METHOD AND APPARATUS OF BARCODE-BASED MOBILE PAYMENT AND SERVICE PROCESSING

TECHNICAL FIELD

[0001] The present disclosure relates to the field of Internet technologies, and in particular, to method and apparatus of barcode-based mobile payment, and method and apparatus of barcode-based mobile service processing.

BACKGROUND

[0002] With the development of the mobile Internet and the popularization of mobile devices, mobile services such as mobile payment are more frequently applied in public areas such as a restaurant and a supermarket. Since a barcode contains information, a service can be processed through barcode scanning with actual applications. The barcode is widely used because of its convenience in service processing. Here, using the barcode to process a service is as follows: a barcode reader scans a barcode generated by a mobile device and uploads the scanned barcode to a server, and the server completes service processing through processes of parsing, authentication, etc. Currently, the method of barcode-based service processing has been widely applied in many public areas.

[0003] In the existing technology, when processing a service based on a barcode on a mobile device and scanned by the barcode reader, the server is subject to service rules of an account bound by the mobile device. For example, during payment, a control limit of an account is used as the upper limit to control a payment action of the mobile device. The control limit is the total limit that the account can expend. However, in a relatively short time after the mobile device is lost, severe property loss can be caused if the payment action of the mobile device is controlled by using the control limit of the corresponding account as the upper limit. Therefore, it is necessary to strengthen control on a service action of the mobile device. In addition, in the existing technology, one account can be bound with one more mobile device in addition to the mobile device of the current account, so that the additional bounded

mobile device can request a service based on the barcode.

SUMMARY

[0004] Implementations of the present disclosure provide a method of barcode-based mobile payment, to strengthen control on mobile payment.

[0005] Implementations of the present disclosure provide an apparatus of barcode-based mobile payment, to strengthen control on mobile payment. The implementations of the present disclosure use the following technical solutions:

[0006] A method of barcode-based mobile payment includes: receiving a two-dimensional barcode used for payment in a first mobile device and scanned by a barcode reader, where the two-dimensional barcode is generated based on a unique identifier (ID) of the first mobile device and account information of an account bound with the first mobile device; and parsing the two-dimensional barcode and performing identity authentication based on the account information and the unique ID of the first mobile device obtained through parsing. After the authentication succeeds, querying a payment limit based on the unique ID of the first mobile device, where the payment limit is the maximum payment limit in a given time period and preconfigured for the first mobile device by the account bound with the first mobile device; and making payment based on the queried payment limit.

[0007] Preferably, the method further includes: updating the payment limit after the payment is completed, where the payment limit is the difference between a control limit and a billing limit, the control limit is the total payment limit in a given time period and preconfigured for the first mobile device by the account bound with the first mobile device, and the billing limit is a used limit of the first mobile device in a given time period.

[0008] Preferably, the method further includes: saving payment information after the payment is completed, where the payment information includes a payment time and a used limit.

[0009] Preferably, the parsing the two-dimensional barcode and performing identity authentication based on the account information and the unique ID of the first mobile device obtained through parsing includes: parsing the two-dimensional barcode to obtain the account information and the unique ID of the first mobile device; and querying, based on the account information and the unique ID of the first mobile

device, a payment status preconfigured for the first mobile device by the account; and when the payment status is enabled, performing identity authentication based on the account information and the unique ID of the first mobile device.

[0010] Preferably, the account is bound with the first mobile device by using a second mobile device. Preferably, the first mobile device is a wearable intelligent device. Preferably, the account is bound with at least two first mobile devices.

[0011] An apparatus of barcode-based mobile payment includes a receiving unit, an authentication unit, a querying unit, and a payment unit, where the receiving unit is configured to receive a barcode used for payment in a first mobile device and scanned by a barcode reader, where the barcode is generated based on a unique ID of the first mobile device and account information of an account bound with the first mobile device; and the authentication unit is configured to: parse the barcode and perform identity authentication based on the account information and the unique ID of the first mobile device obtained through parsing; and the querying unit is configured to: after the authentication succeeds, query a payment limit based on the unique ID of the first mobile device, where the payment limit is the maximum payment limit in a given time period and preconfigured for the first mobile device by the account bound with the first mobile device; and the payment unit is configured to make payment based on the queried payment limit. Preferably, the device further includes an updating unit, and the updating unit is configured to update the payment limit after the payment is completed, where the payment limit is the difference between a control limit and a billing limit, the control limit is the total payment limit in a given time period and preconfigured for the first mobile device by the account bound with the first mobile device, and the billing limit is a used limit of the first mobile device in a given time period.

[0012] Preferably, the device further includes a recoding unit, and the recording unit is configured to save payment information after the payment is completed, where the payment information includes a payment time and a used limit.

[0013] Preferably, the authentication unit includes: an authentication subunit, configured to: parse the barcode to obtain the account information and the unique ID of the first mobile device; query, based on the account information and the unique ID of the first mobile device, a payment status preconfigured for the first mobile device by the account; and when the payment status is enabled, perform identity authentication based on the account information and the unique ID of the first mobile

device.

[0014] A method of barcode-based mobile service processing, where one is bound with a plurality of mobile devices, service rules are preconfigured for each mobile device, and the method includes: receiving a barcode used for service processing in a mobile device and scanned by a barcode reader, where the barcode is generated based on a unique ID of the mobile device and account information of an account bound with the mobile device; parsing the barcode and authenticating whether the mobile device is one of the plurality of mobile devices bound with the account based on the account information and the unique ID of the mobile device obtained through parsing; if yes, querying, based on the unique ID of the mobile device, service rules preconfigured for the mobile device by the account; and performing service processing based on the service rules preconfigured for the mobile device.

[0015] Preferably, the service rules include a service status, and the performing service processing based on the service rules preconfigured for the mobile device includes: querying the service status in the service rules; and when the service status is enabled, performing service processing based on the service rules preconfigured for the mobile device.

[0016] An apparatus of barcode-based mobile service processing, where one account is bound with a plurality of mobile devices, service rules are preconfigured for each mobile device, and the device includes: a barcode receiving unit, a terminal authentication unit, a service rule querying unit, and a service processing unit, where the barcode receiving unit is configured to receive a barcode used for service processing in a mobile device and scanned by a barcode reader, where the barcode is generated based on a unique ID of the mobile device and account information of an account bound with the mobile device; and the terminal authentication unit is configured to: parse the barcode and authenticate whether the mobile device is one of the plurality of mobile devices bound with the account based on the account information and the unique ID of the mobile device obtained through parsing; the service rule querying unit is configured to: if yes, query, based on the unique ID of the mobile device, service rules preconfigured for the mobile device by the account; and the service processing unit is configured to perform service processing based on the service rules preconfigured for the mobile device.

[0017] Preferably, the service rules include a service status, and the service processing unit is configured to: query the service status in the service rules; and

when the service status is enabled, perform service processing based on the service rules preconfigured for the mobile device.

[0018] In the implementations of the present disclosure, at least one of the previous technical solutions achieves the following beneficial effects: after the server receives the barcode used for payment in the mobile device, and the authentication succeeds, payment can be made based on the payment limit preconfigured for the mobile device by the account bound with the mobile device, so that the barcode-based payment action of each mobile device can be controlled by the account. Therefore, the following problem in the existing technology is resolved: Only the payment action for the account is controlled but control on the payment action of the mobile device is weak. In addition, the processing method is provided in the service processing process where one account is bound with the plurality of mobile devices.

BRIEF DESCRIPTION OF DRAWINGS

[0019] Drawings of the present specification that constitute a part of the present disclosure are used to provide further understanding of the present disclosure, and schematic implementations of the present disclosure and descriptions thereof are used to explain the present disclosure, which do not constitute an improper limitation on the present disclosure. In the drawings:

[0020] FIG. 1 is a schematic flowchart illustrating a method of barcode-based mobile payment, according to Implementation 1 of the present disclosure;

[0021] FIG. 2 is a structural block diagram illustrating an apparatus of barcode-based mobile payment, according to Implementation 2 of the present disclosure;

[0022] FIG. 3 is a schematic flowchart illustrating a method of barcode-based mobile service processing, according to Implementation 3 of the present disclosure;

[0023] FIG. 4 is a structural block diagram illustrating an apparatus of barcode-based mobile service processing, according to Implementation 4 of the present disclosure; and

[0024] FIG. 5 is a schematic flowchart illustrating a QR-code-based payment method of a kid's smartwatch, according to Implementation 5 of the present disclosure.

DESCRIPTION OF EMBODIMENTS

[0025] To make the objectives, technical solutions, and advantages of the present disclosure clearer, the following describes the technical solutions of the present disclosure with reference to the accompanying drawings in the implementations of the present disclosure. Apparently, the described implementations are a part rather than all of the implementations of the present disclosure. All other implementations derived by a person of ordinary skill in the existing technologies based on the implementations of the present disclosure without creative efforts shall fall within the protection scope of the present disclosure.

[0026] Before the technical solutions of the present disclosure are described in detail, for clarity, several technical terms are described first. A barcode reader, a control limit, a payment limit, a billing limit, etc. are related to the implementations of the present disclosure. The barcode reader can be a device that reads a barcode. The control limit can be the total payment limit in a given time period. For example, if the control limit is 1000 RMB per day, the total payment limit is 1000 RMB from 00:00 to 24:00 of the day. The payment limit is a limit that can be used for payment in a given time period. The billing limit is a billed limit in a given time period. In the same time period, the control limit can be the sum of the payment limit and the billing limit. For example, if the control limit is 1000 RMB per day, when 300 RMB is first billed, the billing limit is 300 RMB, and the payment limit is 700 RMB. Later, when 500 RMB is billed, the billing limit changes to 800 RMB, and the payment limit changes to 200 RMB. The technical solutions provided by the implementations of the present disclosure are described in detail as follows with reference to the accompanying drawings.

Implementation 1

[0027] As described above, because barcode-based payment is convenient, a barcode reader has been used in many public areas to make barcode-based mobile payment. However, currently, based on the method, a control limit of an account bound with a mobile device is used as the upper limit during payment. For example, if the control limit of the account is 2000 RMB per day, the sum that all mobile devices bound with the account can pay is no more than 2000 RMB in one day. If a mobile device bound with the account is lost or stolen, someone else can make payment by

using the mobile device before the account is prohibited from paying, and property loss is caused. As such, a payment solution is needed to strengthen control on a barcode-based mobile payment action. In view of this defect, a method of barcode-based mobile payment is provided to strengthen control on a payment action of a mobile device. Assume that an execution entity is a server configured to complete payment. FIG. 1 shows a schematic flowchart of the method. The method includes the following steps:

[0028] Step 11: Receive a barcode used for payment in a first mobile device and scanned by a barcode reader. In the present step, the barcode used for payment is sent to a server after the barcode reader scans the barcode used for payment on the mobile device. For example, if a mobile phone is used to perform barcode payment, the barcode reader should scan the barcode generated in the mobile phone, and send the barcode to the server configured to complete payment. The barcode in the mobile device is generated based on a unique ID of the mobile device and account information of an account bound with the mobile device. In the process that the mobile device is bound with the account, the account can be bound with the mobile device used for payment by using an application program installed on another mobile device. Therefore, the account can be bound with the first mobile device by using a second mobile device. For example, the account can be bound with a smartwatch by using an application program installed on a smartphone. As such, the smartwatch is the first mobile device, and the smartphone is the second mobile device. For ease of understanding, the first mobile device can be referred to as a paying terminal (a mobile device used for payment), and the second mobile device can be referred to as an account terminal (a mobile device that the account is located).

[0029] The unique ID of the paying terminal is an ID that uniquely identifies the paying terminal, for example, a Media Access Control (MAC) address, which is a hardware address, or a Universally Unique ID (UUID), which is a number generated on a terminal and unique to the terminal. The paying terminal ID can directly be a MAC address, a UUID, or a combination thereof, or can be generated by applying a transcoding algorithm to the MAC address and the UUID. In addition to the MAC address and the UUID, the ID can include a hardware type (smartphone, smartwatch, etc.), a model, a hardware parameter (screen size, color, etc.), etc. of the mobile device, which are intended to distinguish a mobile device from other mobile devices and express uniqueness of the terminal.

[0030] The paying terminal ID needs to be bound with the account by using the account terminal, so that a mapping relationship exists between the paying terminal ID and the account. The account information of the account bound with the paying terminal ID and the paying terminal ID are stored in the server, to help identity authentication during payment. For example, if the paying terminal ID is abcd, and a name of the account bound with the paying terminal ID is 1234, a mapping relationship between abcd and 1234 is stored in the server, to help identity authentication during payment. It is worthwhile to note that one account can be bound with a plurality of paying terminals. For example, if paying terminal IDs abcd and efgh are both bound with the account name 1234, a mapping relationship between 1234 and each of abcd and efgh is stored in the server.

[0031] The barcode can be generated based on the paying terminal ID and the account information of the account bound with the paying terminal. The process of generating a barcode based on information is a common knowledge to a person skilled in the existing technologies. Details are not described here.

[0032] In the receiving process, a connection is established between the barcode reader and the server through a network for (wired or wireless) transmission, which is a basic data transmission technology.

[0033] It is worthwhile to note that the barcode can include a one-dimensional barcode and a two-dimensional barcode. The one-dimensional barcode is also referred to as a barcode (barcode), which is a graphic ID used to express information and including a plurality of black strips and spacing with different widths arranged based on a certain coding rule. The two-dimensional barcode is also referred to as a QR code. It is a readable barcode with another dimension developed based on the one-dimensional barcode (that is, a barcode) and uses black and white (two colors in sharp contrast) rectangles to express binary data. Information can be obtained after the QR code is scanned and parsed. Therefore, in the present disclosure, both the one-dimensional barcode and the two-dimensional barcode can be used as a barcode to store information. Payment or service processing can be performed based on the information.

[0034] Step 12: Parse the barcode and perform identity authentication based on account information and a unique ID of the paying terminal obtained through parsing.

[0035] In the present step, the process of parsing the barcode is a process of obtaining the information included in the barcode, and can be considered as a reverse

process of generating the barcode based on the information. The barcode can include the paying terminal ID and the account information of the account bound with the paying terminal described in step 11. However, to improve security, other authentication information can be added. For example, a time stamp can be included to authenticate whether the barcode is in a valid time range. The time stamp can be delivered by the server to the account terminal, and then transmitted by the account terminal to the paying terminal; or can be directly delivered to the paying terminal (provided that the paying terminal has a network connection function). For example, if a time stamp has a valid time range of 24 hours, when a time length from a current time to the time stamp exceeds 24 hours, the barcode is determined as invalid.

[0036] In actual application, to prevent the barcode information from being intercepted or tampered, information used to generate the barcode usually needs to be encrypted. In the authentication process, authentication can be performed at least once. For example, when the paying terminal generates a barcode, information such as the paying terminal ID, the time stamp, the account information, etc. can be encrypted by using a private key sent by the server, and an encryption algorithm is marked. When the server authenticates the barcode, the server first determines content in the barcode based on the marked encryption algorithm by using a relationship that a private key digital signature can be authenticated by using a public key, and then parses the content by using the public key. This is the first authentication. If the content cannot be parsed, payment cannot be made. Then, validity of the time stamp is authenticated based on information such as the paying terminal ID, the time stamp, and the account information obtained through parsing. This is the second authentication. Eventually, the third authentication is performed based on the paying terminal ID, the account information, and the mapping relationship stored in the server, to complete three times of authentication.

[0037] In an implementation, to further control a payment action of the paying terminal, the parsing the barcode and performing identity authentication based on account information and a unique ID of the first mobile device obtained through parsing can include: parsing the barcode to obtain the account information and the unique ID of the paying terminal; and querying, based on the account information and the unique ID of the paying terminal, a payment status preconfigured for the paying terminal by the account; and when the payment status is enabled, performing identity authentication based on the account information and the unique ID of the paying

terminal.

[0038] The payment status can be preconfigured for the paying terminal by the account, and stored in the server. The payment status can include enabled and disabled. The account information and the paying terminal ID can be obtained after the barcode is parsed. Then, the payment status preconfigured for the terminal by the account is queried based on the paying terminal ID. If the payment status is enabled, identity authentication can be performed. If the payment status is disabled, payment failure information can be directly returned.

[0039] The payment action of the paying terminal can be better controlled in the method. To be specific, whether the paying terminal can make payment by using the barcode can change at any time.

[0040] Step 13: After the authentication succeeds, query a payment limit based on the unique ID of the paying terminal. In the present step, the payment limit is the maximum payment limit in a given time period and preconfigured for the paying terminal by the account bound with the paying terminal.

[0041] As described above, the control limit is the total payment limit in a given time period, the payment limit is a limit that can be expended in a given time period, and the billing limit is a used limit in a given time period. In the same given time period, the control limit is the sum of the payment limit and the billing limit. Table 1 shows limits preconfigured for two paying terminals abcd and efgh bound with account 1234.

Table 1 (limit unit: RMB)

Account name	Paying terminal ID	Control limit	Billing limit	Payment limit	Given time period
1234	abcd	100	0	100	Day
	efgh	500	10	490	Week

[0042] It can be queried from the table that payment limits of the paying terminals abcd and efgh are respectively 100 RMB and 490 RMB.

[0043] In the present step, the control limit preconfigured for the paying terminal bound with the account plays an important role in controlling the paying action of the terminal.

[0044] Step 14: Make payment based on the queried payment limit. In the present step, payment can be completed when an amount to be used does not exceed the payment limit. Taking Table 1 as an example, if the paying terminal abcd needs to pay 50 RMB, payment can be completed. If the paying terminal abcd needs to pay 150 RMB, payment cannot be completed.

[0045] Because the control limit remains unchanged, after making one payment, the payment limit decreases while the billing limit increases. For the next payment, a latest payment limit needs to be queried. In an implementation, the method can further include the following steps:

[0046] Step 15: Update the payment limit after the payment is completed. In the present step, because the payment limit is the difference between the control limit and the billing limit, after the payment is completed, the payment limit can be updated based on the auto-changing billing limit and the control limit.

[0047] For example, as shown in Table 1, after the mobile device abcd makes payment of 50 RMB in one day, the billing limit in the day is 50 RMB. Since the control limit is 100 RMB per day, the payment limit in the day is 50 RMB. In actual application, the payment can be set in a plurality of methods. For example, when the amount to be used exceeds the payment limit, payment is completed, and a part exceeding the payment limit is deducted from a control limit in a next given time period. As another example, when the amount to be used exceeds the payment limit, payment is completed but the payment status is changed from enabled to disabled, to better control the payment action. In addition, the disabled time can be prolonged (for example, the payment status is changed to enabled ten given time periods later) to further strengthen control on the payment action.

[0048] To better understand the payment action of the mobile device associated with the account, in an implementation, the method can further include step 16: Save payment information after the payment is completed.

[0049] In the present step, the payment information can include a payment time and a used limit. For example, 50 RMB is used at 18:00. In addition, the payment information can include merchant information, a transaction number, a transaction type, etc.

[0050] In an implementation, the paying terminal in this implementation can be a wearable intelligent device, for example, a smartwatch, an intelligent wristband, a sports band (with a screen). For a kid's smartwatch, a control limit in a given time

period is preconfigured to strengthen control on a payment action. In addition, as described in step 15, the payment can be set in a plurality of methods to nurture a kid's self-discipline awareness.

[0051] As described in step 11, during binding, the paying terminal ID can include a hardware type. There can be different hardware types, and different solutions for setting a control limit. Different setting solutions corresponding to different hardware types can be stored in the server. For example, a setting solution corresponding to the kid's smartwatch (or a smartwatch for the aged) can be set based on the paying terminal ID. In this method, different paying terminals can be controlled differently.

[0052] In the method provided in Implementation 1, after the server receives the barcode used for payment in the mobile device, and the authentication succeeds, payment can be made based on the payment limit preconfigured for the mobile device by the account bound with the mobile device. As such, the barcode-based payment action of each mobile device can be controlled by the account. Therefore, the following problem in the existing technology is resolved: Only the payment action for the account is controlled but control on the payment action of the mobile device is weak. In addition, the payment status of the mobile device can be set to more flexibly control the payment action of the mobile device in time.

Implementation 2

[0053] Based on the same disclosing concept, Implementation 2 provides an apparatus of barcode-based mobile payment, to strengthen control on a payment action of a mobile device. As shown in FIG. 2, the device includes: a receiving unit 21, an authentication unit 22, a querying unit 23, and a payment unit 24. The receiving unit 21 can be configured to receive a barcode used for payment in a first mobile device and scanned by a barcode reader. The barcode is generated based on a unique ID of the first mobile device and account information of an account bound with the first mobile device.

[0054] The authentication unit 22 can be configured to: parse the barcode and perform identity authentication based on the account information and the unique ID of the first mobile device obtained through parsing.

[0055] The querying unit 23 can be configured to: after the authentication succeeds, query a payment limit based on the unique ID of the first mobile device,

where the payment limit is the maximum payment limit in a given time period and preconfigured for the first mobile device by the account bound with the first mobile device.

[0056] The payment unit 24 can be configured to make payment based on the queried payment limit. In an implementation, the device can further include an updating unit. The updating unit can be configured to update the payment limit after the payment is completed. The payment limit is the difference between a control limit and a billing limit. The control limit is the total payment limit in a given time period and preconfigured for the first mobile device by the account bound with the first mobile device, and the billing limit is a used limit of the first mobile device in a given time period. In an implementation, the device can further include a recoding unit. The recoding unit can be configured to save payment information after the payment is completed. The payment information can include a payment time and a used limit, and can include merchant information, a transaction number, a transaction type, etc.

[0057] In an implementation, the authentication unit 22 includes an authentication subunit. The authentication subunit can be configured to: parse the barcode to obtain the account information and the unique ID of the first mobile device; query, based on the account information and the unique ID of the first mobile device, a payment status preconfigured for the first mobile device by the account; and when the payment status is enabled, perform identity authentication based on the account information and the unique ID of the first mobile device.

[0058] In an implementation, the account is bound with the first mobile device by using a second mobile device. In an implementation, the first mobile device is a wearable intelligent device, for example, a smartwatch. In an implementation, the account is bound with at least two first mobile devices.

[0059] By using the device provided in Implementation 2, after the server receives the barcode used for payment in the mobile device, and the authentication succeeds, payment can be made based on the payment limit preconfigured for the mobile device by the account bound with the mobile device. As such, the barcode-based payment action of each mobile device can be controlled by the account. Therefore, the following problem in the existing technology is resolved: Only the payment action for the account is controlled but control on the payment action of the mobile device is weak. In addition, the payment status of the mobile device can be set to more flexibly control the payment action of the mobile device in time.

Implementation 3

[0060] As described above, in the existing technology, one account can be bound with only one more mobile device other than a mobile device that the account belongs, so that the bound mobile device can request a barcode-based service. For example, one account can be bound with only one smartwatch by using a mobile phone that the account belongs. The smartwatch can complete various barcode-based services. With the popularization of intelligent devices, one account needs to be bound with a plurality of mobile devices and every mobile device needs to be managed. Therefore, the present implementation provides a method of barcode-based mobile service processing. The method is applied to a service processing scenario that one account is bound with a plurality of mobile devices. In the present implementation, one account can be bound with a plurality of (at least two) mobile devices other than an intelligent terminal that the account belongs. A binding process can be as follows: The account invokes the Bluetooth function of a mobile phone by using an application program on the mobile phone, and is separately connected to the plurality of mobile devices. A unique ID of each mobile device is obtained; and a mapping relationship between the account and the unique IDs of the plurality of mobile devices is established and stored in a server. To control a service action of each mobile device, a set of service rules (for example, allowed or prohibited services) is preconfigured for each terminal and stored in the server. As shown in FIG. 3, the method includes the following steps:

[0061] Step 31: Receive a barcode used for service processing in a mobile device and scanned by a barcode reader.

[0062] The barcode can be generated based on a unique ID of the mobile device and account information of an account bound with the mobile device.

[0063] For example, one account can be bound with one smartphone and two smartwatches other than a mobile phone that the account belongs. An implementation can be establishing a mapping relationship between the account and each of IDs of the smartwatches and the smartphone, and storing the mapping relationship in the server. When a mobile device needs to execute a service, the mobile device can generate a barcode based on an ID of the mobile device, the account information of the account, and service information, so that the barcode reader can scan the barcode. The barcode in the present implementation can be a one-dimensional barcode or a two-dimensional barcode.

[0064] Step 32: Parse the barcode and authenticate whether the mobile device is one of a plurality of mobile devices bound with an account based on account information and a unique ID of the mobile device obtained through parsing.

[0065] The barcode can be parsed after being received. A parsing process is not a focus of the present disclosure. Therefore, details are not described here. When the account information and the mobile device ID included in the barcode are obtained through parsing, whether a mapping relationship exists between the account information and the mobile device ID can be queried in the server. Because the account is bound with the plurality of mobile devices, whether the mobile device is one of the plurality of mobile devices bound with the account needs to be queried.

[0066] Step 33: If yes, query, based on the unique ID of the mobile device, service rules preconfigured for the mobile device by the account.

[0067] If the mobile device is one of the plurality of mobile devices bound with the account, the service rules set for the mobile device by the account can be queried. The service rules can be preconfigured. For example, if the mobile device is a kid's smartwatch, a service rule can be a payment limit (20 RMB per day) etc. If the mobile device is a smartphone for the aged, a family address can be set, so that a taxi can drive the aged home. In addition, a medical record and a health status of the aged can be added, so that the medical record of the aged can be queried in a hospital by using a barcode.

[0068] Step 34: Perform service processing based on the service rules preconfigured for the mobile device. After the service rules preconfigured for the mobile device are queried, service processing can be performed.

[0069] For example, the method of processing a payment service is described in step 14 in Implementation 1. For another example, when a bank queries personal information such as an ID card by using a QR code on the mobile device, service processing can be performed based on the service rules set for the mobile device. The service rules can be that querying can be performed when a bank queries personal information. To further control a payment action of a paying terminal, in an implementation, the step further includes: querying a service status in the service rules; and when the service status is enabled, performing the step.

[0070] For a specific description, refer to description in step 12 in Implementation 1. Details are not described here again.

[0071] In the method provided in Implementation 3, after the server receives the

barcode used for service processing in the mobile device, and the authentication succeeds, service processing can be performed based on the service rules preconfigured for the mobile device by the account bound with the mobile device. That is, barcode-based service actions of the plurality of mobile devices are separately managed by the account.

Implementation 4

[0072] Based on the same disclosing concept, Implementation 4 provides an apparatus of barcode-based mobile service processing. The device is applied to a service processing scenario that one account is bound with a plurality of mobile devices. In the present implementation, one account is bound with a plurality of mobile devices, and service rules are preconfigured for each mobile device. As shown in FIG. 4, the device includes a barcode receiving unit 41, a terminal authentication unit 42, a service rule querying unit 43, and a service processing unit 44.

[0073] The barcode receiving unit 41 can be configured to receive a barcode used for service processing in a mobile device and scanned by a barcode reader. The barcode is generated based on a unique ID of the mobile device and account information of an account bound with the mobile device.

[0074] The terminal authentication unit 42 can be configured to: parse the barcode and authenticate whether the mobile device is one of the plurality of mobile devices bound with the account based on the account information and the unique ID of the mobile device obtained through parsing.

[0075] The service rule querying unit 43 is configured to: when the mobile device is one of the plurality of mobile devices bound with the account, query, based on the unique ID of the mobile device, service rules preconfigured for the mobile device by the account.

[0076] The service processing unit 44 is configured to perform service processing based on the service rules preconfigured for the mobile device.

[0077] In an implementation, the service rules include a service status. The service processing unit 44 can be configured to: query the service status in the service rules; and when the service status is enabled, perform service processing based on the service rules preconfigured for the mobile device.

[0078] By using the device provided in Implementation 4, after the server receives

the barcode used for service processing in the mobile device, and the authentication succeeds, service processing can be performed based on the service rules preconfigured for the mobile device by the account bound with the mobile device. That is, barcode-based service actions of the plurality of mobile devices are separately managed by the account.

Implementation 5

[0079] Based on the same disclosing concept, Implementation 5 provides a QR-code-based payment method for a kid's smartwatch, to strengthen control on a payment action of the kid's smartwatch. Assume that a parent has two kids: a and b, and each kid has one smartwatch. During binding, the parent establishes a connection between the smartwatches and a mobile phone in a specified application program by using the Bluetooth function of the mobile phone. MAC addresses, UUIDs, and smartwatch types of the smartwatches are obtained to generate smartwatch IDs (abcd and efgh). A mapping relationship between an account 1234 and each of the smartwatches is established and stored in the server, to complete binding between the account 1234 and the two smartwatches. A control limit is preconfigured for each of the two smartwatches. As shown in Table 2, the parent M sets control limits for the two smartwatches.

Table 2 (limit unit: RMB)

Account name	Smartwatch ID	Remarks	Control limit	Given time period	Payment status
1234	abcd	Baby a	60	Day	Enabled
	efgh	Baby b	50	Day	Enabled

[0080] The schematic diagram shows a method that kid a makes QR-code-based payment on the smartwatch. Assume that an execution entity is a server configured to complete payment. As shown in FIG. 5, the method includes the following steps:

[0081] Step 51: Receive a QR code used for payment in smartwatch abcd and scanned by a barcode reader. The QR code is generated based on encrypted information obtained after the smartwatch receives a smartwatch ID, an account name, a time stamp

delivered by the server to the mobile phone, an algorithm mark, and a private key transmitted by the mobile phone, and encrypts the smartwatch ID, the account name, and the time stamp based on the algorithm mark by using the private key.

[0082] Step 52: Parse the QR code to obtain information included in the QR code; and perform decryption by using a public key corresponding to a private key delivered to the mobile phone, to perform the first authentication.

[0083] Step 53: After the authentication succeeds, obtain a smartwatch ID, an account name, and a time stamp, and authenticate whether the time stamp is valid, to perform the second authentication.

[0084] Step 54: After the authentication succeeds, query a payment status of the smartwatch based on the smartwatch ID and the account name.

[0085] Step 55: When the payment status is enabled, authenticate whether the binding relationship is correct based on the smartwatch ID (abcd) and the account name (1234), to perform the third authentication. It can be determined that the binding relationship is correct based on Table 2.

[0086] Step 56: After the authentication succeeds, query a payment limit based on the smartwatch ID (abcd).

[0087] Table 3 shows accounting information of the smartwatch stored in the server.

Table 3 (limit unit: RMB)

Smartwatch ID	Remarks	Control limit	Billing limit	Payment limit	Given time period
abcd	Baby a	60	0	60	Day
efgh	Baby b	50	10	40	Day

[0088] Step 57: Make payment based on the queried payment limit. For example, if the payment limit of smartwatch abcd is 60 RMB, and a received payment request is 33 RMB, payment is made.

[0089] Step 58: Update the payment limit after the payment is completed. Table 4 shows updated accounting information.

Table 4 (limit unit: RMB)

Smartwatch ID	Remarks	Control limit	Billing limit	Payment limit	Given time period
abcd	Baby a	60	33	27	Day
efgh	Baby b	50	10	40	Day

[0090] Step 59: Save payment information after the payment is completed. Table 5 shows payment information of smartwatch abcd.

Table 5

Smartwatch ID	Time	Place	Bill number	Billing limit
abcd	2015/10/25 17:45	XX restaurant	10001000	33

[0091] In the method provided in Implementation 5, the payment limit can be preconfigured for the kid's smartwatch bound with the account. Therefore, a QR-code-based payment action is controlled for each kid's smartwatch, so as to strengthen control on kid's consumption awareness. As such, the following problem in the existing technology is resolved: The QR-code-based payment action of the kid's smartwatch can be controlled only by an account of a parent, and the control is weak. For example, the parent is not likely to set the limit to 100, but should control the kid's consumption action. In addition, the payment status of the kid's smartwatch can be set, to more flexibly control the kid's payment action in time.

[0092] A person skilled in the existing technologies should understand that the implementations of the present disclosure can be provided as a method, a system, or a computer program product. Therefore, the present disclosure can use a form of hardware-only implementations, software-only implementations, or implementations with a combination of software and hardware. In addition, the present disclosure can use a form of a computer program product implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

[093] The present disclosure is described with reference to the flowcharts and/or

block diagrams of the method, the device (system), and the computer program product according to the implementations of the present disclosure. It should be understood that computer program instructions can be used to implement each process and/or each block in the flowcharts and/or the block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions can be provided for a general-purpose computer, a dedicated computer, an embedded processor, or a processor of any other programmable data processing device to generate a machine, so that the instructions executed by a computer or a processor of any other programmable data processing device generate an apparatus of implementing a function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[094] These computer program instructions can be stored in a computer readable memory that can instruct the computer or any other programmable data processing device to work in a way, so that the instructions stored in the computer readable memory generate an artifact that includes an instruction device. The instruction device implements a function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[095] These computer program instructions can be loaded onto a computer or another programmable data processing device, so that a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or the another programmable device provide steps for implementing a function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[096] In a typical configuration, the computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory. The memory can include a volatile memory, a random access memory (RAM), a non-volatile memory, and/or another form in a computer readable medium, for example, a read-only memory (ROM) or a flash memory. The memory is an example of the computer readable medium. The computer readable medium includes volatile, non-volatile, movable, and unmovable media that can implement information storage by using any method or technology. Information can be a computer readable instruction, a data structure, a program module, or other data. An example of a computer storage medium includes but is not limited to a parameter random access

memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of random access memory (RAM), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical storage, a cassette magnetic tape, tape and disk storage or another magnetic storage device, or any other non-transmission media that can be configured to store information that a computing device can access. As defined in the present specification, the computer readable medium does not include a transitory computer readable media (transitory media), such as a modulated data signal and a carrier.

[097] It is worthwhile to further note that the terms "include", "comprise", or their any other variant is intended to cover a non-exclusive inclusion, so that a process, a method, an article, or a device that includes a list of elements not only includes those elements but also includes other elements which are not expressly listed, or further includes elements inherent to such process, method, article, or device. An element preceded by "includes a ..." does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or device that includes the element.

[098] A person skilled in the existing technologies should understand that the implementations of the present disclosure can be provided as a method, a system, or a computer program product. Therefore, the present disclosure can use a form of hardware-only implementations, software-only implementations, or implementations with a combination of software and hardware. In addition, the present disclosure can use a form of a computer program product implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

[099] The previous descriptions are merely the implementations of the present disclosure, and are not intended to limit the present disclosure. For a person skilled in the existing technologies, the present disclosure can have various changes and variations. Any modifications, equivalent substitutions and improvements made in the spirit and principle of the present disclosure shall fall in the scope of the claims in the present disclosure.

CLAIMS

What is claimed is:

1. A method for barcode-based mobile payment, the method comprising:

binding an account with a plurality of mobile devices, wherein binding comprises

obtaining unique IDs of each mobile device of the plurality of mobile devices,

establishing and storing mapping relationships between the account and the unique IDs of the plurality of mobile devices at a server that is configured to complete payments;

preconfiguring service rules for each of the plurality of mobile devices for performing service processing for the corresponding mobile device, wherein the service rules include limits preconfigured for each of the plurality of mobile devices bound to the account;

based on a unique ID of a first mobile device, account information of the account bound with the first mobile device, and service information for a payment service to be executed, generating, by the first mobile device, a barcode to execute the payment service;

receiving, at the server and by the first mobile device, the barcode used to execute the payment service, wherein the barcode is scanned by a barcode reader;

parsing the barcode;

performing, by the server, identity authentication to determine whether the first mobile device is one of the plurality of mobile devices bound with the account based on the account information and the unique ID of the first mobile device obtained through parsing, wherein performing the identity authentication comprises

determining whether a mapping relationship exists at the server between the parsed account information and the parsed unique ID of the first mobile device by querying the server; and

in response to a successful authentication, querying the service rules of the account to determine a payment limit based on the unique ID of the first mobile device, wherein the service rules include service rules preconfigured for the first mobile device by the account bound with the first mobile device, wherein the payment limit is a maximum payment limit for expending for a given time period through the first mobile device that is computed as a difference between a control limit that remains unchanged and is preconfigured for the account bound with the first mobile

device and a billing limit used within the given time period by the account bound with the first mobile device;

making the payment service based on the payment limit when an amount to be used for the payment service does not exceed the payment limit; and

updating the payment limit after the payment service is completed, wherein an updated payment limit is computed as a difference between the control limit and the billing limit, the control limit is a total payment limit in the given time period and preconfigured for the first mobile device by the account bound with the first mobile device, and the billing limit is auto-changed to include the amount used of the first mobile device in the given time period.

2. The method according to claim 1, wherein the method further comprises: saving payment information after the payment service is completed, wherein the payment information comprises a payment time and the used amount.

3. The method according to any one of claims 1 to 2, wherein parsing the barcode and performing the identity authentication based on the account information and the unique ID of the first mobile device obtained through parsing comprises:

parsing the barcode to obtain the account information and the unique ID of the first mobile device; and querying, based on the account information and the unique ID of the first mobile device, a payment status preconfigured for the first mobile device by the account; and

when the payment status is enabled, performing the identity authentication based on the account information and the unique ID of the first mobile device.

4. The method according to any one of claims 1 to 3, wherein the method further comprises binding the account with the first mobile device by using a second mobile device.

5. The method according to any one of claims 1 to 4, wherein the first mobile device is a wearable smart device.

6. The method according to any one of claims 1 to 5, wherein the account is bound with at least two mobile devices comprising the first mobile device.

7. The method according to any one of claims 1 to 6, wherein the barcode comprises a QR code.

8. The method according to any one of claims 1 to 7, wherein the first mobile device comprises a smartwatch.

9. The method according to any one of the claims 1 to 8, wherein the method further comprises:

establishing a mapping relationship between the account and the unique ID of the first mobile device and optionally an ID of a second mobile device bound, such as a smartwatch or a smartphone; and

storing the mapping relationship at a server for helping identity authentication during the payment service.

10. The method according to claim 7, further comprising:

performing decryption on the QR code by using a public key corresponding to a private key delivered to the first terminal device, the first terminal device being a smartwatch, wherein the QR code is generated based on encrypting a smartwatch ID, an account name, and a time stamp based on an algorithm mark by using the private key;

when content of the QR code after decryption cannot be parsed, obtaining the smartwatch ID, the account name, and the time stamp through the decryption to authenticate whether the time stamp is valid and to perform a second authentication.

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

after the second authentication succeeded, performing a query on a payment status of the smartwatch based on the smartwatch ID and the account name;

when a payment status is enabled, authenticating whether a binding relationship is correct based on the smartwatch ID and the account name, to perform a third authentication.

12. The method according to any one of claims 1 to 11, wherein the barcode comprises a one dimensional bar code or a two dimensional bar code.

13. An apparatus for barcode-based mobile payment, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 12.