

CLAIMS

What is claimed is:

1. A method for processing two-dimensional barcodes, comprising:

receiving, by a server, an electronic credential acquisition request sent by client
5 software, wherein the electronic credential acquisition request comprises a user identifier;

obtaining an electronic credential that corresponds to the user identifier, and signing the electronic credential and a user public key of the client software by using a server private key to obtain server signature information; and

10 sending the server signature information and the electronic credential to the client software, so that the client software verifies the server signature information, and generates a two-dimensional barcode based on the electronic credential so that a credential verification end device verifies the electronic credential comprised in the two-dimensional barcode, wherein the credential verification end device is configured
15 to generate the electronic credential based on the user identifier.

2. The method according to claim 1, wherein the signing the electronic credential and the user public key of the client software by using the server private key comprises:

allocating a user signature key to the electronic credential, and signing the
20 electronic credential and a first user public key by using the server private key, wherein the allocated user signature key comprises the first user public key; or

obtaining a second user public key sent by the client software, and signing the electronic credential and the second user public key by using the server private key.

3. The method according to claim 2, wherein if the first user public key is signed
25 by using the server private key, the sending the server signature information and the electronic credential to the client software comprises:

sending the allocated user signature key, the server signature information, and the electronic credential to the client software.

4. The method according to any one of claims 1 to 3, wherein before the
30 obtaining the electronic credential that corresponds to the user identifier, the method further comprises:

parsing the electronic credential acquisition request, and obtaining a service

validity time comprised in the electronic credential acquisition request; and
 verifying whether the service validity time complies with a service specification;
 and

the obtaining the electronic credential that corresponds to the user identifier
 5 comprises:

if the service validity time complies with the service specification, obtaining the
 electronic credential that corresponds to the user identifier.

5. The method according to claim 4, wherein the obtaining the electronic
 credential that corresponds to the user identifier comprises:

10 after the credential verification end device generates the electronic credential
 based on the user identifier, receiving the electronic credential synchronized by the
 credential verification end device; or

sending request information for obtaining the electronic credential to the
 credential verification end device based on the user identifier to obtain the electronic
 15 credential.

6. The method according to claim 2, wherein the user signature key is an
 asymmetric key.

7. The method according to claim 4, wherein the method further comprises:

20 broadcasting a public key that corresponds to the server private key, so that the
 client software and the credential verification end device verify the signature
 information based on a server public key.

8. A method for processing two-dimensional barcodes, comprising:

25 receiving, by client software, server signature information and an electronic
 credential that are sent by a server, wherein the server signature information is
 obtained by the server by signing the electronic credential and a user public key of the
 client software by using a server private key;

verifying the server signature information to obtain the electronic credential;

30 obtaining a user key that corresponds to the user public key, and signing the
 electronic credential by using the user key to obtain client software signature
 information; and

generating a two-dimensional barcode based on predetermined security
 information, the client software signature information, the server signature
 information, the electronic credential, and the user public key, so that a credential
 verification end device verifies the electronic credential comprised in the two-

dimensional barcode based on the predetermined security information and the user public key, wherein the predetermined security information has validity duration, and the credential verification end device is configured to generate the electronic credential based on a user identifier.

5 9. The method according to claim 8, wherein before the obtaining the user key that corresponds to the user public key, the method further comprises:

receiving a user signature key allocated to the electronic credential and sent by the server; and

obtaining the user key that corresponds to the user public key comprises:

10 obtaining a first user key comprised in the user signature key allocated by the server to the electronic credential; or

obtaining a second user key generated by the client software and corresponding to the user public key.

15 10. The method according to claim 9, wherein the signing the electronic credential by using the user key comprises:

signing the electronic credential by using the first user key; or

signing the electronic credential by using the second user key.

11. The method according to claim 8, wherein the verifying the server signature information comprises:

20 receiving and storing a server public key broadcast by the server; and

verifying the server signature information based on the server public key, the client software public key, and the electronic credential.

12. The method according to any one of claims 8 to 11, wherein the user public key and the user key are asymmetric keys.

25 13. The method according to claim 12, wherein the generating the two-dimensional barcode based on predetermined security information, the client software signature information, the server signature information, the electronic credential, and the user public key comprises:

setting the validity duration of the predetermined security information; and

30 generating the two-dimensional barcode based on the predetermined security information, the client software signature information, the server signature information, the electronic credential, the user public key, the validity duration of the predetermined security information, and the user identifier.

14. A method for processing two-dimensional barcodes, comprising:

obtaining, by a credential verification end device, a two-dimensional barcode in client software, wherein the two-dimensional barcode is generated by the client software based on predetermined security information, client software signature information, server signature information, an electronic credential, and a user public key, the client software signature information is obtained by the client software by signing the electronic credential, and the server signature information is obtained by a server by signing the electronic credential and the user public key;

verifying validity duration of the predetermined security information, and verifying the client software signature information and the server signature information;

if verification on each of the predetermined security information, the client software signature information, and the server signature information succeeds, obtaining a service validity time comprised in the electronic credential for verification; and

if verification on the service validity time comprised in the electronic credential succeeds, determining that verification on the electronic credential succeeds.

15. The method according to claim 14, wherein before the obtaining the two-dimensional barcode in client software, the method further comprises:

generating the electronic credential based on a user identifier; and

synchronizing the corresponding electronic credential to the server based on the user identifier, so that the server sends the electronic credential to the client software; or

receiving request information for obtaining the electronic credential sent by the server, and sending the electronic credential to the server, wherein the request information for obtaining the electronic credential comprises the user identifier.

16. The method according to claim 15, wherein the verifying the client software signature information and the server signature information comprises:

obtaining the user public key comprised in the two-dimensional barcode, and verifying the client software signature information based on the user public key and the electronic credential;

receiving and storing a server public key corresponding to a server private key and broadcast by the server; and

verifying the server signature information based on the server public key, the client software public key, and the electronic credential.

17. The method according to claim 16, wherein before the determining that verification on the electronic credential succeeds, the method further comprises:

obtaining the user identifier comprised in the two-dimensional barcode, and verifying the user identifier; and

5 the determining that verification on the electronic credential succeeds comprises:
if it is determined that the verification on the user identifier succeeds, determining that the verification on the electronic credential succeeds.

18. A server, comprising:

10 a receiving unit, configured to receive an electronic credential acquisition request sent by client software, wherein the electronic credential acquisition request comprises a user identifier;

a first acquisition unit, configured to obtain an electronic credential that corresponds to the user identifier received by the receiving unit;

15 a signing unit, configured to sign the electronic credential and a user public key of the client software by using a server private key to obtain server signature information; and

20 a sending unit, configured to send the server signature information obtained by the signing unit and the electronic credential obtained by the first acquisition unit to the client software, so that the client software verifies the server signature information within a validity time of a user key, and generates a two-dimensional barcode based on the electronic credential so that a credential verification end device verifies the electronic credential comprised in the two-dimensional barcode, wherein the credential verification end device is configured to generate the electronic credential based on the user identifier.

25 19. The server according to claim 18, wherein the signing unit comprises:

an allocation module, configured to allocate a user signature key to the electronic credential;

30 a first signing module, configured to sign, by using the server private key, the electronic credential and a first user public key allocated by the allocation module, wherein the allocated user signature key comprises the first user public key;

an acquisition module, configured to obtain a second user public key sent by the client software; and

a second signing module, configured to sign, by using the server private key, the electronic credential and the second user public key obtained by the acquisition

module.

20. The server according to claim 19, wherein if the first user public key is signed by using the server private key, the sending unit is further configured to send the allocated user signature key, the server signature information, and the electronic credential to the client software.

21. The server according to any one of claims 18 to 20, wherein the server further comprises:

a parsing unit, configured to: before the first acquisition unit obtains the electronic credential that corresponds to the user identifier, parse the electronic credential acquisition request;

a second acquisition unit, configured to: after the parsing unit parses the electronic credential acquisition request, obtain a service validity time comprised in the electronic credential acquisition request; and

a verification unit, configured to verify whether the service validity time obtained by the second acquisition unit complies with a service specification, wherein the first acquisition unit is further configured to: when the verification unit verifies that the service validity time complies with the service specification, obtain the electronic credential that corresponds to the user identifier.

22. The server according to claim 21, wherein the first acquisition unit comprises:

a receiving module, configured to: after the credential verification end device generates the electronic credential based on the user identifier, receive the electronic credential synchronized by the credential verification end device; and

a processing module, configured to send request information for obtaining the electronic credential to the credential verification end device based on the user identifier to obtain the electronic credential.

23. The server according to claim 19, wherein the user signature key is an asymmetric key.

24. The server according to claim 21, wherein the server further comprises:

a broadcasting unit, configured to broadcast a public key that corresponds to the server private key, so that the client software and the credential verification end device verify the signature information based on a server public key.

25. A client software, comprising:

a first receiving unit, configured to receive server signature information and an

electronic credential that are sent by a server, wherein the server signature information is obtained by the server by signing the electronic credential and a user public key of the client software by using a server private key;

5 a signature verification unit, configured to verify the server signature information to obtain the electronic credential;

an acquisition unit, configured to obtain a user key that corresponds to the user public key;

a signing unit, configured to sign the electronic credential by using the user key obtained by the acquisition unit to obtain client software signature information; and

10 a generation unit, configured to generate a two-dimensional barcode based on predetermined security information, the client software signature information, the server signature information, the electronic credential, and the user public key, so that a credential verification end device verifies the electronic credential comprised in the two-dimensional barcode based on the predetermined security information and the
15 user public key, wherein the predetermined security information has validity duration, and the credential verification end device is configured to generate the electronic credential based on a user identifier.

26. The client software according to claim 25, wherein the client software further comprises:

20 a second receiving unit, configured to: before obtaining the user key that corresponds to the user public key, receive a user signature key allocated to the electronic credential and sent by the server; and

the acquisition unit is further configured to obtain a first user key comprised in the user signature key that is allocated by the server to the electronic credential and
25 that is received by the second receiving unit; and

the acquisition unit is further configured to obtain a second user key generated by the client software and corresponding to the user public key.

27. The client software according to claim 26, wherein the signing unit comprises:

30 a first signing module, configured to sign the electronic credential by using the first user key; and

a second signing module, configured to sign the electronic credential by using the second user key.

28. The client software according to claim 25, wherein the signature verification

unit comprises:

a receiving module, configured to receive a server public key broadcast by the server;

5 a storage module, configured to store the server public key received by the receiving module; and

a signature verification module, configured to verify the server signature information based on the server public key stored by the storage module, the client software public key, and the electronic credential.

10 29. The client software according to any one of claims 25 to 28, wherein the user public key and the user key are asymmetric keys.

30. The client software according to claim 29, wherein the generation unit comprises:

a setting module, configured to set the validity duration of the predetermined security information; and

15 a generation module, configured to generate the two-dimensional barcode based on the predetermined security information, the client software signature information, the server signature information, the electronic credential, the user public key, the validity duration of the predetermined security information, and the user identifier.

31. A credential verification end device, comprising:

20 a first acquisition unit, configured to obtain a two-dimensional barcode in client software, wherein the two-dimensional barcode is generated by the client software based on predetermined security information, client software signature information, server signature information, an electronic credential, and a user public key, the client software signature information is obtained by the client software by signing the electronic credential, and the server signature information is obtained by a server by signing the electronic credential and the user public key;

a first verification unit, configured to verify validity duration of the predetermined security information obtained by the first acquisition unit;

30 a second verification unit, configured to verify the client software signature information and the server signature information;

a third verification unit, configured to: when verification of the first verification unit on the predetermined security information succeeds, verification of the second verification unit on each of the client software signature information and the server signature information succeeds, obtain a service validity time comprised in the

electronic credential for verification; and

a determining unit, configured to: when verification of the third verification unit on the service validity time comprised in the electronic credential succeeds, determine that verification on the electronic credential succeeds.

5 32. The credential verification end device according to claim 31, wherein the credential verification end device further comprises:

a generation unit, configured to generate the electronic credential based on a user identifier before the first acquisition unit obtains the two-dimensional barcode in the client software;

10 a synchronizing unit, configured to synchronize the corresponding electronic credential to the server based on the user identifier, so that the server sends the electronic credential to the client software;

a receiving unit, configured to receive request information for obtaining the electronic credential sent by the server; and

15 a sending unit, configured to send the electronic credential to the server, wherein the request information for obtaining the electronic credential comprises the user identifier.

33. The credential verification end device according to claim 32, wherein the second verification unit comprises:

20 an acquisition module, configured to obtain the user public key comprised in the two-dimensional barcode;

a first signature verification module, configured to verify the client software signature information based on the user public key obtained by the acquisition module and the electronic credential;

25 a receiving module, configured to receive a server public key corresponding to a server private key and broadcast by the server;

a storage module, configured to store the server public key received by the receiving module; and

30 a second verification module, configured to verify the server signature information based on the server public key stored by the storage module, the client software public key, and the electronic credential.

34. The credential verification end device according to claim 33, wherein the credential verification end device further comprises:

a second acquisition unit, configured to: before the determining unit determines

that the verification on the electronic credential succeeds, obtain the user identifier comprised in the two-dimensional barcode; and

a fourth verification unit, configured to verify the user identifier obtained by the second acquisition unit, wherein

5 the determining unit is further configured to: when the fourth verification unit determines that the verification on the user identifier succeeds, determine that the verification on the electronic credential succeeds.

35. A system for processing two-dimensional barcodes, wherein the system comprises:

10 client software, configured to send an electronic credential acquisition request to a server, wherein the electronic credential acquisition request comprises a user identifier;

the server, configured to receive the electronic credential acquisition request sent by the client software, and obtain an electronic credential from a credential
15 verification end device based on the user identifier; and

the credential verification end device, configured to receive and respond to request information for obtaining the electronic credential sent by the server, and send the electronic credential to the server, wherein

the server is further configured to receive the electronic credential sent by the
20 credential verification end device, sign the electronic credential and a user public key of the client software to obtain server signature information, and send the server signature information and the electronic credential to the client software;

the client software is configured to receive the server signature information and the electronic credential that are sent by the server, verify the server signature
25 information to obtain the electronic credential, obtain a user key that corresponds to the user public key, sign the electronic credential by using the user key to obtain client software signature information, and generate a two-dimensional barcode based on predetermined security information, the client software signature information, the server signature information, the electronic credential, and the user public key; and

30 the credential verification end device is configured to obtain the two-dimensional barcode in the client software, verify validity duration of the predetermined security information, and verify the client software signature information and the server signature information; and if verification on each of the predetermined security information, the client software signature information, and the server signature

information succeeds, obtain a service validity time comprised in the electronic credential for verification, and if verification on the service validity time comprised in the electronic credential succeeds, determine that verification on the electronic credential succeeds.