OFFLINE PAYMENT METHOD AND DEVICE

[0001] The present application claims priority to Chinese Patent Application No. 201610448201.7, filed on June 20, 2016 and entitled "OFFLINE PAYMENT METHOD AND DEVICE", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present application relates to network technologies, and in particular, to an offline payment method and device.

BACKGROUND

[0003] Offline payment is a method that payment can be made without a network. This method is gradually applied because this method can make user's payment more convenient without consuming network resources. When smart devices such as smartphones or smart watches are used as consumer terminal devices, the consumer terminal devices also need to be able to make offline payment to facilitate user's payment. In addition, with the development of the mobile Internet, integrating a third-party payment company’s payment method into a consumer terminal device gradually becomes a trend. A user can quickly open a third-party payment application that corresponds to the third-party payment company in the consumer terminal device, and use the third-party payment application to make payment quickly. In this case, a need may arise accordingly, that is, the user can select an account of a payment application from the opened third-party payment application to make offline payment. As such, user's payment can be more convenient.

[0004] However, in related technologies, even if an account of another payment application is selected from the third-party payment application for offline payment, a payment client of the payment application on the consumer terminal device needs to be invoked, and the payment client performs an offline payment procedure of the payment transaction. In this method, procedure processing is relatively cumbersome for the user, and an offline payment identity certificate generated by the another

payment application can be directly obtained after receiving by the consumer terminal device. In other words, the user can easily obtain an offline payment identity certificate of a payment application from the third-party payment application. Consequently, the security is relatively low.

SUMMARY

[0005] The present application provides an offline payment method and device, so that user's payment can be quicker and more secure when a payment application is selected from a third-party payment application integrated into a consumer terminal device to make offline payment.

[0006] The present application is implemented by using the following technical solutions:

[0007] According to a first aspect, an offline payment method is provided, where the method is used to make offline payment by using a target payment application in a third-party payment application integrated into a terminal device, and the method includes: obtaining, by the third-party payment application, an identity authentication identifier of a user that sends an offline payment request, when the third-party payment application receives the offline payment request that corresponds to the target payment application, where the user is a registered user of the target payment application; obtaining, by the third-party payment application, an offline payment certificate issued by the target payment application to the user and stored in the terminal device, when it is determined that the obtained identity authentication identifier is verified based on an identity authentication identifier stored at the time the user enables offline payment of the target payment application; and providing, by the third-party payment application, the offline payment certificate for an offline payment service party, so that the offline payment service party requests the target payment application to process the offline payment of the user based on the offline payment certificate.

[0008] According to a second aspect, an offline payment method is provided, where the method is used to make offline payment by using a target payment application in a third-party payment application integrated into a terminal device, and the method includes: receiving, by an offline payment server of the target payment application, an offline payment activation request sent by a third-party payment

application, where the offline payment activation request includes a user ID of a user and a terminal device ID of the terminal device, and the user is a registered user of the target payment application; and generating, by the offline payment server, an offline payment certificate that corresponds to the user ID, and sending the offline payment certificate to the third-party payment application after encrypting the offline payment certificate by using a terminal device public key that corresponds to the terminal device ID, so that the third-party payment application obtains the offline payment certificate after performing decryption by using a terminal device private key that corresponds to the terminal device ID.

[0009] According to a third aspect, an offline payment device is provided, where the device is applied to a third-party payment application, and is configured to make offline payment by using a target payment application in the third-party payment application integrated into a terminal device, and the device includes: an information acquisition module, configured to obtain an identity authentication identifier of a user that sends an offline payment request when the third-party payment application receives the offline payment request that corresponds to the target payment application, where the user is a registered user of the target payment application; a certificate acquisition module, configured to obtain an offline payment certificate issued by the target payment application to the user and stored in the terminal device, when it is determined that the obtained identity authentication identifier is verified based on an identity authentication identifier stored at the time the user enables offline payment of the target payment application; and a certificate providing module, configured to provide the offline payment certificate for an offline payment service party, so that the offline payment service party requests the target payment application to process the offline payment of the user based on the offline payment certificate.

[0010] According to a fourth aspect, an offline payment device is provided, where the device is applied to an offline payment server of a target payment application, and is configured to make offline payment by using a target payment application in a third-party payment application integrated into a terminal device, and the device includes: a request receiving module, configured to receive an offline payment activation request sent by the third-party payment application, where the offline payment activation request includes a user ID of a user and a terminal device ID of the terminal device, and the user is a registered user of the target payment application; and a certificate providing module, configured to generate an offline payment

certificate that corresponds to the user ID, and send the offline payment certificate to the third-party payment application after encrypting the offline payment certificate by using a terminal device public key that corresponds to the terminal device ID, so that the third-party payment application obtains the offline payment certificate after performing decryption by using a terminal device private key that corresponds to the terminal device ID.

[0011] According to the offline payment method and device provided in the present application, the third-party payment application stores the certificate in the terminal device locally, and can obtain the certificate from the terminal device locally when the certificate is to be used. As such, user's payment can be more convenient when the payment application is selected from the third-party payment application integrated into the consumer terminal device to make offline payment. In addition, when the stored certificate is obtained locally from the terminal device, the identity authentication identifier of the user needs to be first verified, so that the use of the certificate can be more secure.

BRIEF DESCRIPTION OF DRAWINGS

[0012] FIG. 1 is a diagram illustrating an application environment of an offline payment method, according to an example implementation of the present application;

[0013] FIG. 2 illustrates an offline payment activation procedure, according to an example implementation of the present application;

[0014] FIG. 3 illustrates an offline payment use procedure, according to an example implementation of the present application;

[0015] FIG. 4 illustrates an offline payment deactivation procedure, according to an example implementation of the present application;

[0016] FIG. 5 is a structural diagram illustrating an offline payment device, according to an example implementation of the present application;

[0017] FIG. 6 is a structural diagram illustrating another offline payment device, according to an example implementation of the present application;

[0018] FIG. 7 is a structural diagram illustrating still another offline payment device, according to an example implementation of the present application; and

[0019] FIG. 8 is a structural diagram illustrating still another offline payment device, according to an example implementation of the present application.

DESCRIPTION OF IMPLEMENTATIONS

[0020] Example implementations are described in detail here, and examples of the implementations are presented in the accompanying drawings. When the following description relates to the accompanying drawings, the same numbers in different accompanying drawings represent the same or similar elements unless specified otherwise. Implementations described in the following example implementations do not represent all implementations consistent with the present application. On the contrary, they are only examples of devices and methods that are described in the appended claims in detail and that are consistent with some aspects of the present application.

[0021] With the development of the mobile Internet, the integration of a payment method of a third-party payment company into a consumer terminal device gradually becomes a trend. A user can quickly open a third-party payment application that corresponds to the third-party payment company in the consumer terminal device, and use the third-party payment application to make payment quickly. For example, the third-party payment application can be applications such as Android Pay, Samsung Pay, and Huawei Pay. The third-party payment applications can be quickly started and opened in a consumer terminal device (for example, a smart device such as a smartphone). When using the third-party payment application, the user may have the following needs: For example, the user already has an account of a payment application (for example, the application is ALIPAY). The user expects to use the previously mentioned payment application in the third-party payment application to make offline payment after the third-party payment application is opened quickly. For example, the user expects to use offline payment of ALIPAY in Huawei Pay.

[0022] If the payment application is invoked by the third-party payment application, and the payment application performs processing based on an existing offline payment method, efficiency is relatively low, and the procedure is tedious. For example, ALIPAY client software is invoked in Huawei Pay, and the ALIPAY client software interacts with an offline payment server on an ALIPAY backend to make offline payment of ALIPAY. In this method, the third-party payment application is not involved. In addition, an offline code (which can be referred to as an offline payment certificate) generated by the ALIPAY client software can be directly obtained (for example, can be obtained by a merchant serving as an offline payment service party

by directly scanning the code). Consequently, the security is relatively low. Based on this, an implementation of the present application provides an offline payment method. An objective of the method is as follows: When a payment application needs to be selected from a third-party payment application integrated into a consumer terminal device to make offline payment, a method that the third-party payment application applies to the payment application for acquisition of an offline payment certificate is provided, and the third-party payment application stores the certificate in the terminal device locally. As such, the third-party payment application can quickly obtain the certificate in subsequent certificate use. The method provides a procedure for interaction between the third-party payment application and the payment application, so that the payment application can provide an offline code for the third-party payment application. In addition, the procedure is convenient and more secure, and are described in detail below.

[0023] The following describes an offline payment method in the present application. A payment application that interacts with a third-party payment application can be referred to as a target payment application (such as ALIPAY, but is not limited to ALIPAY, can be another application), and the third-party payment application is not limited to applications such as Samsung Pay and Huawei Pay mentioned above. In addition, in the description of the method, an offline code is referred to as an "offline payment certificate", and a form of the offline code is not limited. For example, the offline code can be a two-dimensional code.

[0024] FIG. 1 illustrates devices or modules that participate in an offline payment method and can be involved in an application of the method in an implementation of the present application. For example, a consumer terminal device 11 can include a third-party payment application 12 (such as Huawei Pay), a payment client 13 (ALIPAY client software) of a target payment application, and a trusted execution environment (TEE) 14. The TEE can provide a secure execution environment, and an application that has a relatively high security requirement can run in the environment. For example, the payment client 13 can run in the TEE 14, and the TEE 14 can provide services such as authorization, authentication, and storage for the application.

[0025] An application server 15 and an offline payment server 16 of the target application can be further included in FIG. 1. The application server 15 can be a backend server of the third-party payment application 12. The offline payment server 16 can be a backend server that is of the target payment application and is responsible

for an offline payment service. For example, an offline payment server of ALIPAY can provide offline payment service activation for a registered ALIPAY user. In addition, in FIG. 1, arrows are also used to indicate that these devices or modules can interact with each other. For example, the application server 15 and the offline payment server 16 can interact with each other (for example, send a request and a response), the third-party payment application 12 and the payment client 13 can interact with each other, etc.

[0026] With reference to FIG. 1, the following describes how to perform an offline payment interaction procedure between the target payment application and the third-party payment application. The procedure is an example of interaction between the devices or modules in FIG. 1. Offline payment activation, use, and deactivation between the third-party payment application and the target payment application are separately described in the method.

[0027] Offline payment activation:

[0028] Assume that a registered user of a target payment application wants to enable offline payment, and wants to enable an offline payment feature by using the target payment application in the third-party payment application. In this case, the user can open the third-party payment application, and choose to enable the offline payment of the target payment application in the third-party payment application. A selection method can be flexibly set. For example, a plurality of payment applications can be displayed in an interface of the opened third-party payment application for selection and use of the user. The user can select the target payment application from the applications, and choose to enable the offline payment of the target payment application.

[0029] After receiving the user selection, the third-party payment application learns that the user wants to enable the offline payment that corresponds to the target payment application. In this case, execution of an offline payment activation procedure shown in FIG. 2 can be started. It is worthwhile to note that the procedure shown in FIG. 2 is merely an example procedure. In specific implementations, another procedure can also be used. For example, a sequence between steps is changed. Referring to FIG. 2, the procedure can include the following processing. A TEE can include a payment application authentication center, a local authentication center, and local security storage. The payment application authentication center can be a payment client of the target payment application. In addition, the local authentication

center and the local security storage can be referred to as a local storage device because the local authentication center and the local security storage in the TEE are used when the third-party payment application stores an offline payment certificate in subsequent steps. An application server and an offline payment server of the target payment application also participate in the procedure.

[0030] In step 201 to step 203, the third-party payment application can obtain a user ID and a terminal device ID from the payment client of the target payment application. For example, when learning, based on user selection, that the user wants to enable offline payment of a target payment application, the third-party payment application can send a request to a payment client that is of the target payment application and is located in the same terminal device, to obtain the user ID and the terminal device ID. The user ID is an ID of a user who currently logs in to an account of the target payment application. For example, both a third-party payment application xx Pay and a payment application client software APP are installed on a mobile phone of a user. In this case, the user who currently logs in to the target payment application is a user who logs in to the payment application client software on the mobile phone, and the payment application client software feeds back a user ID of the user and a terminal device ID to the third-party payment application.

[0031] In the present implementation, the user ID returned by the payment client to the third-party payment application can be a token (token) that corresponds to a user account (also referred to as a user ID) of the payment application that the user currently logs in to, the token can be a token that corresponds to the user ID and is generated by the offline payment server of the target payment application for the user after registration of the user; and the server sends the token to the payment client. The terminal device ID can be a unique ID of the terminal device.

[0032] In addition, the payment client not only returns the terminal device ID and the user ID to the third-party payment application, but can also send a terminal device private key of the terminal device to the third-party payment application. Each terminal device can have one corresponding pair of public and private keys. The terminal device private key can be stored in the terminal device, and the terminal device public key can be stored in the offline payment server of the target payment application, so that the offline payment server sends a generated offline payment certificate to the terminal device after encrypting the offline payment certificate by using the terminal device public key. As such, only the terminal device can obtain the

offline payment certificate by performing decryption by using the terminal device private key, to improve the security of sending the certificate, so that only a particular device can use the offline payment certificate of the user. The procedure is also described in subsequent implementations.

[0033] After obtaining the user ID and the terminal device ID sent by the payment client, the third-party payment application can send an offline payment activation request to the target payment application. The offline payment activation request includes the user ID of the user and the terminal device ID of the terminal device. Referring to FIG. 2, for example, in steps 205 and 206, the third-party payment application can forward the request by using its application server, and the application server can use the private key to sign the request when forwarding the request.

[0034] The private key here can be allocated by the offline payment server of the target payment application to the application server in advance. An offline payment server of ALIPAY and Huawei Pay are used as an example. The offline payment server can allocate a service ID (namely, a service identifier) that corresponds to Huawei Pay, generate a pair of public and private keys that correspond to the service ID, send the private key to an application server of Huawei Pay, and still store the public key in the offline payment server of ALIPAY. When the application server interacts with the offline payment server, for example, sends an offline payment activation request to the offline payment server, the application server can sign the request by using the private key allocated by the offline payment server, and correspondingly, the offline payment server verifies the signature by using the public key. If the signature is verified, it indicates that the request is indeed sent by the application server of Huawei Pay. As such, it is ensured that a source of the request is reliable and legal. Certainly, when forwarding the request in step 206, the application server can add the service ID to the request. As such, in step 207, the offline payment server can identify the corresponding public key based on the service ID and verify the signature. Service IDs allocated by the offline payment server of the target payment application to different third-party payment applications can be different. For example, a service ID of a Huawei Pay application is different from a service ID of a Samsung Pay application.

[0035] In steps 208 to 210, the offline payment server of the target payment application allocates the corresponding offline payment certificate to the user. The certificate is equivalent to an ID of the user. For example, in an offline environment

without a network, an identity of the user can be confirmed accordingly provided that the offline payment certificate is provided, and money can be deducted from a payment account of the user.

[0036] The offline payment server can obtain a corresponding user account based on the user ID token included in the request, learn that a user of which account needs to request to enable offline payment, and generate a corresponding offline payment certificate for the account. An algorithm method for generating the certificate can be set by the target payment application autonomously. Then, to ensure the security, the offline payment server can obtain the corresponding terminal device public key based on the terminal device ID included in the request, encrypt the offline payment certificate by using the terminal device public key, and then send the encrypted offline payment certificate to the third-party payment application. In steps 211 and 212 in FIG. 2, the application server returns the encrypted offline payment certificate to the third-party payment application on a terminal device side. The third-party payment application can perform decryption by using the terminal device private key, to obtain the offline payment certificate.

[0037] After obtaining the offline payment certificate, the third-party payment application further needs to store the offline payment certificate in the terminal device where the third-party payment application is located, that is, store the offline payment certificate as in FIG. 2. As shown in FIG. 2, the third-party payment application can store the offline payment certificate in the local storage device of the terminal device, and further cooperate with the local storage device to perform encrypted storage on the certificate. For example, the third-party payment application can send a certificate storage request to the local authentication center in the local storage device. The request includes the offline payment certificate issued by the offline payment server of the target payment application to the user and received by the third-party payment application. In addition, the local authentication center can prompt the user to select an identity authentication method, for example, fingerprint authentication, iris authentication, or another method. After the user selects an authentication method, the third-party payment application can transmit an identity authentication identifier of the user to the local authentication center. The identity authentication identifier is, for example, a fingerprint of the user or an iris of the user.

[0038] The local authentication center can instruct the local security storage to generate a corresponding associated key based on the identity authentication identifier

of the user, and to perform encrypted storage on the offline payment certificate of the user by using the associated key. As such, when the user subsequently needs to make offline payment by using the stored offline payment certificate, the identity authentication identifier of the user needs to be provided, and the certificate can be provided only after the identity authentication identifier is verified, where details are described in a subsequent offline payment use procedure. As such, the use of the certificate can be more secure, and it can be ensured that the offline payment certificate is used by the user in person this time.

[0039] Finally, in steps 224 to 226, the third-party payment application can notify the offline payment server of the target payment application that the offline payment certificate has been stored in the terminal device locally. In this case, the offline payment server can record the offline payment activation information. For example, the information can include the user ID (the ID here can be the user account), the offline payment certificate that corresponds to the account, and can further include information such as an offline payment activation time.

[0040] By using the previous procedure shown in FIG. 2, the third-party payment application requests the target payment application to enable offline payment of a user, obtains an offline payment certificate of the user that is returned by the target payment application, and stores the certificate in the terminal device where the third-party payment application is located. In addition, encrypted storage is performed on the certificate in the terminal device by using an associated key that corresponds to an identity authentication identifier of the user. Next, a process performed by the third-party payment application when the user needs to use the offline payment of the target payment application is described.

[0041] Offline payment use:

[0042] The use procedure is still described by using the application scenario shown in FIG. 2 as an example. A third-party payment application stores an offline payment certificate in a terminal device locally, and performs encrypted storage. When a user needs to make offline payment after purchasing a merchandise, the user can quickly open the third-party payment application in the consumer terminal device, select a target payment application from the third-party payment application, and determine to use the target payment application to make offline payment. After the third-party payment application receives the user selection, in other words, receives an offline payment request that corresponds to the target payment application and is

initiated by the user, the use procedure shown in FIG. 3 can be performed, that is, an offline payment procedure can be performed.

[0043] As shown in FIG. 3, the third-party payment application can send a certificate acquisition request to a local storage device to request to obtain an offline payment certificate of the user. In addition, when the user chooses to use the offline payment of the target payment application in the third-party payment application, the user can be instructed to provide an account ID registered by the user in the target payment application, and add the account ID to the certificate acquisition request, so that local security storage can learn that the third-party payment application needs to obtain an offline payment certificate of which user.

[0044] When storing the offline payment certificate, a payment client can store the offline payment certificate based on a mapping relationship that "an account ID corresponds to an offline payment certificate". Then, in step 303, the corresponding offline payment certificate can be identified based on the account ID of the user who currently requests offline payment, and the certificate can be sent to a local authentication center. The local authentication center can generate a corresponding payment string based on the offline payment certificate, where the payment string can be a payment string (or can be a key string) generated by using the offline payment certificate as a factor and based on a certain algorithm rule; and return the payment string to the local authentication center. In addition, a storage method is not limited to the previous method in detailed implementation, and the offline payment certificate can be stored in another method. For example, a mapping relationship between a payment application and a certificate can be stored. As such, a corresponding certificate can be determined based on an application that the user selects to use for offline payment.

[0045] In step 306 to step 308, the local authentication center can first authenticate the user before returning the payment string to the third-party payment application. If an authentication method selected by the user is fingerprint authentication in the activation procedure shown in FIG. 2, in step 306, the third-party payment application can obtain fingerprint information of the user, and transmit the fingerprint information to the local authentication center. The local authentication center can provide the payment string for the third-party payment application when determining that the obtained identity authentication identifier is verified based on an identity authentication identifier stored at the time the user enables the offline

payment of the target payment application. The local authentication center feeds back the offline payment certificate of the user to the third-party payment application itself. But for better security, it generates the corresponding payment string by using the offline payment certificate based on a certain rule. Subsequently, an offline payment server can convert the payment string into the offline payment certificate to learn of a user's identity, and the offline payment server knows the generation rule used when the local authentication center generates the payment string.

[0046] By using steps 301 to 308, the third-party payment application obtains the offline payment certificate of the user, and obtains the certificate when the identity authentication identifier of the user is verified, so that it can be ensured that the user obtains the offline payment certificate of the user, to further improve the offline payment security. In steps 309 and 310, the third-party payment application can provide the payment string for an offline payment service party. The offline payment service party can be a payment collection system of a merchant. A method that the payment collection system obtains the payment string can be flexibly set to a plurality of methods, for example, a two-dimensional code, NFC, Bluetooth, and a sound wave. For example, when the payment string is presented in a form of a two-dimensional code, the payment collection system of the merchant can obtain the payment string through scanning.

[0047] In steps 311 to 315, the merchant can use the obtained payment string to request the offline payment server of the target payment application to process the offline payment of the user, and provide the payment string for the offline payment server of the target payment application. After obtaining the payment string, the offline payment server of the target payment application can convert the payment string into the corresponding offline payment certificate based on a predetermined rule, can learn of a user account that corresponds to the certificate based on the generation rule of the certificate, and the certificate user, and then can deduct money from a payment account of the user. The payment collection system can provide the third-party consumer application with feedback that money deduction succeeds.

[0048] It can be seen from the previous process that, for example, when the consumer terminal device of the user does not use a network and is in an offline state, if the offline payment of the target payment application needs to be used, the user can open the third-party payment application on the terminal device, and select offline payment of a target payment application from the application. In this case, the

third-party payment application can obtain the pre-stored offline payment certificate of the user from the terminal device locally based on the request of the user, and obtain the certificate only after the identity authentication identifier is verified. Then, the third-party payment application can provide the certificate for the merchant, for example, by using a two-dimensional code scanning method. The merchant sends a request to the offline payment server of the target payment application by carrying the certificate, to request to perform offline payment processing for the user that corresponds to the certificate, that is, deduct money from the payment account of the user, to complete local offline payment.

[0049] Offline payment deactivation:

[0050] A third-party payment application can further interact with a target payment application to cancel offline payment of a user in the target payment application. For an offline payment deactivation procedure, references can be made to FIG. 4. The procedure includes the following: In step 401, the third-party payment application receives an offline payment cancellation request initiated by the user. For example, the user can choose to deactivate offline payment of a target payment application in a page of the third-party payment application. Then, in steps 402 to 409, the third-party payment application obtains a payment string generated by using an offline payment certificate as a factor from a local storage device. For a detailed procedure, references can be made to the description in FIG. 3.

[0051] In steps 410 and 411, the third-party payment application can send the offline payment cancellation request (namely, an offline payment deactivation request) to an offline payment server of the target payment application through forwarding of an application server, and add the obtained payment string to the request. Alternatively, the payment string may not be obtained, but a payment client can return the offline payment certificate to the third-party payment application, and the application adds the offline payment certificate to the offline payment cancellation request. Even if the payment string is obtained, the offline payment server can obtain the offline payment certificate based on the payment string.

[0052] In step 412, the offline payment server of the target payment application can obtain a user account (namely, a user ID, where both the token mentioned above or the user account can be referred to as a user ID) that corresponds to the offline payment certificate obtained based on the received offline payment cancellation request, to learn of a user who requests to cancel offline payment. In addition, offline

payment activation information of the user is deleted. In steps 413 and 414, the offline payment server can feedback an offline payment cancellation success notification to the third-party payment application.

[0053] In addition, in the previous example, the third-party payment application stores the offline payment certificate in a terminal device locally after obtaining the offline payment certificate from the offline payment server of the target payment application. When the user uses the offline payment of the target payment application, the third-party payment application can obtain the certificate from the terminal device locally, and then provide the certificate for an offline payment service party, for example, a payment collection system of a merchant. A procedure is not limited to the procedures shown in FIG. 2 to FIG. 4 in actual implementations. For example, in another example, alternatively, the third-party payment application can store the certificate itself after obtaining the certificate from the target payment application, that is, not by using the payment client of the target payment application.

[0054] In the offline payment method in the present implementation of the present application, a method that a target payment application provides an offline payment certificate of a registered user of the application for a third-party payment application is provided. The third-party payment application can interact with the target payment application to obtain the certificate provided by the target payment application. In addition, the third-party payment application can store the certificate on the terminal device side. When the user subsequently needs to use the offline payment of the target payment application by using the third-party payment application, the third-party payment application can retrieve the stored certificate, and provide the certificate for the merchant after an identity authentication identifier of the user is verified, so that the merchant requests the target payment application to make offline payment of the corresponding user based on the certificate for money deduction. This is a method that the target payment application outputs an offline payment service of the target payment application to the third-party payment application, so that the user can use the offline payment of the target payment application by using the third-party payment application.

[0055] In an example implementation, a non-transitory computer readable storage medium including an instruction is further provided, for example, a memory including an instruction, and the instruction can be executed by a processor of a device to complete the method. For example, the non-transitory computer readable storage

medium can be a ROM, a random access memory (RAM), a CD-ROM, a magnetic tape, a floppy disk, and an optical data storage device.

[0056] To implement the previous method, an implementation of the present application further provides an offline payment device. The device is applied to a third-party payment application, and is configured to make offline payment by using a target payment application in the third-party payment application integrated into a terminal device. As shown in FIG. 5, the device can include an information acquisition module 51, a certificate acquisition module 52, and a certificate providing module 53.

[0057] The information acquisition module 51 is configured to obtain an identity authentication identifier of a user that sends an offline payment request when the third-party payment application receives the offline payment request that corresponds to the target payment application, where the user is a registered user of the target payment application.

[0058] The certificate acquisition module 52 is configured to obtain an offline payment certificate issued by the target payment application to the user and stored in the terminal device, when it is determined that the obtained identity authentication identifier is verified based on an identity authentication identifier stored at the time the user enables offline payment of the target payment application.

[0059] The certificate providing module 53 is configured to provide the offline payment certificate for an offline payment service party, so that the offline payment service party requests the target payment application to process the offline payment of the user based on the offline payment certificate.

[0060] In another example, as shown in FIG. 6, the device can further include an activation request module 54, a certificate receiving module 55, a certificate decryption module 56, and a certificate storage module 57.

[0061] The activation request module 54 is configured to send an offline payment activation request to the target payment application, where the offline payment activation request includes a user ID of the user and a terminal device ID of the terminal device.

[0062] The certificate receiving module 55 is configured to receive the offline payment certificate that corresponds to the user ID and is returned by the target payment application, where the offline payment certificate is encrypted by the target payment application by using a terminal device public key that corresponds to the terminal device ID.

[0063] The certificate decryption module 56 is configured to perform, by the third-party payment application, decryption by using a terminal device private key that corresponds to the terminal device ID, to obtain the offline payment certificate.

[0064] The certificate storage module 57 is configured to store the offline payment certificate in the terminal device.

[0065] The device can further include a certificate deactivation module 58, configured to send an offline payment deactivation request to the target payment application, where the offline payment deactivation request includes the offline payment certificate issued to the user, so that the target payment application can delete the offline payment certificate.

[0066] To implement the previous method, an implementation of the present application further provides an offline payment device. The device is applied to an offline payment server of a target payment application, and is configured to make offline payment by using a target payment application in a third-party payment application integrated into a terminal device. As shown in FIG. 7, the device can include a request receiving module 71 and a certificate providing module 72.

[0067] The request receiving module 71 is configured to receive an offline payment activation request sent by the third-party payment application, where the offline payment activation request includes a user ID of a user and a terminal device ID of the terminal device, and the user is a registered user of the target payment application.

[0068] The certificate providing module 72 is configured to generate an offline payment certificate that corresponds to the user ID, and send the offline payment certificate to the third-party payment application after encrypting the offline payment certificate by using a terminal device public key that corresponds to the terminal device ID, so that the third-party payment application obtains the offline payment certificate after performing decryption by using a terminal device private key that corresponds to the terminal device ID.

[0069] In another example, as shown in FIG. 8, the device can further include a key generation module 73.

[0070] The key generation module 73 is configured to generate a corresponding service ID and a pair of public and private keys that correspond to the service ID for the third-party payment application, and send the private key to the third-party payment application.

[0071] The request receiving module 71 is further configured to obtain the corresponding public key based on the service ID after receiving the offline payment activation request, and verify, by using the public key, that the offline payment activation request is sent by the third-party payment application. The user ID and the terminal device ID included in the offline payment activation request are signed by the third-party payment application by using the private key, and the request further includes the service ID.

[0072] In an example, the device can further include an information deletion module 74.

[0073] The request receiving module 71 is further configured to receive an offline payment deactivation request sent by the third-party payment application, where the offline payment deactivation request includes the offline payment certificate.

[0074] The information deletion module 74 is configured to obtain the corresponding user ID based on the offline payment certificate, and delete offline payment activation information of the user ID.

[0075] The previous descriptions are merely example implementations of the present application, but are not intended to limit the present application. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present application shall fall within the protection scope of the present application.

CLAIMS

1. A method for payment, the method comprising:

sending, by a third-party payment application, a payment activation request to a target payment application, wherein the payment activation request comprises a user identifier (ID) of a user and a terminal device identifier (ID) of a terminal device (206), wherein the user is a registered user of the target payment application;

receiving, by the third-party payment application, a payment certificate that corresponds to the user ID and is returned by the target payment application, wherein the payment certificate is encrypted by the target payment application by using a terminal device public key that corresponds to the terminal device ID (210);

decrypting, by the third-party payment application, the payment certificate by using a terminal device private key that corresponds to the terminal device ID, to generate the payment certificate (211 and 212);

storing, by the third-party payment application, the payment certificate in the terminal device (213);

receiving, by the third-party payment application, a payment request that corresponds to the target payment application;

receiving, by the third-party payment application, an identity authentication identifier of the user(201-203 and 301-306);

determining, by the third-party payment application, that the obtained identity authentication identifier is verified based on an identity authentication identifier stored at the time the user enables payment of the target payment application (207);

retrieving, by the third-party payment application, the payment certificate issued by the target payment application to the user and stored in the terminal device (208-210 and 308); and

providing, by the third-party payment application, the payment certificate for a payment service party, so that the payment service party requests the target payment application to process the payment of the user based on the payment certificate (309-310).

2. The method according to claim 1, wherein storing, by the third-party payment application, the payment certificate in the terminal device comprises:

sending, by the third-party payment application, the identity authentication identifier of the

user to a local storage device of the terminal device, the local storage device being configured to generate an associated key that corresponds to the identity authentication identifier, and uses the associated key to encrypt the payment certificate for storage (223).

3. The method according to claim 1, wherein receiving the payment certificate comprises: receiving, by the third-party payment application, the payment certificate decrypted by using an associated key that corresponds to the identity authentication identifier when a local storage device verifies the identity authentication identifier (224-226).

4. The method according to claim 1, further comprising:

sending, by the third-party payment application, a payment deactivation request to the target payment application, wherein the payment deactivation request comprises the payment certificate issued to the user, so that the target payment application deletes the payment certificate.

5. The method according to any one of claims 1 to 4, wherein the payment certificate is generated from a payment string based on a predetermined rule.

6. The method according to claim 5, wherein the payment string is provided by the third-party payment application.

7. The method according to claim 5, wherein the payment string comprises a two-dimensional code.

8. A device for a payment, the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 7.