CLAIMS

What is claimed is:

1. A resource transfer method, comprising

obtaining, by a terminal device, 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, by the target application, the verification information;

in response to determining that the verification information is verified successfully, obtaining, by the terminal device, device information of a current device, and invoking, by the target application, a local device management rule;

determining, by using the local device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user corresponding to the device information, wherein the identity feature information of the pre-registered user is obtained from pre-stored device account registration information; and

in response to determining that the identity feature information of the target user matches the identity feature information of the pre-registered user corresponding to the device information, sending the resource transfer request to a first server corresponding to the target application, 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 obtaining the device information of the current device and the invoking the local device management rule are performed in response to determining that the verification information is verified successfully and that the quantity of resources that resource transfer is to be performed on satisfies a predetermined verification condition.

3. The method according to claim 1, wherein

obtaining the identity feature information of the pre-registered user corresponding to the device information from the pre-stored device account registration information comprises :

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

4. The method according to claim 3, 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.

5. The method according to any one of claims 1, 3 and 4, 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.

6. The method according to claim 5, 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.

7. 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 corresponding to the device information, 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 corresponding to the target application, to trigger the first server to perform resource transfer processing based on the resource transfer request.

8. 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 local 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.

9. The method according to claim 8, wherein the determining, in the TEE by using the local 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 local device management rule, whether the privacy data of the target user match the privacy data of the pre-registered user.

10. The method according to claim 9, 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.

11. The method according to claim 8, 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 device account registration information and/or the local 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.

12. 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 , in response to determining that the verification information is verified successfully, obtain device information of a current device, invoke a local device management rule by using the target application, and determine, by using the local device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user corresponding to the device information, wherein the identity feature information of the pre-registered user is obtained from pre-stored device account registration information; and

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

13. 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 local 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.

14. 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, by the target application, the verification information ,and in response to determining that the verification information is verified successfully, obtaining device information of a current device, and invoking, by the target application, a local device management rule, and determining, by using the local device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user corresponding to the device information, wherein the identity feature information of the pre-registered user is obtained from pre-stored device account registration information; and

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

15. 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 local 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.

16. 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, by a terminal device, 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, by the target application, the verification information , and in response to determining that the verification information is verified successfully, obtaining device information of a current device, and invoking, by the target application, a local device management rule, and determining, by using the local device management rule, whether the identity feature information of the target user matches identity feature information of a pre-registered user corresponding to the device information, wherein the identity feature information of the pre-registered user is obtained from pre-stored device account registration information; and

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

17. 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 local 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.