What is claimed is:

1. An identity authentication method, comprising:

establishing, by a first device, a communication connection with a second device;

receiving, by the first device, data to be authenticated transmitted by the second device via the communication connection, the data to be authenticated comprising digital authentication information and an identity identifier;

collecting, by the first device, biological characteristic information;

sending, by the first device, the data to be authenticated and the biological characteristic information to a background server;

receiving, by the background server, the data to be authenticated and the biological characteristic information;

obtaining, by the background server, a pre-stored authentication factor and biological characteristic verification information corresponding to the identity identifier, wherein a second preset value is set for referring to a matching rate indicating that the biological characteristic information and the biological characteristic verification information are identical;

performing, by the background server, an authentication on the digital authentication information according to the authentication factor; and

when the authentication performed on the digital authentication information is passed, reducing the second preset value to a first preset value and determining whether the matching rate between the biological characteristic information and the biological characteristic verification information is greater than the first preset value, the first preset value being smaller than the second preset value, and when the matching rate between the biological characteristic information and the biological characteristic verification information is greater than the first preset value, determining that an identity authentication for the second device is passed.

2. The method according to claim 1, wherein the biological characteristic information comprises: fingerprint information and/or vein information; and

collecting, by the first device, the biological characteristic information comprises: when a biological limb is in contact with the first device, collecting the biological characteristic information of a portion of the biological limb in contact with the first device.

3. The method according to claim 1 or 2, wherein receiving, by the first device, the data to be authenticated transmitted by the second device via the communication connection comprises:

receiving, by the first device, the data to be authenticated broadcast by the second device via the communication connection; or

sending, by the first device, an authentication request to the second device via the communication connection; and receiving, by the first device, the data to be authenticated transmitted by the second device in response to the authentication request via the communication connection.

4. The method according to any of claims 1 to 3, wherein the digital authentication information comprises: signature information obtained by digital sign performed on data to be signed using a signature private key; the authentication factor comprises: a signature public key corresponding to the signature private key; performing, by the background server, the authentication on the digital authentication information according to the authentication factor comprises: performing, by the background server, a signature authentication on the digital authentication information using the signature public key and the data to be signed; or

the digital authentication information comprises: encrypted information obtained by encrypting information to be encrypted using a symmetric secret key; the authentication factor comprises: the symmetric secret key; and performing, by the background server, the authentication on the digital authentication information according to the authentication factor comprises: performing, by the background server, the authentication on the encrypted information using the symmetric secret key and the information to be encrypted; or

the digital authentication information comprises: a dynamic password; the authentication factor comprises: a seed secret key for verifying the dynamic password; performing, by the background server, the authentication on the digital authentication information according to the authentication factor comprises: performing, by the background server, the authentication on the dynamic password at least using the seed secret key.

5. The method according to any of claims 1 to 4, wherein establishing, by the first device, the communication connection with the second device comprises:

establishing, by the first device, the communication connection with the second device via a biological limb.

6. An identity authentication system, comprising: a first device and a background server, wherein the first device is configured to:

establish a communication connection with a second device;

receive data to be authenticated transmitted by the second device via the communication connection, the data to be authenticated comprising digital authentication information and an identity identifier;

collect biological characteristic information of a biological limb; and

send the data to be authenticated and the biological characteristic information to the background server;

the background server is configured to:

receive the data to be authenticated and the biological characteristic information;

obtain a pre-stored authentication factor and biological characteristic verification information corresponding to the identity identifier, wherein a second preset value is set for referring to a matching rate indicating that the biological characteristic information and the biological characteristic verification information are identical;

perform an authentication on the digital authentication information according to the authentication factor; and

when the authentication performed on the digital authentication information is passed, reducing the second preset value to a first preset value and determining whether the matching rate between the biological characteristic information and the biological characteristic verification information is greater than the first preset value, the first preset value being smaller than the second preset value, and when the matching rate between the biological characteristic information and the biological characteristic verification information is greater than the first preset value, determine that an identity authentication for the second device is passed.

7. The system according to claim 6, wherein the biological characteristic information comprises: fingerprint information and/or vein information; and

the first device collects the biological characteristic information by an act of: when the biological limb is in contact with the first device, collecting the biological characteristic information of a portion of the biological limb in contact with the first device.

8. The system according to claim 6 or 7, wherein the first device receives the data to be authenticated transmitted by the second device via the communication connection by acts of:

receiving, by the first device, the data to be authenticated broadcast by the second device via the communication connection; or

sending, by the first device, an authentication request to the second device via the

communication connection; and receiving, by the first device, the data to be authenticated transmitted by the second device in response to the authentication request via the communication connection.

9. The system according to any of claims 6 to 8, wherein the digital authentication information comprises: signature information obtained by digital sign performed on data to be signed using a signature private key; the authentication factor comprises: a signature public key corresponding to the signature private key; the background server performs the authentication on the digital authentication information according to the authentication factor by an act of: performing, by the background server, a signature authentication on the digital authentication information using the signature public key and the data to be signed; or

the digital authentication information comprises: encrypted information obtained by encrypting information to be encrypted using a symmetric secret key; the authentication factor comprises: the symmetric secret key; and the background server performs the authentication on the digital authentication information according to the authentication factor by an act of: performing, by the background server, the authentication on the encrypted information using the symmetric secret key and the information to be encrypted; or

the digital authentication information comprises: a dynamic password; the authentication factor comprises: a seed secret key for verifying the dynamic password; the background server performs the authentication on the digital authentication information according to the authentication factor by an act of: performing, by the background server, the authentication on the dynamic password at least using the seed secret key.

10. The system according to any of claims 6 to 9, wherein the first device establishes the communication connection with the second device by an act of:

establishing, by the first device, the communication connection with the second device via a biological limb.

11. A computer program, when run on a processor, configured to perform an identity authentication method according to any of claims 1-5.