

What Is Claimed Is:

1. A computer-executed method for providing secure identity information of a user to a service provider, the method comprising:
 - scanning, by a terminal device associated with the user, a graphic code associated with the service provider to obtain coded information included in the graphic code;
 - querying, via a first communication link, a registration platform based on the coded information to obtain an identifier of the service provider, an encryption key associated with the service provider, and a user-identity-information requirement associated with the service provider;
 - obtaining identity information of the user;
 - determining, based on the user-identity-information requirement associated with the service provider, a verification source and a verification mode;
 - submitting, via a second communication link, the obtained identity information of the user along with the determined verification mode to the determined verification source to allow the verification source to query a trusted database to obtain verified identity information of the user according to the verification mode;
 - receiving, via the second communication link, the verified identity information of the user from the verification source;
 - generating secure identity information for the user by encrypting, using the encryption key, at least the verified identity information of the user, wherein the secure identity information comprises the identifier of the service provider;
 - and
 - sending, via the first communication link, the secure identity information to the registration platform, thereby allowing the registration platform to forward, via a third communication link, the encrypted verified identity information of the user to the service provider.

2. The method according to claim 1, wherein the graphic code is generated by the registration platform for the service provider in advance.
3. The method according to claim 1, wherein obtaining the identity information of the user comprises one or more of:
 - collecting face information using a camera associated with the terminal device;
 - reading identity card information using a near-field communication (NFC) reader associated with the terminal device; and
 - receiving input information from the user.
4. The method according to claim 1, wherein determining the required verification mode comprises:
 - in response to determining that the obtained identity information of the user meets the user-identity-information requirement, determining that the required verification mode is an authentication mode, in which the verification source is configured to return a notification indicating whether the identity information of the user is verified.
5. The method according to claim 1, wherein determining the required verification mode comprises:
 - in response to determining that the obtained identity information of the user partially meets the user-identity-information requirement, determining that the required verification mode is an information mode, in which the verification source is configured to return a notification indicating whether the identity

information of the user is verified and supplementary identity information of the user determined based on the verified identity information of the user.

6. The method according to claim 5, wherein generating the secure identity information for the user further comprises encrypting, using the encryption key, the verified identity information of the user and the supplementary identity information of the user.

7. The method according to claim 1:
wherein determining the verification source comprises determining that the verification source comprises a first verification source and a second verification source; and

wherein the method further comprises:

sending a first part of the identity information of the user to the first verification source and sending a second part of the identity information of the user to the second verification source;

receiving a first verification result from the first verification source, and receiving a second verification result from the second verification source; and

combining the first verification result and the second verification result to obtain a combined verification result.

8. A computer system, comprising:
a processor;
a storage device coupled to the processor and storing instructions, which when executed by the processor cause the processor to perform a method for

providing secure identity information of a user to a service provider, the method comprising:

- scanning a graphic code associated with the service provider to obtain coded information included in the graphic code;

- querying, via a first communication link, a registration platform based on the coded information to obtain an identifier of the service provider, an encryption key associated with the service provider, and a user-identity-information requirement associated with the service provider;

- obtaining identity information of the user;

- determining, based on the user-identity-information requirement associated with the service provider, a verification source and a verification mode;

- submitting, via a second communication link, the obtained identity information of the user along with the determined verification mode to the determined verification source to allow the verification source to query a trusted database to obtain verified identity information of the user according to the verification mode;

- receiving, via the second communication link, the verified identity information of the user from the verification source;

- generating secure identity information for the user by encrypting, using the encryption key, at least the verified identity information of the user, wherein the secure identity information comprises the identifier of the service provider; and

- sending, via the first communication link, the secure identity information to the registration platform, thereby allowing the registration platform to forward, via a third communication link, the encrypted verified identity information of the user to the service provider.

9. The computer system according to claim 8, wherein the graphic code is generated by the registration platform for the service provider in advance.

10. The computer system according to claim 8, wherein obtaining the identity information of the user comprises one or more of:

collecting face information using a camera associated with the computer system;

reading identity card information using a near-field communication (NFC) reader associated with the computer system; and

receiving input information from the user.

11. The computer system according to claim 8, wherein determining the required verification mode comprises:

in response to determining that the obtained identity information of the user meets the user-identity-information requirement, determining that the required verification mode is an authentication mode, in which the verification source is configured to return a notification indicating whether the identity information of the user is verified.

12. The computer system according to claim 8, wherein determining the required verification mode comprises:

in response to determining that the obtained identity information of the user partially meets the user-identity-information requirement, determining that the required verification mode is an information mode, in which the verification source is configured to return a notification indicating whether the identity

information of the user is verified and supplementary identity information of the user determined based on the verified identity information of the user.

13. The computer system according to claim 12, wherein generating the secure identity information for the user further comprises encrypting, using the encryption key, the verified identity information of the user and the supplementary identity information of the user.

14. The computer system according to claim 8:
wherein determining the verification source comprises determining that the verification source comprises a first verification source and a second verification source; and

wherein the method performed by the processor further comprises:

 sending a first part of the identity information of the user to the first verification source and sending a second part of the identity information of the user to the second verification source;

 receiving a first verification result from the first verification source, and receiving a second verification result from the second verification source; and

 combining the first verification result and the second verification result to obtain a combined verification result.

15. A computer-executed method for obtaining secure identity information of a user, the method comprising:

 receiving, by a registration platform from an application running on a terminal device of the user, a query request comprising coded information, wherein the coded information is obtained by scanning, via the terminal device, a

graphic code generated by the registration platform in advance for a service provider, and wherein the query request comprises a field indicating whether a server of the application and the registration platform reside in a same physical entity;

determining registration information of the service provider based on the coded information, wherein the registration information comprises at least an encryption key associated with the service provider and a user-identity-information requirement associated with the service provider;

sending the determined registration information of the service provider and an identifier of the service provider to the application to allow the application to determine a verification source and a verification mode based at least on the registration information;

receiving, by the registration platform from the application, the secure identity information of the user, wherein the secure identity information comprises the identifier of the service provider and encrypted information, wherein the encrypted information is obtained by encrypting verified identity information of the user using the encryption key, and wherein the verified identity information of the user is received by the application from the verification source according to the verification mode; and

sending the encrypted information to the service provider based on the identifier of the service provider.

16. The method according to claim 15, further comprising:
receiving the registration information from the service provider; and
generating the graphic code for the service provider based on the registration information.

17. The method according to claim 16, further comprising generating a service index for the registration information; and storing, by the registration platform, the service index and the registration information associatively.

18. The method according to claim 15, wherein the registration information further comprises routing information of the service provider; and wherein sending the encrypted information to the service provider comprises:
extracting the identifier of the service provider and the encrypted information respectively from the secure identity information;
determining the routing information of the service provider based on the identifier of the service provider; and
sending the encrypted information to a terminal device corresponding to the service provider based on the routing information.

19. The method according to claim 15, wherein:
if the server of the application and the registration platform reside in a same physical entity,
sending the query result to the application comprises providing an application logic of the application with the query result locally; and
receiving the secure identity information of the user from the application comprises obtaining the secure identity information locally from the application logic of the application.