CLAIMS

What is claimed is:

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

retrieving, by an intelligent wearable device configured with an embedded algorithm chip, provisioning data from a provisioning server by using a connected intelligent terminal (S110);

storing, by the intelligent wearable device, the provisioning data;

invoking, by the intelligent wearable device, the embedded algorithm chip by using a micro operating system (S120);

generating a, by the intelligent wearable device, one-time password based on the provisioning data (S120);

transmitting, by the intelligent wearable device, the one-time password to a merchant device;

retrieving, by the merchant device, the one-time password and sending the one-time password to a verification server for verification (S130); and

receiving, by the merchant device, a verification success message sent by the verification server to complete the identity verification (S140).

2. The method according to claim 1, wherein the provisioning server and the verification server are integrated into the same server.

3. The method according to claim 1, wherein the provisioning data comprises a seed and a server timestamp.

4. The method according to claim 1, wherein retrieving and storing the provisioning data comprises:

sending, by the intelligent terminal, a request for enabling a one-time password function to the intelligent wearable device;

communicating, by the intelligent wearable device, with the embedded algorithm chip by using the micro operating system, to obtain a public key in a pair of public key and private key generated by the embedded algorithm chip by using an asymmetric encryption algorithm;

sending, by the intelligent wearable device, the public key to the provisioning server by using

the intelligent terminal;

encrypting, by the provisioning server, the provisioning data by using the public key and returning the encrypted provisioning data to the intelligent wearable device by using the intelligent terminal; and

storing, by the intelligent wearable device, the encrypted provisioning data.

5. The method according to claim 1, wherein after the intelligent wearable device configured with the embedded algorithm chip obtains the provisioning data from the provisioning server by using the connected intelligent terminal, and before the intelligent wearable device stores the provisioning data, the method further comprises:

verifying, by the embedded algorithm chip, the provisioning data retrieved by the intelligent wearable device; and

storing, by the intelligent wearable device, the provisioning data retrieved from the server if verification succeeds.

6. The method according to claim 4, wherein after the returning, by the provisioning server, the encrypted provisioning data to the intelligent wearable device by using the intelligent terminal, and before the storing, by the intelligent wearable device, the encrypted provisioning data, the method further comprises:

decrypting, by the embedded algorithm chip, the encrypted provisioning data by using the paired private key to obtain decrypted provisioning data; and

verifying, by the embedded algorithm chip, the provisioning data.

7. The method according to claim 5 or 6, wherein verifying, by the embedded algorithm chip, the provisioning data comprises:

calculating, by the embedded algorithm chip by using a predetermined one-time password generation algorithm, a one-time password based on the provisioning data, and checking whether the length of the generated one-time password meets a predetermined value; and

determining that verification succeeds if the length of the generated one-time password meets the predetermined value.

8. The method according to claim 1, wherein the intelligent wearable device and the intelligent terminal are connected in a wired or wireless way, and the wireless way comprises a short-distance wireless communications mode.

9. The method according to claim 8, wherein the short-distance wireless communications mode comprises any one of the following:

Bluetooth, infrared, wireless local area network, Wi-Fi Direct, ultra-wide band, ZigBee, and near field communication.

10. The method according to claim 1, wherein the one-time password is generated by a one-time password generation algorithm, and the one-time password generation algorithm comprises a TOTP algorithm and an HOTP algorithm.

11. The method according to claim 1, wherein the intelligent wearable device presents the generated one-time password by using a screen.

12. The method according to claim 1, wherein the merchant device comprises any one of a scanning gun, a vertical scanner, and an embedded scanning module.

13. A system for identity verification, the system comprising a plurality of modules configured to perform the method of any one of claims 1 to 12.