to the intelligent device, wherein the near-field communication signal is used for instructing the intelligent device to determine according to the identity authentication information that the preset user has an administrative permission, and establish a near-field communication connection with a sender device of the near-field

communication signal to allow the sender device to configure the intelligent device.

According to a fourth aspect of the present application, a device configuration method is provided, including:

acquiring, by an intelligent device, identity information included in a near-field communication signal sent by any use when the near-field communication signal is received;

identifying, by the intelligent device, the identity of the user according to the identity information; and

when the user is determined as an administrative user corresponding to the intelligent device, establishing, by the intelligent device, a near-field communication connection with an electronic device used by the user to allow the electronic device to configure the intelligent device.

According to a fifth aspect of the present application, a device configuration apparatus is provided, including:

a sending unit configured to make a user device send a near-field communication signal including identity information of a logged-in user to an intelligent device to instruct the intelligent device to identify the identity of the logged-in user; and

an identifying unit configured to make the user device determine, according to a response of the intelligent device to the near-field communication signal, that the intelligent device determines the logged-in user as an administrative user corresponding to the intelligent device, and establish a near-field communication connection with the intelligent device to configure the intelligent device.

According to a sixth aspect of the present application, a device configuration apparatus is provided, including:

an acquisition unit configured to make a server acquire identity authentication information of an administrative user corresponding to a preset intelligent device when a configuration request sent by a preset user for the intelligent device is received; and

a returning unit configured to make the server return the identity authentication information to the preset user such that the preset user sends a near-field communication signal including the identity authentication information to the intelligent device, wherein the near-field communication signal is used for instructing the intelligent device to determine according to the identity authentication information that the preset user has an administrative permission, and establish a near-field communication connection with a

sender device of the near-field communication signal to allow the sender device to configure the intelligent device.

According to a seventh aspect of the present application, a device configuration apparatus is provided, including:

an acquisition unit configured to make an intelligent device acquire identity information included in a near-field communication signal sent by any user when the near-field communication signal is received;

an identifying unit configured to make the intelligent device identify the identity of the user according to the identity information; and

an establishing unit configured to, when the user is determined as an administrative user corresponding to the intelligent device, make the intelligent device establish a near-field communication connection with an electronic device used by the user to allow the electronic device to configure the intelligent device.

As shown from the foregoing technical solutions, in the present application, an intelligent device identifies the identity of a user who controls it, so that only a user having an administrative permission is allowed to establish a near-field communication connection between a used electronic device and the intelligent device and perform a configuration operation, thus avoiding security dangers when an irrelevant person triggers a related physical key in a hardware mode and enhancing the security of the configuration operation.

Brief Description of the Drawings

FIG. 1 is a schematic structural diagram of an intelligent attendance machine provided with a configuration key in the related art.

FIG. 2 is a flowchart of a device configuration method based on a user side according to an exemplary embodiment of the present application.

FIG. 3 is a flowchart of a device configuration method based on a server side according to an exemplary embodiment of the present application.

FIG. 4 is a flowchart of a device configuration method based on an intelligent device side according to an exemplary embodiment of the present application.

FIG. 5 is a schematic structural diagram of a device configuration system according to an exemplary embodiment of the present application.

FIG. 6 is a flowchart of a device configuration method according to an exemplary embodiment of the present application.

FIG. 7 is a schematic structural diagram of an intelligent attendance machine according to an exemplary embodiment of the present application.

FIG. 8 is a schematic diagram of a page for binding an intelligent attendance machine according to an exemplary embodiment of the present application.

FIG. 9 is a schematic structural diagram of an electronic device based on a user side according to an exemplary embodiment of the present application;

FIG. 10 is a block diagram of a device configuration apparatus based on a user side according to an exemplary embodiment of the present application.

FIG. 11 is a schematic structural diagram of an electronic device based on a server side according to an exemplary embodiment of the present application.

FIG. 12 is a block diagram of a device configuration apparatus based on a server side according to an exemplary embodiment of the present application;

FIG. 13 is a schematic structural diagram of an electronic device based on an intelligent device side according to an exemplary embodiment of the present application.

FIG. 14 is a block diagram of a device configuration apparatus based on an intelligent device side according to an exemplary embodiment of the present application.

Detailed Description

Intelligent devices are applied more and more frequently in the related art. For example, in an enterprise scenario, an intelligent entrance guard, an intelligent attendance machine, an intelligent conference terminal and so on are being widely used to improve the work efficiency within an enterprise. By taking the intelligent attendance machine as an example, attendance data of enterprise members within the enterprise is involved and financial management, personnel control and so on need to be performed according to the attendance data. Thus, only an administrative user within the enterprise has an administrative permission to the intelligent attendance machine, and may set a wireless network used by the intelligent attendance machine, a bound enterprise or department, attendance rules and so on.

In general, the administrative user needs to be authenticated no matter whether the administrative user directly makes editing on the intelligent attendance machine or the electronic device administrative user edits the intelligent attendance machine through a client terminal on an electronic device when the electronic device used by the administrative user and the intelligent attendance machine run the same client terminal of

a preset communication application. An editing operation may be performed only when the administrative user is confirmed to have an administrative permission to the intelligent attendance machine.

However, as the intelligent attendance machine is provided with physical keys such as RESET (located on a lateral side of the intelligent attendance machine in FIG. 1) as shown in FIG. 1, any person may reset the intelligent attendance machine by triggering the RESET key 102. Moreover, it is difficult to determine whether the triggering action is intentional or by mistake, so that the intelligent attendance machine has high hidden security dangers and the normal operation of the intelligent attendance machine cannot be ensured.

Therefore, a new device configuration solution is provided in the present application to solve the foregoing technical problems in the related art. The following embodiments are provided to further describe the present application.

FIG. 2 is a flowchart of a device configuration method based on a user side according to an exemplary embodiment of the present application. As shown in FIG. 2, the method is applied to user device (i.e., an electronic device used by a preset user), and may include the following steps:

In step 202, user device sends a near-field communication signal including identity information of a logged-in user to an intelligent device to instruct the intelligent device to identify the identity of the logged-in user.

In this embodiment, client terminals of a mobile team office platform may be run on the user device and the intelligent device respectively. For example, a client terminal 1 is run on the user device, and a client terminal 2 is run on the intelligent device. A registered account of the preset user is logged on to the client terminal 1, so that the user device or the client terminal 1 run on the user device is configured to uniquely correspond to the preset user. Similarly, the intelligent device or the client terminal 2 run on the intelligent device is also unique and configured to uniquely determine the intelligent device that is distinguished from other intelligent devices. Correspondingly, a server terminal of the mobile team office platform may be run on a server. Then, data interaction among the user device, the intelligent device, and the server may be implemented based on the client terminal 1, the client terminal 2, the server terminal and so on of the mobile team office platform.

In fact, a mobile enterprise office platform not only may implement a communication function but also may serve as an integrated function platform of many other functions, for example, handling of examination and approval events (such as leave request, office supplies application, and finance examination and approval events), attendance events, task events, log events, and other events internal to the enterprise, and handling of events external to the enterprise such as ordering meals and purchasing. This is not limited in the present application.

More specifically, the mobile enterprise office platform may be carried in instant messaging applications in the related art, e.g., Enterprise Instant Messaging (EIM) applications such as Skype For Business®, Microsoft Teams®, Yammer®, Workplace®, Slack®, Enterprise WeChat®, Fxiaoke®, Enterprise Fetion®, and Enterprise Yixin®. However, the instant messaging function is only one of the communication functions supported by the mobile enterprise office platform. The enterprise office platform may further implement more other functions such as those described above, which will not be elaborated here.

In this embodiment, by taking user device as an example, the user device is provided with a client terminal application (APP) of a mobile enterprise office platform, a registered account of a preset user at the mobile enterprise office platform is logged on, and the user device may be configured as a client terminal 1 of the mobile enterprise office platform corresponding to the preset user. The user device may be a mobile device such as a mobile phone or a tablet, or the user device may be a non-mobile user device such as a PC host, which is not limited in the present application. However, when an online "client terminal" such as HTML5 technology is used, the foregoing client terminal 1 may be run on the user device without installing a corresponding application on the user device.

In step 204, the user device determines, according to a response of the intelligent device to the near-field communication signal, that the intelligent device determines the logged-in user as an administrative user corresponding to the intelligent device, and establishes a near-field communication connection with the intelligent device to configure the intelligent device.

In this embodiment, the intelligent device may be applied to any scenario, which is not limited in the present application. For example, in a scenario of a team (such as an enterprise, a school, a government agency, or a public security department), the intelligent device may be bound to a preset team. Therefore, the foregoing configuration request may

include identity information of a local user (i.e., the foregoing preset user), for instructing the server to return identity information corresponding to the intelligent device when the identity information matches an administrative user of the preset team (i.e., a user in the preset team who has an administrative permission), and for a non-administrative user, the identity information may not be returned, thus implementing permission management on the configuration operation.

In this embodiment, the user device may send a configuration request for the intelligent device to a server, and the configuration request is used for instructing the server to return a standard digital digest corresponding to the intelligent device. Then, the user device receives the standard digital digest returned by the server as the identity information of the logged-in user, wherein the standard digital digest is related to a random code previously generated and uploaded by the intelligent device, and the random code is further recorded as a local random code on the intelligent device. Then, the user device adds the standard digital digest to the near-field communication signal as the identity information, for instructing the intelligent device to generate a local digital digest related to the recorded local random code. When the standard digital digest matches the local digital digest, a near-field communication connection with the sender device of the near-field communication signal is established in response to the near-field communication signal, thus allowing the sender device to configure the intelligent device. By generating a random code on the intelligent device, the standard digital digest correspondingly generated may uniquely correspond to the intelligent device, and high security and anti-cheating performances may be achieved because of its randomness.

In this embodiment, the intelligent device may generate a random code and upload it to the server in the process of initial activation and binding. However, the intelligent device may also generate and upload the random code at any other moment. This is not limited in the present application. By use of a random-code-based standard digital digest, the standard digital digest has "randomness", may uniquely correspond to the intelligent device, and may also avoid being guessed by "exhaustion", thus contributive to further improve the security of the configuration operation.

In this embodiment, an algorithm used when the server generates the standard digital digest according to the random code is identical to that used when the intelligent device generates a local digital digest according to a local random code, so that the standard digital digest may be ensured to be the same as the local digital digest when the

random code corresponding to the standard digital digest is the same as the local random code. As a result, the intelligent device may identify the identity of the local user accurately, ensuring that only the administrative user may smoothly complete the configuration operation on the intelligent device.

In this embodiment, the intelligent device may previously acquire a standard digital digest and store it locally, and the intelligent device may be configured at any subsequent moment according to the locally stored standard digital digest. Alternatively, the number of times the intelligent device uses the standard digital digest locally may be limited, so that the user device has to delete the locally stored standard digital digest and has to reacquire the standard digital digest from the server subsequently when the number of times the intelligent device sends a near-field communication signal to the intelligent device according to the locally stored standard digital digest reaches the number of times the standard digital digest is used locally. Alternatively, in order to further improve the security, it may be restricted that the intelligent device is not allowed to store the standard digital digest and has to acquire the standard digital digest from the server each time.

In this embodiment, when the standard digital digest matches the local digital digest, the intelligent device may establish, based on the received near-field communication signal, a near-field communication connection with the user device that sends the near-field communication signal, so that a present user may configure the intelligent device based on the near-field communication connection when the preset user operates on the user device. When the near-field communication connection is based on the Bluetooth Low Energy (BLE) technology, such as based on the ibeacon protocol, the foregoing near-field communication signal may be an Advertising message. However, the type of the near-field communication technology is not limited in the present application, for example, other types of near-field communication technologies such as Near Field Communication (NFC) may also be used.

Correspondingly, FIG. 3 is a flowchart of a device configuration method based on a server side according to an exemplary embodiment of the present application. As shown in FIG. 3, the method is applied to a server, and may include the following steps:

In step 302, a server acquires identity authentication information of an administrative user corresponding to a preset intelligent device when receiving a configuration request sent by a preset user for the intelligent device.

In this embodiment, the preset user may be an administrative user of a preset team,

and the intelligent device is previously bound to the preset team. In other words, when the intelligent device is previously bound to the preset team, the server may authenticate the preset user who sends the configuration request, and return identity authentication information corresponding to the intelligent device to the preset user only when the preset user is an administrative user of the preset team, for ensuring the security of the configuration operation on the intelligent device.

In this embodiment, the identity authentication information may include a standard digital digest corresponding to the intelligent device. The standard digital digest is related to a random code previously generated and uploaded by the intelligent device, and the random code is further recorded as a local random code on the intelligent device. By generating a random code on the intelligent device, the standard digital digest correspondingly generated may uniquely correspond to the intelligent device and high security and anti-cheating performances may be achieved because of its randomness. However, the identity authentication information may also include other content, such as a character string related to a user ID of the administrative user, as long as the authentication may be performed by the intelligent device accordingly, which is not limited in the present application.

In an embodiment, the standard digital digest may be a digital digest of the random code, that is, the server directly generates a corresponding digital digest for the random code as the standard digital digest. Correspondingly, after receiving the near-field communication signal sent by the preset user, the intelligent device also generates a corresponding digital digest for the recorded local random code as the corresponding local digital digest.

In another embodiment, the standard digital digest may be a common digital digest of at least one of the following information and the random code: an activation code of the intelligent device, a serial number of the intelligent device, and identification information of a bound object of the intelligent device (for example, the bound object may be the foregoing preset team, and the corresponding identification information may be an Organization ID (or Org ID for short) of the preset team), thus increasing the complexity of the digital digest in the present application to further improve the security. In particular, when the digital digest is generated from a plurality of types of information at the same time, there may be more combinations of the information, thus reducing the likelihood that the digital digest will be guessed.

In step 304, the server returns the identity authentication information to the preset user such that the preset user sends a near-field communication signal including the identity authentication information to the intelligent device, wherein the near-field communication signal is used for instructing the intelligent device to determine according to the identity authentication information that the preset user has an administrative permission, and establish a near-field communication connection with the sender device of the near-field communication signal to allow the sender device to configure the intelligent device.

In this embodiment, when the identity authentication information includes a standard digital digest corresponding to the intelligent device, the near-field communication signal is used for instructing the intelligent device to generate a local digital digest related to the recorded local random code, and when the standard digital digest matches the local digital digest, it may be determined that the preset user has an administrative permission.

In this embodiment, the server may further update the recorded standard digital digest according to an updated random code generated and uploaded by the intelligent device, and the updated random code is further used by the intelligent device to update the local random code. By updating the standard digital digest and the local random code, leaking of the standard digital digest or the local random code that causes hidden security dangers may be avoided, thus contributive to improve the security.

Correspondingly, FIG. 4 is a flowchart of a device configuration method based on an intelligent device side according to an exemplary embodiment of the present application. As shown in FIG. 4, the method is applied to an intelligent device, and may include the following steps:

In step 402, an intelligent device acquires identity information included in a near-field communication signal when the near-field communication signal sent by any user is received.

In step 404, the intelligent device identifies the identity of the user according to the identity information.

In step 406, when the user is determined as an administrative user corresponding to the intelligent device, the intelligent device establishes a near-field communication connection with an electronic device used by the user to allow the electronic device to configure the intelligent device.

In this embodiment, the intelligent device may upload a generated random code to the server in advance, so that the server generates a standard digital digest related to the random code and sends the standard digital digest to a preset administrative user having an administrative permission to the intelligent device as identity information of the preset administrative user, wherein the random code is further recorded as a local random code of the intelligent device.

Correspondingly, when identifying the identity of the user, the intelligent device may generate a local digital digest related to the recorded local random code, and compare the local digital digest with a to-be-verified digital digest which is the identity information in the near-field communication signal. When the to-be-verified digital digest matches the local digital digest, the intelligent device determines the any user as the administrative user corresponding to the intelligent device.

In this embodiment, when the to-be-verified digital digest is the same as the local digital digest, it indicates that the to-be-verified digital digest is the standard digital digest generated for the intelligent device at the server, then the user is determined as the administrative user, i.e., the user has the administrative permission to the intelligent device, and the administrative user is allowed to perform a configuration operation on the intelligent device when a configuration mode is switched to. When the to-be-verified digital digest is different from the local digital digest, it indicates that the user does not have an administrative permission and is not allowed to perform a configuration operation on the intelligent device.

In this embodiment, the intelligent device may generate an activation code and upload it to the server in the process of initial activation and binding, and the configuration operation on the intelligent device may be implemented subsequently by using the activation code and the corresponding standard digital digest. Moreover, in order to improve the security and prevent the activation code or the standard digital digest from being leaked or stolen, the intelligent device may generate an updated random code and upload it to the server for updating the standard digital digest, and the updated random code may be further used for updating the local random code to invalidate the previously leaked or stolen activation code or standard digital digest.

In an embodiment, the intelligent device may generate the updated random code according to a predefined cycle and upload it to the server, for example, the random code is updated daily, weekly, monthly or according to other cycles.

In another embodiment, the intelligent device may generate an updated random code and upload it to the server upon completion of each configuration operation. More specifically, the intelligent device may determine that the configuration operation has been completed when the near-field communication connection with the user device is disengaged, and then generate and upload the updated random code. This is however not limited in the present application. Then, even if the user device acquires a standard digital digest from the server, the standard digital digest may be stolen by another person. The stolen standard digital digest will be invalidated and cannot be applied to the configuration operation on the intelligent device as long as the user device completes configuration of the intelligent device and the intelligent device generates an updated activation code and uploads it to the server.

As may be seen from the foregoing technical solution, in the present application, an intelligent device identifies the identity of a user who it is operating, so that only a user having an administrative permission may establish a near-field communication connection between a used electronic device and the intelligent device and perform a configuration operation, thus avoiding hidden security dangers when an irrelevant person triggers a related physical key in a hardware mode and contributive to enhance the security of the configuration operation.

In the following, for example, in an enterprise scenario, the technical solution of the present application is described in detail on the assumption that an enterprise administrator A exists in an enterprise AA and the enterprise administrator A performs, through a mobile phone, a configuration operation on an intelligent attendance machine bound to the enterprise AA. FIG. 5 is a schematic structural diagram of a device configuration system according to an exemplary embodiment of the present application. As shown in FIG. 5, assuming that the system is supported by Enterprise WeChat or another similar mobile team office platform, the system includes a mobile phone used by the enterprise administrator A, the intelligent attendance machine, and an Enterprise WeChat server. An Enterprise WeChat client terminal is run on the mobile phone and the intelligent attendance machine respectively, and an Enterprise WeChat server terminal is run on the Enterprise WeChat server. Instead of being provided with a RESET physical key, the intelligent attendance machine may be configured by software as an enterprise instant messaging application "Enterprise WeChat" provides a corresponding "soft switch" or "software switch."

The Enterprise WeChat server may be a physical server including a separate host, a virtual server borne by a host cluster, or a cloud server. In the process of running, the Enterprise WeChat server may run a server-side program of a certain application to implement a related service function of the application. For example, when running a program of a mobile team office platform, the Enterprise WeChat server may be implemented as a server terminal of the mobile team office platform. However, in the technical solution of the present application, the Enterprise WeChat server runs a team information platform and centrally manages team information on the team information platform, including recording and maintaining team information from various teams and implementing interaction of team information among multiple teams.

The mobile phone is just a type of electronic device that may be used by the user. In practice, apparently, the user may also use the following types of electronic devices such as tablet devices, notebook computers, Personal Digital Assistants (PDAs), and wearable devices (such as smart glasses and smart watches), which are not limited in the present application. In the process of running, the electronic device may run a client-terminal-side program of a certain application to implement a related service function of the application, such as the foregoing device configuration function. Similarly, the intelligent attendance machine may also run a client-terminal-side program of a certain application to implement a related service function of the application, such as the foregoing device configuration function.

Moreover, a network via which the mobile phone, the intelligent attendance machine, and the Enterprise WeChat server interact with each other may include a variety of types of wired or wireless networks. In an embodiment, the network may include a Public Switched Telephone Network (PSTN) and the Internet.

Specifically, the system as shown in FIG. 5 may configure the intelligent attendance machine through the device configuration method shown in FIG. 6. The method may include the following steps.

In step 602, a mobile phone acquires an activation code, a serial number, and other information of an intelligent attendance machine.

In this embodiment, the description of "a mobile phone acquires" actually means that an Enterprise WeChat client terminal run on the mobile phone performs an "acquisition" operation. However, this process needs to be supported by hardware of the mobile phone. This applies similarly to other parts of the present application.

In this embodiment, the intelligent attendance machine determines an activation code, a serial number, and other information corresponding to itself first in the following manners, taking the activation code as an example (which applies similarly to the serial number).

In one situation, the intelligent attendance machine may check whether an activation code exists in a storage space after initial boot. If the activation code does not exist, the intelligent attendance machine sends an activation code acquisition request to the Enterprise WeChat server so that the Enterprise WeChat server allocates a uniquely corresponding activation code to the intelligent attendance machine, and the Enterprise WeChat server will establish a unique mapping relationship between the activation code and the intelligent attendance machine.

In another situation, the intelligent attendance machine has stored its own activation code in the storage space before leaving the factory, and the foregoing unique mapping relationship has also been recorded on the Enterprise WeChat server. Thus, the intelligent attendance machine does not need to acquire the activation code from the Enterprise WeChat server.

The same activation code may be applied to the intelligent attendance machine all the time. Alternatively, the intelligent attendance machine may proactively age the activation code in the storage space according to a preset cycle and re-request a new activation code from the Enterprise WeChat server, and then the Enterprise WeChat server may replace the old activation code (that is, the aged activation code) with the new activation code and update the foregoing unique mapping relationship.

In an embodiment, the activation code, the serial number, and other information may be represented as a QR code or a graphic code in another form as shown in FIG. 7, and the intelligent attendance machine may directly display the graphic code. Alternatively, the activation code, the serial number, and other information may be a character string or non-graphical information in another form, and the intelligent attendance machine may display the character string directly, or convert the character string and display the converted graphic code shown in FIG. 7. However, the activation code may also be in another form, and the intelligent attendance machine may also display the activation code in more manners, which is not limited in the present application. Then, the mobile phone may acquire the activation code, the serial number, and other information of the intelligent attendance machine in the following manners.

In one situation, when the activation code on the intelligent attendance machine is in the form of a graphic code, a camera component on the mobile phone may be started to collect the graphic code through a "code scanning" function of the Enterprise WeChat client terminal run on the mobile phone, and then content of the activation code is read by content recognition. By taking the activation code as an example, after the QR code shown in FIG. 7 is read, an activation code corresponding to the QR code may be recognized as "gfd1s5g451f24sg54sg241fd1."

In another situation, when the activation code on the intelligent attendance machine is in the form of a character string, a camera component on the mobile phone may be started to collect the character string through a related function of the Enterprise WeChat client terminal run on the mobile phone, and then the character string is recognized by Optical Character Recognition (OCR) or the like. However, the Enterprise WeChat client terminal run on the mobile phone may also show an input box, so that the enterprise administrator A may manually input the character string shown on the intelligent attendance machine into the mobile phone to help the mobile phone to complete a reading operation on the character string.

In another embodiment, a near-field communication connection may be established between the mobile phone and the intelligent attendance machine, and the mobile phone acquires the activation code, the serial number, and other information from the intelligent attendance machine through the near-field communication connection. Specifically, the intelligent attendance machine may continuously transmit an Advertising message. For example, the Advertising messages may be sent based on the ibeacon protocol of the BLE technology, and the mobile phone may establish a Bluetooth connection between the mobile phone and the intelligent attendance machine by scanning and responding to the Advertising message. Then, the enterprise administrator A may input login information (such as a login account and a password that are usually recorded in a housing or instruction of the intelligent attendance machine) for the intelligent attendance machine to the mobile phone, so that the intelligent attendance machine returns the activation code, the serial number, and other information to the mobile phone after it is determined that the mobile phone (i.e., the enterprise administrator A) has a related permission.

In step 604, the mobile phone sends a binding request for the intelligent attendance machine to the Enterprise WeChat server, and the binding request includes the activation code, the serial number, and other information of the intelligent attendance machine, as

well as an organization ID of the enterprise AA that is expected to be bound to the intelligent attendance machine.

In step 606, the Enterprise WeChat server establishes a binding relationship between the intelligent attendance machine and the enterprise AA according to the foregoing binding request.

In an embodiment, the mobile phone may show a team selection page as shown in FIG. 8. The team selection page includes all teams associated with the enterprise administrator A. Then, the mobile phone may determine one or more selected teams in the team selection page according to a received user selection instruction, and add organization IDs of the selected teams to the foregoing binding request.

In another embodiment, the Enterprise WeChat client terminal on the mobile phone may determine the number of the teams associated with the enterprise administrator A. When there is only one associated team, the Enterprise WeChat client terminal may directly add an organization ID of the team to the foregoing binding request without showing the team selection page as shown in FIG. 8. When there are multiple associated teams, the Enterprise WeChat client terminal may show the team selection page as shown in FIG. 8 and perform processing according to a user selection instruction, which will not be elaborated here.

In step 608, the mobile phone sends an active instruction to the intelligent attendance machine when a binding result returned by the Enterprise WeChat server and indicating a successful binding is received.

In this embodiment, after the Enterprise WeChat server establishes a binding relationship between the intelligent attendance machine and the enterprise AA, only an enterprise member having an administrative permission to the enterprise AA such as the enterprise administrator A may perform a control operation for the intelligent attendance machine, for example, the configuration operation for the intelligent attendance machine.

In step 610, the intelligent attendance machine generates a random code for the received active instruction.

In this embodiment, the intelligent attendance machine may generate a random code in line with a preset rule according to a built-in predefined algorithm. The random code has uniqueness and randomness, so it is difficult to be imitated and guessed and has extremely high information security.

In step 612, the intelligent attendance machine records the random code as a local random code on the one hand, and sends the random code to the Enterprise WeChat server on the other hand.

In this embodiment, after the Enterprise WeChat server receives the foregoing binding request and binds the intelligent attendance machine to the enterprise AA, it will not terminate this binding process, but continue to wait for receiving the random code uploaded by the intelligent attendance machine.

In step 614, the Enterprise WeChat server generates a standard digital digest related to the random code, and associatively records it with the enterprise AA and the intelligent attendance machine.

In this embodiment, the intelligent attendance machine records the random code as a local random code to establish a unique correspondence between the local random code and the intelligent attendance machine. At the same time, the Enterprise WeChat server associatively records the standard digital digest corresponding to the random code with the enterprise AA and the intelligent attendance machine to establish a unique correspondence among the standard digital digest, the enterprise AA, and the intelligent attendance machine. Then, a unique correspondence between the enterprise administrator A and the intelligent attendance machine may be determined according to a matching relationship between the standard digital digest and the local random code and the administrative permission to the enterprise AA that the enterprise administrator A has, so that the enterprise administrator A may perform a configuration operation on the intelligent attendance machine.

In step 616, after completing recording of the standard digital digest, the Enterprise WeChat server returns activation confirmation to the intelligent attendance machine.

In this embodiment, after receiving the activation confirmation, the intelligent attendance machine may disengage the communication connection with the Enterprise WeChat server, and the Enterprise WeChat server completes binding processing on the intelligent attendance machine. In practice, normal attendance processing may be completed by the intelligent attendance machine entirely locally without conducting network communication with the Enterprise WeChat server. Therefore, even if the intelligent attendance machine is installed in an area with a poor network environment after binding, the attendance processing function of the intelligent attendance machine still will not be affected.

In step 618, the enterprise administrator A initiates a configuration request for the intelligent attendance machine to the Enterprise WeChat server through the mobile phone, and the Enterprise WeChat server returns a standard digital digest corresponding to the intelligent attendance machine based on the configuration request.

In this embodiment, as the enterprise administrator A has an administrative permission to the enterprise AA, the enterprise administrator A may request the standard digital digest corresponding to the intelligent attendance machine from the Enterprise WeChat server. Other enterprise members not having the administrative permission cannot obtain the standard digital digest, thus preventing an irrelevant person from configuring the intelligent attendance machine and avoiding hidden security dangers and risks caused by using the physical key in the related art.

In step 620, the mobile phone transmits an Advertising message to the surrounding, and the Advertising message includes the foregoing standard digital digest.

In this embodiment, after acquiring the foregoing standard digital digest from the Enterprise WeChat server, the mobile phone may store the standard digital digest in the cache space of the mobile phone. Even if the mobile phone is in a state of a poor network environment and cannot establish an effective communication connection with the Enterprise WeChat server, the enterprise administrator A still may perform the configuration operation on the intelligent attendance machine through the mobile phone at any time, thus greatly improving the convenience of configuring the intelligent attendance machine.

In step 622, when the Advertising message from the mobile phone is received, the intelligent attendance machine generates a local digital digest related to the previously stored local random code according to the local random code.

In step 624, when the digital digest included in the Advertising message matches the local digital digest, a Bluetooth connection is established between the intelligent attendance machine and the mobile phone so that the enterprise administrator A may perform the configuration operation on the intelligent attendance machine through the mobile phone.

In this embodiment, the same random code is uploaded to the Enterprise WeChat server and locally recorded at the intelligent attendance machine respectively. The random code has uniqueness and uniquely corresponds to the intelligent attendance machine. As a result, the Enterprise WeChat server generates a standard digital digest related to the

random code on the one hand, and the intelligent attendance machine should process the local random code with the same algorithm to obtain a local digital digest on the other hand. Then, the corresponding standard digital digest is also the same as the local digital digest as identical random codes and algorithms are used. In addition, since when the intelligent attendance machine is bound to the enterprise AA, only the enterprise administrator A of the enterprise AA (however, there may be multiple enterprise administrators having administrative permissions in the enterprise AA in another embodiment) has the related administrative permission and may acquire the standard digital digest from the Enterprise WeChat server through the above step 618, a sender of the Advertising message may be determined as the enterprise administrator A when the digital digest included in the Advertising message matches the local digital digest. Thus, the sender device of the Advertising message is allowed to establish a Bluetooth connection with the intelligent attendance machine to implement the configuration operation on the intelligent attendance machine.

The Enterprise WeChat server and the intelligent attendance machine may adopt an MD5 (MD means Message Digest) algorithm or any other digital digest algorithms respectively, which is not limited in the present application, as long as it is ensured that the Enterprise WeChat server and the intelligent attendance machine adopt the same algorithm. During calculation, taking the Enterprise WeChat server as an example, in one situation, a digital digest corresponding to the random code may be directly calculated as the foregoing standard digital digest; in another situation, the random code and at least one of the following information may be combined to calculate a digital digest corresponding to the combined information: an activation code of the intelligent attendance machine, a serial number of the intelligent attendance machine, an organization ID of the enterprise AA, and so on.

In this embodiment, the digital digest included in the Advertising message is matched with the local digital digest by the intelligent attendance machine, and it is determined accordingly whether the sender corresponding to the Advertising message has an administrative permission, so that the participation of the Enterprise WeChat server is not required in the entire process. The intelligent attendance machine has no requirements for the network environment, which allows the enterprise administrator A to implement the configuration operation on the intelligent attendance machine only in a near-field communication environment, thus avoiding problems such as high delay, easy data packet

loss, and reduction of the security caused by a poor network environment.

At the same time, the sender device of the Advertising message has to be located near the intelligent attendance machine in a near-field communication condition, and especially in a team scenario, the intelligent device such as the intelligent attendance machine is often installed in an internal work area of the team, and thus a security risk of the configuration of the intelligent device by most non-team members may be eliminated.

Further, in order to improve the security and prevent the activation code or the standard digital digest from being leaked or stolen, or when the mobile phone where the standard digital digest is stored is lost or stolen, the intelligent attendance machine may generate an updated random code and upload it to the Enterprise WeChat server so that the Enterprise WeChat server updates a previously recorded standard digital digest. The updated random code is further used for updating the local random code recorded on the intelligent attendance machine to invalidate the previously leaked or stolen activation code and standard digital digest.

In one situation, the intelligent attendance machine may generate the updated random code according to a predefined cycle and upload it to the Enterprise WeChat server, for example, the random code is updated daily, weekly, monthly or according to other cycles. In another embodiment, the intelligent attendance machine may generate an updated random code and upload it to the Enterprise WeChat server upon completion of each configuration operation. More specifically, the intelligent attendance machine may determine that the configuration operation has been completed when the Bluetooth connection with the mobile phone is disengaged after step 624, and then generate and upload the updated random code. However, this is not limited in the present application. Then, even if the standard digital digest may be stolen by another person, the stolen standard digital digest will be invalidated and cannot be applied to the configuration operation on the intelligent device as long as the intelligent attendance machine generates an updated activation code and uploads it to the Enterprise WeChat server.

In summary, in the present application, a configuration operation on an intelligent device may be implemented completely by near-field communication between an electronic device and the intelligent device without the installation of a physical key on the intelligent device, thus avoiding hidden security dangers and risks brought about by the physical key and improving the convenience of the configuration operation on the intelligent device.

FIG. 9 is a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application. Referring to FIG. 9, in terms of hardware, the electronic device includes a processor 902, an internal bus 904, a network interface 906, a memory 908, and a nonvolatile memory 910, and apparently may also include hardware required by other services. The processor 902 reads a corresponding computer program from the nonvolatile memory 910 into the memory 908 and then runs the computer program, forming a device configuration apparatus in terms of logic. However, in addition to the software implementation manner, other implementation manners such as logic devices and a combination of software and hardware are not excluded in the present application. In other words, the following processing procedure is performed by, but not limited to, various logic units, and may also be performed by hardware or logic devices.

Referring to FIG. 10, in the software implementation manner, the device configuration apparatus may include a sending unit 1001 and an identifying unit 1002.

The sending unit 1001 is configured to make user device send a near-field communication signal including identity information of a logged-in user to an intelligent device, for instructing the intelligent device to identify the identity of the logged-in user.

The identifying unit 1002 is configured to make the user device determine according to a response of the intelligent device to the near-field communication signal that the intelligent device determines the logged-in user as an administrative user corresponding to the intelligent device, and establish a near-field communication connection with the intelligent device to configure the intelligent device.

Optionally, the apparatus further includes:

a request unit 1003 configured to make the user device send a configuration request for the intelligent device to a server, the configuration request being used for instructing the server to return a standard digital digest corresponding to the intelligent device;

a receiving unit 1004 configured to make the user device receive the standard digital digest returned by the server as the identity information of the logged-in user, wherein the standard digital digest is related to a random code previously generated and uploaded by the intelligent device, and the random code is further recorded as a local random code on the intelligent device; and

an adding unit 1005 configured to make the user device add the standard digital digest to the near-field communication signal as the identity information, for instructing the intelligent device to generate a local digital digest related to the recorded local random code, and when the standard digital digest matches the local digital digest, establish a near-field communication connection with the sender device of the near-field communication signal in response to the near-field communication signal to allow the sender device to configure the intelligent device.

Optionally, the intelligent device is bound to a preset team; the configuration request includes identity information of a local user, for instructing the server to return the standard digital digest corresponding to the intelligent device when the identity information matches the administrative user of the preset team.

FIG. 11 is a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application. Referring to FIG. 11, in terms of hardware, the electronic device includes a processor 1102, an internal bus 1104, a network interface 1106, a memory 1108, and a nonvolatile memory 1110, and apparently may also include hardware required by other services. The processor 1102 reads a corresponding computer program from the nonvolatile memory 1110 into the memory 1108 and then runs the computer program, forming a device configuration apparatus in terms of logic. However, in addition to the software implementation manner, other implementation manners such as logic devices and a combination of software and hardware are not excluded in the present application. In other words, the following processing procedure is performed by, but not limited to, various logic units, and may also be performed by hardware or logic devices.

Referring to FIG. 12, in the software implementation manner, the device configuration apparatus may include an acquisition unit 1201 and a returning unit 1202.

The acquisition unit 1201 is configured to make a server acquire identity authentication information of an administrative user corresponding to a preset intelligent device when a configuration request sent by a preset user for the intelligent device is received.

The returning unit 1202 is configured to make the server return the identity authentication information to the preset user such that the preset user sends a near-field communication signal including the identity authentication information to the intelligent device, wherein the near-field communication signal is used for instructing the intelligent

device to determine according to the identity authentication information that the preset user has an administrative permission, and establish a near-field communication connection with a sender device of the near-field communication signal to allow the sender device to configure the intelligent device.

Optionally, the identity authentication information includes a standard digital digest corresponding to the intelligent device, the standard digital digest is related to a random code previously generated and uploaded by the intelligent device, and the random code is further recorded as a local random code on the intelligent device,

wherein the near-field communication signal is used for instructing the intelligent device to generate a local digital digest related to the recorded local random code, and when the standard digital digest matches the local digital digest, it is determined that the preset user has an administrative permission.

Optionally, the preset user is an administrative user of a preset team, and the intelligent device is previously bound to the preset team.

Optionally, the standard digital digest is a digital digest of the random code;

or the standard digital digest is a common digital digest of at least one of the following information and the random code: an activation code of the intelligent device, a serial number of the intelligent device, and identification information of a bound object of the intelligent device.

Optionally, the apparatus further includes:

an updating unit 1203 configured to make the server update the recorded standard digital digest according to an updated random code generated and uploaded by the intelligent device, wherein the updated random code is further used by the intelligent device to update the local random code.

FIG. 13 is a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application. Referring to FIG. 13, in terms of hardware, the electronic device includes a processor 1302, an internal bus 1304, a network interface 1306, a memory 1308, and a nonvolatile memory 1310, and apparently may also include hardware required by other services. The processor 1302 reads a corresponding computer program from the nonvolatile memory 1310 into the memory 1308 and then runs the computer program, forming a device configuration apparatus in terms of logic. However, in addition to the software implementation manner, other implementation manners such as logic devices and a combination of software and hardware are not

excluded in the present application. In other words, the following processing procedure is performed by, but not limited to, various logic units, and may also be performed by hardware or logic devices.

Referring to FIG. 14, in the software implementation manner, the device configuration apparatus may include an acquisition unit 1401, an identifying unit 1402, and an establishing unit 1403.

The acquisition unit 1401 is configured to make an intelligent device acquire identity information included in a near-field communication signal when the near-field communication signal sent by any user is received.

The identifying unit 1402 is configured to make the intelligent device identify the identity of the user according to the identity information.

The establishing unit 1403 is configured to, when the user is determined as an administrative user corresponding to the intelligent device, make the intelligent device establish a near-field communication connection with an electronic device used by the user to allow the electronic device to configure the intelligent device.

Optionally, the apparatus further includes: an uploading unit 1404 configured to make the intelligent device upload a generated random code to a server so that the server generates a standard digital digest related to the random code and sends the standard digital digest to a preset administrative user having an administrative permission to the intelligent device as identity information of the preset administrative user, wherein the random code is further recorded as a local random code of the intelligent device; and

the identifying unit 1402 is specifically configured to generate, by the intelligent device, a local digital digest related to the recorded local random code, and compare the local digital digest with a to-be-verified digital digest that is the identity information in the near-field communication signal, wherein when the to-be-verified digital digest matches the local digital digest, the intelligent device determines the user as the administrative user corresponding to the intelligent device.

Optionally, the apparatus further includes:

an updating unit 1405 configured to make the intelligent device generate an updated random code and upload it to the server so that the server updates the standard digital digest, wherein the updated random code is further used for updating the local random code.

Optionally, the updating unit 1405 is specifically configured to:

generate the updated random code according to a predefined cycle and upload it to the server;

or generate the updated random code and upload it to the server after completion of a configuration operation.

The systems, apparatuses, modules or units illustrated in the foregoing embodiments specifically may be implemented by a computer chip or an entity, or implemented by a product having a specific function. A typical implementation device is a computer. Specifically, for example, the computer may be a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email transceiver, a game console, a tablet computer, a wearable device, or a combination of any of these devices.

In a typical configuration, the computer includes one or more central processing units (CPUs), an input/output interface, a network interface, and a memory.

The memory may include computer readable media such as a volatile memory, a Random-Access Memory (RAM), and/or a non-volatile memory, e.g., a Read-Only Memory (ROM) or a flash RAM. The memory is an example of a computer readable medium.

The computer readable medium includes non-volatile and volatile media as well as movable and non-movable media, and may implement information storage by means of any method or technology. The information may be a computer readable instruction, a data structure, and a module of a program or other data. An example of the storage medium of a computer includes, but is not limited to, a phase change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other types of RAMs, a ROM, an electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technologies, a compact disk read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical storages, a cassette tape, a magnetic tape/magnetic disk storage or other magnetic storage devices, or any other non-transmission medium, and may be used to store information accessible to the computing device. According to the definition in this text, the computer readable medium does not include transitory media, such as a modulated data signal and a carrier wave.

It should be further noted that the terms "include," "comprise" or other variations thereof are intended to cover non-exclusive inclusion, so that a process, method,

commodity or device including a series of elements not only includes the elements, but also includes other elements not explicitly listed, or further includes elements inherent to the process, method, commodity or device. In the absence of more limitations, an element defined by "including a/an…" does not exclude that the process, method, commodity or device including the element further has other identical elements.

Exemplary embodiments will be described in detail herein, and examples thereof are shown in the accompanying drawings. In the following description involving the accompanying drawings, the same numerals in different accompanying drawings denote the same or similar elements, unless specified otherwise. Implementation manners described in the following exemplary embodiments do not represent all implementation manners consistent with the present application. In contrast, they are merely examples of apparatuses and methods consistent with some aspects of the present application as described in detail in the appended claims.

Terms used in the present application are merely used for describing specific embodiments, instead of limiting the present application. Singular forms "a(n)", "said", and "the" used in the present application and the appended claims also include plural forms, unless clearly specified in the context that other meanings are denoted. It should be further understood that the term "and/or" used herein refers to and includes any or all possible combinations of one or more associated items listed.

It should be understood that, although terms such as "first," "second," and "third" may be used to describe various kinds of information in the present application, these kinds of information should not be limited to the terms. These terms are merely used to distinguish information of the same type from each other. For example, without departing from the scope of the present application, the first information may also be referred to as second information, and similarly, the second information may also be referred to as first information. Depending on the context, the word "if" used herein may be explained as "when...", "as...", or "in response to the determination".

The above descriptions are merely preferred embodiments of the present application, but not intended to limit the present application. Any modification, equivalent replacement, and improvement made without departing from the spirit and principle of the present application shall fall within the protection scope of the present application.