RESOURCE TRANSFER METHODS, APPARATUSES, AND DEVICES

TECHNICAL FIELD

[0001] This specification relates to the field of computer technologies, and in particular, to resource transfer methods, apparatuses, and devices.

BACKGROUND

[0002] With the continuous development of Internet and terminal technologies, people are increasingly dependent on terminal devices in their work and life. People use the terminal device to store important personal information, and can use the terminal device to process various important services (such as a financial service or an instant messaging service). If the terminal device is lost or stolen, problems are caused to the user.

[0003] Currently, applications of some important services often verifies a predetermined corresponding password, fingerprint feature information, facial feature information, etc. to verify validity of initiating a current service. However, if information such as the predetermined payment password is leaked, it poses a significant security threat to resources (such as assets) of the user. That is, when the user's terminal device and the information such as the predetermined payment password are obtained by a thief, the thief can steal resources in an account of the user, for example, can perform operations such as transfer, malicious consumption, and money laundering on the resources in the account of the user. As a result, when the terminal device is lost or stolen, the user is exposed to a risk such as theft of huge data and financial assets. Therefore, a solution to a problem that resources of a user are stolen when information such as a terminal device of the user is lost and predetermined verification information is also stolen needs to be provided.

SUMMARY

[0004] An objective of embodiments of the specification is to provide a solution to a problem that resources of a user are stolen when a terminal device of the user is lost and predetermined verification information is also stolen.

[0005] To implement the above-mentioned technical solutions, the embodiments of this specification are implemented as follows: Embodiments of this specification provide a resource transfer method, where the method includes: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0006] Embodiments of this specification provide a privacy protection-based resource transfer method, applied to a terminal device, where a trusted execution environment (TEE) is set in the terminal device, and the method includes: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0007] Embodiments of this specification provide a resource transfer apparatus, where the apparatus includes: a request acquisition module, configured to obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; a verification module, configured to verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule by using the target application, and determine, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and a request forwarding module, configured to send the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0008] Embodiments of this specification provide a privacy protection-based resource transfer apparatus, where a trusted execution environment (TEE) is set in the apparatus, and the apparatus includes: a resource transfer request module, configured to obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user; a privacy processing module, configured to verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule in the TEE by using the target application, and determine, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and a resource transfer processing module, configured to send the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0009] Embodiments of this specification provide a resource transfer device, including a processor, and a memory, configured to store computer-executable instructions. When the executable instructions are executed, the processor performs the following steps: obtaining a resource transfer request triggered by a target user by using

a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0010] Embodiments of this specification provide a device, where a trusted execution environment TEE is set in the device, and the device includes: a processor, and a memory, configured to store computer-executable instructions. When the executable instructions are executed, the processor performs the following steps: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0011] Embodiments of this specification further provide a storage medium, where the storage medium is configured to store computer-executable instructions. When the executable instructions are executed, the following process is implemented: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; verifying the verification information by using the target application, and invoking, if the verification

succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0012] Embodiments of this specification further provide a storage medium, where the storage medium is configured to store computer-executable instructions. When the executable instructions are executed, the following process is implemented: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

BRIEF DESCRIPTION OF DRAWINGS

[0013] To describe the technical solutions in some embodiments of this specification or in an existing technology more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments or the existing technology. Clearly, the accompanying drawings in the following descriptions merely show some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0014] FIG. 1 shows embodiments of a resource transfer method, according to this specification;

[0015] FIG. 2 is a schematic diagram illustrating a resource transfer page, according to this specification;

[0016] FIG. 3 shows embodiments of another resource transfer method, according to this specification;

[0017] FIG. 4 is a schematic diagram illustrating a structure of a resource transfer system, according to this specification;

[0018] FIG. 5 is a schematic diagram illustrating a structure of another resource transfer system, according to this specification;

[0019] FIG. 6 shows embodiments of a privacy protection-based resource transfer method, according to this specification;

[0020] FIG. 7 shows embodiments of another privacy protection-based resource transfer method, according to this specification;

[0021] FIG. 8 shows embodiments of a resource transfer apparatus, according to this specification;

[0022] FIG. 9 shows embodiments of a privacy protection-based resource transfer apparatus, according to this specification; and

[0023] FIG. 10 shows embodiments of a resource transfer device, according to this specification.

DESCRIPTION OF EMBODIMENTS

[0024] Embodiments of this specification provide a resource transfer method, apparatus, and device.

[0025] To make a person skilled in the art better understand the technical solutions in this specification, the following clearly and comprehensively describes the technical solutions in some embodiments of this specification with reference to the accompanying drawings in some embodiments of this specification. Clearly, the described embodiments are merely some but not all of the embodiments of this specification. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present specification without creative efforts shall fall within the protection scope of the present specification.

[0026] Embodiment 1: As shown in FIG. 1, embodiments of this specification provide a resource transfer method. The method can be performed by a terminal device. The terminal device can be a mobile terminal device such as a mobile phone or a tablet

computer, or can be a device such as a personal computer or a notebook computer, or can be a wearable device such as a watch or a band having an application for performing resource transfer processing, or can be an Internet of Things device having an application for performing resource transfer processing, specifically for example, an in-vehicle device or a smart home device having an application for performing resource transfer processing. The method can specifically include the following steps: Step S102. Obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user.

[0027] The target user can be any user, and can be specifically an owner of a current terminal device, or can be only a user of a current terminal device. The target application can be any application. In embodiments of this specification, the target application can be an application that provides a user with a service related to resource transfer. For example, the target application can be an application corresponding to a certain financial service, or can be an application corresponding to a certain instant messaging service. This can be specifically set based on an actual situation. The resource transfer request can be information for requesting to transfer possession of a specific quantity of resources in a certain account to another account, and the resource transfer request can be embodied in a plurality of different ways. For example, the resource transfer request can be a payment request, an equivalent exchange request, etc. The verification information can be information used to verify current resource transfer. The verification information can be implemented in a plurality of different ways. For example, the verification information can be a verification password, a password, or biometric feature information for resource transfer. The biometric feature information can include one or more of facial feature information, fingerprint feature information, palmprint feature information, iris feature information, heart rate feature information, and voiceprint feature information, specifically for example, a payment password used by the user for payment or facial feature information used for facial recognition-based payment. The identity feature information can be related information used to prove an identity of the target user, for example, facial feature information of the target user, fingerprint feature information of the target user, or identity document information of the target user. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification.

[0028] In implementation, with the continuous development of Internet and terminal technologies, people are increasingly dependent on terminal devices in their work and life. People use the terminal device to store important personal information, and can use the terminal device to process various important services (such as a financial service or an instant messaging service). If the terminal device is lost or stolen, problems are caused to the user. Currently, applications of some important services often verifies a predetermined corresponding password, fingerprint feature information, facial feature information, etc. to verify validity of initiating a current service. However, if information such as the predetermined payment password is leaked, it poses a significant security threat to resources (such as assets) of the user. That is, when the user's terminal device and the information such as the predetermined payment password are obtained by a thief, the thief can steal resources in an account of the user, for example, can perform operations such as transfer, malicious consumption, and money laundering on the resources in the account of the user. As a result, when the terminal device is lost or stolen, the user is exposed to a risk such as theft of huge data and financial assets. Therefore, a solution to a problem that resources of a user are stolen when information such as a terminal device of the user is lost and predetermined verification information is also stolen needs to be provided. The embodiments of this specification provide an implementable technical solution that can specifically include the following content: The user (that is, the target user) can be pre-registered with a transaction platform, a financial service platform, an instant messaging service platform, etc. In practice, the user may not need to be pre-registered with the above-mentioned platform. In addition, the user can perform, in advance on the transaction platform, processing such as binding on a resource account that needs to be used. An application (that is, the target application) that provides a corresponding service can be set on the above-mentioned platform. A resource transfer trigger mechanism can be set in the target application. The trigger mechanism can be implemented in a plurality of different ways, for example, can be implemented by using a predetermined hyperlink, a button, etc. This can be specifically set based on an actual situation. When the target user needs to execute a certain service that needs resource transfer, the target user can start the target application installed in the terminal device, and can find a trigger method of the service in the target application. Then, the target user can trigger execution of the service by using the trigger method, specifically for example, the target user can find a trigger button for transfer in the target application, and then the target user can click the

trigger button, so that the terminal device can perform corresponding processing based on a processing process of the service.

[0029] The terminal device can obtain related data of the service, and can load the data into a page of the target application. As shown in FIG. 2, the page can be a resource transfer request page. The page can include an input box of verification information for performing resource transfer processing. The target user can input, in the input box, verification information (such as a payment password or facial feature information) for performing resource transfer processing. After the input is completed, the terminal device can obtain the verification information input by the target user, and can obtain other related information (such as currently logged-in account information, device information of the terminal device, and an IP address). A resource transfer request can be generated based on the previously obtained information. Then, the resource transfer request can be output to an output port of the terminal device by using the target application. The terminal device can obtain the resource transfer request.

[0030] For example, when the user needs to perform a certain transaction, the user can start the target application to log in to the transaction platform, and can find related information of the transaction in the transaction platform, for example, related information of a transaction object (such as a name and a quantity of the transaction object) and a transaction time. Then, the user can select the related information of the transaction by using the corresponding target application. After selection is completed, the target application can provide a verification information input page. The target user can input verification information. After the input is completed, the target application can generate a resource transfer request based on the related information and the verification information, and can submit the resource transfer request to the terminal device. The terminal device can obtain the resource transfer request.

[0031] Step S104. Verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule by using the target application, and determine, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user.

[0032] The device management rule can be a rule used to verify an identity of a current user of the terminal device. The device management rule can be implemented in a plurality of different ways. This be specifically set based on an actual situation.

[0033] In implementation, to avoid the following case where another person may steal personal information of the user in the terminal device or change registration information of the terminal device after the terminal device of the user is lost or stolen, a device account registration mechanism can be predetermined. Device account registration can be performed by binding the identity feature information of the user of the terminal device with the device information of the terminal device. That is, the terminal device sends an account registration request of the terminal device to a server, where the account registration request includes the identity feature information of the target user that the terminal device belongs to and the device information of the terminal device. Then, the server performs identity verification on the current user. If the identity verification succeeds, the server performs device account registration processing on the terminal device based on the identity feature information and the device information to obtain device account registration information. Then, the server can perform binding processing on the identity feature information and the device information to obtain bound information, store the device account registration information and the bound information, and adjust a state of the terminal device to a registered state. As such, the terminal device can also store the state (that is, the registered state or the unregistered state) of the terminal device and the identity feature information of the user in the above-mentioned registration process.

[0034] After obtaining the resource transfer request, the terminal device can obtain, by using the target application, predetermined verification information for performing resource transfer (for example, the target application can obtain, from a server corresponding to the target application, the predetermined verification information for performing resource transfer) to verify the above-mentioned verification information (for example, determine, through comparison, whether the predetermined verification information for performing resource transfer is the same as the above-mentioned verification information; and if yes, the verification succeeds; otherwise, the verification fails). The device management rule can be predetermined in the terminal device. If the verification succeeds, the local device management rule is invoked by using the target application, and it is determined, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0035] Step S106. Send the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the

identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0036] In implementation, if the identity feature information of the target user matches the identity feature information of the pre-registered user, it is determined that the target user is a user who performs device account registration in advance. In this case, the resource transfer request can be sent to the first server corresponding to the target application, and the first server can perform resource transfer processing based on the resource transfer request.

[0037] The embodiments of this specification provide a resource transfer method, where a resource transfer request triggered by a target user by using a target application is obtained, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; then, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule is invoked by using the target application, and it is determined, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0038] Embodiment 2: As shown in FIG. 3, embodiments of this specification provide a resource transfer method. The method can be performed by a terminal device. The terminal device can be a mobile terminal device such as a mobile phone or a tablet

computer, or can be a device such as a personal computer or a notebook computer, or can be a wearable device such as a watch or a band having an application for performing resource transfer processing, or can be an Internet of Things device having an application for performing resource transfer processing, specifically for example, an in-vehicle device or a smart home device having an application for performing resource transfer processing. The method can specifically include the following steps: Step S302. Obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user.

[0039] The identity feature information can include one or more of biological feature information of the target user, information about a predetermined document of the target user, and a predetermined user key of the target user. The biological feature information of the target user can include one or more of facial feature information, fingerprint feature information, palmprint feature information, iris feature information, heart rate feature information, and voiceprint feature information of the target user. The predetermined document can be a document that can prove an identity of the target user, for example, an identity document, a social security card, and a passport. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification. The predetermined user password can be a password that is predetermined for the target user and that can be used to verify an identity of the target user. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification. The identity feature information can include one or more pieces of the above-mentioned information, and can further include a plurality of types of information. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification.

[0040] Step S304. Verify the verification information by using the target application.

[0041] In practice, the resource transfer request can include the verification information used to perform resource transfer processing and the identity feature information of the target user, and can further include a quantity of resources that resource transfer is to be performed on, specifically for example, a payment amount. Based on this, processing can be further performed in the following method. For details, references can be made to processing in the following steps S306 and S308.

[0042] Step S306. If the verification succeeds, and the quantity of resources that resource transfer is to be performed on satisfies a predetermined verification condition, obtain the identity feature information of the target user and device information of a current device, and obtain identity feature information of a pre-registered user corresponding to the device information from pre-stored device account registration information.

[0043] The predetermined verification condition can be a predetermined condition used to trigger identity verification. For example, the predetermined verification condition can be that the quantity of resources that resource transfer is to be performed on exceeds a predetermined threshold. Specifically for example, the predetermined verification condition can be that a payment amount exceeds 500 RMB. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification. The device information can include one or more of a device identifier of the terminal device, a predetermined device key of the terminal device, and device feature information of the terminal device. The device identifier can be a name, code, etc. of the terminal device. The predetermined device key can be a device key that is predetermined. This can be specifically set based on an actual situation. The device feature information can be a MAC address, an IMEI number, etc. of the terminal device. This can be specifically set based on an actual situation. The device account registration information can be information obtained by a second server after performing the following steps: when the second server receives an account registration request that is of a terminal device corresponding to the device information and that is sent by the terminal device, and detects, based on device information included in the account registration request, that the terminal device is in an unregistered state, the second server verifies an identity of a registered user of the terminal device based on identity feature information included in the account registration request, and performs, based on the identity feature information and the device information, device account registration processing on the terminal device when the verification succeeds.

[0044] In implementation, as shown in FIG. 4, the second server receives an account registration request of a terminal device sent by the terminal device, where the account registration request includes identity feature information of a user that the terminal device belongs to and device information of the terminal device. If the second server detects, based on the device information, that the terminal device is in a

registered state, the second server cancels device account registration processing corresponding to the account registration request. If the second server detects, based on the device information, that the terminal device is in an unregistered state, the second server sends an identity verification request to an identity verification server, where the identity verification request includes the identity feature information; and receives a verification result that is of the identity feature information and that is sent by the identity verification server, where the verification result is obtained by the identity verification server by matching locally stored reference identity feature information of a target user with the identity feature information. The identity verification server can be configured to perform identity verification on the user. The second server determines whether the identity feature information matches the reference identity feature information, to perform identity verification on the user. When the verification succeeds, the second server performs device account registration processing on the terminal device based on the identity feature information and the device information to obtain device account registration information. The second server performs binding processing on the identity feature information and the device information to obtain bound information, stores the device account registration information and the bound information, and adjusts a state of the terminal device to a registered state, so that the terminal device can also store the state information of the terminal device, and the identity feature information of the user and the device account registration information during registration.

[0045] After the above-mentioned processing, the device account registration information of the terminal device can be set in the second server, to ensure that when the terminal device of the user is lost or stolen, the black industry cannot tamper with or erase the device account registration information of the terminal device through offline flashing, damage, vulnerabilities, etc. Therefore, a risk such as theft of huge data and financial assets of the user can be avoided, and processing such as identity registration, deregistration, and recognition management can be implemented on a trusted device owner of the terminal device.

[0046] If the verification succeeds, a quantity of resources that resource transfer is to be performed on is be obtained. Then, the quantity of resources can be matched with the predetermined verification condition. If the quantity of resources that resource transfer is to be performed on satisfies the predetermined verification condition, the identity feature information of the target user and the device information of the current

terminal device can be obtained, and the identity feature information of the pre-registered user corresponding to the device information is obtained from the pre-stored device account registration information.

[0047] Step S308. Invoke a local device management rule by using the target application, and determine, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0048] For specific processing of the above-mentioned step S308, references can be made to related content in Embodiment 1. Details are omitted here for simplicity.

[0049] The above-mentioned step S308 can have various specific processing methods. In addition to being implemented in the method provided in the above-mentioned Embodiment 1, step S308 can be implemented in a plurality of methods. The following further provides an optional processing method that can specifically include processing in the following step A2 and step A4.

[0050] Step A2. Obtain the identity feature information of the target user and device information of a current device, obtain, from device account registration information stored in a second server, first device account registration information that includes the device information, and obtain identity feature information of a pre-registered user corresponding to the device information from the first device account registration information.

[0051] In implementation, to reduce a data storage pressure of the terminal device, the device account registration information can be stored in the second server. As such, after obtaining the identity feature information of the target user and the device information of the current device, the terminal device can send a data request to the second server, where the data request can include the device information. After receiving the data request, the second server can extract the device information from the data request. Then, the second server can obtain, from the pre-stored device account registration information, the first device account registration information that includes the device information, and can send the first device account registration information to the terminal device. The terminal device can extract the identity feature information of the pre-registered user corresponding to the device information from the first device account registration information.

[0052] Step A4. Determine, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0053] Step S310. If the identity feature information of the target user matches the identity feature information of the pre-registered user, verify the verification information; and if the verification succeeds, send the resource transfer request to a first server corresponding to the target application.

[0054] Step S312. If the identity feature information of the target user does not match the identity feature information of the pre-registered user, send a notification message indicating an identity verification abnormality to a third server, to trigger the third server to determine whether to continue to perform resource transfer processing corresponding to the resource transfer request.

[0055] In implementation, if the identity feature information of the target user does not match the identity feature information of the pre-registered user, it can be determined that the target user is not a registered user of the terminal device. In this case, as shown in FIG. 5, a notification message indicating an identity verification abnormality can be reported to the third server, to notify a resource transfer management party that an abnormal behavior is suspected of occurring on a current terminal device, for example, the current terminal device is stolen. A risk prevention and control policy can be set in the third server. After receiving the notification message, the third server can obtain related data in a current resource transfer process, and can analyze the obtained related data by using the risk prevention and control policy, to determine whether to allow the target user to continue to perform resource transfer processing corresponding to the resource transfer request.

[0056] Step S314. If a notification message that is sent by the third server and that indicates to perform resource transfer processing corresponding to the resource transfer request is received, send the resource transfer request to a first server, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0057] The embodiments of this specification provide a resource transfer method, where a resource transfer request triggered by a target user by using a target application is obtained, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; then, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule is invoked by using the target

application, and it is determined, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0058] In addition, a trusted device owner management mechanism added to the terminal device allows to determine, through comparison between identity feature information of a current operation user and identity feature information of a registered user of the terminal device, whether a current operation is the registered user of the terminal device. Therefore, resources (such as financial assets) of the user can be prevented from being maliciously stolen by a relative or a thief. In addition, a processing process of verifying the identity feature information can be implemented at a terminal system layer, and the application does not obtain privacy data related to any identity feature of the user, to protect security of privacy information of the user.

[0059] Embodiment 3: As shown in FIG. 6, embodiments of this specification provide a privacy protection-based resource transfer method. The method can be performed by a terminal device. A trusted execution environment (TEE) can be set in the terminal device. The trusted execution environment can be implemented by using a program written in a predetermined programming language (that is, can be implemented in a form of software), or can be implemented in a form of software and hardware. The terminal device can be a mobile terminal device such as a mobile phone or a tablet computer, or can be a device such as a personal computer or a notebook

computer, or can be a wearable device such as a watch or a band having an application for performing resource transfer processing, or can be an Internet of Things device having an application for performing resource transfer processing, specifically for example, an in-vehicle device or a smart home device having an application for performing resource transfer processing. The method can specifically include the following steps: Step S602. Obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user.

[0060] The identity feature can be related information used to prove an identity of the target user, for example, a facial feature of the target user, a fingerprint feature of the target user, or an identity document feature of the target user. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification. The privacy data can include just the information used to represent the identity feature of the target user, or can also include other related information in addition to the information used to represent the identity feature of the target user, for example, geographical location information, an account number, and a password of the target user. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification.

[0061] Step S604. Verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule in the TEE by using the target application, and determine, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user.

[0062] The privacy data of the user can be related information that is obtained after a corresponding terminal device is pre-registered, that is bound with device information of the terminal device, and that is used to represent the identity of the user. In practice, the privacy data of the user can include other related information in addition to the information used to represent the identity feature of the target user, for example, geographical location information, an account number, and a password of the target user. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification. The TEE can be implemented by using a program written in a predetermined programming language (that is, can be

implemented in a form of software), or can be implemented in a form of software and hardware. The trusted execution environment (TEE) can be a data processing environment that is secure and isolated from another environment. To be specific, processing performed in the trusted execution environment and data generated in a data processing process cannot be accessed by another execution environment or an application outside the executable environment. The trusted execution environment (TEE) can be implemented by creating a small operating system that can run independently in a trusted zone (for example, TrustZone), and the TEE can directly provide a service through a system call (for example, direct processing by a TrustZone kernel). The terminal device can include a rich execution environment (REE) and a TEE. An operating system, such as an Android operating system, an IOS operating system, a Windows operating system, or a Linux operating system, installed on the terminal device can be run in the REE. The REE is characterized by robust functionality, openness, and good scalability, and can provide an upper-layer application with all functions of the terminal device, such as a camera function and a touch function. However, many security risks exist in the REE. For example, the operating system can obtain all data of a certain application, but it is difficult to verify whether the operating system or the application is tampered with. If the operating system or the application is tampered with, user information has a large security hazard. Therefore, processing needs to be performed in the TEE of the terminal device. The TEE has its own execution space. In other words, one operating system also exists in the TEE. The TEE has a higher security level than the REE. Software and hardware resources in the terminal device that are accessible by the TEE are separated from the REE, but the TEE can directly obtain information in the REE, and the REE cannot obtain information in the TEE. The TEE can perform processing such as verification by using a provided interface, to ensure that user information (such as payment information and user privacy information) is not tampered with, no password is hijacked, and information such as a fingerprint feature or a facial feature is not stolen.

[0063] In implementation, the device management rule can be predetermined in the TEE, to prevent the device management rule from being tampered with. The verification information is verified by using the target application. If the verification succeeds, the device management rule in the local TEE is invoked by using the target application. As such, the target application can be prevented from directly operating the privacy data of the user, thereby protecting security of the privacy data of the user. Then,

in the executable environment (TEE), the device management rule can be used to determine whether the identity feature information of the target user matches the identity feature information of the pre-registered user, so that the privacy data are processed in the trusted execution environment (TEE), the privacy data can be protected from being obtained by the target application or another application, and the privacy data can be prevented from being leaked.

[0064] Step S606. Send the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0065] The embodiments of this specification provide a privacy protection-based resource transfer method, applied to a terminal device. A trusted execution environment (TEE) is set in the terminal device, where when a resource transfer request (the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user) triggered by a target user by using a target application is obtained, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule in the TEE is invoked by using the target application, and it is determined, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0066] Embodiment 4: As shown in FIG. 7, embodiments of this specification provide a privacy protection-based resource transfer method. The method can be performed by a terminal device. A trusted execution environment (TEE) can be set in the terminal device. The trusted execution environment can be implemented by using a program written in a predetermined programming language (that is, can be implemented in a form of software), or can be implemented in a form of software and hardware. The terminal device can be a mobile terminal device such as a mobile phone or a tablet computer, or can be a device such as a personal computer or a notebook computer, or can be a wearable device such as a watch or a band having an application for performing resource transfer processing, or can be an Internet of Things device having an application for performing resource transfer processing, specifically for example, an in-vehicle device or a smart home device having an application for performing resource transfer processing. The method can specifically include the following steps: Step S702. Obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user.

[0067] The identity feature can include one or more of a biological feature of the target user, a predetermined document feature of the target user, and a predetermined user key of the target user. The biological feature of the target user can include one or more of a facial feature, a fingerprint feature, a palmprint feature, an iris feature, a heart rate feature, and a voiceprint feature of the target user. The predetermined document can be a document that can prove an identity of the target user, for example, an identity document, a social security card, and a passport. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification. The predetermined user password can be a password that is predetermined for the target user and that can be used to verify an identity of the target user. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification. The identity feature can include one or more pieces of the above-mentioned information, and can further include a plurality of types of information. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification.

[0068] Step S704. Verify the verification information by using the target application.

[0069] In practice, the resource transfer request can include the verification information used to perform resource transfer processing and the identity feature information of the target user, and can further include a quantity of resources that resource transfer is to be performed on, specifically for example, a payment amount. Based on this, processing can be further performed in the following method. For details, references can be made to processing in the following steps S706 and S708.

[0070] Step S706. If the verification succeeds, and the quantity of resources that resource transfer is to be performed on satisfies a predetermined verification condition, invoke a local device management rule in the TEE by using the target application, transmit the privacy data of the target user and device information of a current device to the TEE, and obtain, in the TEE, privacy data of a pre-registered user corresponding to the device information from pre-stored device account registration information.

[0071] The device account registration information can be stored in the TEE of the terminal device, or can be pre-stored in another trusted device (for example, in a specified server (references can be made to the above-mentioned related content of the second server, and details are omitted here for simplicity) or in a blockchain system). In this case, storage address information of the device account registration information can be obtained, and the storage address information can be set in the TEE of the terminal device. When the device account registration information needs to be used, the device account registration information can be obtained based on the storage address information. In addition, to protect security of a data transmission process, a trusted application used to transmit data in resource transfer can be predetermined, the privacy data of the target user and the device information of the current device can be obtained by using the trusted application, and then the privacy data of the target user and the device information of the current device can be transmitted to the TEE by using the trusted application.

[0072] In practice, to ensure data transmission security, data to be transmitted can be encrypted, and then decrypted in the TEE. Based on this, the above-mentioned processing of transmitting the privacy data of the target user and device information of a current device to the TEE can include the following content: performing encryption processing on the privacy data of the target user and the device information of the current device, and transmitting the encrypted privacy data of the target user and the

encrypted device information of the current device to the TEE. Then, in the TEE, decryption processing can be performed on the encrypted privacy data of the target user and the encrypted device information of the current device to obtain the decrypted privacy data of the target user and the decrypted device information of the current device.

[0073] A plurality of encryption algorithms can be used for performing encryption processing, for example, can include a symmetric encryption algorithm or an asymmetric encryption algorithm. There can also be a plurality of symmetric encryption algorithms and a plurality of asymmetric encryption algorithms. This can be specifically set based on an actual situation. No limitation is imposed in the embodiments of this specification.

[0074] Step S708. Determine, in the TEE by using the device management rule, whether the privacy data of the target user match the privacy data of the pre-registered user.

[0075] For specific processing of step S708, references can be made to related content in the above-mentioned embodiments. Details are omitted here for simplicity.

[0076] Step S710. If the privacy data of the target user match the privacy data of the pre-registered user, verify the verification information; and if the verification succeeds, send the resource transfer request to a first server corresponding to the target application.

[0077] Step S712. If the privacy data of the target user do not match the privacy data of the pre-registered user, send a notification message indicating an identity verification abnormality to a third server, to trigger the third server to determine whether to continue to perform resource transfer processing corresponding to the resource transfer request.

[0078] Step S714. If a notification message that is sent by the third server and that indicates to perform resource transfer processing corresponding to the resource transfer request is received, send the resource transfer request to a first server, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0079] In practice, the device account registration information and/or the device management rule stored in the TEE can be further updated. For details, references can be made to processing in the following steps S716 and S718.

[0080] Step S716. Receive an update request for target data in the TEE, where the update request includes data to be updated, the data to be updated are ciphertext, and

the target data include the device account registration information and/or the device management rule.

[0081] Step S718. Transmit the data to be updated to the TEE, decrypt the data to be updated in the TEE, and update the target data based on the decrypted data to be updated.

[0082] The embodiments of this specification provide a privacy protection-based resource transfer method, applied to a terminal device. A trusted execution environment (TEE) is set in the terminal device, where when a resource transfer request (the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user) triggered by a target user by using a target application is obtained, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule in the TEE is invoked by using the target application, and it is determined, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0083] In addition, a trusted device owner management mechanism added to the terminal device allows to determine, through comparison between identity feature information of a current operation user and identity feature information of a registered user of the terminal device, whether a current operation is the registered user of the terminal device. Therefore, resources (such as financial assets) of the user can be

prevented from being maliciously stolen by a relative or a thief. In addition, a processing process of verifying the identity feature information can be implemented at a terminal system layer, and the application does not obtain privacy data related to any identity feature of the user, to protect security of privacy information of the user.

[0084] Embodiment 5: The resource transfer method provided in the embodiments of this specification has been described above. Based on the same idea, embodiments of this specification further provide a resource transfer apparatus, as shown in FIG. 8.

[0085] The resource transfer apparatus includes a request acquisition module 801, a verification module 802, and a request forwarding module 803, where the request acquisition module 801 is configured to obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; the verification module 802 is configured to verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule by using the target application, and determine, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and the request forwarding module 803 is configured to send the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0086] In the embodiments of this specification, the resource transfer request includes a quantity of resources that resource transfer is to be performed on; and the verification module 802 is configured to: if the verification succeeds, and the quantity of resources that resource transfer is to be performed on satisfies a predetermined verification condition, invoke the local device management rule by using the target application, and determine, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0087] In the embodiments of this specification, the request forwarding module 803 is configured to: if the identity feature information of the target user matches the identity feature information of the pre-registered user, verify the verification

information; and if the verification succeeds, send the resource transfer request to the first server corresponding to the target application.

[0088] In the embodiments of this specification, the verification module 802 includes: a first information acquisition unit, configured to obtain the identity feature information of the target user and device information of a current device, and obtain identity feature information of a pre-registered user corresponding to the device information from pre-stored device account registration information; and a first verification unit, configured to determine, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0089] In the embodiments of this specification, the verification module 802 includes: a second information acquisition unit, configured to obtain the identity feature information of the target user and device information of a current device, obtain, from device account registration information stored in a second server, first device account registration information that includes the device information, and obtain identity feature information of a pre-registered user corresponding to the device information from the first device account registration information; and a second verification unit, configured to determine, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0090] In the embodiments of this specification, the device account registration information is information obtained by the second server after performing the following steps: when the second server receives an account registration request that is of a terminal device corresponding to the device information and that is sent by the terminal device, and detects, based on device information included in the account registration request, that the terminal device is in an unregistered state, the second server verifies an identity of a registered user of the terminal device based on identity feature information included in the account registration request, and performs, based on the identity feature information and the device information, device account registration processing on the terminal device when the verification succeeds.

[0091] In the embodiments of this specification, the identity feature information includes one or more of biometric feature information, information about a predetermined document, and a predetermined user key, and the device information

includes one or more of a device identifier, a predetermined device key, and device feature information.

[0092] In the embodiments of this specification, the biometric feature information includes one or more of facial feature information, fingerprint feature information, palmprint feature information, iris feature information, heart rate feature information, and voiceprint feature information.

[0093] In the embodiments of this specification, the apparatus further includes: a notification module, configured to: if the identity feature information of the target user does not match the identity feature information of the pre-registered user, send a notification message indicating an identity verification abnormality to a third server, to trigger the third server to determine whether to continue to perform resource transfer processing corresponding to the resource transfer request; and a sending module, configured to: if a notification message that is sent by the third server and that indicates to perform resource transfer processing corresponding to the resource transfer request is received, send the resource transfer request to the first server, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0094] The embodiments of this specification provide a resource transfer apparatus, where a resource transfer request triggered by a target user by using a target application is obtained, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; then, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule is invoked by using the target application, and it is determined, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource

transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0095] In addition, a trusted device owner management mechanism added to the terminal device allows to determine, through comparison between identity feature information of a current operation user and identity feature information of a registered user of the terminal device, whether a current operation is the registered user of the terminal device. Therefore, resources (such as financial assets) of the user can be prevented from being maliciously stolen by a relative or a thief. In addition, a processing process of verifying the identity feature information can be implemented at a terminal system layer, and the application does not obtain privacy data related to any identity feature of the user, to protect security of privacy information of the user.

[0096] Embodiment 6: Based on the same idea, embodiments of this specification further provide a privacy protection-based resource transfer apparatus, where a trusted execution environment (TEE) is set in the apparatus, as shown in FIG. 9.

[0097] The privacy protection-based resource transfer apparatus includes a resource transfer request module 901, a privacy processing module 902, and a resource transfer processing module 903, where the resource transfer request module 901 is configured to obtain a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user; the privacy processing module 902 is configured to verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule in the TEE by using the target application, and determine, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and the resource transfer processing module 903 is configured to send the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0098] In the embodiments of this specification, the resource transfer request includes a quantity of resources that resource transfer is to be performed on; and the privacy processing module 902 is configured to transmit the privacy data of the target user and device information of a current device to the TEE, and obtain, in the TEE, privacy data of a pre-registered user corresponding to the device information from pre-stored device account registration information; and determine, in the TEE by using the device management rule, whether the privacy data of the target user match the privacy data of the pre-registered user.

[0099] In the embodiments of this specification, the resource transfer processing module 903 is configured to: if the privacy data of the target user match the privacy data of the pre-registered user, verify the verification information; and if the verification succeeds, send the resource transfer request to the first server corresponding to the target application.

[0100] In the embodiments of this specification, the apparatus further includes: an information acquisition module, configured to obtain the identity feature information of the target user and device information of a current device, obtain, from device account registration information stored in a second server, first device account registration information that includes the device information, and obtain identity feature information of a pre-registered user corresponding to the device information from the first device account registration information.

[0101] In the embodiments of this specification, the device account registration information is information obtained by the second server after performing the following steps: when the second server receives an account registration request that is of a terminal device corresponding to the device information and that is sent by the terminal device, and detects, based on device information comprised in the account registration request, that the terminal device is in an unregistered state, the second server verifies an identity of a registered user of the terminal device based on identity feature information comprised in the account registration request, and performs, based on the identity feature information and the device information, device account registration processing on the terminal device when the verification succeeds.

[0102] In the embodiments of this specification, the identity feature includes one or more of a biometric feature, a predetermined document feature, and a predetermined user key, and the device information includes one or more of a device identifier, a predetermined device key, and device feature information.

[0103] In the embodiments of this specification, the biometric feature includes one or more of a facial feature, a fingerprint feature, a palmprint feature, an iris feature, a heart rate feature, and a voiceprint feature.

[0104] In the embodiments of this specification, the apparatus further includes: a notification module, configured to: if the privacy data of the target user do not match the privacy data of the pre-registered user, send a notification message indicating an identity verification abnormality to a third server, to trigger the third server to determine whether to continue to perform resource transfer processing corresponding to the resource transfer request; and a sending module, configured to: if a notification message that is sent by the third server and that indicates to perform resource transfer processing corresponding to the resource transfer request is received, send the resource transfer request to the first server, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0105] In the embodiments of this specification, the privacy processing module 902 is configured to perform encryption processing on the privacy data of the target user and the device information of the current device, and transmit the encrypted privacy data of the target user and the encrypted device information of the current device to the TEE; and the apparatus further includes a decryption module, configured to perform, in the TEE, decryption processing on the encrypted privacy data of the target user and the encrypted device information of the current device to obtain the decrypted privacy data of the target user and the decrypted device information of the current device.

[0106] In the embodiments of this specification, the apparatus further includes: an update request module, configured to receive an update request for target data in the TEE, where the update request includes data to be updated, the data to be updated are ciphertext, and the target data include the device account registration information and/or the device management rule; and an update module, configured to transmit the data to be updated to the TEE, decrypt the data to be updated in the TEE, and update the target data based on the decrypted data to be updated.

[0107] The embodiments of this specification provide a privacy protection-based resource transfer apparatus. A trusted execution environment (TEE) is set in the apparatus, where when a resource transfer request (the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user) triggered by a target user by using a

target application is obtained, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule in the TEE is invoked by using the target application, and it is determined, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0108] In addition, a trusted device owner management mechanism added to the terminal device allows to determine, through comparison between identity feature information of a current operation user and identity feature information of a registered user of the terminal device, whether a current operation is the registered user of the terminal device. Therefore, resources (such as financial assets) of the user can be prevented from being maliciously stolen by a relative or a thief. In addition, a processing process of verifying the identity feature information can be implemented at a terminal system layer, and the application does not obtain privacy data related to any identity feature of the user, to protect security of privacy information of the user.

[0109] Embodiment 7: The privacy protection-based resource transfer apparatus provided in the embodiments of this specification has been described above. Based on the same idea, embodiments of this specification further provide a resource transfer device, as shown in FIG. 10.

[0110] The resource transfer device can be the terminal device provided in the above-mentioned embodiments, and a trusted execution environment (TEE), etc. can be set in the terminal device.

[0111] The resource transfer device can vary greatly due to a configuration or performance difference, and can include one or more processors 1001 and a memory 1002. The memory 1002 can store one or more storage applications or data. The memory 1002 can be temporary storage or persistent storage. The application stored in the memory 1002 can include one or more modules (not shown in the figure), and each module can include a series of computer-executable instructions for the resource transfer device. Still further, the processor 1001 can be configured to communicate with the memory 1002 to execute a series of computer-executable instructions in the memory 1002 on the resource transfer device. The resource transfer device can further include one or more power supplies 1003, one or more wired or wireless network interfaces 1004, one or more input/output interfaces 1005, one or more keyboards 1006, etc.

[0112] Specifically, in the embodiments, the resource transfer device includes a memory and one or more programs. The one or more programs are stored in the memory. The one or more programs can include one or more modules. Each module can include a series of computer-executable instructions for the resource transfer device. One or more processors are configured to execute computer-executable instructions that are included in the one or more programs and that are used to perform the following: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0113] In the embodiments of this specification, the resource transfer request includes a quantity of resources that resource transfer is to be performed on; and the invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a

pre-registered user includes: if the verification succeeds, and the quantity of resources that resource transfer is to be performed on satisfies a predetermined verification condition, invoking the local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0114] In the embodiments of this specification, the sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user includes: if the identity feature information of the target user matches the identity feature information of the pre-registered user, verifying the verification information; and if the verification succeeds, sending the resource transfer request to the first server corresponding to the target application.

[0115] In the embodiments of this specification, the determining, by using the device management rule, whether the identity feature of the target user matches an identity feature of a pre-registered user includes: obtaining the identity feature information of the target user and device information of a current device, and obtaining identity feature information of a pre-registered user corresponding to the device information from pre-stored device account registration information; and determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0116] In the embodiments of this specification, the determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user includes: obtaining the identity feature information of the target user and device information of a current device, obtaining, from device account registration information stored in a second server, first device account registration information that includes the device information, and obtaining identity feature information of a pre-registered user corresponding to the device information from the first device account registration information; and determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0117] In the embodiments of this specification, the device account registration information is information obtained by the second server after performing the following

steps: when the second server receives an account registration request that is of a terminal device corresponding to the device information and that is sent by the terminal device, and detects, based on device information comprised in the account registration request, that the terminal device is in an unregistered state, the second server verifies an identity of a registered user of the terminal device based on identity feature information comprised in the account registration request, and performs, based on the identity feature information and the device information, device account registration processing on the terminal device when the verification succeeds.

[0118] In the embodiments of this specification, the identity feature information includes one or more of biometric feature information, information about a predetermined document, and a predetermined user key, and the device information includes one or more of a device identifier, a predetermined device key, and device feature information.

[0119] In the embodiments of this specification, the biometric feature information includes one or more of facial feature information, fingerprint feature information, palmprint feature information, iris feature information, heart rate feature information, and voiceprint feature information.

[0120] In the embodiments of this specification, the following operations are further included: if the identity feature information of the target user does not match the identity feature information of the pre-registered user, sending a notification message indicating an identity verification abnormality to a third server, to trigger the third server to determine whether to continue to perform resource transfer processing corresponding to the resource transfer request; and if a notification message that is sent by the third server and that indicates to perform resource transfer processing corresponding to the resource transfer request is received, sending the resource transfer request to the first server, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0121] In addition, specifically, in the embodiments, the resource transfer device includes a memory and one or more programs. The one or more programs are stored in the memory. The one or more programs can include one or more modules. Each module can include a series of computer-executable instructions for the resource transfer device. One or more processors are configured to execute computer-executable instructions that are included in the one or more programs and that are used to perform the following: obtaining a resource transfer request triggered by a target user by using a target

application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0122] In the embodiments of this specification, the determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user includes: transmitting the privacy data of the target user and device information of a current device to the TEE, and obtaining, in the TEE, privacy data of a pre-registered user corresponding to the device information from pre-stored device account registration information; and determining, in the TEE by using the device management rule, whether the privacy data of the target user match the privacy data of the pre-registered user.

[0123] In the embodiments of this specification, the transmitting the privacy data of the target user and device information of a current device to the TEE includes: performing encryption processing on the privacy data of the target user and the device information of the current device, and transmitting the encrypted privacy data of the target user and the encrypted device information of the current device to the TEE; and the following operations are further included: performing, in the TEE, decryption processing on the encrypted privacy data of the target user and the encrypted device information of the current device to obtain the decrypted privacy data of the target user and the decrypted device information of the current device.

[0124] In the embodiments of this specification, the following operations are further included: receiving an update request for target data in the TEE, where the update request includes data to be updated, the data to be updated are ciphertext, and the target data include the device account registration information and/or the device management rule; and transmitting the data to be updated to the TEE, decrypting the

data to be updated in the TEE, and updating the target data based on the decrypted data to be updated.

[0125] The embodiments of this specification provide a resource transfer device, where a resource transfer request triggered by a target user by using a target application is obtained, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; then, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule is invoked by using the target application, and it is determined, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0126] In addition, a trusted device owner management mechanism added to the terminal device allows to determine, through comparison between identity feature information of a current operation user and identity feature information of a registered user of the terminal device, whether a current operation is the registered user of the terminal device. Therefore, resources (such as financial assets) of the user can be prevented from being maliciously stolen by a relative or a thief. In addition, a processing process of verifying the identity feature information can be implemented at a terminal system layer, and the application does not obtain privacy data related to any identity feature of the user, to protect security of privacy information of the user.

[0127] Embodiment 8: Further, based on the methods shown in FIG. 1 and FIG. 7, one or more embodiments of this specification further provide a storage medium, configured to store computer-executable instruction information. In specific embodiments, the storage medium can be a USB flash drive, an optical disc, a hard disk, etc. When the computer-executable instruction information stored in the storage medium is executed by a processor, the following process can be implemented: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0128] In the embodiments of this specification, the resource transfer request includes a quantity of resources that resource transfer is to be performed on; and the invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user includes: if the verification succeeds, and the quantity of resources that resource transfer is to be performed on satisfies a predetermined verification condition, invoking the local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0129] In the embodiments of this specification, the sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user includes: if the identity feature information of the target user matches the identity feature information of the pre-registered user, verifying the verification

information; and if the verification succeeds, sending the resource transfer request to the first server corresponding to the target application.

[0130] In the embodiments of this specification, the determining, by using the device management rule, whether the identity feature of the target user matches an identity feature of a pre-registered user includes: obtaining the identity feature information of the target user and device information of a current device, and obtaining identity feature information of a pre-registered user corresponding to the device information from pre-stored device account registration information; and determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0131] In the embodiments of this specification, the determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user includes: obtaining the identity feature information of the target user and device information of a current device, obtaining, from device account registration information stored in a second server, first device account registration information that includes the device information, and obtaining identity feature information of a pre-registered user corresponding to the device information from the first device account registration information; and determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

[0132] In the embodiments of this specification, the device account registration information is information obtained by the second server after performing the following steps: when the second server receives an account registration request that is of a terminal device corresponding to the device information and that is sent by the terminal device, and detects, based on device information comprised in the account registration request, that the terminal device is in an unregistered state, the second server verifies an identity of a registered user of the terminal device based on identity feature information comprised in the account registration request, and performs, based on the identity feature information and the device information, device account registration processing on the terminal device when the verification succeeds.

[0133] In the embodiments of this specification, the identity feature information includes one or more of biometric feature information, information about a predetermined document, and a predetermined user key, and the device information

includes one or more of a device identifier, a predetermined device key, and device feature information.

[0134] In the embodiments of this specification, the biometric feature information includes one or more of facial feature information, fingerprint feature information, palmprint feature information, iris feature information, heart rate feature information, and voiceprint feature information.

[0135] In the embodiments of this specification, the following operations are further included: if the identity feature information of the target user does not match the identity feature information of the pre-registered user, sending a notification message indicating an identity verification abnormality to a third server, to trigger the third server to determine whether to continue to perform resource transfer processing corresponding to the resource transfer request; and if a notification message that is sent by the third server and that indicates to perform resource transfer processing corresponding to the resource transfer request is received, sending the resource transfer request to the first server, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0136] In addition, in other specific embodiments, the storage medium can be a USB flash drive, an optical disc, a hard disk, etc. When computer-executable instruction information stored in the storage medium is executed by a processor, the following process can be implemented: obtaining a resource transfer request triggered by a target user by using a target application, where the resource transfer request includes verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data include information used to represent an identity feature of the target user; verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

[0137] In the embodiments of this specification, the determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user includes: transmitting the privacy data of the target

user and device information of a current device to the TEE, and obtaining, in the TEE, privacy data of a pre-registered user corresponding to the device information from pre-stored device account registration information; and determining, in the TEE by using the device management rule, whether the privacy data of the target user match the privacy data of the pre-registered user.

[0138] In the embodiments of this specification, the transmitting the privacy data of the target user and device information of a current device to the TEE includes: performing encryption processing on the privacy data of the target user and the device information of the current device, and transmitting the encrypted privacy data of the target user and the encrypted device information of the current device to the TEE; and the following operations are further included: performing, in the TEE, decryption processing on the encrypted privacy data of the target user and the encrypted device information of the current device to obtain the decrypted privacy data of the target user and the decrypted device information of the current device.

[0139] In the embodiments of this specification, the following operations are further included: receiving an update request for target data in the TEE, where the update request includes data to be updated, the data to be updated are ciphertext, and the target data include the device account registration information and/or the device management rule; and transmitting the data to be updated to the TEE, decrypting the data to be updated in the TEE, and updating the target data based on the decrypted data to be updated.

[0140] The embodiments of this specification provide a storage medium, where a resource transfer request triggered by a target user by using a target application is obtained, where the resource transfer request includes verification information used to perform resource transfer processing and identity feature information of the target user; then, the verification information is verified by using the target application, and if the verification succeeds, a local device management rule is invoked by using the target application, and it is determined, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and the resource transfer request is sent to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request. As such, in the above-mentioned method, a problem that resources of the target

user are stolen when the terminal device of the target user is lost and the verification information (for example, a key (specifically for example, a payment password) for performing resource transfer) for performing resource transfer is also stolen can be alleviated. In addition, privacy information such as the identity feature information of the user is protected, and is not leaked to the target application that triggers resource transfer. Instead, a result of identity feature verification is directly used to perform subsequent resource transfer processing. Therefore, a risk such as theft or stealing of huge data and financial assets of the user can be avoided, and processing such as identity recognition management can be implemented on a trusted device owner of a terminal device.

[0141] In addition, a trusted device owner management mechanism added to the terminal device allows to determine, through comparison between identity feature information of a current operation user and identity feature information of a registered user of the terminal device, whether a current operation is the registered user of the terminal device. Therefore, resources (such as financial assets) of the user can be prevented from being maliciously stolen by a relative or a thief. In addition, a processing process of verifying the identity feature information can be implemented at a terminal system layer, and the application does not obtain privacy data related to any identity feature of the user, to protect security of privacy information of the user.

[0142] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, processes described in the accompanying drawings do not necessarily need a specific order or a sequential order shown to achieve the desired results. In some implementations, multi-tasking and parallel processing are also possible or may be advantageous.

[0143] In the 1990s, whether a technical improvement is a hardware improvement (for example, an improvement to a circuit structure, such as a diode, a transistor, or a switch) or a software improvement (an improvement to a method procedure) can be clearly distinguished. However, as technologies develop, current improvements to many method procedures can be considered as direct improvements to hardware circuit structures. A designer usually programs an improved method procedure into a hardware circuit, to obtain a corresponding hardware circuit structure. Therefore, a method procedure can be improved using a hardware entity module. For example, a

programmable logic device (PLD) (for example, a field programmable gate array (FPGA)) is such an integrated circuit, and a logical function of the programmable logic device is determined by a user through device programming. The designer performs programming to "integrate" a digital system to a PLD without requesting a chip manufacturer to design and produce an application-specific integrated circuit chip. In addition, at present, instead of manually manufacturing an integrated circuit chip, such programming is mostly implemented by using "logic compiler" software. The logic compiler software is similar to a software compiler used to develop and write a program. Original code needs to be written in a particular programming language for compilation. The language is referred to as a hardware description language (HDL). There are many HDLs, such as the Advanced Boolean Expression Language (ABEL), the Altera Hardware Description Language (AHDL), Confluence, the Cornell University Programming Language (CUPL), HDCal, the Java Hardware Description Language (JHDL), Lava, Lola, MyHDL, PALASM, and the Ruby Hardware Description Language (RHDL). The very-high-speed integrated circuit hardware description language (VHDL) and Verilog are most commonly used. A person skilled in the art should also understand that a hardware circuit that implements a logical method procedure can be readily obtained once the method procedure is logically programmed by using the several described hardware description languages and is programmed into an integrated circuit.

[0144] A controller can be implemented by using any appropriate method. For example, the controller can be a microprocessor or a processor, or a computer-readable medium that stores computer-readable program code (such as software or firmware) that can be executed by the microprocessor or the processor, a logic gate, a switch, an application specific integrated circuit (ASIC), a programmable logic controller, or a built-in microprocessor. Examples of the controller include but are not limited to the following microprocessors: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20, and Silicone Labs C8051F320. The memory controller can also be implemented as a part of the control logic of the memory. A person skilled in the art also knows that, in addition to implementing the controller by using the computer readable program code, logic programming can be performed on method steps to allow the controller to implement the same function in forms of the logic gate, the switch, the application-specific integrated circuit, the programmable logic controller, and the built-in microcontroller. Therefore, the controller can be considered as a hardware component,

and an apparatus configured to implement various functions in the controller can also be considered as a structure in the hardware component. Or the apparatus configured to implement various functions can even be considered as both a software module implementing the method and a structure in the hardware component.

[0145] The system, apparatus, module, or unit illustrated in the embodiments can be specifically implemented by using a computer chip or an entity, or can be implemented by using a product having a certain function. A typical implementation device is a computer. Specifically, the computer can be, for example, a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an e-mail device, a game console, a tablet computer, a wearable device, or any combination of these devices.

[0146] For ease of description, the above-mentioned apparatus is described by dividing functions into various units. Certainly, during implementation of one or more embodiments of this specification, the functions of each unit can be implemented in one or more pieces of software and/or hardware.

[0147] A person skilled in the art should understand that some embodiments of this specification can be provided as methods, systems, or computer program products. Therefore, one or more embodiments of this specification can use a form of hardware only embodiments, software only embodiments, or embodiments with a combination of software and hardware. In addition, one or more embodiments of this specification can use a form of a computer program product that is 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.

[0148] Some embodiments of this specification are described with reference to flowcharts and/or block diagrams of the method, the device (system), and the computer program product according to some embodiments of this specification. 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 another programmable fraudulent case serial-parallel device to generate a machine such that the instructions executed by the computer or the processor of the another programmable fraudulent case serial-

parallel device generate an apparatus for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0149] These computer program instructions can be stored in a computer-readable memory that can instruct the computer or the another programmable fraudulent case serial-parallel device to work in a specific way such that the instructions stored in the computer-readable memory generate an artifact that includes an instruction apparatus. The instruction apparatus implements a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0150] These computer program instructions can alternatively be loaded onto the computer or another programmable fraudulent case serial-parallel device such 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 specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0151] In a typical configuration, a computing device includes one or more central processing units (CPU), input/output interfaces, network interfaces, and memories.

[0152] The memory can include a non-persistent memory, a random access memory (RAM), and/or a non-volatile memory in a computer-readable medium, for example, a read-only memory (ROM) or a flash read-only memory (flash RAM). The memory is an example of the computer-readable medium.

[0153] The computer-readable medium includes persistent, non-persistent, movable, and unmovable media that can store information by using any method or technology. The information can be a computer-readable instruction, a data structure, a program module, or other data. Examples of the computer storage medium include but are not limited to a phase change 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 another optical storage, a cassette magnetic tape, a magnetic tape/magnetic disk storage, another magnetic storage device, or any other non-transmission medium. The computer storage medium can be configured to store information that can be accessed by a computing device. Based on the definition in this specification, the

computer-readable medium does not include transitory media such as a modulated data signal and carrier.

[0154] It is worthwhile to further note that, the terms "include", "comprise", or any other variant thereof are intended to cover a non-exclusive inclusion so that a process, a method, a product or a device that includes a list of elements not only includes those elements but also includes other elements that are not expressly listed, or further includes elements inherent to such process, method, product or device. Without more constraints, an element preceded by "includes a …" does not preclude the existence of additional identical elements in the process, method, product or device that includes the element.

[0155] A person skilled in the art should understand that some embodiments of this specification can be provided as methods, systems, or computer program products. Therefore, one or more embodiments of this specification can use a form of hardware only embodiments, software only embodiments, or embodiments with a combination of software and hardware. In addition, one or more embodiments of this specification can use a form of a computer program product that is 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.

[0156] One or more embodiments of this specification can be described in the general context of computer-executable instructions, for example, a program module. Generally, the program module includes a routine, a program, an object, a component, a data structure, etc. executing a specific task or implementing a specific abstract data type. One or more embodiments of this specification can alternatively be practiced in distributed computing environments where tasks are performed by remote processing devices that are connected through a communication network. In the distributed computing environments, the program module can be located in a local and remote computer storage medium including a storage device.

[0157] The embodiments in this specification are described in a progressive way. For same or similar parts of the embodiments, references can be made to the embodiments mutually. Each embodiment focuses on a difference from other embodiments. Particularly, a system embodiment is similar to a method embodiment, and therefore is described briefly. For related parts, references can be made to related descriptions in the method embodiment.

[0158] The above-mentioned descriptions are merely embodiments of this specification, and are not intended to limit this specification. A person skilled in the art can make various changes and variations to this specification. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of this specification shall fall within the scope of the claims in this specification.

CLAIMS

What is claimed is:

1. A resource transfer method, wherein the method comprises:

obtaining a resource transfer request triggered by a target user by using a target application, wherein the resource transfer request comprises verification information used to perform resource transfer processing and identity feature information of the target user;

verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and

sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

2. The method according to claim 1, wherein the resource transfer request comprises a quantity of resources that resource transfer is to be performed on; and

the invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user comprises:

if the verification succeeds, and the quantity of resources that resource transfer is to be performed on satisfies a predetermined verification condition, invoking the local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

3. The method according to claim 1, wherein the sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user comprises:

if the identity feature information of the target user matches the identity feature information of the pre-registered user, verifying the verification information; and if the

verification succeeds, sending the resource transfer request to the first server corresponding to the target application.

4. The method according to claim 1, wherein the determining, by using the device management rule, whether the identity feature of the target user matches an identity feature of a pre-registered user comprises:

obtaining the identity feature information of the target user and device information of a current device, and obtaining identity feature information of a pre-registered user corresponding to the device information from pre-stored device account registration information; and

determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

5. The method according to claim 1, wherein the determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user comprises:

obtaining the identity feature information of the target user and device information of a current device, obtaining, from device account registration information stored in a second server, first device account registration information that comprises the device information, and obtaining identity feature information of a pre-registered user corresponding to the device information from the first device account registration information; and

determining, by using the device management rule, whether the identity feature information of the target user matches the identity feature information of the pre-registered user.

6. The method according to claim 5, wherein the device account registration information is information obtained by the second server after performing the following steps: when the second server receives an account registration request that is of a terminal device corresponding to the device information and that is sent by the terminal device, and detects, based on device information comprised in the account registration request, that the terminal device is in an unregistered state, the second server verifies an identity of a registered user of the terminal device based on identity feature information comprised in the account registration request, and performs, based on the identity feature information and the device information, device account registration processing on the terminal device when the verification succeeds.

7. The method according to any one of claims 4 to 6, wherein the identity feature information comprises one or more of biometric feature information, information about a predetermined document, and a predetermined user key, and the device information comprises one or more of a device identifier, a predetermined device key, and device feature information.

8. The method according to claim 7, wherein the biometric feature information comprises one or more of facial feature information, fingerprint feature information, palmprint feature information, iris feature information, heart rate feature information, and voiceprint feature information.

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

if the identity feature information of the target user does not match the identity feature information of the pre-registered user, sending a notification message indicating an identity verification abnormality to a third server, to trigger the third server to determine whether to continue to perform resource transfer processing corresponding to the resource transfer request; and

if a notification message that is sent by the third server and that indicates to perform resource transfer processing corresponding to the resource transfer request is received, sending the resource transfer request to the first server, to trigger the first server to perform resource transfer processing based on the resource transfer request.

10. A privacy protection-based resource transfer method, applied to a terminal device, wherein a trusted execution environment (TEE) is set in the terminal device, and the method comprises:

obtaining a resource transfer request triggered by a target user by using a target application, wherein the resource transfer request comprises verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data comprise information used to represent an identity feature of the target user;

verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and

sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

11. The method according to claim 10, wherein the determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user comprises:

transmitting the privacy data of the target user and device information of a current device to the TEE, and obtaining, in the TEE, privacy data of a pre-registered user corresponding to the device information from pre-stored device account registration information; and

determining, in the TEE by using the device management rule, whether the privacy data of the target user match the privacy data of the pre-registered user.

12. The method according to claim 11, wherein the transmitting the privacy data of the target user and device information of a current device to the TEE comprises:

performing encryption processing on the privacy data of the target user and the device information of the current device, and transmitting the encrypted privacy data of the target user and the encrypted device information of the current device to the TEE; and

the method further comprises:

performing, in the TEE, decryption processing on the encrypted privacy data of the target user and the encrypted device information of the current device to obtain the decrypted privacy data of the target user and the decrypted device information of the current device.

13. The method according to claim 10, wherein the method further comprises:

receiving an update request for target data in the TEE, wherein the update request comprises data to be updated, the data to be updated are ciphertext, and the target data comprise the device account registration information and/or the device management rule; and

transmitting the data to be updated to the TEE, decrypting the data to be updated in the TEE, and updating the target data based on the decrypted data to be updated.

14. A resource transfer apparatus, wherein the apparatus comprises:

a request acquisition module, configured to obtain a resource transfer request triggered by a target user by using a target application, wherein the resource transfer

request comprises verification information used to perform resource transfer processing and identity feature information of the target user;

a verification module, configured to verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule by using the target application, and determine, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and

a request forwarding module, configured to send the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

15. A privacy protection-based resource transfer apparatus, wherein a trusted execution environment (TEE) is set in the apparatus, and the apparatus comprises:

a resource transfer request module, configured to obtain a resource transfer request triggered by a target user by using a target application, wherein the resource transfer request comprises verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data comprise information used to represent an identity feature of the target user;

a privacy processing module, configured to verify the verification information by using the target application, and invoke, if the verification succeeds, a local device management rule in the TEE by using the target application, and determine, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and

a resource transfer processing module, configured to send the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

16. A resource transfer device, wherein the resource transfer device comprises:

a processor; and

a memory, configured to store computer-executable instructions, wherein when the executable instructions are executed, the processor performs the following steps:

obtaining a resource transfer request triggered by a target user by using a target application, wherein the resource transfer request comprises verification information

used to perform resource transfer processing and identity feature information of the target user;

verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and

sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

17. A privacy protection-based resource transfer device, wherein a trusted execution environment (TEE) is set in the device, and the device comprises:

a processor; and

a memory, configured to store computer-executable instructions, wherein when the executable instructions are executed, the processor performs the following steps:

obtaining a resource transfer request triggered by a target user by using a target application, wherein the resource transfer request comprises verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data comprise information used to represent an identity feature of the target user;

verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and

sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

18. A storage medium, wherein the storage medium is configured to store computer-executable instructions, and when the executable instructions are executed by a processor, the following process is implemented:

obtaining a resource transfer request triggered by a target user by using a target application, wherein the resource transfer request comprises verification information used to perform resource transfer processing and identity feature information of the target user;

verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule by using the target application, and determining, by using the device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user; and

sending the resource transfer request to a first server corresponding to the target application if the identity feature information of the target user matches the identity feature information of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.

19. A storage medium, wherein the storage medium is configured to store computer-executable instructions, and when the executable instructions are executed by a processor, the following process is implemented:

obtaining a resource transfer request triggered by a target user by using a target application, wherein the resource transfer request comprises verification information used to perform resource transfer processing and privacy data of the target user, and the privacy data comprise information used to represent an identity feature of the target user;

verifying the verification information by using the target application, and invoking, if the verification succeeds, a local device management rule in the TEE by using the target application, and determining, in the TEE by using the device management rule, whether the privacy data of the target user match privacy data of a pre-registered user; and

sending the resource transfer request to a first server corresponding to the target application if the privacy data of the target user match the privacy data of the pre-registered user, to trigger the first server to perform resource transfer processing based on the resource transfer request.