What is claimed is:

1. A method for authenticating user identity, comprising: generating a first verification code by a server; displaying the first verification code to a user in an application scenario of a service requiring user identity authentication, wherein the displaying of the first verification code is performed by the server; receiving a second verification code sent by the user via another application that is other than the application scenario; comparing the second verification code sent by the user and the first verification code generated by the server; and determining whether the user has passed identity authentication based on a result of the comparison.

2. The method as described in claim 1, wherein the determining of whether the user has passed identity authentication based on the results of the comparing comprises: in the event that the second verification code from the user is identical to the first verification code generated by the server, determining the user to have passed identity authentication.

3. The method as described in claim 1, wherein the application scenario of the service requiring user identity authentication corresponds to a web page or a client application.

4. The method as described in claim 1, wherein: the other application corresponds to an application capable of sending a message to the server; and the message includes the second verification code.

5. The method as described in claim 4, wherein the determining of whether the user has passed identity authentication based on the results of the comparing comprises: in the event that the second verification code from the user is identical to the first verification code generated by the server, comparing a user ID of the other application used to send the message against a user ID registered on the server; and in the event that the user ID of the other application used to send the message is identical to the user ID registered on the server, determining the user to have passed identity authentication.

6. The method as described in claim 5, wherein: the other application corresponds to a text messaging application; the message corresponds to a text message; and the user ID of the other application corresponds to a mobile telephone number or telephone number.

7. The method as described in claim 4, wherein: the other application corresponds to a text messaging application; and the message corresponds to a text message.

8. The method as described in claim 1, further comprising: displaying a prompt in the application scenario, the prompt being used to prompt the user to send the second verification code to the server using the application other than the application scenario.

9. The method as described in claim 1, further comprising: displaying a prompt in the application other than the application scenario, the prompt being used to prompt the user to

send the second verification code to the server using the application other than the application scenario.

10. The method as described in claim 1, wherein the first verification code is randomly generated.

11. The method as described in claim 1, wherein the first verification code corresponds to a unique random number.

12. A system for authenticating user identity, comprising: at least one processor configured to: generate a first verification code by a server; display the first verification code to a user in an application scenario of a service requiring user identity authentication, wherein the displaying of the first verification code is performed by the server; receive a second verification code sent by the user via another application that is other than the application scenario; compare the second verification code sent by the user and the first verification code generated by the server; and determine whether the user has passed identity authentication based on a result of the comparison; and a memory coupled to the at least one processor and configured to provide the at least one processor with instructions.

13. The system as described in claim 12, the determining of whether the user has passed identity authentication based on the results of the comparing comprises: in the event that the second verification code from the user is identical to the first verification code generated by the server, determine the user to have passed identity authentication.

14. The system as characterized in claim 12, wherein the application scenario of the service requiring authentication of user identity is a web page or client application.

15. The system as described in claim 12, wherein: the other application corresponds to an application capable of sending a message to the server; and the message includes the second verification code.

16. The system as described in claim 15, wherein the determining of whether the user has passed identity authentication based on the results of the comparing comprises: in the event that the second verification code from the user is identical to the first verification code generated by the server, compare a user ID of the other application used to send the message against a user ID registered on the server; and, in the event that the user ID of the other application used to send the message is identical to the user ID registered on the server, determine the user to have passed identity authentication.

17. The system as described in claim 16, wherein: the other application corresponds to a text messaging application; and the user ID of the other application corresponds to a mobile phone number or telephone number.

18. The system as described in claim 15, wherein: the other application corresponds to a text messaging application; and the message corresponds to a text message.

19. A computer program product for authenticating user identity, the computer program product being embodied in a tangible non-transitory computer readable storage medium and comprising computer instructions for: generating a first verification code by a server; displaying the first verification code to a user in an application scenario of a service requiring user identity authentication, wherein the displaying of the first verification code is performed by the server; receiving a second verification code sent by the user via another application that is other than the application scenario; comparing the second verification code sent by the user and the first verification code generated by the server; and determining whether the user has passed identity authentication based on a result of the comparison.