

CLAIMS

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

receiving, by a mobile device of a user from an acquisition device configured to determine
5 a characteristic of an item to be purchased by the user by reading the machine-readable
representation on the item, an interactive instruction initiated for the item;

obtaining, by the mobile device, identity information of the user in response to the receiving
of the interactive instruction;

receiving, by the mobile device, a near field message from the acquisition device, wherein
10 the near field message comprises acquisition device identification information, wherein in
response to determining that the near field message is received by the mobile device
corresponding to the user, the near field message is used to instruct the mobile device to send the
acquisition device identification information, user identification information of the user, and a
signal strength of the near field message to a server end, so that the server end marks the user as
15 a candidate user corresponding to the mobile device in response to determining that the signal
strength is greater than predetermined strength;

sending, by the mobile device, an identification request to the 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
20 database to the user, wherein the user account is an account of the user on an application
installed on the mobile device of the user; and

performing, by the mobile device, 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
25 mobile device.

2. The method according to claim 1, wherein the near field message is transmitted within a
coverage area that is adjustable based on a transmit power.

3. The method according to claim 2, wherein the coverage area is near the mobile device.

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

5

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

6. The method according to claim 5, 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.

7. 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 mobile device, 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.

8. A device for identity authentication, the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 7.

30