

Claims

1. A method comprising:

receiving, by a first computing platform, a first request sent by a second computing platform, the first request comprising a first identifier, wherein the first identifier is used for identifying the second computing platform and is allocated to the second computing platform by the first computing platform after the second computing platform accesses the first computing platform;

obtaining a second identifier corresponding to the first identifier, the second identifier being used for identifying an identity of the second computing platform in the first computing platform;

obtaining a third identifier corresponding to the first request, the third identifier being an account of a login user registered on the first computing platform;

encrypting the third identifier using the second identifier to transform the third identifier to a fourth identifier, the fourth identifier being used for identifying the login user whose registration information on the first computing platform is encrypted based on the identity of the second computing platform and

returning the fourth identifier to the second computing platform, the fourth identifier differentiating identity information of the login user from another identity information of the login user returned to another second computing platform.

2. The method of claim 1, wherein the first request further comprises a service processing parameter, and prior to encrypting the third identifier using the second identifier to obtain the fourth identifier, the method further comprises performing corresponding service processing on the service processing parameter based on the third identifier, to obtain a service processing result.

3. The method of claim 2, further comprising returning the service processing result when the fourth identifier is returned to the second computing platform.

4. The method of claim 1, wherein, prior to receiving, by the first computing platform, the first request sent by the second computing platform, the method further comprises:

presenting an authorization page in response to the login user accessing the first computing platform from the second computing platform;

obtaining a call-back address corresponding to the second computing platform inputted from the second computing platform;

in response to detecting an authorization operation of the login user in the authorization page to authorize accessing the first computing platform from the second computing platform, adding a preset authorization code to the call-back address, and jumping to a page corresponding to the call-back address; and

returning a corresponding authorization token to the second computing platform responsive to the token request, upon receiving the token request sent by the second computing platform, wherein the token request comprises an authorization code.

5. The method of claim 4, wherein receiving, by the first computing platform, the request sent by the second computing platform comprises:

detecting, by the first computing platform, that the second computing platform calls a corresponding API interface in the first computing platform using the authorization token; and

receiving, by the first computing platform, the first request transmitted by the second computing platform through the API interface.

6. The method of claim 4, wherein the third identifier comprises a label, and obtaining the third identifier corresponding to the first request comprises:

locating an API interface corresponding to the authorization token;

checking whether one or more parameters in the API interface comprise a parameter that includes the label; and

obtaining the parameter that includes the label as the third identifier if affirmative.

7. The method of claim 1, wherein obtaining the second identifier corresponding to the first identifier comprises:

obtaining an association database, the association database comprising an association relationship between the first identifier and the second identifier;

searching the first identifier in the association database; and

obtaining the second identifier that matches the first identifier.

8. The method of claim 1, wherein encrypting the third identifier using the second identifier to transform the third identifier to the fourth identifier comprises:

obtaining an encryption key; and

encrypting the third identifier using the encryption key and the second identifier to transform the third identifier to the fourth identifier.

9. One or more computing-readable media storing executable instructions that, when executed by one or more processors of a first computing platform, cause the one or more processors to perform acts comprising:

receiving a first request sent by a second computing platform, the request comprising a first identifier and a fourth identifier, wherein the first identifier is used for identifying the second computing platform and is allocated to the second computing platform by the first computing platform after the second computing platform accesses the first computing platform, and the fourth identifier is returned to the second computing platform by the first computing platform and is used for identifying a login user registered on the first computing platform whose registration information on the first computing platform is encrypted based on an identity of the second computing platform in the first computing platform;

obtaining a second identifier corresponding to the first identifier, the second identifier being used for identifying the identity of the second computing platform in the first computing platform; and

decrypting the fourth identifier using the second identifier to transform the fourth identifier to a third identifier, the third identifier being an account of the login user registered on the first computing platform, the fourth identifier differentiating identity information of the login user from another identity information of the login user returned to another second computing platform.

10. The one or more computing-readable media of claim 9, wherein the request further comprises a service processing parameter, and after decrypting the fourth identifier using the second identifier to obtain the third identifier, the method further comprises:

performing corresponding service processing on the service processing parameter based on the third identifier to obtain a second service processing result;

encrypting the third identifier using the second identifier to transform the third identifier to the fourth identifier; and

returning the fourth identifier and the service processing result to the second computing platform.

11. The one or more computing-readable media of claim 9, wherein decrypting the fourth identifier using the second identifier to obtain the third identifier comprises:

obtaining a decryption key; and

decrypting the fourth identifier using the decryption key and the second identifier to transform the fourth identifier to the third identifier.

12. The one or more computing-readable media of claim 9, wherein the acts further comprise adding a label to the third identifier after decrypting the fourth identifier using the second identifier to obtain the third identifier.

13. An apparatus comprising:

one or more processors;

memory;

a first request receiving module stored in the memory and that when executed by the one or more processors, receives a request sent by a second computing platform, the request comprising a first identifier, the first identifier being used for identifying the second computing platform and allocated to the second computing platform by the first computing platform after the second computing platform accesses the first computing platform;

a second identifier acquisition module stored in the memory and that when executed by the one or more processors, obtains a second identifier corresponding to the first identifier, the second identifier used for identifying an identity of the second computing platform in the first computing platform and related to an identity document of the second computing platform;

a third identifier acquisition module stored in the memory and that when executed by the one or more processors, obtains a third identifier corresponding to the first request, the third identifier being an account of a login user registered on the first computing platform;

an encryption module stored in the memory and that when executed by the one or more processors, encrypts to encrypt the third identifier using the second identifier to transform the third identifier to a fourth identifier, the fourth identifier being returned to the second computing platform by the first computing platform and used for identifying the login user whose registration information on the first computing platform is encrypted based on the identity of the second computing platform in the first computing platform; and

an identifier returning module stored in the memory and that when executed by the one or more processors, returns the fourth identifier to the second computing platform, the fourth identifier differentiating identity information of the login user from another identity information of the login user returned to another second computing platform.

14. The apparatus of claim 13, wherein the first request further comprises a service processing parameter, and the apparatus further comprises a first service processing module stored in the memory and that when executed by the one or more processors, performs corresponding service processing on the service processing parameter based on the third identifier to obtain a service processing result.

15. The apparatus of claim 14, further comprising a first result returning module stored in the memory and that when executed by the one or more processors, returns the service processing result when the fourth identifier is returned to the second computing platform.

16. The apparatus of claim 13, further comprising:

an authorization page presentation module stored in the memory and that when executed by the one or more processors, presents an authorization page in response to the login user accessing the first computing platform from the second computing platform;

a call-back address acquisition module stored in the memory and that when executed by the one or more processors, obtains a call-back address corresponding to the second computing platform inputted from the second computing platform;

an authorization code adding module stored in the memory and that when executed by the one or more processors, adds a preset authorization code to the call-back address and jumps to a page corresponding to the call-back address after an authorization operation of the login in user in the authorization page to authorize accessing the first computing platform from the second computing platform is detected; and

an authorization module stored in the memory and that when executed by the one or more processors, returns a corresponding authorization token to the second computing platform for a token request, after the token request sent by the second computing platform is received, wherein the token request comprises an authorization code.

17. The apparatus of claim 16, wherein the first request receiving module comprises:

an interface calling sub-module stored in the memory and that when executed by the one or more processors, detects that the second computing platform calls a corresponding API interface in the first computing platform using the authorization token; and

a request receiving sub-module stored in the memory and that when executed by the one or more processors, receives the first request transmitted by the second computing platform through the API interface.

18. The apparatus of claim 16, wherein the third identifier comprises a label, and the third identifier acquisition module comprises:

an interface positioning sub-module stored in the memory and that when executed by the one or more processors, locates the API interface corresponding to the authorization token;

an interface determination sub-module stored in the memory and that when executed by the one or more processors, checks whether one or more parameters in the API interface comprise a parameter that includes the label; and

an identifier obtaining sub-module stored in the memory and that when executed by the one or more processors, obtains parameter that includes the label as the third identifier, in response to the parameters in the API interface comprising the parameter that includes the label.

19. The method of claim 13, wherein the second identifier acquisition module comprises:

- an association database obtaining sub-module stored in the memory and that when executed by the one or more processors, obtains an association database, the association database comprising an association relationship between the first identifier and the second identifier;

- a matching sub-module stored in the memory and that when executed by the one or more processors, searches the first identifier in the association database; and

- a second identifier obtaining sub-module stored in the memory and that when executed by the one or more processors, obtains the second identifier matching the first identifier.

20. The apparatus of claim 13, wherein the encryption module comprises:

- a key acquisition sub-module stored in the memory and that when executed by the one or more processors, obtains an encryption key; and

- an encryption sub-module stored in the memory and that when executed by the one or more processors, encrypts the third identifier using the encryption key and the second identifier to transform the third identifier to the fourth identifier.