PAYMENT METHOD, INTERMEDIATE SERVICE SYSTEM, WALLET SYSTEM, AND MERCHANT SYSTEM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to a payment method, an intermediate service system, a wallet system, and a merchant system.

BACKGROUND

[0002] With development of Internet technologies, there are increasingly more merchant systems and wallet systems in the Internet field. To facilitate cooperation and interconnection between different merchant systems and different wallet systems, an intermediate service system emerges. The intermediate service system can provide an intermediate service between the merchant system and the wallet system, for example, provide a payment channel and a risk control service.

[0003] There is often an account takeover (ATO) risk on the Internet, that is, a wrongdoer accesses an account by using a technical means without authorization of an authorized user. The ATO risk can also be referred to as an account theft risk. In the payment field, the ATO risk not only causes property losses to the authorized user, but also causes claim losses to the wallet system.

[0004] Therefore, in a payment procedure, the wallet system needs to perform risk control to prevent the ATO risk. For example, the payment procedure is as follows: When a user requests to use the wallet system for payment in the merchant system, a terminal device can jump from an interaction page of the merchant system to an interaction page of the wallet system, or jump from an interaction page of the merchant system to an interaction page of the intermediate service system, and then jump from the interaction page of the intermediate service system to an interaction page of the wallet system. After the terminal device jumps to the interaction page of the wallet system, the wallet system can collect device information of the terminal device, and compare the device information with a device fingerprint associated with a current account of the wallet system, to identify whether there is the ATO risk in the current account. Further, the wallet

system performs a subsequent payment procedure based on an ATO risk identification result.

[0005] However, in the payment procedure, the terminal device needs to jump to the wallet system. The jump process reduces payment efficiency, and may decrease a payment success probability, affecting payment experience. If the terminal device does not jump to the wallet system, the wallet system cannot collect the device information of the terminal device. Consequently, ATO risk identification cannot be performed, resulting in a reduction in payment security.

[0006] It should be noted that the above-mentioned content of the related technology is merely information known to the inventor, and neither means that the information has entered the public domain before the application date of this specification, nor means that the information can become the existing technology of this specification.

SUMMARY

[0007] This specification provides a payment method, an intermediate service system, a wallet system, and a merchant system, to avoid at least one of the above-mentioned technical problems.

[0008] According to a first aspect, this specification provides a payment method, applied to an intermediate service system that provides an intermediate service between a merchant system and a wallet system, and including: when a target terminal device displays an interaction page of the merchant system, receiving a payment request from the merchant system, where the payment request indicates that a user requests to use the wallet system for payment in the merchant system; obtaining first device information corresponding to the target terminal device based on the payment request, where the first device information is device information collected by the wallet system from the target terminal device in advance; sending the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result; and receiving the payment result from the wallet system, and sending the payment result to the merchant system, so that the target terminal device displays the payment result on the interaction page of the merchant system, where in a process of performing the payment method by the intermediate service system, the target terminal device does not jump to an interaction page of the wallet system.

[0009] According to a second aspect, this specification provides a payment method, applied to

a wallet system. The method includes: when a target terminal device displays an interaction page of a merchant system and a user triggers use of the wallet system for payment in the merchant system, receiving first device information corresponding to the target terminal device from an intermediate service system, where the first device information is device information that is obtained by the intermediate service system based on a payment request received from the merchant system and that is collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; performing risk control based on the first device information, and determining a payment result corresponding to the payment request based on a risk control result; and sending the payment result to the intermediate service system, to forward the payment result to the merchant system through the intermediate service system, so that the target terminal device displays the payment result on the interaction page of the merchant system, where in a process of performing the payment method by the wallet system, the target terminal device does not jump to an interaction page of the wallet system.

[0010] According to a third aspect, this specification provides a payment method, applied to a merchant system. The method includes: displaying an interaction page of the merchant system through a target terminal device; in response to detecting that a user requests to use a wallet system for payment in the merchant system, sending a payment request to an intermediate service system, where the payment request is used to enable the intermediate service system to obtain first device information corresponding to the target terminal device, and send the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result, where the first device information is device information collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; and receiving the payment result forwarded by the wallet system through the intermediate service system, and displaying the payment result on the interaction page of the merchant system, where in a process of performing the payment method by the merchant system, the target terminal device does not jump to an interaction page of the wallet system.

[0011] According to a fourth aspect, this specification provides an intermediate service system, configured to provide an intermediate service between a merchant system and a wallet system, and

including: at least one storage medium that stores at least one instruction set for payment; and at least one processor that is communicatively connected to the at least one storage medium. The at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set. The payment method includes: when a target terminal device displays an interaction page of the merchant system, receiving a payment request from the merchant system, where the payment request indicates that a user requests to use the wallet system for payment in the merchant system; obtaining first device information corresponding to the target terminal device based on the payment request, where the first device information is device information collected by the wallet system from the target terminal device in advance; sending the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result; and receiving the payment result from the wallet system, and sending the payment result to the merchant system, so that the target terminal device displays the payment result on the interaction page of the merchant system, where in a process of performing the payment method by the intermediate service system, the target terminal device does not jump to an interaction page of the wallet system.

[0012] According to a fifth aspect, this specification provides a wallet system, including: at least one storage medium that stores at least one instruction set for payment; and at least one processor that is communicatively connected to the at least one storage medium. The at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set. The payment method includes: when a target terminal device displays an interaction page of a merchant system and a user triggers use of the wallet system for payment in the merchant system, receiving first device information corresponding to the target terminal device from an intermediate service system, where the first device information is device information that is obtained by the intermediate service system based on a payment request received from the merchant system and that is collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; performing risk control based on the first device information, and determining a payment result corresponding to the payment request based on a risk control result; and sending the payment result to the intermediate service system, to forward the payment result to the merchant system through the

intermediate service system, so that the target terminal device displays the payment result on the interaction page of the merchant system, where in a process of performing the payment method by the wallet system, the target terminal device does not jump to an interaction page of the wallet system.

[0013] According to a sixth aspect, this specification provides a merchant system, including: at least one storage medium that stores at least one instruction set for payment; and at least one processor that is communicatively connected to the at least one storage medium. The at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set. The payment method includes: displaying an interaction page of the merchant system through a target terminal device; in response to detecting that a user requests to use a wallet system for payment in the merchant system, sending a payment request to an intermediate service system, where the payment request is used to enable the intermediate service system to obtain first device information corresponding to the target terminal device, and send the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result, where the first device information is device information collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; and receiving the payment result forwarded by the wallet system through the intermediate service system, and displaying the payment result on the interaction page of the merchant system, where in a process of performing the payment method by the merchant system, the target terminal device does not jump to an interaction page of the wallet system.

[0014] According to a seventh aspect, this specification provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set. When the at least one instruction set is executed by at least one processor, the method according to any one of the first aspect, the second aspect, or the third aspect is implemented.

[0015] It can be learned from the above-mentioned technical solutions that according to the payment method, the intermediate service system, the wallet system, and the merchant system provided in this specification, the target terminal device displays the interaction page of the

merchant system to the user, or displays an interaction page of the intermediate service system to the user, and does not need to display the interaction page of the wallet system to the user. That is, the target terminal device does not jump to the interaction page of the wallet system in a process in which the merchant system, the intermediate service system, and the wallet system cooperate with each other to complete payment. Therefore, a disadvantage of relatively poor experience of the user caused due to a jump to the interaction page of the wallet system is avoided, to improve experience of using a payment service by the user; and impact of a jump to the interaction page of the wallet system on a payment success rate and efficiency can be avoided, that is, the payment success rate and efficiency can be improved. In addition, the wallet system can perform risk control based on the first device information. Therefore, payment security and reliability can still be implemented when there is no jump.

[0016] Other functions of the payment method, the intermediate service system, the wallet system, and the merchant system provided in this specification are partially listed in the following descriptions. Creative aspects of the payment method, the intermediate service system, the wallet system, and the merchant system provided in this specification can be fully explained by practice or by using the methods, apparatuses, and combinations described in the following detailed examples.

BRIEF DESCRIPTION OF DRAWINGS

[0017] To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following descriptions show merely some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0018] FIG. 1 is a schematic diagram of an application scenario of a payment method according to an embodiment of this specification;

[0019] FIG. 2A is a schematic diagram of an interaction page according to an embodiment of this specification;

[0020] FIG. 2B is a schematic diagram of an interaction page according to another embodiment of this specification;

[0021] FIG. 3 is a diagram of a hardware structure of a service system according to an embodiment of this specification;

[0022] FIG. 4 is a schematic interaction diagram of a payment method according to an embodiment of this specification;

[0023] FIG. 5 is a schematic diagram of an interaction page according to another embodiment of this specification;

[0024] FIG. 6 is a schematic interaction diagram of a payment method according to another embodiment of this specification;

[0025] FIG. 7 is a schematic diagram of an interaction page according to another embodiment of this specification;

[0026] FIG. 8 is a schematic interaction diagram of a payment method according to another embodiment of this specification; and

[0027] FIG. 9 is a schematic diagram of an interaction page according to another embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0028] Example embodiments are described in detail herein, and examples of the example embodiments are presented in the accompanying drawings. When the following descriptions relate to the accompanying drawings, unless specified otherwise, same numbers in different accompanying drawings represent same or similar elements. Implementations described in the following example embodiments do not represent all implementations consistent with this specification. On the contrary, the embodiments are merely examples of apparatuses and methods that are described in the appended claims in details and consistent with some aspects of this specification.

[0029] It should be understood that the terms "include" and "have" in the embodiments of this specification and any variants thereof are intended to cover a non-exclusive inclusion, for example, a product or device that includes a series of components are not necessarily limited to those components that are clearly listed, but can include other components that are not clearly listed or inherent to such product or device.

[0030] In the embodiments of this specification, the term "and/or" describes an association

relationship between associated objects and indicates that three relationships can exist. For example, "A and/or B" can indicate the following three cases: Only A exists, both A and B exist, and only B exists. The character "/" usually indicates an "or" relationship between associated objects.

[0031] In the embodiments of this specification, the term "a plurality of" refers to two or more, and other quantifiers are similar to this term.

[0032] The terms "first", "second", "third", and the like in this specification are used to distinguish between similar or same objects or entities, and do not necessarily mean limiting a specific order or sequence, unless otherwise indicated. It should be understood that the terms used in such a way is interchangeable in appropriate cases, for example, can be implemented in an order other than those illustrated or described in the embodiments of this specification.

[0033] The term "unit/module" used in this specification means any known or later developed hardware, software, firmware, artificial intelligence, fuzzy logic, or a combination of hardware code or/and a combination of software code, and can perform functions related to the element.

[0034] To facilitate understanding of this specification by a reader, an application scenario of this specification is described herein.

[0035] The technical solutions provided in this specification are applicable to a payment scenario including a merchant system, a wallet system, and an intermediate service system. The intermediate service system is a system that provides an intermediate service between the merchant system and the wallet system.

[0036] For example, the technical solutions provided in this specification are applicable to a payment scenario 100 shown in FIG. 1. The payment scenario 100 includes a user 101, a target terminal device 102, a merchant system, a wallet system, and an intermediate service system.

[0037] As shown in FIG. 1, the merchant system includes a merchant client 103 and a merchant server 104, and the wallet system includes a wallet client 105 and a wallet server 106. In some embodiments, the intermediate service system includes an intermediate server 108. In some other embodiments, as shown in FIG. 1, the intermediate service system includes an intermediate service client 107 and an intermediate server 108. In this embodiment, an example in which the intermediate service system includes the intermediate service client 107 and the intermediate server 108 is mainly used for description. The merchant client 103, the wallet client 105, and the intermediate service client 107 are deployed in the target terminal device 102.

[0038] In some embodiments, one or more applications (apps) can be installed on the target terminal device 102. The app includes but is not limited to a web browser app program, a search app program, a chat app program, a shopping app program, a video app program, a financial app program, an instant messaging tool, a mailbox client, social platform software, or the like. For example, an app (that is, the merchant client 103) of the merchant system, an app (that is, the wallet client 105) of the wallet system, and an app (that is, the intermediate service client 107) of the intermediate service system are installed on the target terminal device 102.

[0039] In some embodiments, the target terminal device 102 can be an electronic device that provides an interaction function to the user 101. For example, the target terminal device 102 includes a mobile device, a tablet computer, a laptop computer, a device built in a motor vehicle or similar content, or any combination thereof that can provide an interaction function. In some embodiments, the mobile device can include a smart home device, a smart mobile device, a virtual reality device, an augmented reality device or a similar device, or any combination thereof. In some embodiments, the smart home apparatus can include a smart television, a desktop computer, or any combination. In some embodiments, the smart mobile device can include a smartphone, a personal digital assistant, a game device, a navigation device, or any combination thereof. In some embodiments, the apparatus built in the motor vehicle can include a vehicle-mounted computer, a vehicle-mounted television, or the like.

[0040] For example, the target terminal device 102 can display an interaction page to the user 101, and the user 101 can perform a corresponding operation on the interaction page, to implement interaction with at least one of the merchant system, the wallet system, or the intermediate service system.

[0041] For example, the merchant client 103 can display an interaction page to the user 101 through the target terminal device 102. The user 101 can initiate a payment request on the interaction page, to request to use the wallet system for payment in the merchant system.

[0042] Correspondingly, the merchant system, the wallet system, and the intermediate service system cooperate with each other to perform the payment method provided in this specification, so that payment can be performed by using the wallet system in the merchant system, to obtain a payment result. The merchant system can display the payment result to the user 101 through the target terminal device 102.

[0043] The merchant server 104, the wallet server 106, and the intermediate server 108 each

can be various types of servers, for example, can be a cloud server or a local server.

[0044] A communication connection medium between the merchant client 103 and the merchant server 104, a communication connection medium between the wallet client 105 and the wallet server 106, a communication connection medium between the intermediate service client 107 and the intermediate server 108, a communication connection medium between the merchant server 104 and the intermediate server 108, and a communication connection medium between the wallet server 106 and the intermediate server 108 each can be a network. The network can facilitate exchange of information or data.

[0045] In some embodiments, the network can be any type of wired or wireless network, or a combination thereof. For example, the network can include a cable network, a wired network, an optical fiber network, a telecommunication network, an intranet, the Internet, a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), a metropolitan area network (MAN), a public switched telephone network (PSTN), a Bluetooth networkTM, a short-range wireless network (ZigBeeTM), a near field communication (NFC) network, or a similar network.

[0046] In some embodiments, the network can include one or more network access points. For example, the network can include a wired or wireless network access point, for example, a base station or an Internet switching point. Through the access point, one or more components of the merchant client 103 and the merchant server 104 can be connected to the network to exchange data or information.

[0047] It can be understood that the above-mentioned example is merely used to describe an example of an application scenario to which the payment method in this specification may be applicable, and cannot be understood as a limitation on the application scenario.

[0048] To facilitate understanding of the technical solutions in this specification by a reader, a related technology is described in detail herein with reference to the above-mentioned payment scenario.

[0049] Payment phase (or referred to as an application phase)

[0050] The merchant client 103 displays an interaction page of the merchant system through the target terminal device 102. As shown in FIG. 2A and FIG. 2B, the merchant client 103 can display an interaction page A to the user 101 through the target terminal device 102. The interaction page A includes products for sale. The user 101 can tap to select one or more products from the

products for sale, and initiate a purchase request to the merchant system by tapping a virtual button of "Place order now".

[0051] The merchant client 103 can output an interaction page B on the target terminal device 102. As shown in FIG. 2A and FIG. 2B, the interaction page B can display a payment method that can be selected by the user 101 to the user 101.

[0052] Still with reference to FIG. 2A and FIG. 2B, it can be learned that the user 101 can tap to select a payment method from the interaction page B as a target payment method, to initiate a payment request to the merchant system. The payment request is used to request to use a wallet system corresponding to the target payment method for payment in the merchant system.

[0053] In response to the payment request initiated by the user 101, the merchant system sends the payment request to the intermediate service system.

[0054] Correspondingly, the intermediate service system obtains the payment request sent by the merchant system, and sends the payment request to the wallet system.

[0055] It should be noted that during this period (that is, a period starting when the merchant system sends the payment request to the intermediate server and ending when the intermediate server sends the payment request to the wallet system), the target terminal device 102 can output an interaction page of the merchant system, or can output an interaction page of the intermediate service system. However, after the wallet system obtains the payment request, the target terminal device 102 outputs an interaction page of the wallet system.

[0056] For example, in some embodiments, before the intermediate service system sends the payment request to the wallet system, the target terminal device 102 can output an interaction page of the merchant system. However, after the wallet system obtains the payment request, the target terminal device 102 outputs an interaction page of the wallet system.

[0057] For example, as shown in FIG. 2A, before the wallet system obtains the payment request, the target terminal device 102 can keep outputting an interaction page of the merchant system. However, when the wallet system obtains the payment request, the wallet client 105 can output an interaction page C on the target terminal device 102. That is, the target terminal device 102 jumps from the interaction page B of the merchant system to the interaction page C of the wallet system. The interaction page C is used to prompt the user 101 that payment is in progress.

[0058] In some other embodiments, before the intermediate service system sends the payment request to the wallet system, the target terminal device 102 can first output an interaction page of

the merchant system, and then output an interaction page of the intermediate service system. However, after the wallet system obtains the payment request, the target terminal device 102 outputs an interaction page of the wallet system.

[0059] For example, as shown in FIG. 2B, before the wallet system obtains the payment request, the target terminal device 102 can first output an interaction page of the merchant system. However, when the intermediate service system obtains the payment request sent by the merchant system, the intermediate service client 107 can display an interaction page E to the user through the target terminal device 102. The interaction page E can include prompt information that is shown in FIG. 2B and that is used to prompt the user to wait. Then, when the wallet system obtains the payment request, the wallet client 105 can output an interaction page C on the target terminal device 102.

[0060] When a jump to the wallet system is made, the wallet system (for example, the wallet client 105) can obtain device information of the target terminal device 102, and perform ATO risk identification based on the device information, to obtain a risk identification result.

[0061] Correspondingly, the wallet system can determine a payment result based on the risk identification result, and can send the payment result to the merchant system in a direct manner or an indirect manner. In an example of the indirect manner, the wallet system sends the payment result to the merchant system through the intermediate server.

[0062] Still with reference to FIG. 2A and FIG. 2B, it can be learned that when the merchant system obtains the payment result, the merchant client 103 can output an interaction page D on the target terminal device 102. The interaction page D is used to display the payment result to the user 101.

[0063] That is, in the related technology, to implement payment, there is a jump from the interaction page of the merchant system to the interaction page of the wallet system, or there is first a jump from the interaction page of the merchant system to the interaction page of the intermediate service system, and then a jump from the interaction page of the intermediate service system to the interaction page of the wallet system. When a jump to the wallet system is made, the wallet system can obtain device information of the target terminal device, perform ATO risk identification based on the device information, and determine a payment result based on the risk identification.

[0064] However, according to the above-mentioned technical solution, there are at least the

following technical problems: The jump process reduces payment efficiency, and may decrease a payment success probability, affecting payment experience. If the target terminal device does not jump to the wallet system, the wallet system cannot collect the device information of the target terminal device. Consequently, ATO risk identification cannot be performed, resulting in a reduction in payment security.

[0065] It should be noted that the above-mentioned content of the related technology is merely information known to the inventor, and neither means that the information has entered the public domain before the application date of this specification, nor means that the information can become the existing technology of this specification.

[0066] Therefore, to avoid at least one of the above-mentioned technical problems, this specification provides a technical concept with creative efforts: A merchant system displays an interaction page to a user through a target terminal device. The user initiates a payment request to the merchant system through the interaction page. The merchant system sends the payment request to an intermediate service system. The intermediate service system prestores first device information of the target terminal device that is collected and transmitted by a wallet system, and sends the first device information to the wallet system when the intermediate service system receives the payment request sent by the merchant system. When there is no jump from an interaction page of the target terminal device to an interaction page of the wallet system, the wallet system performs risk control based on the first device information, determines a payment result corresponding to the payment request based on a risk control result, and sends the payment result to the merchant system through the intermediate service system. The merchant system displays the payment result on the target terminal device.

[0067] Based on the above-mentioned analysis, it can be learned that compared with the related technology, in the technical solutions provided in this specification, there is no need to perform switching from the interaction page of the target terminal device to the interaction page of the wallet system. Therefore, a disadvantage of relatively poor experience of the target user caused due to a jump to the interaction page of the wallet system can be avoided, to improve experience of using a payment service by the target user; and impact of a jump to the interaction page of the wallet system on a payment success rate and efficiency can be avoided, that is, the payment success rate and efficiency can be improved. In addition, even if there is no switching, the wallet system can still perform risk control based on the first device information. Therefore,

payment security and reliability can still be implemented.

[0068] FIG. 3 is a diagram of a hardware structure of a service system 300 according to an embodiment of this specification. The service system 300 can be a merchant system, an intermediate service system, or a wallet system.

[0069] As shown in FIG. 3, the service system 300 can include at least one storage medium 303 and at least one processor 302. In some embodiments, the service system 300 can further include a communication port 304 and an internal communication bus 301. In some embodiments, the service system 300 can further include an I/O component 305.

[0070] The internal communication bus 301 can be connected to different system components. For example, the internal communication bus 301 can be connected to the storage medium 303, the processor 302, the communication port 304, and the I/O component 305.

[0071] The I/O component 305 supports an input/output between the service system 300 and another component.

[0072] The communication port 304 is used for data communication between the service system 300 and the outside. For example, the communication port 304 can be used for data communication between the service system 300 and a network. The communication port 304 can be a wired communication port, or can be a wireless communication port.

[0073] The storage medium 303 can include a data storage apparatus. The data storage apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 3031, a read-only storage medium (ROM) 3032, or a random access storage medium (RAM) 3033. The storage medium 303 further includes at least one instruction set stored in the data storage apparatus. The instruction set includes computer program code, and the computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, and the like for performing the payment method provided in this specification.

[0074] The at least one processor 302 can be communicatively connected to the at least one storage medium 303. The at least one processor 302 is configured to execute the at least one instruction set. When the service system 300 runs, the at least one processor 302 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the payment method provided in this specification. The processor 302 can perform all steps included in the payment method. The processor 302 can be in a form of one or more processors. In some

embodiments, the processor 302 can include one or more hardware processors, for example, a microcontroller, a microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit, processor, or the like that can perform one or more functions, or any combination thereof.

[0075] To merely describe a problem, only one processor 302 is shown in the service system 300 in the accompanying drawings. However, it should be noted that the service system 300 in this specification can further include a plurality of processors. Therefore, the operations and/or method steps disclosed in this specification can be performed by one processor, or can be jointly performed by a plurality of processors. For example, if the processor 302 in the service system 300 described in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or separately performed by two different processors 302 (for example, a first processor performs step A and a second processor performs step B, or a first processor and a second processor jointly perform steps A and B).

[0076] FIG. 4 is a schematic interaction diagram of a payment method according to an embodiment of this specification. It should be noted that a target terminal device does not jump to an interaction page of a wallet system in a process in which a merchant system, an intermediate service system, and the wallet system cooperate to perform the payment method.

[0077] As shown in FIG. 4, the method includes S401 to S408.

[0078] S401: The merchant system displays an interaction page to a user through the target terminal device.

[0079] S402: In response to detecting that the user requests to use the wallet system for payment in the merchant system, the merchant system sends a payment request to the intermediate service system. That is, the payment request indicates that the user requests to use the wallet system for payment in the merchant system.

[0080] It can be understood that to avoid tedious description, the content that has been described above is not described in detail again in this embodiment. For example, for implementation principles of S401 and S402, references can be made to the above-mentioned example.

[0081] S403: The intermediate service system obtains first device information corresponding to the target terminal device based on the payment request, where the first device information is device information collected by the wallet system from the target terminal device in advance.

[0082] Different terminal devices may correspond to different device information. Device information of the target terminal device includes but is not limited to a type, a model, and screen resolution of the target terminal device.

[0083] For example, the wallet system can collect the device information of the target terminal device in advance. For ease of distinction, the device information is referred to as the first device information. The wallet system sends the first device information to the intermediate service system. For example, the wallet system can collect the first device information corresponding to the target terminal device before S401, and send the first device information to the intermediate service system. Correspondingly, the intermediate service system obtains the first device information, and stores the first device information. When receiving the payment request, the intermediate service system can obtain the stored first device information based on the payment request.

[0084] In S403, the intermediate service system can obtain the first device information corresponding to the target terminal device based on the payment request. For example, the payment request can carry indication information, and the indication information can indicate a storage location or a storage identifier of the first device information. In this way, the intermediate service system can obtain the first device information based on the indication information. For another example, the payment request can carry the first device information. In this way, the intermediate service system can directly parse the payment request to obtain the first device information. Because the payment request is from the merchant system, S403 can be understood as follows: The first device information is transferred to the intermediate service system by the merchant system. That is, when detecting that the user initiates the payment request, the merchant system transfers the first device information to the intermediate service system by using the payment request.

[0085] It should be noted that in S403, the target terminal device can display an interaction page of the merchant system to the user, or can display an interaction page of the intermediate service system to the user.

[0086] If the target terminal device displays the interaction page of the merchant system to the

user, the interaction page of the merchant system in S403 may be the same as or different from the interaction page of the merchant system in S402.

[0087] If the target terminal device displays the interaction page of the intermediate service system to the user, references can be made to FIG. 5. As shown in FIG. 5, the intermediate service system displays an interaction page E to the user through the target terminal device. Content of the interaction page E is not limited in this embodiment. For example, the interaction page E can include prompt information that is shown in FIG. 5 and that is used to prompt the user to wait.

[0088] S404: The intermediate service system sends the first device information to the wallet system.

[0089] Correspondingly, the wallet system obtains the first device information sent by the intermediate service system.

[0090] Similarly, in S404, the target terminal device can display an interaction page of the merchant system to the user, or can display an interaction page of the intermediate service system to the user. The interaction page displayed by the target terminal device to the user in S404 and the interaction page displayed to the user in S403 may be the same or different.

[0091] S405: The wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result.

[0092] With reference to the above-mentioned example, the wallet system can perform ATO risk control on the wallet system based on the first device information, to obtain a risk control result. For example, the wallet system maintains a device fingerprint library in advance, and the device fingerprint library stores device fingerprints respectively corresponding to different accounts. The device fingerprint can be identification information that can uniquely identify a terminal device and that is generated by collecting and analyzing hardware, software, a network characteristic, user behavior information, and the like of the device. The device fingerprint can be used to track and identify a behavior pattern of the device, to help identify a potential account theft risk. The wallet system can obtain a device fingerprint corresponding to a current account from the device fingerprint library, and compare the first device information with the device fingerprint corresponding to the current account, to determine whether there is an ATO risk in the current account. When there is an ATO risk in the current account, identity verification needs to be performed on the user. When there is no ATO risk in the current account, identity verification does

not need to be performed on the user. The risk control result can indicate whether there is an ATO risk in the current account, or can indicate whether identity verification needs to be performed on the user.

[0093] Further, the wallet system can determine, based on the risk control result, whether to pay, to obtain the payment result.

[0094] With reference to the above-mentioned analysis, it can be learned that in this embodiment, the merchant system generates the payment request, to indicate, by using the payment request, the intermediate service system to obtain the device information (that is, the first device information) of the target terminal device in the wallet system. Correspondingly, the intermediate service system obtains the first device information based on the payment request, and sends the first device information to the wallet system. Correspondingly, when obtaining the first device information, the wallet system performs ATO risk control based on the first device information.

[0095] That is, in this embodiment, an interaction sequence of the merchant system, the intermediate service system, and the wallet system along a link is as follows: The merchant system indicates the first device information by using the payment request, and the intermediate service system obtains the first device information, and transfers the first device information to the wallet system, so that even when the terminal device does not jump to the wallet system, the wallet system can still obtain the first device information, and implement ATO risk control based on the first device information, to ensure payment security without jumping to the wallet system.

[0096] Similarly, in S405, the target terminal device can display an interaction page of the merchant system to the user, or can display an interaction page of the intermediate service system to the user. The interaction page displayed by the target terminal device to the user in S405 and the interaction page displayed to the user in S404 may be the same or different.

[0097] S406: The wallet system sends the payment result to the intermediate service system.

[0098] Correspondingly, the intermediate service system obtains the payment result sent by the wallet system.

[0099] Similarly, in S406, the target terminal device can display an interaction page of the merchant system to the user, or can display an interaction page of the intermediate service system to the user. The interaction page displayed by the target terminal device to the user in S406 and the interaction page displayed to the user in S405 may be the same or different.

[0100] S407: The intermediate service system sends the payment result to the merchant system.

[0101] Correspondingly, the merchant system obtains the payment result sent by the intermediate service system.

[0102] Similarly, in S407, the target terminal device can display an interaction page of the merchant system to the user, or can display an interaction page of the intermediate service system to the user. The interaction page displayed by the target terminal device to the user in S407 and the interaction page displayed to the user in S406 may be the same or different.

[0103] S408: The merchant system displays the payment result to the user through the target terminal device.

[0104] For example, the merchant system displays an interaction page D to the user through the target terminal device. As shown in FIG. 5, the interaction page D is used to display the payment result to the user.

[0105] With reference to the above-mentioned analysis, it can be learned that in this embodiment, from S401 to S408, the target terminal device displays the interaction page of the merchant system to the user, or displays the interaction page of the intermediate service system to the user, and does not need to display the interaction page of the wallet system to the user. That is, the target terminal device does not jump to the interaction page of the wallet system in a process in which the merchant system, the intermediate service system, and the wallet system cooperate with each other to complete payment. Therefore, a disadvantage of relatively poor experience of the user caused due to a jump to the interaction page of the wallet system is avoided, to improve experience of using a payment service by the user; and impact of a jump to the interaction page of the wallet system on a payment success rate and efficiency can be avoided, that is, the payment success rate and efficiency can be improved. In addition, the wallet system can perform risk control based on the first device information. Therefore, payment security and reliability can still be implemented when there is no jump.

[0106] To facilitate understanding of the technical solutions in this specification by a reader, the payment method in this specification is further described herein with reference to FIG. 6. As shown in FIG. 6, the method includes two phases: a preparation phase and a payment phase. The preparation phase includes S601 to S605. The payment phase includes S611 to S624. At least in the payment phase, a target terminal device outputs an interaction page of a merchant system, or outputs an interaction page of an intermediate service system. That is, in S611 to S624, the target

terminal device does not display an interaction page of a wallet system to a user.

[0107] Preparation phase

[0108] S601: The wallet system collects first device information from the target terminal device.

[0109] With reference to the above-mentioned example, a wallet client, for example, a wallet app, of the wallet system is deployed in the target terminal device. The wallet client collects device information of the target terminal device, to obtain the first device information.

[0110] For example, the wallet app includes a software development kit (SDK) that is used to collect information from the target terminal device to obtain the first device information.

[0111] S602: The wallet system sends the first device information to the intermediate service system.

[0112] Correspondingly, the intermediate service system obtains the first device information sent by the wallet system.

[0113] For example, the wallet client obtains the first device information, and sends the first device information to a wallet server. The wallet server sends the first device information to an intermediate server. Correspondingly, the intermediate server obtains the first device information sent by the wallet server.

[0114] S603: The intermediate service system generates a first identifier of the target terminal device in the wallet system based on the first device information, and stores the first identifier and the first device information in a first database.

[0115] The first identifier is used to distinguish the target terminal device from another terminal device in the wallet system.

[0116] The first identifier does not carry the first device information. That is, the first device information cannot be derived based on the first identifier. Therefore, disclosure of the first device information can be avoided, and security of the first device information can be improved, to avoid a potential theft caused due to disclosure of the first device information.

[0117] With reference to the above-mentioned example, this step can be understood as follows: The intermediate service system further includes the first database. When obtaining the first device information sent by the wallet server, the intermediate server generates the first identifier based on the first device information. The intermediate server stores the first device information and the first identifier in the first database.

[0118] S604: The intermediate service system sends the first identifier to the wallet system.

[0119] Correspondingly, the wallet system obtains the first identifier sent by the intermediate service system.

[0120] That is, for the first identifier, on one hand, the intermediate server stores the first identifier in the first database. On the other hand, the intermediate server sends the first identifier to the wallet server. Correspondingly, the wallet server obtains the first identifier sent by the intermediate server.

[0121] S605: The wallet system writes the first identifier into target storage space in the target terminal device.

[0122] Correspondingly, the target storage space stores the first identifier written by the wallet system. The target storage space is not limited in this embodiment. For example, the target storage space is nonvolatile storage space in the target terminal device. The target storage space can be shared storage space that can be accessed jointly by the wallet system and the merchant system.

[0123] For example, the wallet server sends the first identifier to the wallet client. The wallet client writes the first identifier into the target storage space. Correspondingly, the target storage space stores the first identifier written by the wallet client.

[0124] Payment phase

[0125] S611: The merchant system displays an interaction page to the user through the target terminal device.

[0126] S612: In response to detecting that the user requests, on the interaction page in S611, to use the wallet system for payment in the merchant system, the merchant system reads the first identifier from the target storage space in the target terminal device, and generates a payment request that carries the first identifier.

[0127] For example, a merchant client can perform real-time detection on the interaction page in S611. If the user requests, on the interaction page in S611, a target operation of using the wallet system for payment in the merchant system, the merchant client can read the first identifier from the target storage space. The merchant client can send the first identifier to a merchant server. The merchant server generates a payment request that includes the first identifier.

[0128] S613: The merchant system sends the payment request to the intermediate service system.

[0129] Correspondingly, the intermediate service system obtains the payment request sent by

the merchant system.

[0130] S614: The intermediate service system queries the first database based on the first identifier, to obtain the first device information.

[0131] With reference to the above-mentioned example, it can be learned that in the preparation phase, the intermediate service system stores the first identifier and the first device information in the first database. Correspondingly, in this step, the intermediate service system can query the first database by using the first identifier, to obtain the first device information corresponding to the first identifier.

[0132] In the transfer process of the first identifier, the wallet system writes the first identifier into the target storage space in the target terminal device, and the merchant system reads the first identifier from the target storage space in the target terminal device, and includes the first identifier in the payment request for transfer to the intermediate service system. In the transfer process of the first identifier, the first device information obtained by the intermediate service system based on the first identifier is definitely the device information collected by the wallet system from the target terminal device, that is, accuracy of the first device information is ensured.

[0133] S615: The intermediate service system sends the first device information to the wallet system.

[0134] Correspondingly, the wallet system obtains the first device information sent by the intermediate service system.

[0135] S616: The wallet system performs risk control based on the first device information, to obtain a risk control result.

[0136] In some embodiments, S616 can include: determining the risk control result based on the first device information and device fingerprint information that corresponds to a current account and that is stored in the wallet system. The risk control result indicates whether identity verification needs to be performed on the user.

[0137] The wallet system can maintain a device fingerprint library. The device fingerprint library stores device fingerprint information corresponding to different accounts of the wallet system. The device fingerprint information corresponding to each account can be collected by the wallet system from a terminal device previously used for the account in a historical time period.

[0138] In some embodiments, the wallet system can perform consistency comparison between the first device information and the device fingerprint information. If there is relatively low

consistency between the first device information and the device fingerprint information, the wallet system can generate a risk control result indicating that identity verification needs to be performed on the user. If there is high consistency between the first device information and the device fingerprint information, the wallet system can generate a risk control result indicating that identity verification does not need to be performed on the user.

[0139] S617: When the risk control result indicates that identity verification needs to be performed on the user, the wallet system sends an identity verification instruction to the intermediate service system. The identity verification instruction is used to indicate the intermediate service system to collect to-be-verified information of the user.

[0140] Correspondingly, the intermediate service system obtains the identity verification instruction sent by the wallet system.

[0141] For example, when the wallet system performs risk control based on the first device information, the wallet system may obtain a risk control result indicating a risk or a relatively high risk. In a case of the risk control result, the wallet system can send the identity verification instruction to the intermediate service system, to implement identity verification on the user by using the identity verification instruction.

[0142] That is, in S616, if the risk control result obtained by the wallet system indicates that identity verification needs to be performed on the user, S617 to S624 continue to be performed.

[0143] The to-be-verified information is information that can be used to distinguish between different users. The to-be-verified information is not limited in this embodiment. For example, the to-be-verified information can be a face image, can be a payment password, or can be an SMS verification code.

[0144] S618: The intermediate service system collects the to-be-verified information of the user based on the identity verification instruction.

[0145] For example, with reference to the above-mentioned example and FIG. 7, it can be learned that an intermediate service client can display an interaction page F to the user through the target terminal device. The interaction page F is used to indicate the user to enter the SMS verification code. The user enters the SMS verification code on the interaction page F. Correspondingly, the intermediate service client collects the to-be-verified information (that is, the SMS verification code) of the user.

[0146] S619: The intermediate service system sends the to-be-verified information to the

wallet system.

[0147] Correspondingly, the wallet system obtains the to-be-verified information sent by the intermediate service system.

[0148] With reference to the above-mentioned analysis, it can be learned that in some embodiments, the identity verification instruction can be used to indicate the intermediate service system to collect the to-be-verified information of the user. In some other embodiments, the identity verification instruction can alternatively be used to indicate the merchant system to collect the to-be-verified information of the user. An implementation principle of collecting the to-be-verified information of the user by the merchant system is described below.

[0149] S620: The wallet system performs identity verification on the user based on the to-be-verified information, to obtain an identity verification result.

[0150] With reference to the above-mentioned example, the wallet system determines whether the SMS verification code is correct, to implement identity verification on the user by determining whether the SMS verification code is correct.

[0151] For example, if the SMS verification code is correct, the wallet system determines an identity verification result indicating that the identity verification succeeds. If the SMS verification code is incorrect, the wallet system determines an identity verification result indicating that the identity verification fails.

[0152] S621: The wallet system determines a payment result based on the identity verification result.

[0153] For example, if the identity verification succeeds, the wallet system determines a payment result indicating a payment success. If the identity verification fails, the wallet system determines a payment result indicating a payment failure.

[0154] With reference to the above-mentioned analysis, it can be learned that in some embodiments, the risk control result may indicate that an identity of the user needs to be verified. In some other embodiments, the wallet system may alternatively obtain a risk control result indicating no risk or a very low risk. In the risk control result, the wallet system may not perform identity verification on the user. For example, the wallet system can directly perform payment to obtain a payment result.

[0155] S622: The wallet system sends the payment result to the intermediate service system.

[0156] Correspondingly, the intermediate service system obtains the payment result sent by

the wallet system.

[0157] S623: The intermediate service system sends the payment result to the merchant system.

[0158] Correspondingly, the merchant system obtains the payment result sent by the intermediate service system.

[0159] S624: The merchant system displays an interaction page that includes the payment result to the user through the target terminal device.

[0160] With reference to the above-mentioned example, it can be learned that the payment result may indicate a payment success, or may indicate a payment failure. As shown in FIG. 7, if the payment result indicates a payment success, the interaction page D that can be displayed by the merchant client to the user through the target terminal device is an interaction page D1 shown in FIG. 7.

[0161] Based on the above-mentioned analysis, it can be learned that the above-mentioned example is mainly that when the terminal device does not jump to the wallet system, the wallet system performs ATO risk control based on the first device information. In some other embodiments, the intermediate service system can further provide some risk control recommendations for ATO risk control by the wallet system, that is, the intermediate service system can further provide an auxiliary risk control service to the wallet system, to further improve payment security and reliability. A case in which the intermediate service system provides auxiliary risk control to the wallet system is described in detail herein based on FIG. 8.

[0162] As shown in FIG. 8, the method includes two phases: a preparation phase and a payment phase. The preparation phase includes S801 to S809. The payment phase includes S811 to S823. At least in the payment phase, a target terminal device outputs an interaction page of a merchant system, or outputs an interaction page of an intermediate service system. That is, in S811 to S823, the target terminal device does not display an interaction page of a wallet system to a user.

[0163] Preparation phase

[0164] S801: The wallet system collects first device information from the target terminal device.

[0165] S802: The wallet system sends the first device information to the intermediate service system.

[0166] S803: The intermediate service system generates a first identifier of the target terminal device in the wallet system based on the first device information, and stores the first identifier and

the first device information in a first database.

[0167] S804: The intermediate service system sends the first identifier to the wallet system.

[0168] S805: The wallet system writes the first identifier into target storage space in the target terminal device.

[0169] S806: The merchant system collects second device information from the target terminal device.

[0170] With reference to the above-mentioned example, a merchant client, for example, a merchant app, of the merchant system is deployed in the target terminal device. The merchant client collects device information of the target terminal device, to obtain the second device information.

[0171] For example, the merchant app includes a merchant SDK. The merchant SDK is a kit for collecting the device information from the target terminal device.

[0172] S807: The merchant system sends the second device information to the intermediate service system.

[0173] Correspondingly, the intermediate service system obtains the second device information sent by the system.

[0174] For example, the merchant client obtains the second device information, and sends the second device information to a merchant server. The merchant server sends the second device information to an intermediate server. Correspondingly, the intermediate server obtains the second device information sent by the merchant server.

[0175] S808: The intermediate service system generates a second identifier of the target terminal device in the merchant system based on the second device information, and stores the second identifier and the second device information in a second database.

[0176] The second identifier is used to distinguish the target terminal device from another terminal device in the merchant system.

[0177] Similarly, the second identifier does not carry the second device information. That is, the second device information cannot be derived based on the second identifier. Therefore, disclosure of the second device information can be avoided, and security of the second device information can be improved, to avoid a potential theft caused due to disclosure of the second device information.

[0178] With reference to the above-mentioned example, S808 can be understood as follows:

The intermediate service system further includes the second database. When obtaining the second device information sent by the merchant server, the intermediate server generates the second identifier based on the second device information. The intermediate server stores the second device information and the second identifier in the second database.

[0179] The first database and the second database can be a same database in the intermediate service system, or can be two different databases in the intermediate service system. This is not limited in this embodiment.

[0180] If the first database and the second database are two different databases in the intermediate service system, in the intermediate service system, the first database is used to store an identifier and device information of a terminal device in the wallet system, and the second database is used to store an identifier and device information of the terminal device in the merchant system.

[0181] S809: The intermediate service system sends the second identifier to the merchant system.

[0182] Correspondingly, the merchant system obtains the second identifier sent by the intermediate service system.

[0183] That is, for the second identifier, on one hand, the intermediate server stores the second identifier in the second database. On the other hand, the intermediate server sends the second identifier to a wallet server. Correspondingly, the merchant server obtains the second identifier sent by the intermediate server, and can store the second identifier in a memory of the merchant server.

[0184] With reference to the above-mentioned analysis, it can be learned that S801–S805 can be understood as a preparation process of the wallet system in the intermediate service system, and S806–S809 can be understood as a preparation process of the merchant system in the intermediate service system. It can be understood that there is no inevitable sequence relationship between the preparation process of the wallet system and the preparation process of the merchant system. The above-mentioned example is merely used to describe examples of implementation principles of the preparation process of the wallet system and the preparation process of the merchant system.

[0185] In addition, it should be noted that the procedure of the preparation phase can be performed based on a preset time interval, or can be performed based on a preset trigger condition.

[0186] In an example of performing the procedure of the preparation phase based on the preset

time interval, each of the wallet system and the merchant system can collect device information of the target terminal device based on the preset time interval. The intermediate service system can determine an identifier of the target terminal device in each of the wallet system and the merchant system based on the device information collected by each of the wallet system and the merchant system. The wallet system stores the identifier in the wallet system in the target storage space.

[0187] In an example of performing the procedure of the preparation phase based on the preset trigger condition, for example, the preset trigger condition can be that device information of the target terminal device changes. In this way, when the device information of the target terminal device changes, the wallet system, the merchant system, and the intermediate service system cooperate to perform the procedure of the preparation phase. For example, if a version of the target terminal device is updated, the wallet system, the merchant system, and the intermediate service system are triggered to cooperate to perform the procedure of the preparation phase. For another example, the preset trigger condition can be detecting that a client is run. For example, when the merchant system detects that the merchant client is run, the merchant system performs the procedure of the preparation phase. When the wallet system detects that a wallet client is run, the wallet system performs the procedure of the preparation phase.

[0188] Payment phase

[0189] S811: The merchant system displays an interaction page to the user through the target terminal device.

[0190] S812: In response to detecting that the user requests, on the interaction page in S811, to use the wallet system for payment in the merchant system, the merchant system reads the first identifier from the target storage space in the target terminal device, and obtains the second identifier.

[0191] For example, that the merchant system obtains the second identifier can be understood as follows: When detecting the request of the user, the merchant system obtains the second identifier stored in the preparation phase.

[0192] S813: The merchant system generates a payment request that carries the first identifier and the second identifier.

[0193] S814: The merchant system sends the payment request to the intermediate service system.

[0194] Correspondingly, the intermediate service system obtains the payment request sent by

the merchant system.

[0195] S815: The intermediate service system queries the first database based on the first identifier, to obtain the first device information.

[0196] S816: The intermediate service system queries the second database based on the second identifier, to obtain the second device information.

[0197] With reference to the above-mentioned example, it can be learned that in the preparation phase, the intermediate service system stores the second identifier and the second device information in the second database. Correspondingly, in this step, the intermediate service system can query the second database by using the second identifier, to obtain the second device information corresponding to the second identifier.

[0198] S817: The intermediate service system performs risk analysis based on at least one of the first device information and the second device information, to generate risk control recommendation information.

[0199] The risk control recommendation information is used to assist the wallet system in performing risk control. For example, the risk control recommendation information can be understood as information recommended for payment by the wallet system due to a payment risk. For example, the risk control recommendation information is that there is a relatively low risk, and payment is recommended. For another example, the risk recommendation information is that there is a very high risk and payment is not recommended. For another example, the risk control recommendation information is that there is a relatively high risk and further verification is recommended before it is determined whether to perform payment.

[0200] In an example, the intermediate service system can perform ATO risk analysis of the wallet system based on the first device information, to obtain risk control recommendation information for performing ATO risk analysis from a dimension of the wallet system. In another example, the intermediate service system can perform ATO risk analysis of the merchant system based on the second device information, to obtain risk control recommendation information for performing ATO risk analysis from a dimension of the merchant system. In still another example, the intermediate service system can perform ATO risk analysis of the wallet system based on the first device information, and perform ATO risk analysis of the merchant system based on the second device information, to obtain risk control recommendation information for performing ATO risk analysis from two dimensions: the merchant system and the wallet system.

[0201] When the intermediate service system performs risk control from two dimensions: the merchant system and the wallet system, risk control security and reliability can be improved.

[0202] S818: The intermediate service system sends the first device information and the risk control recommendation information to the wallet system.

[0203] Correspondingly, the wallet system obtains the first device information and the risk control recommendation information that are sent by the intermediate service system.

[0204] S819: The wallet system performs risk control based on the first device information and the risk control recommendation information, to obtain a risk control result.

[0205] For example, the wallet system can perform ATO risk identification based on the first device information, to obtain a first risk control result. The wallet system can obtain a second risk control result based on the risk control recommendation information. Correspondingly, the wallet system can obtain a final risk control result with reference to the first risk control result and the second risk control result. For example, if at least one of the first risk control result and the second risk control result indicates that there is an ATO risk in the current account, the final risk control result indicates that there is an ATO risk in the current account. If both the first risk control result and the second risk control result indicate that there is no ATO risk in the current account, the final risk control result indicates that there is no ATO risk in the current account.

[0206] S820: When the risk control result indicates that identity verification needs to be performed on the user, the wallet system sends an identity verification instruction to the intermediate service system. The identity verification instruction is used to indicate the merchant system to collect to-be-verified information of the user.

[0207] Correspondingly, the intermediate service system obtains the identity verification instruction sent by the wallet system.

[0208] With reference to the above-mentioned analysis, it can be learned that the identity verification instruction can be used to indicate the intermediate service system to collect the to-be-verified information of the user, or can be used to indicate the merchant system to collect the to-be-verified information of the user. In the above-mentioned example, descriptions are provided by using the identity verification instruction that is used to indicate the intermediate service system to collect the to-be-verified information of the user. Therefore, in this embodiment, descriptions are provided by using the identity verification instruction that is used to indicate the merchant system to collect the to-be-verified information of the user.

[0209] S821: The intermediate service system sends the identity verification instruction to the merchant system.

[0210] Correspondingly, the merchant system obtains the identity verification instruction sent by the intermediate service system.

[0211] S822: The merchant system collects the to-be-verified information of the user based on the identity verification instruction.

[0212] For example, with reference to the above-mentioned example and FIG. 9, it can be learned that the merchant client can display an interaction page F to the user through the target terminal device. The interaction page F is used to indicate the user to enter an SMS verification code. The user enters the SMS verification code on the interaction page F. Correspondingly, the merchant client collects the to-be-verified information (that is, the SMS verification code) of the user.

[0213] S823: The merchant system sends the to-be-verified information to the intermediate service system.

[0214] Correspondingly, the intermediate service system obtains the to-be-verified information sent by the merchant system.

[0215] S824: The intermediate service system sends the to-be-verified information to the wallet system.

[0216] Correspondingly, the wallet system obtains the to-be-verified information sent by the intermediate service system.

[0217] S825: The wallet system performs identity verification on the user based on the to-be-verified information, to obtain an identity verification result.

[0218] S826: The wallet system determines a payment result based on the identity verification result.

[0219] S827: The wallet system sends the payment result to the intermediate service system.

[0220] Correspondingly, the intermediate service system obtains the payment result sent by the wallet system.

[0221] S828: The intermediate service system sends the payment result to the merchant system.

[0222] Correspondingly, the merchant system obtains the payment result sent by the intermediate service system.

[0223] S827: The merchant system displays an interaction page that includes the payment

result to the user through the target terminal device.

[0224] With reference to the above-mentioned example, it can be learned that the payment result may indicate a payment success, or may indicate a payment failure. As shown in FIG. 9, if the payment result indicates a payment success, the interaction page D that can be displayed by the merchant client to the user through the target terminal device is an interaction page D1 shown in FIG. 9.

[0225] It should be noted that the above-mentioned example is merely used to describe an example of a possible implementation of the payment method in this specification, and cannot be understood as a limitation on the implementation of the payment method in this specification.

[0226] For example, some of the above-mentioned operations of the merchant client can be implemented by the merchant server, some of the above-mentioned operations of the merchant server can also be implemented by the merchant client, some of the above-mentioned operations of the payment client can be implemented by the payment server, and some of the above-mentioned operations of the payment server can also be implemented by the payment client.

[0227] For another example, the intermediate service system can include two subsystems. For example, one subsystem is configured to perform a risk analysis operation, and the other subsystem is configured to perform an operation other than the risk analysis operation.

[0228] For another example, based on the above-mentioned technical concept, some of the above-mentioned technical features can be combined to obtain a new embodiment; a new technical feature can be added based on the above-mentioned example to obtain a new embodiment; some technical features can be reduced based on the above-mentioned example to obtain a new embodiment; some technical features in the above-mentioned example can be replaced with other technical features; or some technical features and the order in the above-mentioned example can be adjusted to obtain a new embodiment. Implementations are not listed one by one herein.

[0229] According to the above-mentioned technical concept, this specification further provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by a processor, the steps in the payment method in this specification are implemented.

[0230] In some possible implementations, various aspects of this specification can be further implemented in a form of a program product, including program code. When the program product

runs on the service system 300, the program code is used to enable the service system 300 to perform the steps in the payment method described in this specification. The program product configured to implement the above-mentioned method can be a portable compact disc read-only memory (CD-ROM) that includes program code, and can run on the service system 300. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable medium can be a readable signal medium or a readable storage medium. The readable storage medium can be, for example, an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus, or device, an infrared system, apparatus, or device, or a semiconductor system, apparatus, or device, or any combination thereof. More specific examples of the readable storage medium include an electrical connection including one or more conducting wires, a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any proper combination thereof. The computer-readable storage medium can include a data signal propagated in a baseband or as part of a carrier, and carries readable program code. The propagated data signal can be in a plurality of forms, and includes but is not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can alternatively be any readable medium other than the readable storage medium, and the readable medium can send, propagate, or transmit a program used by or in combination with an instruction execution system, apparatus, or device. The program code included in the readable storage medium can be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, optical cable, an RF medium, or any proper combination thereof. Program code for performing an operation of this specification can be written in any combination of one or more program design languages. The program design language includes an object-oriented program design language, for example, Java or C++, and further includes a conventional procedural program design language, for example, "C" language, or a similar program design language. The program code can be completely executed on the service system 300, partially executed on the service system 300, executed as an independent software

package, partially executed on the service system 300 and partially executed on a remote query system, or completely executed on a remote service system 300.

[0231] It should be noted that collection, storage, use, processing, transmission, provision, disclosure, and the like of related information (for example, a face image, a payment password, and an SMS verification code) of a user in the technical solutions in this specification all comply with related laws and regulations, and do not violate public order and good morals.

[0232] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in a sequence different from that in the embodiments and desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular sequence or consecutive sequence to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

[0233] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the detailed disclosure can be presented only by using an example, and can impose no limitation. Although it is not explicitly stated herein, a person skilled in the art can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be provided in this specification, and fall within the spirit and scope of the example embodiments of this specification.

[0234] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "one embodiment", "embodiments", and/or "some embodiments" mean/means that specific features, structures, or characteristics described with reference to the embodiment can be included in at least one embodiment of this specification. Therefore, it can be emphasized and understood that two or more references to "embodiments", "one embodiment", or "alternative embodiments" in various parts of this specification do not necessarily refer to a same embodiment. In addition, specific features, structures, or characteristics can be properly combined in one or more embodiments of this specification.

[0235] It should be understood that in the above-mentioned descriptions of the embodiments of this specification, to help understand a feature, for the purpose of simplifying this specification, various features are combined in a single embodiment, accompanying drawing, or description thereof in this specification. However, this does not mean that the combination of these features is

necessary. It is entirely possible for a person skilled in the art to mark some devices and understand the devices as separate embodiments when reading this specification. That is, the embodiments of this specification can also be understood as an integration of a plurality of secondary embodiments. Content of each secondary embodiment is also true when features are less than all features in one of the above-mentioned disclosed embodiments.

[0236] Each patent, patent application, publication of a patent application, and other materials, for example, articles, books, instructions, publications, documents, and products, that are cited in this specification and that are other than any document that is inconsistent or conflict with this document or that imposes limiting impact on the widest scope of the claims can be incorporated herein by reference and used for all purposes now or later associated with this document. In addition, the terms in this document shall prevail if there is any inconsistency or conflict between the descriptions, definitions, and/or use of the related terms in any material and the descriptions, definitions, and/or use of the related terms in this document.

[0237] Finally, it should be understood that the principles of the implementation solutions of this specification are described in the implementation solutions of the application disclosed in this specification. Other modified embodiments also fall within the scope of this specification. Therefore, the embodiments disclosed in this specification are merely examples and not limitations. A person skilled in the art can use an alternative configuration according to the embodiments of this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

CLAIMS

What is claimed is:

1. A payment method, applied to an intermediate service system that provides an intermediate service between a merchant system and a wallet system, and comprising:

when a target terminal device displays an interaction page of the merchant system, receiving a payment request from the merchant system, wherein the payment request indicates that a user requests to use the wallet system for payment in the merchant system;

obtaining first device information corresponding to the target terminal device based on the payment request, wherein the first device information is device information collected by the wallet system from the target terminal device in advance;

sending the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result; and

receiving the payment result from the wallet system, and sending the payment result to the merchant system, so that the target terminal device displays the payment result on the interaction page of the merchant system, wherein

in a process of performing the payment method by the intermediate service system, the target terminal device does not jump to an interaction page of the wallet system.

2. The method according to claim 1, wherein the payment request comprises a first identifier of the target terminal device in the wallet system, the first identifier is read by the merchant system from target storage space in the target terminal device, and the first identifier stored in the target storage space is written by the wallet system; and

the obtaining first device information corresponding to the target terminal device based on the payment request comprises:

querying a first database based on the first identifier, to obtain the first device information, wherein the first database stores respective identifiers of different terminal devices in the wallet system and device information collected by the wallet system.

3. The method according to claim 2, wherein the method further comprises:

receiving the first device information from the wallet system;

generating the first identifier based on the first device information, and storing the first

identifier and the first device information in the first database; and

sending the first identifier to the wallet system, so that the wallet system writes the first identifier into the target storage space.

4. The method according to claim 1, wherein the method further comprises:

obtaining second device information corresponding to the target terminal device based on the payment request, wherein the second device information is device information collected by the merchant system from the target terminal device in advance; and

performing risk analysis based on at least one of the first device information and the second device information, to generate risk control recommendation information; and

the sending the first device information to the wallet system comprises: sending the first device information and the risk control recommendation information to the wallet system, so that the wallet system performs risk control based on the first device information and the risk control recommendation information, and determines the payment result corresponding to the payment request based on the risk control result.

5. The method according to claim 4, wherein the payment request comprises a second identifier of the target terminal device in the merchant system, and the obtaining second device information corresponding to the target terminal device based on the payment request comprises:

querying a second database based on the second identifier, to obtain the second device information, wherein the second database stores respective identifiers of different terminal devices in the merchant system and device information collected by the merchant system.

6. The method according to claim 5, wherein the method further comprises:

receiving the second device information from the merchant system;

generating the second identifier based on the second device information, and storing the second identifier and the second device information in the second database; and

sending the second identifier to the merchant system.

7. The method according to claim 1, wherein when the risk control result indicates that identity verification needs to be performed on the user, the method further comprises:

receiving an identity verification instruction from the wallet system;

collecting to-be-verified information of the user based on the identity verification instruction, or indicating the merchant system to collect to-be-verified information of the user; and

sending the to-be-verified information to the wallet system, so that the wallet system

determines an identity verification result based on the to-be-verified information, and determines the payment result based on the identity verification result.

8. A payment method, applied to a wallet system, wherein the method comprises:

when a target terminal device displays an interaction page of a merchant system and a user triggers use of the wallet system for payment in the merchant system, receiving first device information corresponding to the target terminal device from an intermediate service system, wherein the first device information is device information that is obtained by the intermediate service system based on a payment request received from the merchant system and that is collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system;

performing risk control based on the first device information, and determining a payment result corresponding to the payment request based on a risk control result; and

sending the payment result to the intermediate service system, to forward the payment result to the merchant system through the intermediate service system, so that the target terminal device displays the payment result on the interaction page of the merchant system, wherein

in a process of performing the payment method by the wallet system, the target terminal device does not jump to an interaction page of the wallet system.

9. The method according to claim 8, wherein the performing risk control based on the first device information comprises:

determining the risk control result based on the first device information and device fingerprint information stored in the wallet system, wherein the risk control result indicates whether identity verification needs to be performed on the user.

10. The method according to claim 9, wherein when the risk control result indicates that identity verification needs to be performed on the user, the determining a payment result corresponding to the payment request based on a risk control result comprises:

sending an identity verification instruction to the intermediate service system, wherein the identity verification instruction is used to indicate the intermediate service system to collect to-be-verified information of the user or the merchant system to collect to-be-verified information of the user;

receiving the to-be-verified information, and performing identity verification on the user

based on the to-be-verified information, to obtain an identity verification result; and

determining the payment result based on the identity verification result.

11. The method according to claim 8, wherein the method further comprises:

receiving risk control recommendation information from the intermediate service system, wherein the risk control recommendation information is determined by the intermediate service system based on at least one of the first device information or second device information, and the second device information is device information collected by the merchant system from the target terminal device in advance; and

the performing risk control based on the first device information comprises: performing risk control based on the first device information and the risk control recommendation information.

12. The method according to claim 8, wherein the method further comprises:

collecting the first device information from the target terminal device;

sending the first device information to the intermediate service system, so that the intermediate service system generates a first identifier of the target terminal device in the wallet system based on the first device information, and stores the first identifier and the first device information in a first database;

receiving the first identifier from the intermediate service system; and

writing the first identifier into target storage space in the target terminal device.

13. A payment method, applied to a merchant system, wherein the method comprises:

displaying an interaction page of the merchant system through a target terminal device;

in response to detecting that a user requests to use a wallet system for payment in the merchant system, sending a payment request to an intermediate service system, wherein the payment request is used to enable the intermediate service system to obtain first device information corresponding to the target terminal device, and send the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result, wherein the first device information is device information collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; and

receiving the payment result forwarded by the wallet system through the intermediate service system, and displaying the payment result on the interaction page of the merchant system, wherein

in a process of performing the payment method by the merchant system, the target terminal device does not jump to an interaction page of the wallet system.

14. The method according to claim 13, wherein the payment request comprises a first identifier of the target terminal device in the wallet system, the first identifier is used to enable the intermediate service system to query a first database to obtain the first device information, and the first database stores respective identifiers of different terminal devices in the wallet system and device information collected by the wallet system; and the method further comprises:

reading the first identifier from target storage space in the target terminal device, wherein the first identifier stored in the target storage space is written by the wallet system.

15. The method according to claim 13, wherein the payment request is further used to enable the intermediate service system to obtain second device information corresponding to the target terminal device, and the second device information is device information collected by the merchant system from the target terminal device in advance; and

at least one of the first device information and the second device information is used to enable the intermediate service system to generate risk control recommendation information, and the risk control recommendation information is used to assist the wallet system in performing risk control.

16. The method according to claim 15, wherein the payment request comprises a second identifier of the target terminal device in the merchant system, the second identifier is used to enable the intermediate service system to query a second database to obtain the second device information, and the second database stores respective identifiers of different terminal devices in the merchant system and device information collected by the merchant system.

17. An intermediate service system, configured to provide an intermediate service between a merchant system and a wallet system, and comprising:

at least one storage medium that stores at least one instruction set for payment; and

at least one processor that is communicatively connected to the at least one storage medium, wherein the at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set, and the payment method comprises:

when a target terminal device displays an interaction page of the merchant system, receiving a payment request from the merchant system, wherein the payment request indicates that a user requests to use the wallet system for payment in the merchant system;

obtaining first device information corresponding to the target terminal device based on the payment request, wherein the first device information is device information collected by the wallet system from the target terminal device in advance;

sending the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result; and

receiving the payment result from the wallet system, and sending the payment result to the merchant system, so that the target terminal device displays the payment result on the interaction page of the merchant system, wherein

in a process of performing the payment method by the intermediate service system, the target terminal device does not jump to an interaction page of the wallet system.

18. A wallet system, comprising:

at least one storage medium that stores at least one instruction set for payment; and

at least one processor that is communicatively connected to the at least one storage medium, wherein the at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set, and the payment method comprises:

when a target terminal device displays an interaction page of a merchant system and a user triggers use of the wallet system for payment in the merchant system, receiving first device information corresponding to the target terminal device from an intermediate service system, wherein the first device information is device information that is obtained by the intermediate service system based on a payment request received from the merchant system and that is collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system;

performing risk control based on the first device information, and determining a payment result corresponding to the payment request based on a risk control result; and

sending the payment result to the intermediate service system, to forward the payment result to the merchant system through the intermediate service system, so that the target terminal device displays the payment result on the interaction page of the merchant system, wherein

in a process of performing the payment method by the wallet system, the target terminal

device does not jump to an interaction page of the wallet system.

19. A merchant system, comprising:

at least one storage medium that stores at least one instruction set for payment; and

at least one processor that is communicatively connected to the at least one storage medium, wherein the at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set, and the payment method comprises:

displaying an interaction page of the merchant system through a target terminal device;

in response to detecting that a user requests to use a wallet system for payment in the merchant system, sending a payment request to an intermediate service system, wherein the payment request is used to enable the intermediate service system to obtain first device information corresponding to the target terminal device, and send the first device information to the wallet system, so that the wallet system performs risk control based on the first device information, and determines a payment result corresponding to the payment request based on a risk control result, wherein the first device information is device information collected by the wallet system from the target terminal device in advance, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; and

receiving the payment result forwarded by the wallet system through the intermediate service system, and displaying the payment result on the interaction page of the merchant system, wherein in a process of performing the payment method by the merchant system, the target terminal device does not jump to an interaction page of the wallet system.

20. A computer-readable non-transitory storage medium, wherein the computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the method according to any one of claims 1 to 16 is implemented.