

CLAIMS

1. A method for identity authentication, the method comprising:

receiving, by an interactive end from an acquisition device configured to determine a

5 characteristic of an item to be purchased by a user by reading the machine-readable representation on the item, an interactive instruction initiated for the item;

obtaining, by the interactive end, identity information of the user in response to the receiving of the interactive instruction; and

10 sending, by the interactive end, an identification request to a server end, wherein the identification request comprises the identity information, wherein the server end is configured to identify the user based on the identity information, and determine a user account mapped in a database to the user, wherein the user account is an account of the user on an application installed on a client device of the user; and

15 performing, by the interactive end, an interactive operation in accordance with the interactive instruction on the user account to complete the purchase of the item by the user, wherein the purchase of the item is completed without requiring the user to interact with the client device.

2. The method according to claim 1, further comprising:

20 transmitting, by the interactive end, a near field message to the client device, wherein the near field message comprises interactive-end identification information of the interactive end.

3. The method according to claim 2, wherein in response to determining that the near field message is received by the client device corresponding to the user, the near field message is used
25 to instruct the client device to send the interactive-end identification information, user identification information of the user, and signal strength of the near field message to the server end, so that the server end marks the user as a candidate user corresponding to the interactive end in response to determining that the signal strength is greater than predetermined strength.

4. The method according to claim 2, wherein the near field message is transmitted within a coverage area that is adjustable based on a transmit power.

5. The method according to claim 4, wherein the coverage area is near the interactive end.

6. The method according to claim 2, wherein the near field message is within a predetermined duration.

7. The method according to claim 1, wherein the identity information comprises biometric feature information.

8. The method according to claim 7, wherein the biometric feature information comprises at least one of:

face information, fingerprint information, palm print information, eye print information, iris information, and gait information.

9. The method according to claim 1, wherein the identifying of the user based on the identity information comprises matching, by the server end, the identity information against standard identity information of a candidate user corresponding to the interactive end, wherein the matching of the identity information comprises:

matching, by the server end, the identity information against standard identity information corresponding to each candidate user to obtain a corresponding similarity;

determining whether a highest similarity is greater than a predetermined similarity threshold, and that a difference between the highest similarity and a second highest similarity is greater than a predetermined confounding difference value; and

in response to determining that the highest similarity is greater than the predetermined similarity threshold, and that the difference between the highest similarity and the second highest similarity is greater than the predetermined confounding difference value, determining that a respective candidate user corresponding to the highest similarity matches the user.

10. A device for identity authentication, the device comprising a plurality of modules

configured to perform the method of any one of claims 1 to 9.