

INFORMATION PROCESSING

TECHNICAL FIELD

[0001] One or more embodiments of this specification relate to the field of computer application technologies, and in particular, to information processing methods and apparatuses.

BACKGROUND

[0002] With rapid development of computer and Internet technologies, human production and life become more convenient. As a popular encoding scheme for mobile devices in recent years, an information code technology such as barcodes and QR codes brings great convenience to application scenarios such as payment, check-in, and information acquisition. For example, for a financial application, a payment code of a current financial institution is often embedded in the financial application, and a user can open the payment code for scanning by a manufacturer to complete payment. However, for security reasons, information codes such as payment codes currently can be used only on a client of the current financial institution. Consequently, the user needs to install clients of various financial applications on a terminal device, causing inconvenience in resource occupation and use.

SUMMARY

[0003] One or more embodiments of this specification describe information processing methods and apparatuses, to improve convenience of using an information code and reduce resource occupation of a terminal device.

[0004] According to a first aspect, an information processing method is provided. The method is performed by an information code server end, and includes the following: receiving an information code processing request from a second client, where the information code processing request is sent after the second client scans a third-party information code embedded in a first client; performing risk identification based on the information code processing request; executing corresponding processing logic based on identified risk information and a predetermined security rule; and sending a processing result of the processing logic to the first client.

[0005] In some embodiments, the performing risk identification based on the information

code processing request includes the following: obtaining the risk information through identification based on at least one of transaction information, device information, environment information, and time information that are included in the information code processing request; or querying for historical data of the user based on user information included in the information code processing request, and obtaining the risk information through identification based on the historical data of the user.

[0006] In some other embodiments, the executing corresponding processing logic based on identified risk information and a predetermined security rule includes the following: 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.

[0007] In some embodiments, the security verification includes 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.

[0008] In some other embodiments, the password verification includes the following: determining, based on user information included 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 includes 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.

[0009] In some embodiments, the digital certificate verification includes the following: determining, based on user information included 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.

[0010] In some other embodiments, the password and digital certificate verification includes the following: determining, based on user information included 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.

[0011] In some embodiments, the information code includes a payment code, and the processing logic includes payment processing.

[0012] According to a second aspect, an information processing method is provided. The method is performed by a first client, and includes the following: in response to a trigger event of opening a third-party information code, presenting an interface that includes 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; and after a processing result of the processing logic that is sent by an information code server end is obtained, presenting an interface that includes the processing result.

[0013] In some embodiments, the trigger event of opening the third-party information code includes the following: a user triggers a component for opening the third-party information code in the first client; or a user performs a predetermined gesture operation on a lock screen.

[0014] In some other embodiments, the method further includes the following: after a password verification message that includes 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, where the message includes password type information.

[0015] According to a third aspect, an information processing apparatus is provided. The apparatus is disposed on an information code server end. The apparatus includes: a receiving unit, configured to receive an information code processing request from a second client, where the information code processing request is sent after the second client scans a third-party information code embedded in a first client; an identification unit, configured to perform risk identification based on the information code processing request; an execution unit, configured to execute corresponding processing logic based on identified risk information and a predetermined security rule; and a sending unit, configured to send a processing result of the processing logic to the first client.

[0016] In some embodiments, the identification unit is specifically configured to obtain the

risk information through identification based on at least one of transaction information, device information, environment information, and time information that are included in the information code processing request; or query for historical data of the user based on user information included in the information code processing request, and obtain the risk information through identification based on the historical data of the user.

[0017] In some other embodiments, the execution unit includes: 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.

[0018] In some embodiments, the security verification includes 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.

[0019] In some other embodiments, when performing password verification, the verification subunit is specifically configured to determine, based on user information included 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 includes 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.

[0020] In some embodiments, when performing digital certificate verification, the verification subunit is specifically configured to determine, based on user information included 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.

[0021] In some other embodiments, when performing password and digital certificate verification, the verification subunit is specifically configured to determine, based on user information included 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.

[0022] In some embodiments, the information code includes a payment code, and the processing logic includes payment processing.

[0023] According to a fourth aspect, an information processing apparatus is provided. The apparatus is disposed on a first client. The apparatus includes: a presentation unit, configured to: in response to a trigger event of opening a third-party information code, present an interface that includes 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; and an interaction unit, configured to obtain a processing result of the processing logic that is sent by an information code server end, where the presentation unit is further configured to present an interface that includes the processing result.

[0024] In some embodiments, the trigger event of opening the third-party information code includes the following: a user triggers a component for opening the third-party information code in the first client; or a user performs a predetermined gesture operation on a lock screen.

[0025] In some embodiments, the interaction unit is further configured to receive a password verification message that includes 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.

[0026] According to a fifth aspect, a computing device is provided, including a memory and a processor. The memory stores executable code, and when executing the executable code, the processor implements the method of the first aspect.

[0027] According to the methods and the apparatuses provided in the embodiments of this specification, the third-party information code is embedded in the first client, so that the user does not need to install clients of information codes one by one, thereby reducing resource occupation of the terminal device and improving convenience of using the information code.

[0028] In addition, at the information code server end, risk identification and the security rule are used to ensure security of the processing logic corresponding to the information code.

BRIEF DESCRIPTION OF DRAWINGS

[0029] To describe the technical solutions in the embodiments of this application or in the existing technology more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments or the existing technology. Clearly, the accompanying drawings in the following description show some embodiments of this application, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0030] FIG. 1 is a flowchart illustrating an information processing method, according to some embodiments;

[0031] FIG. 2a is a schematic diagram illustrating a method for embedding a third-party payment code, according to some embodiments;

[0032] FIG. 2b is a schematic diagram illustrating a redirect from an interface that includes a payment code to an interface that includes payment success information, according to some embodiments;

[0033] FIG. 2c is a schematic diagram illustrating an interface for presenting a processing result in a form of a notification message, according to some embodiments;

[0034] FIG. 3 is a flowchart illustrating an information processing method, according to some embodiments;

[0035] FIG. 4 is a flowchart illustrating use of a user confirmation method in a payment procedure, according to some embodiments;

[0036] FIG. 5 is a flowchart illustrating use of a password verification method in a payment procedure, according to some embodiments;

[0037] FIG. 6 is a flowchart illustrating use of a digital certificate verification method in a payment procedure, according to some embodiments;

[0038] FIG. 7 is a flowchart illustrating use of a password and digital certificate verification method in a payment procedure, according to some embodiments;

[0039] FIG. 8 is a flowchart illustrating a redirect to a third-party information code client in a payment procedure, according to some embodiments;

[0040] FIG. 9 is a schematic block diagram illustrating an information processing apparatus, according to some embodiments; and

[0041] FIG. 10 is a schematic block diagram illustrating an information processing apparatus, according to some other embodiments.

DESCRIPTION OF EMBODIMENTS

[0042] The following describes the solutions provided in this specification with reference to the accompanying drawings.

[0043] The core idea of this specification is that third-party information codes can be embedded in a client, so that a user does not need to install clients of the information codes one by one, thereby reducing resource occupation of a terminal device and improving convenience of using the information code.

[0044] The following describes specific implementations of the above-mentioned concept.

[0045] FIG. 1 is a flowchart illustrating an information processing method, according to some embodiments. The method is performed by a first client. A third-party information code is embedded in the first client. As shown in FIG. 1, the method includes the following steps.

[0046] Step 101: In response to a trigger event of opening the third-party information code, the first client presents an interface that includes 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.

[0047] Step 103: After obtaining a processing result of the processing logic, the first client presents an interface that includes the processing result.

[0048] The following describes execution methods of the steps shown in FIG. 1. In the technical solution provided in the embodiments of this application, the information code can be a graph, for example, a barcode or a QR code, that can include encoded information. The QR code is used as an example for description in subsequent embodiments of the disclosure. In addition, the information code can be used to perform functions such as payment, transfer, check-in, and provision of identity information. The payment code is used as an example to complete the payment function in subsequent embodiments.

[0049] "In response to a trigger event of opening the third-party information code, the first client presents an interface that includes 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" in step 101 is first described in detail.

[0050] The trigger event of opening the third-party information code can include but is not limited to the following two methods.

[0051] Method 1: A user triggers a component for opening the third-party information code in the first client.

[0052] When the third-party information code is embedded in the first client, a link of the third-party information code is usually presented in the first client in a form of a component. As

shown in FIG. 2a, the first client can be a "wallet" client, and the third-party payment code can be embedded in the "wallet" client in a form of a card. After the user taps the card, the third-party payment code is presented.

[0053] Method 2: A user performs a predetermined gesture operation on a lock screen.

[0054] To open the third-party information code more conveniently, the first client can set a shortcut gesture of the lock screen as the predetermined gesture operation, for example, double-tapping the lock screen. After the user double-taps the lock screen, the first client presents the third-party information code to the user.

[0055] In addition to the above-mentioned methods, another event, for example, invoking an interface that includes the third-party information code in the first client through voice, can be used as the trigger event of opening the third-party information code.

[0056] The second client can be a client configured to obtain information from the third-party information code. For example, a client of a merchant scans a third-party payment code embedded in a "wallet" client of a user, to implement a payment function of a product or a service provided by the merchant. For another example, a client of a company scans a third-party check-in code embedded in a client of an employee, to implement a check-in function of the employee in the company.

[0057] The second client usually triggers the processing logic of the third-party information code by sending a processing request to a server (referred to as an "information code server" in this specification) of the third-party information code. The information code server completes the corresponding processing logic, and sends a processing result to the first client. In addition, the information code server can further return the processing result to the second client.

[0058] For example, the second client sends a code payment request to the information code server, and after completing a payment procedure, the information code server sends a payment processing result to the first client and the second client.

[0059] The following describes "after obtaining a processing result of the processing logic, the first client presents an interface that includes the processing result" in step 103 in detail.

[0060] After the information code server sends the processing result to the first client, the first client can present, in the following methods, for example, the interface that includes the processing result.

[0061] Method 1: Redirect from a current interface to the interface that includes the processing result of the processing logic. The processing result can include information indicating whether the processing succeeds, and can further include other information related to the processing logic.

[0062] As shown in FIG. 2b, a redirect is made from an interface that includes a payment

code to an interface that includes payment success information. The interface can include a payment amount, transaction related information, etc. in addition to the payment success information.

[0063] Method 2: Present, in a form of a notification message, the interface that includes the processing result of the processing logic.

[0064] As shown in FIG. 2c, a notification message is displayed on an interface. In FIG. 2c, an example that the notification message is displayed from the top of a screen is used, but this display location and form of the notification message do not constitute a limitation. When the user taps the notification message, information including payment success is presented. The interface can include a payment amount, transaction related information, etc. in addition to the payment success information.

[0065] The presentation operation involved in this application can include but is not limited to at least one of a rendering operation and a display operation. This is not specifically limited in the embodiments. Specifically, content presented by an execution body is a rendering result output by the rendering operation. The rendering operation can be performed by a rendering engine in a network-side server based on page source code of a target page. Then the rendering result is stored in a form of a bitmap image, a vector image, etc., and is provided for the execution body to output the rendering result. Or the rendering operation can be performed by the execution body based on page source code of a target page, and then the execution body directly outputs the rendering result.

[0066] FIG. 3 is a flowchart illustrating an information processing method, according to some embodiments. The method is performed by an information code server end. The information code server end can be a server, or can be a server cluster including a plurality of servers. As shown in FIG. 3, the method can include the following steps.

[0067] Step 301: Receive an information code processing request from a second client, where the information code processing request is sent after the second client scans a third-party information code embedded in a first client.

[0068] Step 303: Perform risk identification based on the information code processing request.

[0069] Step 305: Execute corresponding processing logic based on identified risk information and a predetermined security rule.

[0070] Step 307: Send a processing result of the processing logic to the first client.

[0071] Because some information codes such as payment codes have very high requirements for security. In some feasible methods, related functions of the first client can be implemented by providing a software development kit (SDK) for the first client. However, in these methods, a

third-party SDK needs to be integrated into the first client.

[0072] In some implementations, the SKD is not provided for the first client, and the functions are implemented by code of the first client. Therefore, risk identification and the security rule in the embodiments shown in FIG. 3 need to be used to ensure security of the processing logic.

[0073] The following describes execution methods of the steps shown in FIG. 3. "Perform risk identification based on the information code processing request" in step 303 is first described in detail.

[0074] In some feasible methods, the risk information can be obtained through identification based on at least one of transaction information, device information, and environment information that are included in the information code processing request.

[0075] Taking a payment code scenario as an example, the transaction information can include merchant information, a transaction amount, payment channel information, etc. For example, the transaction amount in the transaction information can be used as a basis, and it is considered that corresponding risks exist when the transaction amount exceeds predetermined different thresholds. For example, it can be considered that corresponding risks exist when a current transaction is determined as a fraud based on a plurality of pieces of information such as the merchant information and the transaction amount in the transaction information.

[0076] The device information can be a device type, an identifier of the device, etc. used by a user. For example, if a user uses a common device, it is considered that there is a low risk or there is no risk. If the user uses a device that is not commonly used, it is considered that certain risks exist.

[0077] The environment information can be a type of a network, an identifier of a network, etc. where the user is located. For example, if the user uses a common local area network, it is considered that a risk is relatively low. If the user uses a local area network that is not commonly used, it is considered that a certain risk exists.

[0078] The time information can be time information of scanning the information code by the second client, time information of sending the information code request, etc. For example, if a difference between the time information of scanning the information code by the second client and time information of presenting the information code exceeds a predetermined duration threshold, it is considered that a certain risk exists.

[0079] In some other feasible methods, historical data of the user can be queried for based on user information included in the information code processing request, and the risk information can be obtained through identification based on the historical data of the user.

[0080] The historical data of the user can include, for example, whether a password has been

modified, whether a historical transaction behavior of the user is abnormal, etc.

[0081] The risk information can be represented by using risk scenario information. For example, the risk information is represented as "the user has modified a password", "a payment amount is greater than X and the user has an available digital certificate", "a payment amount is greater than an available balance of a current payment channel", "not a device commonly used by the user", "not a common network environment".

[0082] The risk information can alternatively be represented by using a risk level. For example, risks are classified into a high risk, a medium risk, and a low risk. For another example, risks are classified into a level-1 risk, a level-2 risk, a level-3 risk, and a level-4 risk.

[0083] "Execute corresponding processing logic based on identified risk information and a predetermined security rule" in step 305 is described in detail below.

[0084] The processing logic involved in this step can include a security verification portion and also includes processing logic of the information code. Whether to perform security verification and what kind of security verification is to be performed can be determined based on the risk information obtained through risk identification.

[0085] In some implementations, the predetermined security rule can be first queried for based on the identified risk information, to determine whether to perform security verification; and in response to determining to perform security verification, security verification corresponding to the risk information can be performed, and then the processing logic corresponding to the information code can be executed; or in response to determining not to perform security verification, the processing logic corresponding to the information code can be performed.

[0086] The security verification performed above can include 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.

[0087] Content of the security rule actually includes a correspondence between risk information and security verification. For example, if a difference between time of scanning the information code and time of presenting the information code exceeds a predetermined duration threshold, for example, a payment code is requested for payment after the payment code is presented for over one minute, the security verification method of user confirmation can be used.

[0088] If a user password is modified, the security verification method of password verification can be used, where the password can include a personal identification number (PIN) password, or can include a biometric password such as fingerprint, face, or iris.

[0089] If a historical transaction behavior of the user is abnormal, the security verification method of password verification can be used.

[0090] If a payment amount exceeds X yuan, and the user does not have an available digital certificate, the certificate verification method is used.

[0091] If a payment amount exceeds Y yuan, and the user has an available digital certificate, the certificate verification method is used.

[0092] X and Y are predetermined amount thresholds.

[0093] If a payment amount is greater than an available balance of a current payment channel, the method of redirecting to the client corresponding to the third-party information code is used.

[0094] If a payment amount exceeds a predetermined payment limit, the method of redirecting to the client corresponding to the third-party information code is used.

[0095] If a current transaction is determined as a fraud, the method of redirecting to the client corresponding to the third-party information code is used.

[0096] The above-mentioned security rules are merely examples, and all security rules cannot be enumerated here. All replacements, conversions, or similar extensions within the spirit and the principle fall within the scope of this application.

[0097] The following describes the above-mentioned security verification methods. The user confirmation can include the following: sending a message for confirming the current processing logic to the first client; and after a request that includes "confirmed" information of the user and is returned by the first client is received within predetermined duration, considering that the current verification is passed; or if a request that includes "confirmed" information of the user and is returned by the first client is not received within predetermined duration, or a request that includes "unconfirmed" information of the user and is returned by the first client is received, considering that the current verification fails.

[0098] In this verification method, after receiving a request that includes confirmation information of the user, the first client presents a prompt interface for inputting the confirmation information by the user, and after obtaining the "confirmed" information or the "unconfirmed" information input by the user, sends the "confirmed" information or the "unconfirmed" information to the information code server end.

[0099] The password verification can include the following: determining, based on user information included in the information code processing request, password type information and first password information that are most recently set by the user; sending a password verification message that includes 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. If the first password information is consistent with the second password information, it is considered that the current verification is

passed; otherwise, it is considered that the current verification fails.

[0100] In this verification method, after receiving the password verification message that includes the password type information and is sent by the information code server end, the first client presents a prompt interface for inputting a password of a corresponding type, and sends, to the information code server end, the second password information input by the user.

[0101] The digital certificate verification can include the following: determining, based on user information included 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. If the first digital certificate information is consistent with the second digital certificate information, it is considered that the current verification is passed; otherwise, it is considered that the current verification fails. The first digital certificate information can be signature information of the server end, and the second digital information can be signature information of the client.

[0102] In this verification method, the first client sends the second digital certificate information to the information code server end after receiving the message that is used for verifying a digital certificate and is sent by the information code server end.

[0103] The password and digital certificate verification can include the following: determining, based on user information included in the information code processing request, password type information and first password information that are most recently set by the user and first digital certificate information corresponding 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.

[0104] In this verification method, after receiving the message that is used for verifying a password and a digital certificate and is sent by the information code server end, the first client presents a prompt interface for inputting a password of a corresponding type, and sends, to the information code server end, the second digital certificate information and the second password information input by the user.

[0105] The redirect to the client corresponding to the third-party information code includes the following: sending, to the first client, a link indicating to redirect to the client corresponding to the third-party information code, where the link includes processing logic information

corresponding to the information code, for example, related payment information corresponding to a payment code. After receiving the link, the first client redirects to the client corresponding to the third-party information code, so that the client corresponding to the third-party information code interacts with the information code server to complete subsequent processing logic.

[0106] The following uses a payment procedure corresponding to a payment code as an example to describe the above-mentioned verification methods in detail with reference to specific embodiments.

[0107] FIG. 4 is a flowchart illustrating use of a user confirmation method in a payment procedure, according to some embodiments. As shown in FIG. 4, the procedure can include the following steps.

[0108] Step 401: A second client scans a third-party information code of a first client.

[0109] Step 403: The second client sends a code payment request to a verification execution module on an information code server end.

[0110] Step 405: The verification execution module performs risk consultation with a security module.

[0111] Step 407: The security module sends a query for a security rule and historical data of a user to a storage module.

[0112] Step 409: The storage module sends the security rule and the historical data of the user to the security module.

[0113] Step 411: The security module performs risk identification to determine a verification method to be used. In this procedure, it is determined that the user confirmation method is to be used.

[0114] Step 413: The security module notifies the verification execution module of information about the user confirmation method.

[0115] Step 415: The verification execution module sends a message requesting the user to confirm payment information to the first client.

[0116] After receiving the message, the first client presents, to the user, an interface requesting the user to confirm payment information, and the user can select "confirmed" or "unconfirmed" on the interface.

[0117] Step 417: The verification execution module triggers payment logic after obtaining a payment request including that the user confirms the payment information.

[0118] Triggering the processing logic actually means interacting with a payment server to complete user payment processing. For example, the payment server deducts a corresponding payment amount from a user account, to pay a merchant. This portion of payment logic can use an existing interaction processing procedure. Details are omitted here for simplicity.

[0119] For specific processing methods for sending the code payment request, performing risk identification, and determining the verification method in the above-mentioned procedure, references can be made to related descriptions in the above-mentioned method embodiments. Details are omitted here for simplicity in this procedure.

[0120] In addition, in the procedure shown in the above-mentioned embodiments and procedures shown in subsequent embodiments, the verification execution module, the security module, and the storage module can be disposed on a same server, or can be respectively disposed on different servers. Information can be forwarded between these modules by using other modules. The other modules are not shown in the figures. Information can be forwarded between the first client and the verification execution module and between the second client and the verification execution module by using a network device such as a routing device, an access device, or a forwarding device corresponding to the first client or the second client. These devices are not shown in the figures.

[0121] FIG. 5 is a flowchart illustrating use of a password verification method in a payment procedure, according to some embodiments. As shown in FIG. 5, the procedure can include the following steps.

[0122] Step 501: A second client scans a third-party information code of a first client.

[0123] Step 503: The second client sends a code payment request to a verification execution module on an information code server end.

[0124] Step 505: The verification execution module performs risk consultation with a security module.

[0125] Step 507: The security module sends a query for a security rule and historical data of a user to a storage module.

[0126] Step 509: The storage module sends the security rule and the historical data of the user to the security module.

[0127] Step 511: The security module performs risk identification to determine a verification method to be used. In this procedure, it is determined that the password verification method is to be used.

[0128] For example, if the historical data of the user indicate that the user has modified a password, the historical data of the user include the latest first password information of the user.

[0129] Step 513: The security module sends information about using the password verification method and the first password information of the user to the verification execution module.

[0130] Step 515: The verification execution module extracts password type information from the first password information.

[0131] To be specific, the latest password type, for example, fingerprint information, face information, or a PIN password, used by the user is obtained from the first password information.

[0132] Step 517: The verification execution module sends a password verification message that includes the password type information to the first client.

[0133] After receiving the password verification message, the first client presents, to the user, an interface requesting the user to input a password of the type. For example, the user needs to input a fingerprint, a face, a PIN, etc. as second password information.

[0134] Step 519: The first client sends, to the verification execution module, the second password information input by the user based on the password type information.

[0135] Step 521: The verification execution module performs password verification by using the first password information and the second password information.

[0136] Step 523: Trigger payment logic after the verification succeeds.

[0137] Still further, after the password verification, information about current password verification after password modification can be further sent to the storage module. This part is recorded in the storage module as new historical data of the user.

[0138] FIG. 6 is a flowchart illustrating use of a digital certificate verification method in a payment procedure, according to some embodiments. As shown in FIG. 6, the procedure can include the following steps.

[0139] Step 601: A second client scans a third-party information code of a first client.

[0140] Step 603: The second client sends a code payment request to a verification execution module on an information code server end.

[0141] Step 605: The verification execution module performs risk consultation with a security module.

[0142] Step 607: The security module sends a query for a security rule and historical data of a user to a storage module.

[0143] Step 609: The storage module sends the security rule and the historical data of the user to the security module.

[0144] Step 611: The security module performs risk identification to determine a verification method to be used. In this procedure, it is determined that the digital certificate verification method is to be used.

[0145] For example, the historical data of the user indicate that the user has installed a digital certificate, and a payment amount exceeds X yuan. Therefore, it is determined that the digital certificate verification method needs to be used.

[0146] Step 613: The security module requests digital certificate information from the

storage module.

[0147] Step 615: The storage module extracts first digital certificate information of the user based on a user identity, etc., and sends the first digital certificate information to the security module.

[0148] Step 617: The security module sends information about using the digital certificate verification method and the first digital certificate information to the verification execution module.

[0149] Step 619: The verification execution module sends a digital certificate verification message to the first client.

[0150] Step 621: The first client obtains local second digital certificate information, and sends the local second digital certificate information to the verification execution module.

[0151] After receiving the digital certificate verification message, the first client invokes information about a locally installed digital certificate as the second digital certificate information.

[0152] Step 623: The verification execution module performs verification by using the first digital certificate information and the second digital certificate information.

[0153] Step 625: Trigger payment logic after the verification succeeds.

[0154] In addition, in the above-mentioned verification procedure, if it is determined that the digital certificate verification method is to be used but the client does not install a digital certificate, the second client can be triggered to install the digital certificate to be used for the verification method. The payment logic is triggered after the second client installs the digital certificate.

[0155] FIG. 7 is a flowchart illustrating use of a password and digital certificate verification method in a payment procedure, according to some embodiments. As shown in FIG. 7, the procedure can include the following steps.

[0156] Step 701: A second client scans a third-party information code of a first client.

[0157] Step 703: The second client sends a code payment request to a verification execution module on an information code server end.

[0158] Step 705: The verification execution module performs risk consultation with a security module.

[0159] Step 707: The security module sends a query for a security rule and historical data of a user to a storage module.

[0160] Step 709: The storage module sends the security rule and the historical data of the user to the security module.

[0161] Step 711: The security module performs risk identification to determine a verification

method to be used. In this procedure, it is determined that the password and digital certificate verification method is to be used.

[0162] Step 713: The security module requests password and digital certificate information from the storage module.

[0163] Step 715: The storage module extracts first password information and first digital certificate information of the user based on a user identity, etc., and sends the first password information and the first digital certificate information to the security module.

[0164] Step 717: The security module sends information about using the password and digital certificate verification method, the first password information, and the first digital certificate information to the verification execution module.

[0165] Step 719: The verification execution module sends a password and digital certificate verification message to the first client, where the message includes password type information.

[0166] After receiving the password and digital certificate verification message, the first client presents, to the user, an interface requesting the user to input a password of the type. For example, the user needs to input a fingerprint, a face, a PIN, etc. as second password information. In addition, the first client invokes information about a locally installed digital certificate as second digital certificate information.

[0167] Step 721: The first client obtains second password information input by the user and the local second digital certificate information, and sends the second password information and the local second digital certificate information to the verification execution module.

[0168] Step 723: The verification execution module performs verification by using the first password information, the second password information, the first digital certificate information, and the second digital certificate information.

[0169] It is considered that the verification is passed only when the password information and the digital certificate pass the verification.

[0170] Step 725: Trigger payment logic after the verification succeeds.

[0171] FIG. 8 is a flowchart illustrating a redirect to a third-party information code client in a payment procedure, according to some embodiments. As shown in FIG. 8, the procedure can include the following steps.

[0172] Step 801: A second client scans a third-party information code of a first client.

[0173] Step 803: The second client sends a code payment request to a verification execution module on an information code server end.

[0174] Step 805: The verification execution module performs risk consultation with a security module.

[0175] Step 807: The security module sends a query for a security rule and historical data of

a user to a storage module.

[0176] Step 809: The storage module sends the security rule to the security module.

[0177] Step 811: The security module performs risk identification to determine to redirect to a client corresponding to the third-party information code.

[0178] For example, the historical data of the user are a payment limit set by the user, and a current payment amount exceeds the payment limit. Therefore, a redirect is made to the client corresponding to the third-party information code.

[0179] Step 813: The security module sends information about the verification method to the verification execution module.

[0180] Step 815: The verification execution module sends, to the first client, a link that indicates to redirect to the client corresponding to the third-party information code.

[0181] Step 817: After the user taps the link, the first client redirects to the client corresponding to the third-party information code.

[0182] Step 819: The client corresponding to the third-party information code sends a payment request to the verification execution module, so that the verification execution module triggers payment logic.

[0183] It can be seen from the above-mentioned embodiments that in this application, the user identity can be verified by using different verification methods, so that security is improved as much as possible while user experience is ensured.

[0184] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some situations, the actions or steps described in the claims can be performed in an order different from the order in the embodiments and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular execution order to achieve the desired results. In some implementations, multi-tasking and concurrent processing is feasible or can be advantageous.

[0185] FIG. 9 is a schematic block diagram illustrating an information processing apparatus, according to some embodiments. The apparatus is disposed on an information code server end. As shown in FIG. 9, the apparatus 900 includes a receiving unit 910, an identification unit 920, an execution unit 930, and a sending unit 940. Main functions of the units are as follows.

[0186] The receiving unit 910 is configured to receive an information code processing request from a second client, where the information code processing request is sent after the second client scans a third-party information code embedded in a first client.

[0187] The identification unit 920 is configured to perform risk identification based on the information code processing request.

[0188] The execution unit 930 is configured to execute corresponding processing logic based on identified risk information and a predetermined security rule.

[0189] The sending unit 940 is configured to send a processing result of the processing logic to the first client.

[0190] In some implementations, the identification unit 920 is specifically configured to obtain the risk information through identification based on at least one of transaction information, device information, environment information, and time information that are included in the information code processing request; or query for historical data of a user based on user information included in the information code processing request, and obtain the risk information through identification based on the historical data of the user.

[0191] In some implementations, the execution unit 930 can include a determining subunit 931, a verification subunit 932, and an execution subunit 933.

[0192] The determining subunit 931 is configured to query for the predetermined security rule based on the identified risk information, to determine whether to perform security verification.

[0193] The verification subunit 932 is configured to: if the determining subunit 931 determines to perform security verification, perform security verification corresponding to the risk information.

[0194] The execution subunit 933 is configured to: if the security verification is passed, execute the processing logic corresponding to the information code; or if the determining subunit 931 determines not to perform security verification, execute the processing logic corresponding to the information code.

[0195] The security verification can include but is not limited to 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.

[0196] In some implementations, when performing password verification, the verification subunit 932 is specifically configured to determine, based on user information included 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 includes 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.

[0197] In some other implementations, when performing digital certificate verification, the verification subunit 932 is specifically configured to determine, based on user information included 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.

[0198] In still some other implementations, when performing password and digital certificate verification, the verification subunit 932 is specifically configured to determine, based on user information included 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.

[0199] It is worthwhile to note that the units and the subunits in the above-mentioned apparatus can be disposed in one device or module for implementation, or can be disposed in a plurality of devices or modules for implementation. For example, the receiving unit 910, the sending unit 940, the verification subunit 932, and the execution subunit 933 can be disposed in the verification execution module in the embodiments shown in FIG. 4 to FIG. 8. The identification unit 920 and the determining subunit 931 can be disposed in the security module in the embodiments shown in FIG. 4 to FIG. 8.

[0200] FIG. 10 is a schematic block diagram illustrating an information processing apparatus, according to some other embodiments. The apparatus is disposed on a first client. As shown in FIG. 10, the apparatus 1000 includes a presentation unit 1001 and an interaction unit 1002. Main functions of the units are as follows.

[0201] The presentation unit 1001 is configured to: in response to a trigger event of opening a third-party information code, present an interface that includes 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.

[0202] The interaction unit 1002 is configured to obtain a processing result of the processing logic.

[0203] The presentation unit 1001 is further configured to present an interface that includes the processing result.

[0204] The trigger event of opening the third-party information code can include the following: a user triggers a component for opening the third-party information code in the first client; or a user performs a predetermined gesture operation on a lock screen.

[0205] In feasible methods, when presenting the interface that includes the processing result, the presentation unit 1001 is specifically configured to redirect from a current interface to the interface that includes the processing result; or present, in a form of a notification message, an interface that includes the processing result.

[0206] Still further, the interaction unit 1002 can be configured to receive a password verification message that includes 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, where the message includes the password type information.

[0207] The presentation unit 1001 is further configured to: after the interaction unit 1002 receives the password verification message that includes the password type information and the message for verifying a password and a digital certificate, present a prompt interface for inputting a password of a corresponding type.

[0208] According to some embodiments of another aspect, a computer-readable storage medium is further provided. The computer-readable storage medium stores a computer program, and when the computer program is executed on a computer, the computer is enabled to perform the method described in FIG. 1 or FIG. 3.

[0209] According to some embodiments of still another aspect, a computing device is further provided, including a memory and a processor. The memory stores executable code, and when executing the executable code, the processor implements the method described in FIG. 1 or FIG. 3.

[0210] The embodiments in this specification are described in a progressive way. For same or similar parts of the embodiments, mutual references can be made to the embodiments. Each embodiment focuses on a difference from other embodiments. In particular, the apparatus embodiments are basically similar to the method embodiments, and therefore are described briefly. For related parts, references can be made to related descriptions in the method embodiments.

[0211] A person skilled in the art should be aware that, in the above-mentioned one or more examples, functions described in this application can be implemented by hardware, software, firmware, or any combination thereof. When being implemented by software, these functions can be stored in a computer-readable medium or transmitted as one or more instructions or codes in

the computer-readable medium.

[0212] The specific implementations mentioned above provide further detailed explanations of the objectives, technical solutions, and beneficial effects of this application. It should be understood that the above-mentioned descriptions are merely specific implementations of this application and are not intended to limit the protection scope of this application. Any modifications, equivalent replacements, improvements, etc. made on the basis of the technical solutions of this application should all fall within the protection scope of this application.

CLAIMS

What is claimed is:

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

receiving an information code processing request from a second client, wherein the information code processing request is sent after the second client scans a third-party information code embedded in a first client;

performing risk identification based on the information code processing request;

executing corresponding processing logic based on identified risk information and a predetermined security rule; and

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

2. The method according to claim 1, wherein the performing risk identification based on the information code processing request comprises:

obtaining the risk information through identification based on 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 user information comprised in the information code processing request, and obtaining the risk information through 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 of opening a third-party information code, presenting an interface 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; and

after a processing result of the processing logic that is sent by an information code server end is obtained, presenting an interface that comprises the processing result.

10. The method according to claim 9, wherein the trigger event of opening the third-party information code comprises:

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

or

a user performs a predetermined gesture operation on a lock screen.

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 receive an information code processing request from a second client, wherein the information code processing request is sent after the second client scans a third-party information code embedded in a first client;

an identification unit, configured to perform risk identification based on the information code processing request;

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

a sending unit, configured to send a processing result of the 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 identification based on 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 user information comprised in the information code processing request, and obtain the risk information through 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 of opening a third-party information code, present an interface 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; and

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

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 of opening the third-party information code comprises:

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

a user performs a predetermined gesture operation on a lock screen.

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.