CLAIMS

1. An authorization method for a joint account, performed by client software, wherein the joint account is jointly managed by *N* joint managers, *N* is a natural number greater than 1, and the method comprises:

obtaining a user-side authentication parameter of the joint account, wherein the user-side authentication parameter is the same as or corresponding to a network-side authentication parameter of the joint account, and is used to perform authentication on operation permission for the joint account (110);

dividing the user-side authentication parameter into *N* parts;

generating a corresponding joint management authentication parameter based on each part; and

writing each joint management authentication parameter into a device controlled by each joint manager (120).

2. The method according to claim 1, wherein obtaining a user-side authentication parameter of the joint account comprises:

generating the user-side authentication parameter and the network-side authentication parameter of the joint account, and

uploading the network-side authentication parameter to a server.

3. The method according to claim 2, wherein the user-side authentication parameter and the network-side authentication parameter comprise a private key and a public key of an asymmetric encryption algorithm.

4. The method according to claim 1, wherein obtaining a user-side authentication parameter of the joint account comprises receiving the user-side authentication parameter generated by a server from the server.

5. The method according to claim 1, wherein dividing the user-side authentication parameter

into *N* parts, and generating a corresponding joint management authentication parameter based on each part comprises:

dividing the user-side authentication parameter into *N* segments, and

using each segment and a corresponding segment sequence number as one joint management authentication parameter.

6. The method according to claim 1, wherein the device controlled by each joint manager comprises a near field communication (NFC) chip of each joint manager.

7. An authorization device comprising multiple units configured to perform operations according to the method of any one of claims 1 to 6.

8. An authorization method for a joint account, performed by a server, wherein the joint account is jointly managed by *N* joint managers, *N* is a natural number greater than 1, and the method comprises:

obtaining a user-side authentication parameter and a network-side authentication parameter of the joint account, and storing the network-side authentication parameter, wherein the user-side authentication parameter is the same as or corresponding to the network-side authentication parameter, and is used to perform authentication on operation permission for the joint account (310);

dividing the user-side authentication parameter into *N* parts;

generating a corresponding joint management authentication parameter based on each part; and

separately sending joint management authentication parameters to client software of different joint managers (320).

9. The method according to claim 8, wherein dividing the user-side authentication parameter into *N* parts, and generating a corresponding joint management authentication parameter based on each part comprises:

dividing the user-side authentication parameter into *N* segments; and

using each segment and a corresponding segment sequence number as one joint

management authentication parameter.

10. The method according to claim 8, wherein obtaining a user-side authentication parameter and a network-side authentication parameter of the joint account comprises:

generating symmetric keys or passwords based on a predetermined algorithm; and

using the symmetric keys or passwords as the user-side authentication parameter and the network-side authentication parameter.

11. An authorization method for a joint account, performed by client software of a joint manager of the joint account, wherein the joint account is jointly managed by *N* joint managers, *N* is a natural number greater than 1, and the method comprises:

receiving a joint management authentication parameter sent by a server, wherein the joint management authentication parameter is generated based on one part after the server divides a user-side authentication parameter into *N* parts, and the user-side authentication parameter is used to perform authentication on operation permission for the joint account (410); and

storing the joint management authentication parameter (420).

12. The method according to claim 11, wherein the joint management authentication parameter comprises one of *N* segments of the user-side authentication parameter and a corresponding segment sequence number.

13. The method according to claim 11, wherein storing the joint management authentication parameter comprises:

storing the joint management authentication parameter in a device comprising the client software, or

storing the joint management authentication parameter in a storage medium separated from a device comprising the client software.

14. An authentication device comprising multiple units configured to perform operations according to the method of any one of claims 8 to 10.

15. An authentication device comprising multiple units configured to perform operations according to the method of any one of claims 11 to 13.

16. An authentication method for a joint account, performed by client software, wherein the joint account is jointly managed by *N* joint managers, *N* is a natural number greater than 1, and the method comprises:

obtaining *N* joint management authentication parameters of the joint account (610);

restoring one part of a user-side authentication parameter based on each joint management authentication parameter;

combining *N* parts into the user-side authentication parameter (620); and

initiating an authentication request to a server by using the user-side authentication parameter, wherein the server performs authentication on operation permission for the joint account based on a network-side authentication parameter, wherein the network-side authentication parameter is the same as or corresponding to the user-side authentication parameter (630).

17. The method according to claim 16, wherein obtaining *N* joint management authentication parameters of the joint account comprises:

obtaining the *N* joint management authentication parameters of the joint account from devices comprising client software of the *N* joint managers; or

reading the *N* joint management authentication parameters of the joint account from storage media of the *N* joint managers.

18. The method according to claim 17, wherein the storage media of the *N* joint managers comprise a near field communication (NFC) chip of each joint manager.

19. The method according to claim 16, wherein restoring one part of a user-side authentication parameter based on each joint management authentication parameter, and combining *N* parts into the user-side authentication parameter comprises:

restoring one segment of the user-side authentication parameter and a corresponding segment sequence number based on each joint management authentication parameter; and

connecting *N* segments based on corresponding segment sequence numbers to obtain the user-side authentication parameter.

20. The method according to claim 16, wherein the user-side authentication parameter and the network-side authentication parameter comprise a private key and a public key of an asymmetric encryption algorithm; and

initiating an authentication request to a server by using the user-side authentication parameter, so the server performs authentication on operation permission for the joint account based on a network-side authentication parameter comprises:

performing digital signature on the authentication request initiated to the server by using the private key, wherein the server performs signature authentication on the authentication request by using the public key.

21. An authentication device comprising multiple units configured to perform operations according to the method of any one of claims 16-20.

22. An authentication method for a joint account, performed by a server, wherein the joint account is jointly managed by *N* joint managers, *N* is a natural number greater than 1, and the method comprises:

receiving *N* joint management authentication parameters uploaded by client software (710);

restoring one part of a user-side authentication parameter based on each joint management authentication parameter;

combining *N* parts into the user-side authentication parameter (720); and

performing authentication on operation permission for the joint account based on a network-side authentication parameter, wherein the network-side authentication parameter is the same as or corresponding to the user-side authentication parameter (730).

23. The method according to claim 22, wherein restoring one part of a user-side authentication parameter based on each joint management authentication parameter, and combining *N* parts into the user-side authentication parameter comprises:

restoring one segment of the user-side authentication parameter and a corresponding

segment sequence number based on each joint management authentication parameter; and

connecting *N* segments based on corresponding segment sequence numbers to obtain the user-side authentication parameter.

24. The method according to claim 22, wherein receiving *N* joint management authentication parameters uploaded by client software comprises receiving the *N* joint management authentication parameters respectively uploaded by client software of the *N* joint managers.

25. The method according to claim 22, wherein the method further comprises:

receiving a joint account operation request sent by client software of a joint manager, wherein the joint account operation request comprises operation content; and

sending a joint management authentication parameter upload request to client software of (*N*–1) other joint managers, wherein the joint management authentication parameter upload request comprises the operation content.

26. An authentication device comprising multiple units configured to perform operations according to the method of any one of claims 22 to 25.

27. An authentication method for a joint account, performed by client software, wherein the joint account is jointly managed by *N* joint managers, *N* is a natural number greater than 1, and the method comprises:

obtaining a joint management authentication parameter of a joint manager (810); and

uploading the joint management authentication parameter to a server, wherein the server restores one part of a user-side authentication parameter based on the joint management authentication parameter, combines the part with (*N*–1) other parts into the user-side authentication parameter, and then performs authentication on operation permission for the joint account by using a network-side authentication parameter that is the same as or corresponding to the user-side authentication parameter (820).

28. The method according to claim 27, wherein obtaining a joint management authentication parameter of a joint manager comprises:

obtaining the joint management authentication parameter from a device comprising client software of the joint manager; or

reading the joint management authentication parameter from a storage medium of the joint manager.

29. The method according to claim 27, wherein the method further comprises sending a joint account operation request to the server, wherein the joint account operation request comprises operation content.

30. The method according to claim 27, wherein the method further comprises:

receiving a joint management authentication parameter upload request sent by the server, wherein the joint management authentication parameter upload request comprises operation content in a joint account operation request initiated by the joint manager; and

the uploading the joint management authentication parameter to a server comprises:

uploading the joint management authentication parameter to the server in response to the joint management authentication parameter upload request.

31. An authentication device comprising multiple units configured to perform operations according to the method of any one of claims 27-30.