

IMPLEMENTATION OF ONE-TOUCH LOGIN SERVICE

TECHNICAL FIELD

[0001] One or more embodiments of this specification relate to network information technologies, and in particular, to methods and apparatuses for
5 implementing a one-touch login service.

BACKGROUND

[0002] With the rapid development of networks, various service applications are generated based on the networks. A user only needs to download an application client device, that is, an application (APP), of a corresponding service application from a
10 terminal device, and perform registration and login by using the application client device to enjoy the corresponding service application, for example, watch a movie or buy a product.

[0003] To facilitate use of the user, a new method for logging in to an APP, that is, a one-touch login method, is currently available. In a one-touch login method, an
15 authentication SDK is embedded in advance into an application client device that is usually a mobile phone. When the user requests to log in, the user communicates with an operator server by using the SDK to collect a mobile phone number of the user. After obtaining authorization from the user, the application client device obtains a token invoked by an interface, and transfers the token to an application server. The application
20 server obtains, by using the token, information such as a mobile phone number of the user who grants the authorization to log in to the APP.

[0004] As shown in FIG. 1, in a one-touch login service, the user only needs to tap a related "one-touch login" key, and does not need to enter a mobile phone number, a user name, a password, an SMS verification code, etc. Therefore, the user can more
25 conveniently and quickly complete a registration and login procedure, and the procedure that may originally require approximately 20 seconds is shortened to approximately 2 seconds, thereby significantly facilitating use of the user.

[0005] However, the security of the current one-touch login service is low, and consequently, private data of the user are easily disclosed. Therefore, a securer method for implementing a one-touch login service is required.

SUMMARY

5 [0006] Methods and apparatuses for implementing a one-touch login service are described in one or more embodiments of this specification, so that the security of a one-touch login service can be improved.

[0007] According to a first aspect, a method for implementing a one-touch login service is provided, including the following: obtaining information about a first IP
10 address from a verification request sent by an application client device; sending a token to the application client device; obtaining information about a second IP address from a number acquisition request sent by an application server; and determining 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 a token carried in the number
15 acquisition request, a mobile phone number of a terminal device in which the application client device is located, 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.

20 [0008] The verification request includes 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 newly defined verification request that carries an APP ID and the IP address.

25 [0009] When the verification request includes the mobile phone identity verification request that carries the APP ID, the information about the first IP address, and the timestamp, the sending the token to the application client device includes the following: performing identity verification based on the mobile phone identity verification request, and sending the token to the application client device after the
30 identity verification succeeds.

[0010] Before the obtaining the information about the first IP address, the method further includes the following: 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 includes the following: 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. The sending the token to the application client device includes the following: encrypting the token by using the symmetric key, and sending the encrypted token to the application client device.

10 **[0011]** According to a second aspect, a method for implementing a one-touch login service is provided, including the following: adding information about an IP address of a terminal device to a verification request, and sending the verification request to an operator server; receiving a token sent by the operator server; sending the information about the IP address of the terminal device and the received token to an application server; and determining that one-touch login succeeds if login authorization sent by the application server is received.

[0012] The verification request includes 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 newly defined verification request that carries an APP ID and the IP address.

[0013] Before the sending the mobile phone identity verification request to the operator server, the method further includes the following: 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 includes the following: 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. The receiving the token sent by the operator server includes the following: receiving an encrypted token sent by the operator server, and decrypting the encrypted token by using the symmetric key to obtain the token.

[0014] According to a third aspect, a method for implementing a one-touch login service is provided, including the following: performing login pre-authorization after receiving a login request sent by an application client device; receiving 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 located; adding 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
5 by the operator server, of the terminal device in which the application client device is located is received, performing login authorization based on the mobile phone number.

[0015] Information is exchanged with the operator server by using an https link.

[0016] According to a fourth aspect, an apparatus for implementing a one-touch login service is provided, including the following: a first IP address acquisition module,
10 configured to obtain information about a first IP address from a verification request sent by an application client device; a token sending module, configured to send a token to the application client device; a second IP address acquisition module, configured to obtain information about a second IP address from a number acquisition request sent by an application server; and an authorization processing module, configured to
15 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 a token carried in the number acquisition request, a mobile phone number of a terminal device in which the application client device is located, and send the mobile phone number to the application server, or if the first IP address is different from the second IP address,
20 refuse to send the mobile phone number of the terminal device to the application server.

[0017] According to a fifth aspect, an apparatus for implementing a one-touch login service is provided, including the following: a verification request module, configured to add information about an IP address of a terminal device to a verification request, and send the verification request to an operator server; a token receiving
25 module, configured to receive a 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; and a login authorization module, configured to determine that one-touch login succeeds if login authorization sent by the application server is received.

30 **[0018]** According to a sixth aspect, an apparatus for implementing a one-touch login service is provided, including the following: 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 located; 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,
5 sent by the operator server, of the terminal device in which the application client device is located is received, perform login authorization based on the mobile phone number.

[0019] According to a seventh aspect, a computing device is provided, including a memory and a processor. The memory stores executable code, and when executing the executable code, the processor implements the method described in any embodiment of
10 this specification.

[0020] The methods and apparatuses for implementing a one-touch login service provided in the embodiments of this specification can prevent an application server from providing a corresponding application service for a terminal device of an attacker, and improve the security.

15 BRIEF DESCRIPTION OF DRAWINGS

[0021] To describe the technical solutions in the embodiments of this specification or in the existing technology more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments or the existing technology. Clearly, the accompanying drawings in the following descriptions show
20 some embodiments of this application, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0022] FIG. 1 is a schematic diagram illustrating an operation of a one-touch login service;

[0023] FIG. 2 is a schematic diagram illustrating a system architecture to which an
25 embodiment of this specification is applied;

[0024] FIG. 3 is a flowchart illustrating a method for implementing a one-touch login service on an operator server, according to an embodiment of this specification;

[0025] FIG. 4 is a flowchart illustrating a method for implementing a one-touch login service on an application client device, according to an embodiment of this
30 specification;

[0026] FIG. 5 is a flowchart illustrating a method for implementing a one-touch login service on an application server, according to an embodiment of this specification;

[0027] FIG. 6 is a flowchart illustrating a method in which an operator server, an application client device, and an application server cooperate to implement a one-touch login server, according to an embodiment of this specification;

[0028] FIG. 7 is a schematic diagram illustrating a structure of a one-touch login service apparatus, according to an embodiment of this specification;

[0029] FIG. 8 is a schematic diagram illustrating a structure of a one-touch login service apparatus, according to another embodiment of this specification; and

[0030] FIG. 9 is a schematic diagram illustrating a structure of a one-touch login service apparatus, according to still another embodiment of this specification.

10

DESCRIPTION OF EMBODIMENTS

[0031] Solutions provided in this specification are described below with reference to the accompanying drawings.

[0032] To facilitate understanding of the methods provided in this specification, a system architecture involved in and applicable to this specification is described first.

15 As shown in FIG. 2, the system architecture mainly includes three network nodes: an application client device, an application server, and an operator server.

[0033] The application client device is installed on and runs in a terminal device, and the terminal device can include but is not limited to an intelligent mobile terminal, a smart household device, a network device, a wearable device, a smart medical device, a personal computer (PC), etc. The intelligent mobile terminal can include a mobile phone, a tablet computer, a notebook computer, a personal digital assistant (PDA), an Internet vehicle, etc. The smart household device can include a smart appliance device, such as a smart TV, a smart air conditioner, a smart water heater, a smart refrigerator, a smart air purifier, etc. The smart household device can further include a smart door lock, a smart socket, a smart light, a smart camera, etc. A network device can include a switch, a wireless AP, a server, etc. The wearable device can include a smart watch, smart glasses, a smart band, a virtual reality device, an augmented reality device, a hybrid reality device (that is, a device that can support virtual reality and augmented reality), etc. The smart medical device can include a smart thermometer, a smart blood pressure monitor, a smart blood glucometer, etc.

25
30

[0034] The application client device can be various types of applications, including but not limited to a payment application, a multimedia playback application, a map

application, a text editing application, a financial application, a browser application, an instant messaging application, etc.

[0035] The operator server is a server-end device of a provider that provides a network service, and can be a single server or a server group including multiple servers.

5 The operator server is responsible for providing network services for various applications, for example, performing security authentication and providing a mobile phone number for one-touch login.

[0036] The application server is a specific application server, and specifically provides a corresponding application service for the application client device. For
10 example, for an application client device such as Alipay, the application server is a server that provides an Alipay service.

[0037] It should be understood that a quantity of application client devices, a quantity of application servers, and a quantity of operator servers in FIG. 2 are merely examples. Any quantity can be selected and disposed based on implementation needs.

15 **[0038]** As shown in FIG. 2, the application client device, the application server, and the operator server interact with each other via a network. The network can include various connection types, such as a wired or wireless communication link or an optical fiber cable.

[0039] A method for implementing a one-touch login service provided in this
20 specification relates to three network nodes shown in FIG. 2. Therefore, processing performed by the operator server, processing performed by the application client device, and processing performed by the application server in a one-touch login service are separately described below by using different embodiments.

[0040] First, processing performed by the operator server in the one-touch login
25 service is described.

[0041] FIG. 3 is a flowchart illustrating a method for implementing a one-touch login service on an operator server, according to an embodiment of this specification. As shown in FIG. 3, the method includes the following steps.

[0042] Step 301: Obtain information about a first IP address from a verification
30 request sent by an application client device.

[0043] Step 303: Send a token to the application client device.

[0044] Step 305: Obtain information about a second IP address from a number acquisition request sent by an application server.

[0045] Step 307: 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, perform step 309, or if the first IP address is different from the second IP address, perform step 311.

[0046] Step 309: Obtain, based on a token carried in the number acquisition request,
5 a mobile phone number of a terminal device in which the application client device is located, and send the mobile phone number to the application server.

[0047] Step 311: Refuse to send the mobile number of the terminal device to the application server.

[0048] In an existing one-touch login service, the following cases may occur: An
10 attacker uses a terminal device X to steal a token to be sent to an application client device; after that, the attacker pretends, by using the terminal device X, to be a terminal device Y in which the application client device is located to send the token to the application server. Because the used token is correct, the application server can obtain, from an operator server, a mobile phone number of the terminal device Y in which the
15 application client device is located, and consequently, the application server mistakenly considers that the terminal device X that sends the token is the terminal device Y in which the application client device is located, that is, considers that the attacker is an authorized user of the application client device, and therefore provides a corresponding application service for the attacker, for example, playing video information that only
20 the authorized user has the permission to watch or transferring money, thereby causing a security problem to use of the user and causing the leakage of private data of the user.

[0049] It can be determined from the process shown in FIG. 3 that the operator server obtains, before sending the token, the first IP address sent by the application client device (the first IP address corresponds to an IP address of a terminal device that
25 requests one-touch login from the operator server before the token is sent, for example, the first IP address is denoted as an IP address of the terminal device Y), and obtains, after sending the token, the second IP address sent by the application server (the second IP address corresponds to an IP address of a terminal device that requests one-touch login by using the application server after the token is sent). If the two IP addresses are
30 the same, it can be considered that in a one-touch login service, a terminal device that communicates with the operator server before the token is sent and a terminal device that communicates with the application server after the token is sent are the same terminal device, and are the terminal device Y, that is, a terminal device that currently performs the one-touch login service with the application server (that is, a terminal

device that sends the token to the application server) is the terminal device Y used by the authorized user, and the sent token is not stolen by the attacker, and no attack behavior occurs. Therefore, the operator server can provide the mobile phone number of the terminal device Y in which the application client device is located for the application server, so that the application server provides a corresponding application service for the terminal device Y that is currently connected to the application server. On the contrary, if the two IP addresses are different, it can be considered that in a one-touch login service, the terminal device Y that communicates with the operator server before the token is sent and the terminal device X that communicates with the application server after the token is sent are not the same terminal device, that is, the terminal device X that is currently connected to the application server is not the terminal device Y used by the authorized user, but the terminal device X used by an attacker who has stolen the token, and attack behavior has occurred. Therefore, the operator server does not provide, for the application server, the mobile phone number of the terminal device Y in which the application client device is located, so that the application server cannot provide a corresponding application service for the terminal device X of the attacker that is currently connected to the application server. It can be determined that the method in this embodiment of this specification prevents the application server from providing a corresponding application service of the application client device for a terminal device of an attacker, and improves the security.

[0050] The process shown in FIG. 3 is described below with reference to a specific embodiment.

[0051] First, for step 301, the operator server obtains the information about the first IP address from the verification request sent by the application client device.

[0052] It can be understood that the application client device sends the verification request to the operator server by using the terminal device Y in which the application client device is located, and the verification request carries an IP address of the terminal device Y, which is denoted as the first IP address.

[0053] The verification request that carries the first IP address can include any one or more of the following: Verification request 1: In a one-touch login service, before the operator server sends the token, the application client device sends a login verification request to the operator server so as to verify the identity of the application client device. Therefore, the login verification request can carry the IP address of the terminal device and is sent to the operator server. Correspondingly, the verification

request in step 301 can be a login verification request that carries an APP ID, an APP sign, a KEY ID, a timestamp, and the first IP address.

[0054] Verification request 2: In a one-touch login service, before the operator server sends the token, the application client device sends a mobile phone identity verification request to the operator server to verify the identity of the terminal device in which the application client device is located. Therefore, the mobile phone identity verification request can be used to carry the first IP address, and is sent to the operator server. Correspondingly, the verification request in step 301 can be a mobile phone identity verification request that carries an APP ID, the first IP address, and a timestamp.

[0055] Verification request 3: Before the operator server sends the token, the application client device can send the first IP address to the operator server by using a newly defined verification request. Correspondingly, the verification request in step 301 can be a newly defined verification request that carries an APP ID and the first IP address.

[0056] The verification request in step 301 is the verification request 2, that is, the mobile phone identity verification request that carries the APP ID, the first IP address, and the timestamp. In this case, to improve the security and avoid leakage of the first IP address of the terminal device Y and other information, encryption processing can be performed. Specifically, before step 301, the operator server receives, by using an https link, a login verification request sent by the application client device. After login verification succeeds, the operator server generates a symmetric key, and sends the symmetric key to the application client device by using the https link. In this way, the application client device encrypts, by using the symmetric key, the mobile phone identity verification request that carries the APP ID, the first IP address, and the timestamp, and then sends the encrypted mobile phone identity verification request to the operator server. Correspondingly, an implementation process of step 301 includes the following: The operator server decrypts, by using the symmetric key, the mobile phone identity verification request sent by the application client device, and obtains the information about the first IP address from the decrypted mobile phone identity verification request.

[0057] Next, for step 303, the operator server sends the token to the application client device.

[0058] Here, after receiving the mobile phone identity verification request, the operator server performs identity verification based on the mobile phone identity

verification request, and sends the token to the application client device after the identity verification succeeds.

[0059] As described above, if the operator server generates the symmetric key, in step 303, the operator server encrypts the token by using the symmetric key, and sends
5 the encrypted token to the application client device to prevent leakage of the token as far as possible.

[0060] After the application client device obtains the token, if the token is encrypted, the application client device can decrypt the encrypted token by using the pre-obtained symmetric key to obtain the token. After the application client device
10 obtains the token, the application client device can send the token to the application server. In addition, for subsequent validity verification, the application client device also denotes the IP address of the terminal device in which the application client device is located as the second IP address, and also sends the second IP address to the application server. The application server adds the received token and the second IP
15 address to the number acquisition request, and sends the number acquisition request to the operator server.

[0061] Next, for step 305, the information about the second IP address is obtained from the number acquisition request sent by the application server.

[0062] When this step is performed, the operator server obtains two IP addresses
20 from the application client device and the application server.

[0063] Next, in step 307 to step 311, as described above, the operator server determines whether the two IP addresses are the same. If the two IP addresses are the same, it can be considered that, in a one-touch login service, a terminal device that communicates with the operator server before the token is sent and a terminal device
25 that communicates with the application server after the token is sent are the same terminal device, and are the terminal device Y, that is, a terminal device that currently performs a one-touch login service with the application server is the terminal device Y used by the authorized user. Therefore, the operator server can provide, for the application server, the mobile phone number of the terminal device Y in which the application client device is located, so that the application server provides a
30 corresponding application service for the terminal device Y that is currently connected to the application server. On the contrary, if the two IP addresses are different, it can be considered that in a one-touch login service, the terminal device Y that communicates with the operator server before the token is sent and the terminal device X that

communicates with the application server after the token is sent are not the same terminal device, that is, the terminal device X that is currently connected to the application server is not the terminal device Y used by the authorized user, but the terminal device X used by an attacker who has stolen the token, and attack behavior has occurred. Therefore, the operator server does not provide, for the application server, the mobile phone number of the terminal device Y in which the application client device is located, so that the application server cannot provide a corresponding application service for the terminal device X that is currently connected to the application server. It can be determined that the method in this embodiment of this specification prevents the application server from providing a corresponding application service of the application client device for a terminal device of an attacker, and improves the security.

[0064] It should be noted that, in this embodiment of this specification, the IP address can be either or two of an Internet Protocol Version 4 (IPv4) address and an Internet Protocol Version 6 (IPv6) address.

[0065] In embodiments of this specification, the application client device can communicate with the application server by using a dedicated link. Before the symmetric key is obtained, the application client device can communicate with the operator server by using an https link. After the symmetric key is obtained, the application client device can communicate with the operator server by using the http link. The application server can communicate with the operator server by using the https link.

[0066] Processing performed by the application client device in the one-touch login service is described below.

[0067] FIG. 4 is a flowchart illustrating a method for implementing a one-touch login service on an application client device, according to an embodiment of this specification. As shown in FIG. 4, the method includes the following: Step 401: Add information about an IP address of a terminal device to a verification request, and send the verification request to an operator server.

[0068] For descriptions of specific implementation of step 401, reference can be made to all the previous descriptions of step 301.

[0069] For example, the verification request in step 401 includes 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 newly defined verification request that carries an APP ID and the IP address.

[0070] For another example, in a implementation, the verification request is the mobile phone identity verification request that carries the APP ID, the information about the IP address of the terminal device, and the timestamp. In this case, before the sending the mobile phone identity verification request to the operator server, the method further includes the following: The application client device sends a login verification request to the operator server by using an https link, and receives, by using the https link, a symmetric key sent by the operator server. In step 401, the application client device encrypts the mobile phone identity verification request by using the symmetric key, and sends the encrypted mobile phone identity verification request to the operator server. In step 403, a token sent by the operator server is received.

[0071] For descriptions of specific implementation of step 403, reference can be made to all the previous descriptions of step 303. For example, the application client device receives an encrypted token sent by the operator server, and decrypts the encrypted token by using the symmetric key to obtain the token.

[0072] Step 405: Send the information about the IP address of the terminal device and the received token to an application server.

[0073] To perform validity verification on the operator server, when sending the token to the application server, the application client device needs to add the IP address of the terminal device in which the application client device is located.

[0074] Step 407: If login authorization sent by the application server is received, one-touch login succeeds, and if the login authorization sent by the application server is not received, the one-touch login fails.

[0075] Processing performed by the application server in the one-touch login service is described below.

[0076] FIG. 5 is a flowchart illustrating a method for implementing a one-touch login service on an application server, according to an embodiment of this specification. As shown in FIG. 5, the method includes the following: Step 501: Receive a login request sent by an application client device, and perform login pre-authorization.

[0077] When an application client device needs to use a one-touch login service, the application client device first sends a login request to the application server to trigger start of the one-touch login service. The application server performs login pre-authorization, for example, sends a pre-login interface to the application client device.

Then, the application client device performs step 401 to step 405. For details, reference can be made to all related descriptions of step 401 to step 405.

[0078] Step 503: Receive a token sent by the application client device and information about an IP address of a terminal device in which the application client
5 device is located.

[0079] Here, if the token is not stolen by an attacker, a terminal device that communicates with the application server in step 503 and the terminal device in step 501 are the same terminal device, for example, denoted as a terminal device Y. In step 503, the application server receives an IP address of the terminal device Y.

10 [0080] On the contrary, if the token is stolen by the attacker, the terminal device that communicates with the application server in step 503 and the terminal device in step 501 are not the same terminal device. For example, the terminal device that performs communication in step 503 is denoted as a terminal device X. In step 503, the application server receives an IP address of the terminal device X.

15 [0081] Step 505: 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.

[0082] In step 505, the application server can send the number acquisition request to the operator server by using an https link.

20 [0083] For processing performed after the operator server receives the number acquisition request, reference can be made to all the previous descriptions of step 305 to step 311.

[0084] Step 507: If a mobile phone number, sent by the operator server, of the terminal device in which the application client device is located is received, perform
25 login authorization based on the mobile phone number.

[0085] A method for implementing a one-touch login service is described below with reference to cooperated processing of the application client device, the application server, and the operator server. In this method, before the operator server sends a token, as an example for description, the application client device uses the previous
30 verification request 2, that is, the mobile phone identity verification request, to carry the IP address of the terminal device. As shown in FIG. 6, the method includes the following steps.

[0086] Step 601: The application client device sends, by using a dedicated link, a login request to an application server that the application client device belongs to.

[0087] In step 601, the application client device is an application (APP) installed in a terminal device. The application client device can send the login request in this step after being triggered by a user.

[0088] There is a dedicated link between the application client device and the application server. Therefore, the login request can be sent by using the dedicated link instead of a public network.

[0089] Step 603: After receiving the login request, the application server performs login pre-authorization, including the following: sending a pre-login interface to the application client device by using the dedicated link.

10 [0090] Step 605: The application server sends a login verification request to an operator server by using an https link.

[0091] Here, the https link is an encrypted link, and sending the login verification request by using the https link can further improve the security.

[0092] In step 605, the login verification request can include information such as an application client device identifier (APP ID), an application client device signature (APP sign), a key identifier (KEY ID), and a timestamp.

[0093] Step 607: The operator server performs authentication on an identity of the application client device based on the received login verification request, and after the authentication succeeds, generates a session key and sends the key to the application client device by using the https link.

[0094] Here, the key is a symmetric key.

[0095] Step 609: The application client device generates a mobile phone identity verification request that carries an APP ID, an IP address of a terminal device in which the application client device is located, and a timestamp, encrypts the mobile phone identity verification request by using the symmetric key, and sends the encrypted mobile phone identity verification request to the operator server by using the http link.

[0096] Here, the IP address of the terminal device in which the application client device is located that is carried in the mobile phone identity verification request can include an IPv4 address and an IPv6 address.

30 [0097] Step 611: The operator server decrypts the mobile phone identity verification request by using the key, performs identity verification, obtains information about a first IP address from the mobile phone identity verification request after the identity verification succeeds, encrypts a token by using the symmetric key, and sends the encrypted token to the application client device.

[0098] Here, the operator server stores the IP address, obtained before the token is sent, of the terminal device in which the application client device is located, and the IP address is denoted as the first IP address.

5 [0099] Step 613: After decrypting the token by using the symmetric key, the application client device sends the token and the IP address of the terminal device in which the application client device is located to the application server by using a dedicated link.

[0100] Step 615: The application server adds an APP ID, the received token, and the IP address to a number acquisition request, and sends the number acquisition request
10 to the operator server by using the https link.

[0101] Step 617: The operator server determines whether an IP address (recorded as a second IP address) sent by the application server is the same as the previously obtained first IP address, and if the second IP address is the same as the first IP address, the operator server sends, to the application server by using the https link, a mobile
15 phone number of the terminal device that is queried from a gateway, or otherwise, current one-touch login fails.

[0102] For example, when one-touch login fails, the operator server returns a number acquisition failure message to the application server.

[0103] Step 619: If the application server receives the mobile phone number, sent
20 by the operator server, of the terminal device in which the application client device is located, the application server performs successful login authorization on the application client device based on the mobile phone number by using the dedicated link.

[0104] In an embodiment of this specification, an apparatus for implementing a one-touch login service is provided, and is disposed in an operator server. As shown in
25 FIG. 7, the apparatus includes the following: a first IP address acquisition module 701, configured to obtain information about a first IP address from a verification request sent by an application client device; a token sending module 702, configured to send a token to the application client device; a second IP address acquisition module 703, configured to obtain information about a second IP address from a number acquisition request sent
30 by an application server; and an authorization processing module 704, 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 a token carried in the number acquisition request, a mobile phone number of a terminal device in which the application client device is located, 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.

[0105] In an embodiment of this specification, the first IP address acquisition module 701 is configured to obtain the first IP address from any one or more 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 newly defined verification request that carries an APP ID and the first IP address.

[0106] In an embodiment of this specification, the verification request is the mobile phone identity verification request that carries the APP ID, the information about the first IP address, and the timestamp. The first IP address acquisition module 701 is configured to obtain the information about the first IP address from the mobile phone identity verification request. The token sending module 702 is configured to perform identity verification based on the mobile phone identity verification request, and send the token to the application client device after the identity verification succeeds.

[0107] In an embodiment of this specification, the apparatus for implementing a one-touch login service that is applied to the operator server further includes the following: a login verification module, configured to receive, by using an https link, a login verification request sent by the application client device, and perform login verification based on the login verification request; and a key generation module, configured to generate a symmetric key after the verification performed by the login verification module succeeds, and send the symmetric key to the application client device by using the https link. The first IP address acquisition module 701 is configured to decrypt, by using the generated symmetric key, the mobile phone identity verification request sent by the application client device, and obtain the information about the first IP address from the decrypted mobile phone identity verification request. The token sending module 702 is configured to encrypt the token by using the symmetric key, and send the encrypted token to the application client device.

[0108] In an embodiment of this specification, an apparatus for implementing a one-touch login service is provided, and is disposed in an application client device. As shown in FIG. 8, the apparatus includes the following: a verification request module 801, configured to add information about an IP address of a terminal device in which the application client device is located to a verification request, and send the verification request to an operator server; a token receiving module 802, configured to receive a

token sent by the operator server; a forwarding module 803, configured to send the information about the IP address of the terminal device in which the application client device is located and the received token to an application server; and a login authorization module 804, configured to determine that one-touch login succeeds if
5 login authorization sent by the application server is received.

[0109] In an embodiment of this specification, the verification request module 801 is configured to send any one or more of the following requests to the operator server: 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
10 ID, the first IP address, and a timestamp; and a newly defined verification request that carries an APP ID and the first IP address.

[0110] In an embodiment of this specification, when the verification request module 801 sends the mobile phone identity verification request that carries the APP ID, the first IP address, and the timestamp, the apparatus for implementing a one-touch
15 login service that is applied to the application client device further includes the following: a login request module, configured to send a login verification request to the operator server by using an https link, and receive, by using the https link, a symmetric key sent by the operator server. The verification request module 801 is configured to encrypt the mobile phone identity verification request by using the symmetric key, and
20 send the encrypted mobile phone identity verification request to the operator server. The token receiving module 802 is configured to receive the encrypted token sent by the operator server, and decrypt the encrypted token by using the symmetric key to obtain the token.

[0111] In an embodiment of this specification, an apparatus for implementing a
25 one-touch login service is provided, and is disposed in an application server. As shown in FIG. 9, the apparatus includes the following: a pre-login module 901, configured to perform login preprocessing after a login request sent by an application client device is received; a network factor acquisition module 902, configured to receive a token sent by the application client device and information about an IP address of a terminal device
30 in which the application client device is located; a number acquisition module 903, 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 904, configured to: if a mobile phone

number of the terminal device in which the application client device is located is received, perform login authorization based on the mobile phone number.

[0112] In an embodiment of this specification, the number acquisition module 903 is configured to send the number acquisition request to the operator server by using an https link. The authorization execution module 904 is configured to receive, by using the https link, the mobile phone number of the terminal device in which the application client device is located that is sent by the operator server.

[0113] One implementation of this specification provides a computer-readable storage medium. The computer-readable storage medium stores a computer program. When the computer program is executed on a computer, the computer is enabled to perform the method in any implementation in this specification.

[0114] One implementation of this specification provides a computing device, including a memory and a processor. The memory stores executable code, and when executing the executable code, the processor implements the method in any implementation in this specification.

[0115] It can be understood that a structure shown in embodiments of this specification does not constitute a specific limitation on the apparatus in the embodiments of this specification. In other embodiments of this specification, the apparatus can include more or fewer components than those shown in the figure, or can combine some components, or can split some components, or can have different component arrangements. The components shown in the figure can be implemented by hardware, software, or a combination of software and hardware.

[0116] Content such as information exchange and execution processes between modules in the apparatus and the system is based on a same concept as that in the method embodiment of this specification. For specific content, reference can be to the descriptions in the method embodiment of this specification. Details are omitted here.

[0117] The embodiments in this specification are described in a progressive way. For same or similar parts of the embodiments, reference can be made to the embodiments mutually. Each embodiment focuses on a difference from other embodiments. In particular, the apparatus embodiment is basically similar to the method embodiment, and therefore is described briefly. For related parts, references can be made to related descriptions in the method embodiment.

[0118] A person skilled in the art should be aware that in the previous one or more examples, functions described in this application can be implemented by hardware,

software, widget, or any combination thereof. When being implemented by software, these functions can be stored in a computer-readable medium or transmitted as one or more instructions or codes in the computer-readable medium.

[0119] The specific implementations mentioned above provide further detailed
5 explanations of the objectives, technical solutions, and beneficial effects of this
application. It should be understood that the previously mentioned descriptions are
merely specific implementations of this application and are not intended to limit the
protection scope of this application. Any modifications, equivalent replacements,
improvements, etc. made on the basis of the technical solutions of this application shall
10 all fall within the protection scope of this application.

CLAIMS

What is claimed is:

1. A method for implementing a one-touch login service, comprising:
obtaining information about a first IP address from a verification request sent by
5 an application client device;
sending a token to the application client device;
obtaining information about a second IP address from a number acquisition
request sent by an application server; and
determining whether the first IP address is the same as the second IP address; and
10 if the first IP address is the same as the second IP address, obtaining, based on a token
carried in the number acquisition request, a mobile phone number of a terminal device
in which the application client device is located, 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
15 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;
20 a mobile phone identity verification request that carries an APP ID, the first IP
address, and a timestamp; and
a newly defined 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
25 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;
30 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
5 comprises:

adding information about an IP address of a terminal device to a verification request, and sending the verification request to an operator server;

receiving a token sent by the operator server;

10 sending the information about the IP address of the terminal device and the received token to an application server; and

determining 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:

15 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 newly defined verification request that carries an APP ID and the IP address.

20 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
25 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

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

receiving 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 located;

5 adding 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

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

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

9. An apparatus for implementing a one-touch login service, comprising:

15 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;

 a token sending module, configured to send a token to the application client device;

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

20 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 a token carried in the number acquisition request, a mobile phone number of a terminal device in which the application client device is located, and send the mobile phone number to the application server, or if the first IP
25 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, comprising:

30 a verification request module, configured to add information about an IP address of a terminal device to a verification request, and send the verification request to an operator server;

 a token receiving module, configured to receive a 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; 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, comprising:

5 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 located;

10 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 in which the application client device is located is received, perform login authorization based on the mobile phone number.

15 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.