CLAIMS

What is claimed is:

1. A method for implementing a one-touch login service, comprising:

obtaining, by an operator server, information about a first IP address from a verification request sent by an application client device, wherein the first IP address is an IP address of a terminal device on which the application client device that sends the verification request is installed, before the operator server sends a token;

after obtaining the information about the first IP address, sending, by the operator server, the token to the application client device, such that after receiving the token, the application client device sends information about a second IP address and the received token to an application server, wherein the second IP address is an IP address of a terminal device on which the application client device that sends the token to the application server is installed, after the operator server sends the token;

obtaining, by the operator server, the information about the second IP address from a number acquisition request sent by the application server; and

determining, by the operator server, whether the first IP address is the same as the second IP address; and if the first IP address is the same as the second IP address, obtaining, based on the token carried in the number acquisition request, a mobile phone number of the terminal device on which the application client device is installed, and sending the mobile phone number to the application server; or if the first IP address is different from the second IP address, refusing to send the mobile phone number of the terminal device to the application server.

2. The method according to claim 1, wherein the verification request comprises at least one of the following requests:

a login verification request that carries an APP ID, an APP sign, a KEY ID, a timestamp, and the first IP address;

a mobile phone identity verification request that carries an APP ID, the first IP address, and a timestamp; and

a verification request that carries an APP ID and the first IP address.

3. The method according to claim 2, wherein when the verification request comprises the mobile phone identity verification request that carries the APP ID, the information about the first IP address, and the timestamp,

before the obtaining the information about the first IP address, the method further comprises: receiving, by using an https link, a login verification request sent by the application client device, generating a symmetric key after login verification succeeds, and sending the symmetric key to the application client device by using the https link;

the obtaining the information about the first IP address comprises: decrypting, by using the generated symmetric key, the mobile phone identity verification request sent by the application client device, and obtaining the information about the first IP address from the decrypted mobile phone identity verification request; and

the sending the token to the application client device comprises: encrypting the token by using the symmetric key, and sending the encrypted token to the application client device.

4. A method for implementing a one-touch login service, wherein the method comprises:

before receiving a token, adding, by an application client device installed on a terminal device, information about an IP address of the terminal device to a verification request, and sending the verification request to an operator server;

receiving, by the application client device, the token sent by the operator server;

after receiving the token, sending, by the application client device, the information about the IP address of the terminal device and the received token to an application server; and

determining, by the application client device, that one-touch login succeeds if login authorization sent by the application server is received.

5. The method according to claim 4, wherein the verification request comprises at least one of the following requests:

a login verification request that carries an APP ID, an APP sign, a KEY ID, a timestamp, and the IP address;

a mobile phone identity verification request that carries an APP ID, the IP address, and a timestamp; and

a verification request that carries an APP ID and the IP address.

6. The method according to claim 5, wherein when the verification request comprises the mobile phone identity verification request that carries the APP ID, the IP address, and the timestamp,

before the sending the mobile phone identity verification request to the operator server, the method further comprises: sending a login verification request to the

operator server by using an https link, and receiving, by using the https link, a symmetric key sent by the operator server;

the sending the verification request to the operator server comprises: encrypting the mobile phone identity verification request by using the symmetric key, and sending the encrypted mobile phone identity verification request to the operator server; and

the receiving the token sent by the operator server comprises: receiving an encrypted token sent by the operator server, and decrypting the encrypted token by using the symmetric key to obtain the token.

7. A method for implementing a one-touch login service, wherein the method comprises:

receiving, by an application server, a login request sent by an application client device, and performing login pre-authorization;

receiving, by the application server, a token sent by the application client device and information about an IP address of a terminal device on which the application client device is installed;

adding, by the application server, the received token and the information about the IP address to a number acquisition request, and sending the number acquisition request to an operator server; and

if a mobile phone number, sent by the operator server, of the terminal device on which the application client device is installed is received, performing, by the application server, login authorization based on the mobile phone number.

8. The method according to claim 7, wherein the application server exchanges information with the operator server by using an https link.

9. An apparatus for implementing a one-touch login service, applied to an operator server, comprising:

a first IP address acquisition module, configured to obtain information about a first IP address from a verification request sent by an application client device, wherein the first IP address is an IP address of a terminal device on which the application client device that sends the verification request is installed, before the operator server sends a token;

a token sending module, configured to send the token to the application client device after the information about the first IP address has been obtained, such that after receiving the token, the application client device sends information about a second IP address and the received token to an application server, wherein the second IP address

is an IP address of a terminal device on which the application client device that sends the token to the application server is installed, after the operator server sends the token;

a second IP address acquisition module, configured to obtain the information about the second IP address from a number acquisition request sent by the application server; and

an authorization processing module, configured to determine whether the first IP address is the same as the second IP address, and if the first IP address is the same as the second IP address, obtain, based on the token carried in the number acquisition request, a mobile phone number of the terminal device on which the application client device is installed, and send the mobile phone number to the application server, or if the first IP address is different from the second IP address, refuse to send the mobile phone number of the terminal device to the application server.

10. An apparatus for implementing a one-touch login service, applied to an application client device installed on a terminal device, comprising:

a verification request module, configured to add information about an IP address of the terminal device to a verification request, and send the verification request to an operator server before the application client device receives a token;

a token receiving module, configured to receive the token sent by the operator server;

a forwarding module, configured to send the information about the IP address of the terminal device and the received token to an application server after the application client device receives the token; and

a login authorization module, configured to determine that one-touch login succeeds if login authorization sent by the application server is received.

11. An apparatus for implementing a one-touch login service, applied to an application server, comprising:

a pre-login module, configured to receive a login request sent by an application client device, and perform login pre-authorization;

a network factor acquisition module, configured to receive a token sent by the application client device and information about an IP address of a terminal device in which the application client device is installed;

a number acquisition module, configured to add the received token and the information about the IP address to a number acquisition request, and send the number acquisition request to an operator server; and

an authorization execution module, configured to: if a mobile phone number, sent by the operator server, of the terminal device on which the application client device is located is installed, perform login authorization based on the mobile phone number.

12. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and when executing the executable code, the processor implements the method according to any one of claims 1 to 8.