CLAIMS

What is claimed is:

1. An information processing method, performed by an information code server end, and comprising:

in response to a second client scanning a third-party information code embedded in a first client, receiving, by the information code server end, an information code processing request from the second client, wherein the information code processing request comprises at least one of transaction information, device information, environment information, time information, or user information;

performing, by the information code server end, risk identification based on the information code processing request received by the information code server end, wherein performing the risk identification comprises obtaining risk information based on the information code processing request received by the information code server end;

executing, by the information code server end, corresponding processing logic based on the obtained risk information and a predetermined security rule; and

sending a processing result of the executed corresponding processing logic to the first client.

2. The method according to claim 1, wherein the performing risk identification comprises:

obtaining the risk information through risk identification based on the at least one of transaction information, device information, environment information, and time information that are comprised in the information code processing request; or

querying for historical data of the user based on the user information comprised in the information code processing request, and obtaining the risk information through risk identification based on the historical data of the user.

3. The method according to claim 1, wherein the executing corresponding processing logic based on identified risk information and a predetermined security rule comprises:

querying for the predetermined security rule based on the identified risk information, to determine whether to perform security verification; and

in response to determining to perform security verification, performing security verification corresponding to the risk information, and then executing the processing logic corresponding to the information code; or

in response to determining not to perform security verification, executing the processing logic corresponding to the information code.

4. The method according to claim 3, wherein the security verification comprises:

user confirmation, password verification, digital certificate verification, password and digital certificate verification, or a redirect to a client corresponding to the third-party information code.

5. The method according to claim 4, wherein the password verification comprises:

determining, based on user information comprised in the information code processing request, password type information and first password information that are most recently set by a user;

sending a password verification message that comprises the password type information to the first client; and

obtaining second password information sent by the first client, and performing verification by using the second password information and the first password information.

6. The method according to claim 4, wherein the digital certificate verification comprises:

determining, based on user information comprised in the information code processing request, first digital certificate information corresponding to the user information;

sending a message for verifying a digital certificate to the first client; and

obtaining second digital certificate information sent by the first client, and performing verification by using the second digital certificate information and the first digital certificate information.

7. The method according to claim 4, wherein the password and digital certificate verification comprises:

determining, based on user information comprised in the information code processing request, password type information, first password information, and first digital certificate information that correspond to the user information;

sending a message for verifying a password and a digital certificate to the first client; and

obtaining second password information and second digital certificate information that are sent by the first client, and performing verification by using the first password information, the second password information, the first digital certificate information, and the second digital certificate information.

8. The method according to any one of claims 1 to 7, wherein the information code comprises a payment code, and the processing logic comprises payment processing.

9. An information processing method, performed by a first client, and comprising:

in response to a trigger event, caused by a user, of causing the first client to present a third-party information code, presenting, by the first client, an interface of the first client that comprises the third-party information code, so that a second client scans the third-party information code, and triggers processing logic of the third-party information code including risk identification; and

after obtaining, by the first client, a processing result of the processing logic including the risk identification and sent by an information code server end, presenting, by the first client, an

interface that comprises the processing result.

10. The method according to claim 9, wherein the trigger event caused by the user comprises:

the user triggers a component for presenting the third-party information code in the first client; or

the user performs a predetermined gesture operation on a lock screen of the first client.

11. The method according to claim 9 or 10, further comprising:

after a password verification message that comprises password type information and is sent by the information code server end is received, presenting a prompt interface for inputting a password of the type, and sending, to the information code server end, second password information input by the user; or

sending second digital certificate information to the information code server end after a message that is used for verifying a digital certificate and is sent by the information code server end is received; or

after a message that is used for verifying a password and a digital certificate and is sent by the information code server end is received, presenting a prompt interface for inputting a password of the type, and sending, to the information code server end, second digital certificate information and second password information input by the user, wherein the message comprises password type information.

12. An information processing apparatus, disposed on an information code server end, wherein the apparatus comprises:

a receiving unit, configured to in response to a second client scanning a third-party information code embedded in a first client, receive an information code processing request from the second client, wherein the information code processing request comprises at least one of transaction information, device information, environment information, time information, or user information;

an identification unit, configured to perform risk identification based on the information code processing request received by the receiving unit, wherein performing the risk identification comprises obtaining risk information based on the information code processing request received by the receiving unit;

an execution unit, configured to execute corresponding processing logic based on the obtained risk information and a predetermined security rule; and

a sending unit, configured to send a processing result of the executed corresponding processing logic to the first client.

13. The apparatus according to claim 12, wherein the identification unit is specifically configured to:

obtain the risk information through risk identification based on the at least one of transaction information, device information, environment information, and time information that are comprised in the information code processing request; or

query for historical data of the user based on the user information comprised in the information code processing request, and obtain the risk information through risk identification based on the historical data of the user.

14. The apparatus according to claim 12, wherein the execution unit comprises:

a determining subunit, configured to query for the predetermined security rule based on the identified risk information, to determine whether to perform security verification;

a verification subunit, configured to: if the determining subunit determines to perform security verification, perform security verification corresponding to the risk information; and

an execution subunit, configured to: if the security verification is passed, execute the processing logic corresponding to the information code; or if the determining subunit determines not to perform security verification, execute the processing logic corresponding to the information code.

15. The apparatus according to claim 14, wherein the security verification comprises:

user confirmation, password verification, digital certificate verification, password and digital certificate verification, or a redirect to a client corresponding to the third-party information code.

16. The apparatus according to claim 15, wherein when performing password verification, the verification subunit is specifically configured to determine, based on user information comprised in the information code processing request, password type information and first password information that are most recently set by a user; send a password verification message that comprises the password type information to the first client; and obtain second password information sent by the first client, and perform verification by using the second password information and the first password information.

17. The apparatus according to claim 15, wherein when performing digital certificate verification, the verification subunit is specifically configured to determine, based on user information comprised in the information code processing request, first digital certificate information corresponding to the user information; send a message for verifying a digital certificate to the first client; and obtain second digital certificate information sent by the first client, and perform verification by using the second digital certificate information and the first digital certificate information.

18. The apparatus according to claim 15, wherein when performing password and digital certificate verification, the verification subunit is specifically configured to determine, based on user information comprised in the information code processing request, password type information,

first password information, and first digital certificate information that correspond to the user information; send a message for verifying a password and a digital certificate to the first client; and obtain second password information and second digital certificate information that are sent by the first client, and perform verification by using the first password information, the second password information, the first digital certificate information, and the second digital certificate information.

19. The apparatus according to any one of claims 12 to 18, wherein the information code comprises a payment code, and the processing logic comprises payment processing.

20. An information processing apparatus, disposed on a first client, wherein the apparatus comprises:

a presentation unit, configured to: in response to a trigger event, caused by a user, of causing the first client to present a third-party information code, present an interface of the first client that comprises the third-party information code, so that a second client scans the third-party information code, and triggers processing logic of the third-party information code including risk identification; and

an interaction unit, configured to obtain a processing result of the processing logic including the risk identification that is sent by an information code server end, wherein

after the interaction unit obtains the processing result, the presentation unit is further configured to present an interface that comprises the processing result.

21. The apparatus according to claim 20, wherein the trigger event caused by the user comprises:

the user triggers a component for presenting the third-party information code in the first client; or

the user performs a predetermined gesture operation on a lock screen of the first client.

22. The apparatus according to either of claims 20 and 21, wherein the interaction unit is further configured to receive a password verification message that comprises password type information and is sent by the information code server end, and send, to the information code server end, second password information input by the user; or receive a message that is used for verifying a digital certificate and is sent by the information code server end, and send second digital certificate information to the information code server end; or receive a message that is used for verifying a password and a digital certificate and is sent by the information code server end, and send second digital certificate information to the information code server end; and

the presentation unit is further configured to present a prompt interface for inputting a password of the type.

23. A computing device, comprising a memory and a processor, wherein the memory stores

executable code, and when executing the executable code, the processor implements the method according to any one of claims 1 to 11.