

CLAIMS

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

receiving, by an interactive end, an interactive instruction initiated for a user;

5 obtaining, by the interactive end, identity information of the user based on 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 identification request is used to instruct the server end to match the identity information against standard identity information of a candidate user corresponding to the interactive end, to determine a user account corresponding to the user, wherein the user account is used to respond to an interactive operation corresponding to the interactive instruction, and wherein a user near the interactive end is marked as a candidate user corresponding to the interactive end by the server end.

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

performing, by the interactive end, an interactive operation on the determined user account in response to the interactive instruction in response to determining the user account corresponding to the user.

20 3. The method according to claim 1, further comprising:

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

25 4. The method according to claim 3, wherein in response to determining that the near field message is received by a client device corresponding to the user, the near field message is used 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.

5. The method according to claim 3, wherein the near field message is transmitted within a coverage area that is adjustable based on a transmit power.

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

7. The method according to claim 1, wherein the near field message is within a predetermined duration.

10 8. The method according to claim 1, wherein the identity information comprises biometric feature information, and wherein the standard identity information comprises standard biometric feature information.

15 9. The method according to claim 6, wherein the biometric feature information and the standard biometric feature information each comprise at least one of:

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

20 10. The method according to claim 1, wherein matching, by the server end, the identity information against standard identity information of the candidate user corresponding to the interactive end comprises:

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

25 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

30 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.

11. A device for identity authentication, the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 10.