

[0039] sending a query result to the first application, wherein the query result comprises identification information of the first service provider, the public key of the first service provider, and the first identity information;

5 [0040] receiving secure identity information from the first application, wherein the secure identity information comprises the identification information of the first service provider and encrypted information, and the encrypted information is obtained by encrypting the verified first identity information by using the public key of the first service provider; and

10 [0041] sending the encrypted information to the first service provider according to the identification information of the first service provider.

[0042] In one embodiment, before receiving a query request from the first application, the method further comprises:

[0043] receiving the registration information from the first service provider; and

15 [0044] generating a two-dimensional code for the first service provider based on the registration information.

[0045] In one embodiment, the registration information further comprises routing information of the first service provider; and sending the encrypted information to the first service provider specifically comprises:

20 [0046] extracting the identification information of the first service provider and the encrypted information respectively from the secure identity information;

[0047] determining the routing information of the first service provider according to the identification information of the first service provider; and

25 [0048] sending the encrypted information to a terminal corresponding to the first service provider according to the routing information.

[0049] According to a possible design, the registration platform and a server of a specific application are located in the same physical entity; moreover, the query request comprises a first field, in the case that the first field has a first value, the first application is indicated to be the specific application, and in the

30

user may be collected or received through the client. In addition, other steps, including the steps of the trusted application interacting with the verification source, as well as the steps of interacting with the registration platform, are all performed through the server.

5 **[00147]** FIG. 3 shows a method for obtaining secure identity information according to another embodiment. In the embodiment of FIG. 3, a registration platform and a specific application are located in the same physical entity, so it is simply shown as a trusted application + a registration platform. Hereinafter, the entity where the trusted application and the registration platform are located is
10 referred to as a unified server.

[00148] In this case, the registration platform can still interface with multiple trusted applications, including a local specific application and other applications. The service provider still initiates a registration request to the registration platform in advance by using the registration information to obtain
15 and display a two-dimensional code. Each trusted application still obtains two-dimensional code information of the service provider through scanning and initiates a query request to the registration platform for the read two-dimensional code. In one embodiment, the query request may include a specific field (hereinafter referred to as a first field), which is used to indicate whether the
20 trusted application initiating the request is a local trusted application of the registration platform.

[00149] It is assumed that the registration platform receives a query request from a first application. In addition to the two-dimensional code information, the query request further includes the first field. In the case that the
25 first field has a first value (for example, the value is 1), the first application is indicated to be a local specific application of the registration platform, and in the case that the first field has a second value (for example, the value is 0), the first application is indicated not to be a local specific application.

[00150] If the first field has the second value, that is, request information
30 received by the registration platform comes from a non-local trusted application,

[00186] an encrypted information sending unit 55 configured to send the encrypted information to the first service provider according to the identification information of the first service provider.

5 [00187] In one embodiment, the above apparatus 500 further includes a two-dimensional code generation unit 50 configured to receive the registration information from the first service provider; and generate a two-dimensional code for the first service provider based on the registration information.

[00188] In one embodiment, the registration information further includes routing information of the first service provider; and the encrypted information
10 sending unit 55 is specifically configured to:

[00189] extract the identification information of the first service provider and the encrypted information respectively from the secure identity information;

[00190] determine the routing information of the first service provider according to the identification information of the first service provider; and

15 [00191] send the encrypted information to a terminal corresponding to the first service provider according to the routing information.

[00192] According to a possible design, the registration platform and a server of a specific application are located in the same physical entity; moreover, the query request received by query request receiving unit 51 includes a first field.

20 In the case that the first field has a first value, the first application is indicated to be the specific application, and in the case that the first field has a second value, the first application is indicated not to be the specific application.

[00193] Further, in one embodiment, the first field has a first value; at this time, query result sending unit 53 may locally provide the query result to
25 application logic of the first application; moreover, secure information receiving unit 54 may obtain the secure identity information locally from the application logic of the first application.

[00194] According to an embodiment of another aspect, a computer-readable storage medium having a computer program stored thereon is further
30 provided, wherein when the computer program is executed in a computer, the

What Is Claimed Is

1 1. A method for providing secure identity information, wherein the
2 method is performed by a trusted application server, comprising:
3 obtaining two-dimensional code information corresponding to a two-
4 dimensional code scanned by a user, wherein the two-dimensional code is
5 generated by a registration platform in advance for a first service provider;
6 sending a query request to the registration platform, wherein the query
7 request comprises the two-dimensional code information;
8 receiving a query result from the registration platform, wherein the query
9 result comprises identification information of the first service provider, a public
10 key of the first service provider, and first identity information required by the first
11 service provider;
12 obtaining second identity information of the user;
13 sending the second identity information of the user to a verification source
14 to obtain a verification result;
15 generating secure identity information, wherein the secure identity
16 information comprises the identification information of the first service provider
17 and encrypted information, the encrypted information is obtained by encrypting
18 verified first identity information by using the public key of the first service
19 provider, and the verified first identity information is determined based on the
20 second identity information and the verification result; and
21 sending the secure identity information to the registration platform, such
22 that the registration platform sends the encrypted information to the first service
23 provider.

1 2. The method according to claim 1, wherein obtaining the second
2 identity information of the user comprises collecting the second identity
3 information through a terminal where a client of the trusted application is located.

1 3. The method according to claim 2, wherein collecting the second
2 identity information comprises one or more of:
3 collecting face information through a camera on the terminal; and
4 reading identity card information through an NFC function of the terminal
5 and controls thereon.

1 4. The method according to claim 1, wherein obtaining the second
2 identity information of the user comprises receiving input information of the user
3 through the client of the trusted application.

1 5. The method according to claim 1, further comprising determining
2 the verification source and a required verification mode according to the required
3 first identity information and the obtained second identity information.

1 6. The method according to claim 5, wherein the obtained second
2 identity information comprises the required first identity information; and
3 wherein determining the verification source and the required verification
4 mode comprises determining that the required verification mode is an
5 authentication mode, and in the authentication mode, the verification result is a
6 notification result of whether the verification is successful.

1 7. The method according to claim 5, wherein the obtained second
2 identity information is a part of the required first identity information; and

3 wherein determining the verification source and the required verification
4 mode comprises determining that the required verification mode is an information
5 mode, and in the information mode, the verification result comprises a
6 notification of whether the verification is successful, and supplementary identity
7 information determined based on at least a part of the successfully verified second
8 identity information.

1 8. The method according to claim 5, wherein determining the
2 verification source and the required verification mode comprises determining that
3 the verification source comprises a first verification source and a second
4 verification source; and
5 wherein sending the second identity information of the user to the
6 verification source to obtain a verification result comprises:
7 sending a first part of the second identity information to the first
8 verification source, and sending a second part of the second identity information
9 to the second verification source;
10 receiving a first result from the first verification source, and receiving a
11 second result from the second verification source; and
12 combining the first result and the second result to obtain the verification
13 result.

1 9. The method according to claim 1, wherein generating the secure
2 identity information comprises:
3 obtaining verified first identity information based on the second identity
4 information and the verification result;
5 encrypting the verified first identity information by using the public key of
6 the first service provider to obtain the encrypted information; and
7 generating the secure identity information based on the encrypted
8 information and the two-dimensional code information.

1 10. The method according to claim 9, wherein the verification result is
2 a notification result of successful verification in the authentication mode; and
3 wherein obtaining the verified first identity information based on the
4 second identity information and the verification result comprises: using the
5 successfully verified second identity information as the verified first identity
6 information.

1 11. The method according to claim 9, wherein the verification result
2 comprises a notification of successful verification, and supplementary identity
3 information determined based on at least a part of the successfully verified second
4 identity information; and
5 wherein obtaining the verified first identity information based on the
6 second identity information and the verification result comprises: using the
7 successfully verified second identity information and the supplementary identity
8 information as the verified first identity information.

1 12. A method for obtaining secure identity information, wherein the
2 method is performed by a registration platform, comprising:
3 receiving a query request from a first application, wherein the query
4 request comprises two-dimensional code information, and the two-dimensional
5 code information is obtained by scanning, by using the first application, a two-
6 dimensional code generated by the registration platform in advance for a first
7 service provider;
8 determining registration information of the first service provider based on
9 the two-dimensional code information, wherein the registration information
10 comprises at least a public key of the first service provider and first identity
11 information required by the first service provider;
12 sending a query result to the first application, wherein the query result

13 comprises identification information of the first service provider, the public key of
14 the first service provider, and the first identity information;
15 receiving secure identity information from the first application, wherein
16 the secure identity information comprises the identification information of the
17 first service provider and encrypted information, and the encrypted information is
18 obtained by encrypting verified first identity information by using the public key
19 of the first service provider; and
20 sending the encrypted information to the first service provider according
21 to the identification information of the first service provider.

1 13. The method according to claim 12, before receiving a query
2 request from the first application, further comprising:
3 receiving the registration information from the first service provider; and
4 generating a two-dimensional code for the first service provider based on
5 the registration information.

1 14. The method according to claim 13, further comprising
2 generating a service index for the registration information; and
3 storing the service index and the registration information associatively.

1 15. The method according to claim 12, wherein the registration
2 information further comprises routing information of the first service provider;
3 and
4 the sending the encrypted information to the first service provider
5 comprises:
6 extracting the identification information of the first service provider and
7 the encrypted information respectively from the secure identity information;
8 determining the routing information of the first service provider according
9 to the identification information of the first service provider; and

10 sending the encrypted information to a terminal corresponding to the first
11 service provider according to the routing information.

1 16. The method according to claim 12, wherein the registration
2 platform and a server of a specific application are located in the same physical
3 entity; and
4 wherein the query request comprises a first field, in the case that the first
5 field has a first value, the first application is indicated to be the specific
6 application, and in the case that the first field has a second value, the first
7 application is indicated not to be the specific application.

1 17. The method according to claim 16, wherein the first field has a
2 first value;
3 wherein sending the query result to the first application comprises
4 providing an application logic of the first application with the query result locally;
5 and
6 wherein receiving secure identity information from the first application
7 comprises obtaining the secure identity information locally from the application
8 logic of the first application.

1 18. An apparatus for providing secure identity information, wherein
2 the apparatus is deployed in a trusted application server, the apparatus
3 comprising:
4 a two-dimensional code obtaining unit, configured to obtain two-
5 dimensional code information corresponding to a two-dimensional code scanned
6 by a user, wherein the two-dimensional code is generated by a registration
7 platform in advance for a first service provider;
8 a query request sending unit, configured to send a query request to the
9 registration platform, wherein the query request comprises the two-dimensional

10 code information;
11 a query result receiving unit, configured to receive a query result from the
12 registration platform, wherein the query result comprises identification
13 information of the first service provider, a public key of the first service provider,
14 and first identity information required by the first service provider;
15 an identity information obtaining unit, configured to obtain second identity
16 information of the user;
17 a verification sending unit, configured to send the second identity
18 information of the user to a verification source to obtain a verification result;
19 a secure information generation unit, configured to generate secure
20 identity information, wherein the secure identity information comprises the
21 identification information of the first service provider and encrypted information,
22 the encrypted information is obtained by encrypting verified first identity
23 information by using the public key of the first service provider, and the verified
24 first identity information is determined based on the second identity information
25 and the verification result; and
26 a secure information sending unit, configured to send the secure identity
27 information to the registration platform, such that the registration platform sends
28 the encrypted information to the first service provider.

1 19. An apparatus for obtaining secure identity information, wherein
2 the apparatus is deployed in a registration platform, the apparatus comprising:
3 a query request receiving unit, configured to receive a query request from
4 a first application, wherein the query request comprises two-dimensional code
5 information, and the two-dimensional code information is obtained by scanning,
6 by using the first application, a two-dimensional code generated by the
7 registration platform in advance for a first service provider;
8 a registration information determination unit, configured to determine
9 registration information of the first service provider based on the two-dimensional

10 code information, wherein the registration information comprises at least a public
11 key of the first service provider and first identity information required by the first
12 service provider;
13 a query result sending unit, configured to send a query result to the first
14 application, wherein the query result comprises identification information of the
15 first service provider, the public key of the first service provider, and the first
16 identity information;
17 a secure information receiving unit, configured to receive secure identity
18 information from the first application, wherein the secure identity information
19 comprises the identification information of the first service provider and
20 encrypted information, and the encrypted information is obtained by encrypting
21 verified first identity information by using the public key of the first service
22 provider; and
23 an encrypted information sending unit, configured to send the encrypted
24 information to the first service provider according to the identification
25 information of the first service provider.

1 20. A computer-readable storage medium, having a computer program
2 stored thereon, wherein when the computer program is executed in a computer,
3 the computer is caused to perform the method according to any one of claims 1 to
4 17.

1 21. A computing device, comprising a memory and a processor, and
2 characterized in that an executable code is stored in the memory, and when the
3 processor executes the executable code, the method according to any one of
4 claims 1 to 17 is performed.