CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:

receiving, at a server, an authentication request from a terminal, the authentication request including at least one of a user identifier of a user and a wearable device identifier of the user, the server storing a relationship between the user identifier, the wearable device identifier, and a server authentication key;

acquiring, by the server, downlink authentication information, and issuing, to the terminal, a detection instruction that includes the downlink authentication information and the wearable device identifier;

receiving, by the server, a detection acknowledgment returned by the terminal that includes uplink authentication information, the uplink authentication information being generated by a wearable device designated in the detection instruction according to a device authentication key and the downlink authentication information, the device authentication key being the same as, or corresponding to, the server authentication key; and

authenticating, by the server, the user including matching the downlink authentication information with the uplink authentication information by using the server authentication key of the user, wherein the user passes the authentication if the matching succeeds.

2. The computer-implemented method of claim 1, wherein:

the server further stores a user public key of the user, wherein the user public key corresponds to the user identifier, the wearable device identifier, and the server authentication key of the user, and wherein the user public key and a user private key stored in the terminal are a pair of keys;

the detection acknowledgment returned by the terminal is signed by using the user private key stored in the terminal; and

the computer-implemented method further comprises performing signature verification on the detection acknowledgment of the terminal according to the user public key of the user, wherein authenticating the user fails if the verification fails.

3. The computer-implemented method of claim 1, wherein:

the server further stores a terminal identifier, wherein the terminal identifier corresponds to the user identifier, the wearable device identifier, and the server authentication key of the user;

the authentication request further includes a terminal identifier for sending the authentication request; and

the computer-implemented method further comprises failing the authentication of the user when the terminal identifier corresponding to the user identifier or the wearable device identifier in the authentication request is different from the terminal identifier for sending the authentication request.

4. The computer-implemented method of claim 1, wherein:

the server further stores a server private key, wherein the server private key and a terminal public key stored in the terminal are a pair of keys; and

the computer-implemented method further comprises signing the detection instruction by using the server private key.

5. The computer-implemented method of claim 1, wherein the detection instruction and the detection acknowledgment are transmitted through an encrypted channel between the server and the terminal.

6. The computer-implemented method of claim 1, wherein:

the server is a payment server and the authentication request is a payment request; and

the computer-implemented method further comprises providing a payment service for users passing the authentication.

7. The computer-implemented method of claim 1, wherein authenticating the user includes authenticating an identity of the user relative to a login by the user to a personal account.

8. The computer-implemented method of claim 1, wherein authenticating the user includes authenticating an identity of the user making a payment through a third-party payment platform.

9. A computer-implemented method, comprising:

sending, by a terminal connected to a wearable device of a user, an authentication request to a server according to an operation of the user, the authentication request including at least one of a user identifier and a wearable device identifier of the user;

receiving, at the terminal, a detection instruction of the server, the detection instruction including downlink authentication information and the wearable device identifier;

sending, by the terminal, the downlink authentication information to a wearable device designated in the detection instruction, and receiving uplink authentication information returned by the wearable device, the uplink authentication information being generated by the wearable device according to a stored device authentication key and the downlink authentication information, and the device authentication key being the same as, or corresponding to, a server authentication key stored in the server;

sending, to the server, a detection acknowledgment that includes the uplink authentication information; and

authenticating the user, including receiving a user authentication result determined by the server according to the uplink authentication information, the downlink authentication information, and the server authentication key.

10. The computer-implemented method of claim 9, wherein:

the terminal stores a user private key of the user, wherein the user private key and a user public key stored in the server are a pair of keys; and

the computer-implemented method further comprises signing the detection acknowledgment by using the user private key of the user.

11. The computer-implemented method of claim 9, wherein:

the terminal stores a terminal public key, wherein the terminal public key and a server private key stored in the server are a pair of keys;

the detection instruction issued by the server is signed by using the server private key.

12. The computer-implemented method of claim 9, wherein the authentication request is a payment request, and wherein the terminal completes a payment operation of the user after the

user authentication result is the authentication being successful.

13. The computer-implemented method of claim 12, further comprising:

performing signature verification on the detection instruction of the server according to the terminal public key; and

rejecting the detection instruction if the verification fails.

14. The computer-implemented method of claim 1, wherein the authentication request includes an identity of the user relative to a login by the user to a personal account.

15. The computer-implemented method of claim 1, wherein the authentication request includes an identity of the user making a payment through a third-party payment platform.

16. The computer-implemented method of claim 1, further comprising providing, for display to the user, a message indicating that authorization has occurred.

17. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, at a server, an authentication request from a terminal, the authentication request including at least one of a user identifier of a user and a wearable device identifier of the user, the server storing a relationship between the user identifier, the wearable device identifier, and a server authentication key;

acquiring, by the server, downlink authentication information, and issuing, to the terminal, a detection instruction that includes the downlink authentication information and the wearable device identifier;

receiving, by the server, a detection acknowledgment returned by the terminal that includes uplink authentication information, the uplink authentication information being generated by a wearable device designated in the detection instruction according to a device authentication key and the downlink authentication information, the device authentication key being the same as, or corresponding to, the server authentication key; and

authenticating, by the server, the user including matching the downlink authentication information with the uplink authentication information by using the server authentication key of

the user, wherein the user passes the authentication if the matching succeeds.

18. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

sending, by a terminal connected to a wearable device of a user, an authentication request to a server according to an operation of the user, the authentication request including at least one of a user identifier and a wearable device identifier of the user;

receiving, at the terminal, a detection instruction of the server, the detection instruction including downlink authentication information and the wearable device identifier;

sending, by the terminal, the downlink authentication information to a wearable device designated in the detection instruction, and receiving uplink authentication information returned by the wearable device, the uplink authentication information being generated by the wearable device according to a stored device authentication key and the downlink authentication information, and the device authentication key being the same as, or corresponding to, a server authentication key stored in the server;

sending, to the server, a detection acknowledgment that includes the uplink authentication information; and

authenticating the user, including receiving a user authentication result determined by the server according to the uplink authentication information, the downlink authentication information, and the server authentication key.

19. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing instructions, that when executed by the one or more computers, perform operations using methods comprising:

receiving, at a server, an authentication request from a terminal, the authentication request including at least one of a user identifier of a user and a wearable device identifier of the user, the server storing a relationship between the user identifier, the wearable device identifier, and a server authentication key;

acquiring, by the server, downlink authentication information, and issuing, to the terminal, a detection instruction that includes the downlink authentication information and the wearable device identifier;

receiving, by the server, a detection acknowledgment returned by the terminal that includes uplink authentication information, the uplink authentication information being generated by a wearable device designated in the detection instruction according to a device authentication key and the downlink authentication information, the device authentication key being the same as, or corresponding to, the server authentication key; and

authenticating, by the server, the user including matching the downlink authentication information with the uplink authentication information by using the server authentication key of the user, wherein the user passes the authentication if the matching succeeds.

20. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing instructions, that when executed by the one or more computers, perform operations using methods comprising:

sending, by a terminal connected to a wearable device of a user, an authentication request to a server according to an operation of the user, the authentication request including at least one of a user identifier and a wearable device identifier of the user;

receiving, at the terminal, a detection instruction of the server, the detection instruction including downlink authentication information and the wearable device identifier;

sending, by the terminal, the downlink authentication information to a wearable device designated in the detection instruction, and receiving uplink authentication information returned by the wearable device, the uplink authentication information being generated by the wearable device according to a stored device authentication key and the downlink authentication information, and the device authentication key being the same as, or corresponding to, a server authentication key stored in the server;

sending, to the server, a detection acknowledgment that includes the uplink authentication information; and

authenticating the user, including receiving a user authentication result determined by the server according to the uplink authentication information, the downlink authentication information, and the server authentication key.