Claims

1. An information interaction method, comprising:

receiving, by a terminal, an authentication factor issued by a first server terminal, the authentication factor carrying an authentication key and account information of a user, and a dynamic time factor, the first server terminal being a server terminal that completes a first service operation after authenticating the terminal when the terminal requests the first service operation (S101);

generating, by the terminal, bound authentication information by using the authentication factor and device information of the terminal, and returning, by the terminal, the bound authentication information to the first server terminal, such that the first server terminal performs authorization through the first service operation according to the bound authentication information (S102); and

generating, by the terminal, a graphical identifier for completing the first service operation offline according to the authentication factor, the graphical identifier carrying authentication information of the first service operation, the authentication information of the first service operation comprising the authentication key of the user, device account information, and a dynamic password, the dynamic password being generated according to the dynamic time factor, and the device account information being generated according to the account information of the user and the device information of the terminal (S103).

2. The method of claim 1, before the step of generating a graphical identifier for completing the first service operation offline according to the authentication factor, further comprising:

receiving a display instruction for displaying the graphical identifier for completing the first service operation offline (S1031); and

generating the graphical identifier for completing the first service operation offline according to the authentication factor after the display instruction is received (S1032);

wherein after the step of generating a graphical identifier for completing the first service operation offline according to the authentication factor, the method further comprises:

displaying, by the terminal, the graphical identifier, to complete the first service operation in an offline state by using the graphical identifier (S1033).

3. The method of claim 2, wherein a displaying mode of the graphical identifier comprises one or a combination of: a bar code and a QR code; and

after the step of displaying, by the terminal, the graphical identifier, the method further

comprises:

switching the displaying mode of the graphical identifier when receiving a switch instruction for the displaying mode of the graphical identifier (S1034).

4. The method of claim 1, wherein the terminal receives, through a second terminal, the authentication factor issued by the first server terminal; and returns the bound authentication information to the first server terminal through the second terminal.

5. The method of claim 1, before the step of receiving an authentication factor issued by a first server terminal, further comprising:

sending, by the terminal, an account identity verification request to the first server terminal;

receiving a verification result sent by the first server terminal after identity verification is successful;

sending an authorization verification request for the offline first service operation to the first server terminal; and

receiving the authentication factor issued by the first server terminal after authorization verification is successful.

6. The method of claim 1, wherein the dynamic password remains unchanged in a same time window, and in a next time window, the dynamic password is regenerated according to the dynamic time factor, to change dynamically.

7. The method of claim 1, wherein the dynamic password is specifically obtained through calculation by using the authentication key of the user, the dynamic time factor, the device account information, and a preset password length according to a one-time password calculating method.

8. The method of claim 2, further comprising:

acquiring, by a second server terminal, the authentication information of the first service operation carried in the graphical identifier displayed on the terminal (S201);

generating a first service operation request by using the authentication information of the first service operation and service data, and sending the first service operation request to the first server terminal, such that the first server terminal performs authentication according to the authentication information of the first service operation carried in the first service operation

request, and completes the first service operation after the authentication is successful (S202); and

receiving a result of the first service operation returned by the first server terminal (S203).

9. The method of claim 8, further comprising:

receiving, by the first server terminal, the first service operation request sent by the second server terminal (S301); and

performing authentication according to the authentication information carried in the first service operation request (S302), and completing, by the first server terminal, the first service operation when the authentication is successful. (S303)

10. The method of claim 9, before the step of receiving a first service operation request sent by a second server terminal, further comprising:

performing, by the first server terminal, online account binding on the terminal.

11. The method of claim 10, wherein the step of performing, by the first server terminal, online account binding on the terminal specifically comprises:

receiving an account identity verification request sent by the terminal, the account identity verification request carrying account information of the user (S401);

determining whether the account identity verification request passes verification, and sending a verification result of successful verification to the terminal if the verification is successful (S402);

receiving an authorization verification request, sent by the terminal, for completing the first service operation offline (S403);

determining whether verification on the authorization verification request is successful, if the verification is successful, generating the authentication key of the user, and calculating a dynamic time factor of the first server terminal (S404);

generating an authentication factor by using the authentication key of the user, the dynamic time factor, and the account information of the user (S405);

issuing the authentication factor to the terminal (S406);

receiving bound authentication information submitted by the terminal, the bound authentication information being generated by binding the authentication factor and the device account information (S407); and

performing authorization verification on the bound authentication information, and

completing the authorization verification after authorization is successful (S408).

12. The method of claim 10, wherein the step of performing, by the first server terminal, online account binding on the terminal specifically comprises:

receiving an account identity verification request sent by the second terminal, the account identity verification request carrying the account information of the user (S501);

determining whether the account identity verification request passes verification, and sending a verification result of successful verification to the second terminal if the verification is successful (S502);

receiving an authorization verification request, sent by the second terminal, for completing the first service operation offline (S503);

determining whether verification on the authorization verification request is successful, if the verification is successful, generating the authentication key of the user, and calculating a dynamic time factor of the first server terminal (S504);

generating an authentication factor by using the authentication key of the user, the dynamic time factor, and the account information of the user (S505);

issuing the authentication factor to the second terminal, such that the second terminal sends the authentication factor to the terminal (S506);

receiving bound authentication information that is returned by the terminal and submitted by the second terminal, the bound authentication information being generated by the terminal through binding the authentication factor and the device account information of the terminal (S507); and

performing authorization verification on the bound authentication information, and completing the authorization verification after authorization is successful (S508).

13. The method of claim 11 or 12, after the step of generating the authentication key of the user, further comprising:

generating a compressed string from the authentication key of the user and the account information of the user, the compressed string having a one-to-one mapping relationship with the authentication key and the account information of the user; and

generating the authentication factor by using the authentication key of the user, the dynamic time factor, and the account information of the user, which specifically comprises: generating the authentication factor by using the authentication key of the user, the compressed string, and the dynamic time factor.

14. The method of claim 9, wherein the step of performing authentication according to the authentication information of the first service operation carried in the first service operation request specifically comprises:

checking whether a binding relationship between the device account information and the authentication key that are carried in the authentication information of the first service operation is correct, and checking whether the dynamic password is valid according to the dynamic time factor in the authentication factor; wherein if yes, the authentication is successful.

15. An apparatus comprising:

a terminal;

a first server terminal; and

a second server terminal;

wherein the apparatus is configured to perform the method of any one of claims 1 to 14.