

CLAIMS

What is claimed is:

1. A computer-implemented method for identity authentication and registration number binding, comprising:

receiving, by one or more servers of a data authentication platform, a user identity authentication request of a user sent by a client of the data authentication platform, wherein the user identity authentication request comprises first user authentication information and user identification information, and the one or more servers of the data authentication platform pre-store second user authentication information and a registration number and a secret token that correspond to the user identification information;

obtaining, by the one or more servers according to the user identification information, the second user authentication information pre-stored in the one or more servers of the data authentication platform;

matching, by the one or more servers, the first user authentication information in the received user identity authentication request with the obtained second user authentication information pre-stored in the one or more servers of the data authentication platform;

in response to the matching succeeding and in response to receiving, by the one or more servers from the client of the data authentication platform, a request for obtaining the registration number, obtaining, by the one or more servers, the registration number and the secret token that correspond to the user identification information, wherein obtaining the registration number and the secret token comprises:

sending a plurality of registration numbers of the user to the client of the data authentication platform, and

obtaining the registration number that is selected by the user from the plurality of registration numbers from the client and the secret token that corresponds to the registration number selected by the user; and

sending, by the one or more servers, the obtained registration number and the secret token to a third-party organization server.

2. The method according to claim 1, wherein

before receiving the user identity authentication request sent by the client of the data authentication platform, the method further comprises:

generating, by the one or more servers, the secret token that corresponds to the user identification information by using the registration number that corresponds to the user

identification information; and

sending, by the one or more servers, the generated secret token to the third-party organization server.

3. The method according to claim 1, wherein the one or more servers of the data authentication platform pre-store a unique identification (ID) corresponding to the user identification information; and

after receiving the user identity authentication request sent by the client of the data authentication platform, the method further comprises: obtaining, by the one or more servers, according to the unique ID, the second user authentication information pre-stored in the one or more servers of the data authentication platform.

4. The method according to claim 1, further comprising:

receiving, by the third-party organization server, the registration number and the secret token from the one or more servers of the data authentication platform;

matching, by the third-party organization server, the received secret token corresponding to the registration number with pre-stored secret tokens sent by the one or more servers of the data authentication platform;

in response to the matching between the received secret token and the pre-stored secret tokens succeeding, saving, by the third-party organization server, the received registration number in association with pre-stored user identification information in the third-party organization server;

receiving, by the third-party organization server, a user number binding request from a third-party organization client, wherein the user number binding request comprises the first user authentication information and the user identification information;

obtaining, by the third-party organization server, according to the user identification information, third user authentication information pre-stored in the third-party organization server;

matching, by the third-party organization server, the first user authentication information in the received user number binding request with the obtained third user authentication information pre-stored in the third-party organization server;

in response to the matching between the first user authentication information and the third user authentication information succeeding, obtaining, by the third-party organization server, the saved registration number according to the user identification information in the received user number binding request; and

sending, by the third-party organization server, the obtained saved registration number to

the third-party organization client.

5. The method according to claim 4, wherein the third-party organization server pre-stores a unique identification (ID) corresponding to the user identification information; and

after receiving the user number binding request from the third-party organization client, the method further comprises: obtaining, by the third-party organization server according to the unique ID, the third user authentication information pre-stored in the third-party organization server.

6. The method according to claim 5, wherein before receiving the registration number and the secret token from one or more servers of the data authentication platform, the method further comprises: receiving, by the third-party organization server, the secret token from the one or more servers of the data authentication platform, wherein the secret token is generated by the one or more servers of the data authentication platform according to the registration number.

7. The method according to claim 4, further comprising:

receiving, by the third-party organization client, the registration number from the third-party organization server; and

receiving, by the third-party organization client, a confirmation by the user for binding the registration number.

8. The method according to claim 7, wherein receiving the registration number from the third-party organization server comprises:

receiving a registration number selected by the user and sent by the third-party organization server; or

receiving each registration number sent by the third-party organization server and obtaining a registration number selected by the user.

9. The method according to claim 4, wherein the registration number corresponds to a payment account, and the method further comprises:

receiving, by the third-party organization server, from the third-party organization client, a confirmation of the registration number sent from the third-party organization server, wherein the confirmation indicates a success in binding the payment account with a payment application maintained by the third-party organization server and accessible from the third-party organization client.

10. One or more non-transitory computer-readable storage media storing instructions executable by one or more processors, wherein execution of the instructions causes the one or more processors to perform operations comprising:

receiving a user identity authentication request of a user sent by a client of a data authentication platform, wherein the user identity authentication request comprises first user authentication information and user identification information, and one or more servers of the data authentication platform pre-store second user authentication information and a registration number and a secret token that correspond to the user identification information;

obtaining, according to the user identification information, the second user authentication information pre-stored in the one or more servers of the data authentication platform;

matching the first user authentication information in the received user identity authentication request with the obtained second user authentication information pre-stored in the one or more servers of the data authentication platform;

in response to the matching succeeds and in response to receiving, from the client of the data authentication platform, a request for obtaining the registration number, obtaining the registration number and the secret token that correspond to the user identification information, wherein obtaining the registration number and the secret token comprises:

 sending a plurality of registration numbers of the user to the client of the data authentication platform, and

 obtaining the registration number that is selected by the user from the plurality of registration numbers from the client and the secret token that corresponds to the registration number selected by the user; and

 sending the obtained registration number and secret token to a third-party organization server.

11. The one or more non-transitory computer-readable storage media according to claim 10, wherein before receiving the user identity authentication request sent by the client of the data authentication platform, the operations further comprise:

 generating the secret token by using the registration number; and

 sending the generated secret token to the third-party organization server.

12. The one or more non-transitory computer-readable storage media according to claim 10, wherein the operations further comprise:

 receiving the registration number and the secret token from the one or more servers of the data authentication platform;

 matching the received secret token corresponding to the registration number with pre-stored secret tokens sent by the one or more servers of the data authentication platform;

 in response to the matching between the received secret token and the pre-stored secret tokens succeeding, saving the received registration number in association with pre-stored user

identification information in the third-party organization server;

receiving a user number binding request from a third-party organization client, wherein the user number binding request comprises the first user authentication information and the user identification information;

obtaining, according to the user identification information, third user authentication information pre-stored in the third-party organization server;

matching the first user authentication information in the received user number binding request with the obtained third user authentication information pre-stored in the third-party organization server;

in response to the matching between the first user authentication information and the third user authentication information succeeding, obtaining the saved registration number according to the user identification information in the received user number binding request; and

sending the obtained saved registration number to the third-party organization client.

13. The one or more non-transitory computer-readable storage media according to claim 12, wherein the operations further comprise:

receiving the registration number from the third-party organization server; and

receiving a confirmation by the user for binding the registration number.

14. The one or more non-transitory computer-readable storage media according to claim 12, wherein the registration number corresponds to a payment account, and the operations further comprise:

receiving, from the third-party organization client, a confirmation of the registration number sent from the third-party organization server, wherein the confirmation indicates a success in binding the payment account with a payment application maintained by the third-party organization server and accessible from the third-party organization client.

15. A system comprising one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

receiving a user identity authentication request of a user sent by a client of a data authentication platform, wherein the user identity authentication request comprises first user authentication information and user identification information, and one or more servers of the data authentication platform pre-store second user authentication information and a registration number and a secret token that correspond to the user identification information;

obtaining, according to the user identification information, the second user authentication

information pre-stored in the one or more servers of the data authentication platform;

matching the first user authentication information in the received user identity authentication request with the obtained second user authentication information pre-stored in the one or more servers of the data authentication platform;

in response to the matching succeeding and in response to receiving, from the client of the data authentication platform, a request for obtaining the registration number, obtaining the registration number and the secret token that correspond to the user identification information, wherein obtaining the registration number and the secret token comprises:

 sending a plurality of registration numbers of the user to the client of the data authentication platform, and

 obtaining the registration number that is selected by the user from the plurality of registration numbers from the client and the secret token that corresponds to the registration number selected by the user; and

 sending the obtained registration number and the secret token to a third-party organization server.

16. The system according to claim 15, wherein before receiving the user identity authentication request sent by the client of the data authentication platform, the operations further comprise:

 generating the secret token by using the registration number; and

 sending the generated secret token to the third-party organization server.

17. The system according to claim 15, wherein the operations further comprise:

 receiving the registration number and the secret token from the one or more servers of the data authentication platform;

 matching the received secret token corresponding to the registration number with pre-stored secret tokens sent by the one or more servers of the data authentication platform;

 in response to the matching between the received secret token and the pre-stored secret tokens succeeding, saving the received registration number in association with pre-stored user identification information in the third-party organization server;

 receiving a user number binding request from a third-party organization client, wherein the user number binding request comprises the first user authentication information and the user identification information;

 obtaining, according to the user identification information, third user authentication information pre-stored in the third-party organization server;

 matching the first user authentication information in the received user number binding

request with the obtained third user authentication information pre-stored in the third-party organization server;

in response to the matching between the first user authentication information and the third user authentication information succeeding, obtaining the saved registration number according to the user identification information in the received user number binding request; and

sending the obtained saved registration number to the third-party organization client.

18. The system according to claim 17, wherein the operations further comprise:

receiving the registration number from the third-party organization server; and

receiving a confirmation by the user for binding the registration number.

19. The system according to claim 17, wherein the registration number corresponds to a payment account, and the operations further comprise:

receiving, from the third-party organization client, a confirmation of the registration number sent from the third-party organization server, wherein the confirmation indicates a success in binding the payment account with a payment application maintained by the third-party organization server and accessible from the third-party organization client.