

ACCOUNT OPENING METHODS, SYSTEMS, AND APPARATUSES

[0001] This application claims priority to Chinese Patent Application No. 202110808788.9, filed with the China National Intellectual Property Administration on July 16, 2021 and entitled "ACCOUNT OPENING METHODS, SYSTEMS, AND APPARATUSES", which is incorporated
5 herein by reference in its entirety.

TECHNICAL FIELD

[0002] This specification relates to the field of data security technologies, and in particular, to account opening methods, systems, and apparatuses.

BACKGROUND

10 [0003] Innovative payment in offline scenarios has attracted increasing attention from the country and various institutions, and therefore, hardware wallets receive more attention. The biggest characteristic of the hardware wallet is that digital objects change from "cloud" to "end". Correspondingly, an opening stage of the hardware wallet, namely, opening of a hardware wallet account, becomes a crucial risk point.

15 [0004] How to provide a trusted method for opening a hardware wallet account becomes a problem that urgently needs to be solved.

SUMMARY

[0005] One or more embodiments of this specification provide account opening methods, systems, and apparatuses, to improve account opening credibility.

20 [0006] According to a first aspect of this specification, an account opening method is provided. The method is applied to a terminal device, the terminal device includes a trusted execution environment (TEE) and an encryption hardware-based secure element, and the method includes the following: obtaining a user public key of a current user in the TEE; signing the user public key in the TEE by using a predetermined manufacturer private key, to obtain a user certificate; signing
25 opening information in the secure element by using a user private key corresponding to the user public key, where the opening information is generated based on device information of the terminal device; generating an opening request in the TEE based on at least the user certificate and signed

opening information; and in the TEE, generating an opening request packet based on the opening request, and sending the opening request packet to a server that opens an account, so that the server opens an account for the current user based on the opening request packet.

5 [0007] In some feasible methods, the obtaining a user public key of a current user includes the following: generating a corresponding user public/private key pair in the TEE by using a device public/private key pair generated in advance and a user identifier of the current user, where the user public/private key pair includes the user public key and the user private key corresponding to the user public key.

10 [0008] In some feasible methods, the generating an opening request includes the following: obtaining a manufacturer digital certificate, where the manufacturer digital certificate includes a manufacturer public key corresponding to the manufacturer private key; and generating the opening request based on the user certificate, the manufacturer digital certificate, and the signed opening information.

15 [0009] In some feasible methods, the generating an opening request packet based on the opening request includes the following: encrypting the opening request in the TEE by using a symmetric key, to obtain an encrypted opening request; encrypting the symmetric key by using a server public key of the server, to obtain a first encrypted key after encryption; and generating the opening request packet based on the encrypted opening request and the first encrypted key.

20 [0010] In some feasible methods, the method further includes the following: randomly generating the symmetric key by using a predetermined random key generation method.

[0011] In some feasible methods, the method further includes the following: obtaining a predetermined server public key agreed upon with the server from the TEE; or obtaining the server public key from the server by using a predetermined key negotiation algorithm.

25 [0012] In some feasible methods, the method further includes the following: obtaining an opening reply packet that is fed back by the server based on the opening request packet; and opening an account based on the opening reply packet.

30 [0013] In some feasible methods, the opening reply packet includes an opening reply ciphertext encrypted by using the symmetric key and a second encrypted key obtained by encrypting the symmetric key by using a server private key corresponding to the server public key; and the opening an account based on the opening reply packet includes the following: decrypting the second encrypted key by using the server public key, to obtain a symmetric key; when it is determined that the symmetric key obtained through decryption is the same as the symmetric key generated in advance in the TEE, decrypting the opening reply ciphertext by using the symmetric key, to obtain an opening reply plaintext; and opening an account based on the opening reply
35 plaintext.

[0014] According to a second aspect of this specification, an account opening method is provided, including: The method is applied to a server, and includes the following: receiving an opening request packet sent by a terminal device based on a current user, where the opening request packet includes an opening request, the opening request includes a user certificate and signed opening information, the user certificate is obtained by signing a user public key of the current user by using a manufacturer private key predetermined in the terminal device, the signed opening information is obtained by signing opening information by using a user private key corresponding to the current user, and the opening information is generated based on device information of the terminal device; performing first verification on the user certificate by using a manufacturer public key corresponding to the manufacturer private key; if the first verification is passed, performing second verification on the signed opening information by using the user public key in the user certificate; and if the second verification is passed, determining an opening reply packet by using the device information in the opening information, and sending the opening reply packet to the terminal device, so that the terminal device opens an account based on the opening reply packet.

[0015] In some feasible methods, the opening request further includes a manufacturer digital certificate, and the manufacturer digital certificate includes the manufacturer public key corresponding to the manufacturer private key; and the performing first verification on the user certificate includes the following: performing third verification on the manufacturer digital certificate by using an obtained manufacturer root public key; and if the third verification is passed, performing first verification on the user certificate by using the manufacturer public key.

[0016] In some feasible methods, the opening request is an encrypted opening request obtained through encryption by using a symmetric key, and the opening request packet further includes a first encrypted key obtained by encrypting the symmetric key by using a server public key; and before the performing first verification on the user certificate, the method further includes the following: decrypting the first encrypted key by using a server private key corresponding to the server public key, to obtain the symmetric key; and decrypting the encrypted opening request by using the symmetric key, to obtain an opening request plaintext.

[0017] In some feasible methods, the determining an opening reply packet by using the device information in the opening information includes the following: determining an opening reply by using the device information; encrypting the opening reply by using the symmetric key, to obtain an opening reply ciphertext; encrypting the symmetric key by using the server private key, to obtain a second encrypted key after encryption; and forming the opening reply packet based on the opening reply ciphertext and the second encrypted key.

[0018] According to a third aspect of this specification, an account opening system is provided. The account opening system includes a terminal device and a server, the terminal device is

configured to perform the method according to the first aspect, and the server is configured to perform the method according to the second aspect.

5 [0019] According to a fourth aspect of this specification, an account opening apparatus is provided. The apparatus is applied to a terminal device, the terminal device includes a trusted execution environment (TEE) and an encryption hardware-based secure element, and the apparatus includes: a first acquisition module, configured to obtain a user public key of a current user in the TEE; a first signature module, configured to sign the user public key in the TEE by using a predetermined manufacturer private key, to obtain a user certificate; a second signature module, configured to sign opening information in the secure element by using a user private key
10 corresponding to the user public key, where the opening information is generated based on device information of the terminal device; a request generation module, configured to generate an opening request in the TEE based on at least the user certificate and signed opening information; and a generating and sending module, configured to: in the TEE, generate an opening request packet based on the opening request, and send the opening request packet to a server that opens an account,
15 so that the server opens an account for the current user based on the opening request packet.

[0020] According to a fifth aspect of this specification, an account opening apparatus is provided. The apparatus is applied to a server, and includes: a packet receiving module, configured to receive an opening request packet sent by a terminal device based on a current user, where the opening request packet includes an opening request, the opening request includes a user certificate and
20 signed opening information, the user certificate is obtained by signing a user public key of the current user by using a manufacturer private key predetermined in the terminal device, the signed opening information is obtained by signing opening information by using a user private key corresponding to the current user, and the opening information is generated based on device information of the terminal device; a first verification module, configured to perform first
25 verification on the user certificate by using a manufacturer public key corresponding to the manufacturer private key; a second verification module, configured to: if the first verification is passed, perform second verification on the signed opening information by using the user public key in the user certificate; and a determining and sending module, configured to: if the second verification is passed, determine an opening reply packet by using the device information in the opening information, and send the opening reply packet to the terminal device, so that the terminal
30 device opens an account based on the opening reply packet.

[0021] According to a sixth aspect of this specification, a computer-readable storage medium is provided. The computer-readable storage medium stores a computer program. When the computer program is executed on a computer, the computer is enabled to perform the terminal device-side
35 account opening method provided in one or more embodiments of this specification.

[0022] According to a seventh aspect of this specification, a computing device is provided. The computing device includes a memory and a processor, the memory stores executable code, and when executing the executable code, the processor implements the terminal device-side account opening method provided in one or more embodiments of this specification.

5 [0023] According to an eighth aspect of this specification, a computer-readable storage medium is provided. The computer-readable storage medium stores a computer program, and when the computer program is executed on a computer, the computer is enabled to perform the server-side account opening method provided in one or more embodiments of this specification.

[0024] According to a ninth aspect of this specification, a computing device is provided. The
10 computing device includes a memory and a processor, the memory stores executable code, and when executing the executable code, the processor implements the server-side account opening method provided in one or more embodiments of this specification.

[0025] According to the account opening methods and apparatuses provided in the embodiments of this specification, the opening information is signed in the secure element with highest security
15 by using the user private key, so that accuracy and integrity of the opening information are ensured, and the opening information is prevented from being stolen and tampered with. In the TEE of the terminal device with relatively high security, the user public key is signed by using the predetermined manufacturer private key, to obtain the user certificate, the opening request packet is generated based on the signed opening information, and the opening request packet is sent to
20 the server that opens an account in the TEE. The user certificate in the opening request packet can indicate that the opening request packet is from a real physical device produced by a device manufacturer, and processes of generating and sending the opening request packet are completed in the TEE and the secure element, so that a loss of related information in the packet generation process is reduced, and credibility of the opening request packet is improved to some extent,
25 thereby improving credibility of opening a corresponding account.

BRIEF DESCRIPTION OF DRAWINGS

[0026] To describe technical solutions in embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following description merely show some embodiments
30 of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0027] FIG. 1 is a schematic diagram illustrating an implementation framework, according to some embodiments disclosed in this specification;

[0028] FIG. 2 is a schematic flowchart illustrating an account opening method, according to some embodiments of this specification;

[0029] FIG. 3 is another schematic flowchart illustrating an account opening method, according to some embodiments of this specification;

5 [0030] FIG. 4 is a schematic diagram illustrating a framework of an account opening system, according to some embodiments of this specification;

[0031] FIG. 5 is a schematic diagram illustrating a framework of an account opening apparatus, according to some embodiments of this specification; and

[0032] FIG. 6 is a schematic diagram illustrating a framework of an account opening apparatus,

10 according to some embodiments of this specification.

DESCRIPTION OF EMBODIMENTS

[0033] The following describes the technical solutions of the embodiments of this specification in detail with reference to the accompanying drawings.

[0034] Embodiments of this specification disclose account opening methods and apparatuses.

15 The following describes an application scenario and an inventive concept of account opening. Details are as follows:

[0035] A hardware wallet usually relies on a real physical device, and opening of a hardware wallet account also relies on the real physical device. If an account opening device is an unreal physical device such as a fake mobile phone or a cloud mobile phone, a false hardware wallet is

20 prone to appear, which endangers object security of a user who opens the account. To solve the above-mentioned problem, in a current account opening process, device information of a terminal device is obtained from an application (APP) level, an account opening request packet is assembled by using the device information, and the account opening request packet is sent to a server that opens an account, to apply for account opening. In this process, information acquisition at the APP

25 level is prone to black-industry attacks and simulations, and the server still cannot effectively identify whether an account opening device is a real physical device.

[0036] In view of the above, some embodiments of this specification provide an account opening method, applied to a terminal device. FIG. 1 is a schematic diagram illustrating an implementation framework, according to some embodiments disclosed in this specification. The terminal device

30 includes a trusted execution environment (TEE) and an encryption hardware-based secure element. When detecting that a current user initiates an account opening request, the terminal device obtains a user public key of the current user in the TEE, and signs a user public key by using a predetermined manufacturer private key, to obtain a user certificate; signs, in the secure element

by using a user private key corresponding to the user public key, opening information generated based on device information of the terminal device; and in the TEE, generates an opening request packet based on at least the user certificate and signed opening information, and sends the opening request packet to a server that opens an account, so that the server opens an account for the current user based on the opening request packet. In some feasible methods, the terminal device can generate the opening information in the TEE or the secure element based on the device information.

[0037] An account that this solution is applicable to can be a hardware wallet account, or can be another account that relies on a physical device and has a relatively high security requirement, for example, an identity authentication account or a bank related account, etc.

[0038] The manufacturer private key is a private key stored on the terminal device by a manufacturer of the terminal device on a production line of the terminal device, and the manufacturer private key can prove, to some extent, that the terminal device is a real physical device produced by the manufacturer.

[0039] In the embodiments, the opening information is signed in the secure element with highest security by using the user private key, so that accuracy and integrity of the opening information are ensured, and the opening information is prevented from being stolen and tampered with. In the TEE of the terminal device with relatively high security, the user public key is signed by using the predetermined manufacturer private key, to obtain the user certificate, the opening request packet is generated based on the signed opening information, and the opening request packet is sent to the server that opens an account in the TEE. The user certificate in the opening request packet can indicate that the opening request packet is from a real physical device produced by a device manufacturer, and processes of generating and sending the opening request packet are completed in the TEE and the secure element, so that a loss of related information in the packet generation process is reduced, and credibility of the opening request packet is improved to some extent, thereby improving credibility of opening a corresponding account.

[0040] With reference to specific embodiments, the following describes in detail the account opening method provided in this specification.

[0041] FIG. 2 is a schematic flowchart illustrating an account opening method, according to this specification. The method is applied to a terminal device. The terminal device can be any device that has data computing, processing, and storage, for example, can be a computer, a mobile phone, a tablet computer, a smart watch, or a payment card. In some embodiments of this specification, the terminal device includes a trusted execution environment (TEE) and an encryption hardware-based secure element, and the method includes S210 to S250:

[0042] S210: Obtain a user public key of a current user in the TEE.

[0043] The trusted execution environment (TEE) is an area on a processor, for example, a central

processing unit (CPU), of the terminal device. This area provides more secure space for data and code execution, and ensures confidentiality and integrity of data and code. By creating a small operating system that runs independently, the area implements secure storage, secure computing, and other data processing involving security and privacy.

5 **[0044]** The encryption hardware-based secure element can include but is not limited to a secure element (SE), and is usually provided in a chip form. The secure element includes an encryption/decryption logic circuit, so that external malicious resolution attacks can be prevented, and data security can be protected. It is worthwhile to note that the secure element is an environment where encryption protection is performed on data based on hardware, and therefore,
10 the secure element has a higher security level than the TEE. In a case, the secure element can be a built-in secure element of the terminal device, or can be an external secure element of the terminal device. For example, when the terminal device is a mobile phone, the external secure element can be a secure element supported by a subscriber identity module (SIM) card.

[0045] In some implementations, when detecting that the current user initiates the account
15 opening request, the terminal device obtains the user public key of the current user in the TEE. The account opening application can be initiated by the current user based on an account opening related application. The account opening related application can provide an account opening interface. The account opening interface displays an account opening button. The account opening button can be tapped to trigger the account opening application. Correspondingly, in a case, the
20 terminal device further includes a rich execution environment (REE), and the account opening related application can run in the REE.

[0046] In some examples, the account opening related application can be ALIPAY Wallet. Correspondingly, the current user can be an ALIPAY user, and the account can be a hardware wallet account that needs to be opened for the ALIPAY user in ALIPAY Wallet.

25 **[0047]** In other examples, the account opening related application can be an application of bank x, the current user is a user of bank x, and the account can be a wallet account that bank x needs to open for the current user. The above-mentioned examples are only examples of this specification. The account opening related application can be another application that can open an account. The current user can be a user of the another application that can open an account, and the account is
30 an account that the another application that can open an account needs to open for the current user.

[0048] In some embodiments of this specification, S210 can include the following: generating a corresponding user public/private key pair in the TEE by using a device public/private key pair generated in advance and a user identifier of the current user. The user public/private key pair includes the user public key and the user private key corresponding to the user public key.

35 **[0049]** When detecting that the current user initiates the account opening application, the

terminal device obtains the device public/private key pair generated in advance and the user identifier of the current user in the TEE, and generates the corresponding user public/private key pair based on the device public/private key pair and the user identifier by using a key generation algorithm such as a national secret algorithm. The user identifier can be a user identity (ID) of the current user. The device public/private key pair can be a public/private key pair generated when the account opening related application is enabled for the first time, and is stored in the TEE.

[0050] In some implementations, after the user public/private key pair is generated, the user public key in the user public/private key pair is stored in the TEE, and the user private key in the user public/private key pair is stored in the secure element, to prevent the user public/private key pair from being tampered with.

[0051] S220: Sign the user public key in the TEE by using a predetermined manufacturer private key, to obtain a user certificate. The manufacturer private key is a key stored in hardware of the terminal device by a manufacturer of the terminal device on a production line of the terminal device. The manufacturer private key can be stored in the TEE of the terminal device. Therefore, the obtained user certificate can include the user public key and a first signature obtained after the user public key is signed by using the manufacturer private key.

[0052] S230: Sign opening information in the secure element by using the user private key corresponding to the user public key. The opening information is generated based on device information of the terminal device.

[0053] In a case, the device information can include but is not limited to a device name, a device identifier, a device model, a manufacturer identifier, etc. of the terminal device. The device identifier is used to uniquely identify the terminal device, for example, can be embodied as a medium access control (MAC) address. The device model can indicate a device type (a computer, a smartphone, a payment card, or a smart watch) and a specific model in this type. The device information is pre-stored in the TEE of the terminal device, so that the device information is prevented from being tampered with.

[0054] In some feasible methods, the terminal device can generate the opening information in the TEE or the secure element based on the device information. Further, the terminal device performs hash value calculation on the opening information in the secure element by using a predetermined hash algorithm, to obtain a hash value corresponding to the opening information. The terminal device encrypts the hash value by using the user private key stored in the secure element, to obtain a digital signature for the opening information.

[0055] S240: Generate an opening request in the TEE based on at least the user certificate and signed opening information. The opening request is used to request a server that opens an account to open an account. The opening request can include the user certificate and the signed opening

information. The user certificate is used to indicate that the terminal device that opens an account is a real physical terminal device, and the signed opening information is used to assist the server in verifying whether the opening information is accurate, complete, and authentic. After the verification is passed, the server can generate an opening reply by using the opening information, and feed back the opening reply to the terminal device. The terminal device can open an account based on the opening reply.

[0056] In some embodiments of this specification, S240 can include the following steps 11 and 12:

[0057] Step 11: Obtain a manufacturer digital certificate, where the manufacturer digital certificate includes a manufacturer public key corresponding to the manufacturer private key.

[0058] Step 12: Generate the opening request based on the user certificate, the manufacturer digital certificate, and the signed opening information.

[0059] In the embodiments, to better improve account opening credibility, the manufacturer digital certificate is obtained in the TEE in S140. The manufacturer digital certificate includes the manufacturer public key corresponding to the manufacturer private key. The manufacturer digital certificate is stored in the terminal device by the manufacturer of the terminal device on the production line of the terminal device. In a case, the manufacturer digital certificate is stored in the TEE of the terminal device. In some implementations, the manufacturer digital certificate can be a certificate issued by a certificate authority (CA) to the manufacturer of the terminal device.

The manufacturer digital certificate is used to verify authenticity of the user certificate.

[0060] After obtaining the user certificate, the manufacturer digital certificate, and the signed opening information, the terminal device generates the opening request in the TEE based on the user certificate, the manufacturer digital certificate, and the signed opening information. The opening request includes the user certificate, the manufacturer digital certificate, and the signed opening information. Subsequently, after the opening request is sent to the server, the server can first verify authenticity of the manufacturer digital certificate. After the verification on authenticity of the manufacturer digital certificate is passed, the server verifies authenticity of the user certificate by using the manufacturer public key in the manufacturer digital certificate. Correspondingly, credibility of the opening request is higher, and therefore, credibility of the opening account is higher. Verifying authenticity of the manufacturer digital certificate can be verifying authenticity of the manufacturer digital certificate based on a manufacturer root public key obtained by the server from the manufacturer of the terminal device.

[0061] S250: In the TEE, generate an opening request packet based on the opening request, and send the opening request packet to the server that opens an account, so that the server opens an account for the current user based on the opening request packet.

[0062] In some implementations, the terminal device can generate the opening request packet in the TEE based on the opening request and a predetermined packet format. The predetermined packet format is a format that is set based on a data transmission protocol between the terminal device and the server that opens an account. Further, the opening request packet is sent to the server that opens an account. Correspondingly, the server opens an account for the current user based on the opening request packet.

[0063] In the embodiments, the opening information is signed in the secure element with highest security by using the user private key, so that accuracy and integrity of the opening information are ensured, and the opening information is prevented from being stolen and tampered with. In the TEE of the terminal device with relatively high security, the user public key is signed by using the predetermined manufacturer private key, to obtain the user certificate, the opening request packet is generated based on the signed opening information, and the opening request packet is sent to the server that opens an account in the TEE. The user certificate in the opening request packet can indicate that the opening request packet is from a real physical device produced by a device manufacturer, and processes of generating and sending the opening request packet are completed in the TEE and the secure element, so that a loss of related information in the packet generation process is reduced, and credibility of the opening request packet is improved to some extent, thereby improving credibility of opening a corresponding account.

[0064] To prevent the opening request packet from being intercepted and the device information in the opening request packet from being stolen during transmission, in some embodiments of this specification, the opening request packet can be encrypted for transmission. Correspondingly, S250 can include the following steps 21 to 23:

[0065] Step 21: Encrypt the opening request in the TEE by using a symmetric key, to obtain an encrypted opening request.

[0066] Step 22: Encrypt the symmetric key by using a server public key of the server, to obtain a first encrypted key after encryption.

[0067] Step 23: Generate the opening request packet based on the encrypted opening request and the first encrypted key. The opening request packet includes the encrypted opening request and the first encrypted key. In a case, the first encrypted key can be added to a packet header of the opening request packet.

[0068] In some feasible methods, to better improve confidentiality of the opening request, before step 21, the method can further include the following step: The symmetric key is randomly generated in the TEE by using a predetermined random key generation method. Using a random symmetric key to encrypt the opening request in an account opening procedure can increase difficulty in stealing related information in the opening request packet to some extent, and improve

confidentiality and security of the related information in the opening request packet. The predetermined random key generation method can include but is not limited to symmetric encryption algorithms such as the Data Encryption Standard (DES), the Triple Data Encryption Algorithm (3DES), and the Advanced Encryption Standard (AES).

5 [0069] The server public key can be a key agreed upon between the terminal device and the server, and can be predetermined in the terminal device, or can be delivered to the terminal device when needed by the terminal device. Correspondingly, in some feasible methods, before step 22, the method can further include the following steps: A predetermined server public key agreed upon with the server is obtained in the TEE; or the server public key is obtained from the server that
10 opens an account by using a predetermined key negotiation algorithm. The predetermined key negotiation algorithm can be any current algorithm that can be used for key negotiation. This is not limited in the embodiments.

[0070] The symmetric key is encrypted by using the server public key, to obtain the first encrypted key after encryption. The opening request packet is generated based on the
15 predetermined packet format, the encrypted opening request, and the first encrypted key. The opening request packet is sent to the server. Subsequently, the server generates an opening reply packet based on the opening request packet, and feeds back the opening reply packet to the terminal device. The terminal device can open an account based on the opening reply packet.

[0071] In the embodiments, based on existing general capabilities of the manufacturer of the
20 terminal device and a lightweight data processing method, a highly reliable data encryption solution similar to a one-device one-key solution is implemented, and confidentiality and integrity in a data transmission process are ensured.

[0072] In some embodiments of this specification, after step S250, the method further includes the following steps 31 and 32:

25 [0073] Step 31: Obtain the opening reply packet that is fed back by the server based on the opening request packet.

[0074] Step 32: Open an account based on the opening reply packet. The opening reply packet can include information indicating the terminal device to open an account. Correspondingly, the terminal device opens an account based on the information in the opening reply packet.

30 [0075] In some implementations, the terminal device can obtain, by using the TEE, the opening reply packet that is fed back by the server based on the opening request packet, and further open an account in the TEE based on the opening reply packet.

[0076] To ensure security of the opening reply packet and further to ensure account opening credibility, information included in the opening reply packet that is fed back by the server to the
35 terminal device is encrypted information. In some feasible methods, the opening reply packet

includes an opening reply ciphertext encrypted by using the symmetric key and a second encrypted key obtained by encrypting the symmetric key by using a server private key corresponding to the server public key.

[0077] Correspondingly, step 32 can include the following steps 321 to 323:

5 [0078] Step 321: Decrypt the second encrypted key by using the server public key, to obtain a symmetric key.

[0079] Step 322: When it is determined that the symmetric key obtained through decryption is the same as the symmetric key generated in advance in the TEE, decrypt the opening reply ciphertext by using the symmetric key, to obtain an opening reply plaintext.

10 [0080] Step 323: Open an account based on the opening reply plaintext.

[0081] In the implementations, after obtaining the opening reply packet by using the TEE, the terminal device parses the opening reply packet to obtain the opening reply ciphertext and the second encrypted key in the opening reply packet, and decrypts the second encrypted key by using the server public key, to obtain the symmetric key. It is determined whether the symmetric key
15 obtained through decryption is the same as the symmetric key generated in advance in the TEE. When it is determined that the symmetric key obtained through decryption is the same as the symmetric key generated in advance in the TEE, it can be considered that the opening reply packet is a packet actually delivered by the server. Correspondingly, in the TEE, the terminal device decrypts the opening reply ciphertext by using the symmetric key, to obtain the opening reply
20 plaintext, and further opens an account based on the opening reply plaintext.

[0082] In the above-mentioned account opening procedure, data transmitted between the server and the terminal device are encrypted and decrypted by using the randomly generated symmetric key and a server public/private key pair, and subsequent steps are performed after each party confirms authenticity of a data sender and authenticity and integrity of data, so that account
25 opening credibility is improved.

[0083] Corresponding to the above-mentioned method embodiments, FIG. 3 is another schematic flowchart illustrating an account opening method, according to this specification. The method is applied to a server, and the server can be implemented by any device, apparatus, platform, server, or device cluster that has computing and processing capabilities. The server is configured to open
30 an account for a terminal device that sends an opening request packet. In some embodiments of this specification, the method can include the following steps S310 to S340:

[0084] S310: Receive the opening request packet sent by the terminal device based on a current user. The opening request packet includes an opening request, the opening request includes a user certificate and signed opening information, the user certificate is obtained by signing a user public
35 key of the current user by using a manufacturer private key predetermined in the terminal device,

the signed opening information is obtained by signing opening information by using a user private key corresponding to the current user, and the opening information is generated based on device information of the terminal device;

[0085] In a case, the terminal device includes a trusted execution environment (TEE) and an encryption hardware-based secure element. The above-mentioned opening request packet, the opening request, and the user certificate can be generated in the TEE of the terminal device, and the signed opening information can be generated in the secure element of the terminal device. In some implementations, the opening request packet is sent by the terminal device to the server by using the TEE.

[0086] The current user is a user an account is to be opened for. In a case, the current user can be a user of an account opening related application disposed in the terminal device. The terminal device can further include a rich execution environment (REE), and the account opening related application can run in the REE. For example, the account opening related application can be ALIPAY Wallet. Correspondingly, the current user can be an ALIPAY user, and the account can be a hardware wallet account that needs to be opened for the ALIPAY user in ALIPAY Wallet. ALIPAY Wallet can run in the REE of the terminal device.

[0087] It is worthwhile to note that for generation processes of the opening request packet, the opening request, the user certificate, and the signed opening information, references can be made to the generation processes described in the above-mentioned embodiments of the account opening method applied to the terminal device, and details are omitted here for simplicity.

[0088] In some implementations, the server can communicate with one or more terminal devices, and receive opening request packets sent by the one or more terminal devices; and then perform, for each opening request packet, the account opening method procedure provided in the embodiments of this specification. After receiving the opening request packet, the server parses the opening request packet to obtain the user certificate and the signed opening information in the opening request packet.

[0089] S320: Perform first verification on the user certificate by using a manufacturer public key corresponding to the manufacturer private key. In some implementations, the manufacturer public key corresponding to the manufacturer private key can be predetermined for the server. Correspondingly, after receiving the opening request packet, the server obtains, for the terminal device from a local predetermined storage area, the manufacturer public key corresponding to the manufacturer private key, and then performs first verification on the user certificate by using the manufacturer public key. In other implementations, after receiving the opening request packet, the server can download, for the terminal device, the manufacturer public key from a server corresponding to a manufacturer of the terminal device, and then perform first verification on the

user certificate by using the manufacturer public key.

[0090] S330: If the first verification is passed, perform second verification on the signed opening information by using the user public key in the user certificate. In this step, if the first verification is passed, it can indicate that the user public key in the user certificate is authentic and complete, and can indicate that the terminal device is a real physical device produced by a manufacturer. Correspondingly, it can be determined that the opening request packet is sent by a real physical terminal. Further, the server parses the user certificate to obtain the user public key in the user certificate, and performs second verification on the signed opening information by using the user public key.

[0091] In some implementations, if the first verification fails, it can be considered that the user public key in the user certificate is tampered with, or the terminal device is not a real terminal device produced by a corresponding manufacturer. Subsequently, the server can no longer perform subsequent steps. In a case, the server can further send, to the terminal device, information indicating that the terminal device cannot open an account.

[0092] S340: If the second verification is passed, determine an opening reply packet by using the device information in the opening information, and send the opening reply packet to the terminal device, so that the terminal device opens an account based on the opening reply packet. In this step, if the second verification is passed, it can indicate that the opening information is authentic and complete. Correspondingly, the server parses the opening information to obtain the device information, and further, determines the opening reply packet by using the device information and sends the opening reply packet to the terminal device.

[0093] In the embodiments, the server verifies the opening request packet sent by the terminal device twice, to determine that the terminal device is a real physical terminal device and that the opening request packet is a real packet sent by the terminal device, and then feeds back the opening reply packet to the terminal device, so that credibility of opening an account by the terminal device is improved to some extent.

[0094] In some embodiments of this specification, the opening request further includes a manufacturer digital certificate, and the manufacturer digital certificate includes the manufacturer public key corresponding to the manufacturer private key. Correspondingly, S320 can include the following steps 41 and 42:

[0095] Step 41: Perform third verification on the manufacturer digital certificate by using an obtained manufacturer root public key. The manufacturer root public key can be locally predetermined by the server, or can be obtained through downloading from the server corresponding to the manufacturer of the terminal device after the server receives the opening request packet sent by the terminal device.

[0096] Step 42: If the third verification is passed, perform first verification on the user certificate by using the manufacturer public key.

[0097] To better prove that the terminal device is a real physical terminal and ensure account opening credibility, the opening request can further include the manufacturer digital certificate.

5 The manufacturer digital certificate includes the manufacturer public key corresponding to the manufacturer private key. Correspondingly, the server performs third verification on the manufacturer digital certificate by using the obtained manufacturer root public key. If the third verification is passed, it indicates that the manufacturer digital certificate is credible, in other words, the manufacturer is credible, and further, the manufacturer digital certificate is parsed to obtain the

10 manufacturer public key in the manufacturer digital certificate, and first verification is performed on the user certificate by using the manufacturer public key.

[0098] In some embodiments of this specification, the opening request is an encrypted opening request obtained through encryption by using a symmetric key, and the opening request packet further includes a first encrypted key obtained by encrypting the symmetric key by using a server

15 public key.

[0099] Correspondingly, before S320, the method can further include the following steps 51 and 52:

[0100] Step 51: Decrypt the first encrypted key by using a server private key corresponding to the server public key, to obtain the symmetric key.

20 [0101] Step 52: Decrypt the encrypted opening request by using the symmetric key, to obtain an opening request plaintext.

[0102] To ensure security of the packet during transmission, the opening request is an encrypted opening request obtained through encryption by using the symmetric key, and correspondingly, the opening request packet can further include the first encrypted key obtained by encrypting the

25 symmetric key by using the server public key. The server parses the opening request packet to obtain the first encrypted key and the encrypted opening request in the opening request packet, decrypts the first encrypted key by using the predetermined server private key corresponding to the server public key, to obtain the symmetric key, further decrypts the encrypted opening request by using the symmetric key, to obtain the opening request plaintext, and further generates the

30 opening reply packet based on the device information in the opening request plaintext.

[0103] In some embodiments of this specification, S340 can include the following steps 61 to 64:

[0104] Step 61: Determine an opening reply by using the device information.

[0105] Step 62: Encrypt the opening reply by using the symmetric key, to obtain an opening reply ciphertext.

35 [0106] Step 63: Encrypt the symmetric key by using the server private key, to obtain a second

encrypted key after encryption.

[0107] Step 64: Form the opening reply packet based on the opening reply ciphertext and the second encrypted key.

5 [0108] To ensure security of the packet during transmission, in step S340, the server first determines the opening reply by using the device information, and encrypts the opening reply by using the symmetric key obtained by decrypting the opening request packet, to obtain the opening reply ciphertext. The server encrypts the symmetric key by using the server private key, to obtain the second encrypted key after encryption. Further, the server assembles a packet based on a predetermined packet format, the opening reply ciphertext, and the second encrypted key, to form
10 the opening reply packet. The server sends the opening reply packet to the terminal device, so that the terminal device opens an account based on the opening reply packet. Encrypting the packet by using the symmetric key included in the opening request packet and the server private key and then transmitting the encrypted opening reply packet ensure security of the packet during transmission and improve account opening credibility.

15 [0109] Specific embodiments of this specification have been described above, and other embodiments fall within the scope of the appended claims. In some situations, the actions or steps described in the claims can be performed in an order different from the order in the embodiments and the desired results can still be achieved. In addition, processes described in the accompanying drawings do not necessarily require a specific order or a sequential order shown to achieve the
20 desired results. In some implementations, multitasking and parallel processing are also possible or may be advantageous.

[0110] Corresponding to the above-mentioned method embodiments, some embodiments of this specification provide an account opening system 400. A schematic block diagram of the system is shown in FIG. 4. The system includes a terminal device 410 and a server 420. The terminal device
25 410 is configured to perform the above-mentioned terminal device-side account opening method. The server 420 is configured to perform the above-mentioned server-side account opening method. In some implementations, the server can open accounts for a plurality of terminal devices 410.

[0111] Corresponding to the above-mentioned method embodiments, some embodiments of this specification provide an account opening apparatus 500, applied to a terminal device. The terminal
30 device includes a trusted execution environment (TEE) and an encryption hardware-based secure element. A schematic block diagram of the apparatus is shown in FIG. 5. The apparatus includes: a first acquisition module 510, configured to obtain a user public key of a current user in the TEE; a first signature module 520, configured to sign the user public key in the TEE by using a predetermined manufacturer private key, to obtain a user certificate; a second signature module
35 530, configured to sign opening information in the secure element by using a user private key

corresponding to the user public key, where the opening information is generated based on device information of the terminal device; a request generation module 540, configured to generate an opening request in the TEE based on at least the user certificate and signed opening information; and a generating and sending module 550, configured to: in the TEE, generate an opening request
5 packet based on the opening request, and send the opening request packet to a server that opens an account, so that the server opens an account for the current user based on the opening request packet.

[0112] In some feasible methods, the first acquisition module 510 is specifically configured to: in the TEE, generate a corresponding user public/private key pair by using a device public/private
10 key pair generated in advance and a user identifier of the current user, where the user public/private key pair includes the user public key and the user private key corresponding to the user public key.

[0113] In some feasible methods, the request generation module 540 is specifically configured to: obtain a manufacturer digital certificate, where the manufacturer digital certificate includes a manufacturer public key corresponding to the manufacturer private key; and generate the opening
15 request based on the user certificate, the manufacturer digital certificate, and the signed opening information.

[0114] In some feasible methods, the generating and sending module 550 is specifically configured to: encrypt the opening request in the TEE by using a symmetric key, to obtain an encrypted opening request; encrypt the symmetric key by using a server public key of the server,
20 to obtain a first encrypted key after encryption; and generate the opening request packet based on the encrypted opening request and the first encrypted key.

[0115] In some feasible methods, the apparatus further includes: a key generation module (not shown in the figure), configured to randomly generate the symmetric key by using a predetermined random key generation method.

[0116] In some feasible methods, the apparatus further includes: a second acquisition module (not shown in the figure), configured to obtain a predetermined server public key agreed upon with the server from the TEE; or obtain the server public key from the server by using a predetermined key negotiation algorithm.

[0117] In some feasible methods, the apparatus further includes: a third acquisition module (not shown in the figure), configured to obtain an opening reply packet that is fed back by the server based on the opening request packet; and an account opening module (not shown in the figure), configured to open an account based on the opening reply packet.

[0118] In some feasible methods, the opening reply packet includes an opening reply ciphertext encrypted by using the symmetric key and a second encrypted key obtained by encrypting the
35 symmetric key by using a server private key corresponding to the server public key; and the

account opening module is specifically configured to: decrypt the second encrypted key by using the server public key, to obtain a symmetric key; and when it is determined that the symmetric key obtained through decryption is the same as the symmetric key generated in advance in the TEE, decrypt the opening reply ciphertext by using the symmetric key, to obtain an opening reply plaintext; and open an account based on the opening reply plaintext.

[0119] Corresponding to the above-mentioned method embodiments, some embodiments of this specification provide an account opening apparatus 600, applied to a server. The server is configured to open an account for a terminal device that sends an opening request packet. A schematic block diagram of the apparatus is shown in FIG. 6. The apparatus includes: a packet receiving module 610, configured to receive the opening request packet sent by the terminal device based on a current user, where the opening request packet includes an opening request, the opening request includes a user certificate and signed opening information, the user certificate is obtained by signing a user public key of the current user by using a manufacturer private key predetermined in the terminal device, the signed opening information is obtained by signing opening information by using a user private key corresponding to the current user, and the opening information is generated based on device information of the terminal device; a first verification module 620, configured to perform first verification on the user certificate by using a manufacturer public key corresponding to the manufacturer private key; a second verification module 630, configured to: if the first verification is passed, perform second verification on the signed opening information by using the user public key in the user certificate; and a determining and sending module 640, configured to: if the second verification is passed, determine an opening reply packet by using the device information in the opening information, and send the opening reply packet to the terminal device, so that the terminal device opens an account based on the opening reply packet.

[0120] In some feasible methods, the opening request further includes a manufacturer digital certificate, and the manufacturer digital certificate includes the manufacturer public key corresponding to the manufacturer private key; and the first verification module 620 is specifically configured to: perform third verification on the manufacturer digital certificate by using an obtained manufacturer root public key; and if the third verification is passed, perform first verification on the user certificate by using the manufacturer public key.

[0121] In some feasible methods, the opening request is an encrypted opening request obtained through encryption by using a symmetric key, and the opening request packet further includes a first encrypted key obtained by encrypting the symmetric key by using a server public key; and the apparatus further includes: a first decryption module (not shown in the figure), configured to: before first verification is performed on the user certificate, decrypt the first encrypted key by using a server private key corresponding to the server public key, to obtain the symmetric key; and

a second decryption module (not shown in the figure), configured to decrypt the encrypted opening request by using the symmetric key, to obtain an opening request plaintext.

[0122] In some feasible methods, the determining and sending module 640 is specifically configured to: determine an opening reply by using the device information; encrypt the opening
5 reply by using the symmetric key, to obtain an opening reply ciphertext; encrypt the symmetric key by using the server private key, to obtain a second encrypted key after encryption; and form the opening reply packet based on the opening reply ciphertext and the second encrypted key.

[0123] The above-mentioned apparatus embodiments correspond to the method embodiments. For detailed descriptions, references can be made to the descriptions of the method embodiments,
10 and details are omitted here for simplicity. The apparatus embodiments are obtained based on the corresponding method embodiments, and have the same technical effects as the corresponding method embodiments. For detailed descriptions, references can be made to the corresponding method embodiments.

[0124] Some embodiments of this specification further provide a computer-readable storage
15 medium. The computer-readable storage medium stores a computer program, and when the computer program is executed on a computer, the computer is enabled to perform the terminal device-side account opening method provided in this specification.

[0125] Some embodiments of this specification further provide a computing device, including a memory and a processor. The memory stores executable code, and when executing the executable
20 code, the processor implements the terminal device-side account opening method provided in this specification.

[0126] Some embodiments of this specification further provide a computer-readable storage medium. The computer-readable storage medium stores a computer program, and when the computer program is executed on a computer, the computer is enabled to perform the server-side
25 account opening method provided in this specification.

[0127] Some embodiments of this specification further provide a computing device, including a memory and a processor. The memory stores executable code, and when executing the executable code, the processor implements the server-side account opening method provided in this specification.

[0128] The embodiments of this specification are described in a progressive way. For same or
30 similar parts of the embodiments, mutual references can be made to the embodiments. Each embodiment focuses on a difference from other embodiments. Particularly, storage medium embodiments and computing device embodiments are basically similar to the method embodiments, and therefore are described briefly. For related descriptions, references can be made
35 to the descriptions in the method embodiments.

[0129] A person skilled in the art should be aware that in the above-mentioned one or more examples, functions described in the embodiments of this specification can be implemented by hardware, software, firmware, or any combination thereof. When being implemented by software, these functions can be stored in a computer-readable medium or transmitted as one or more instructions or codes in the computer-readable medium.

[0130] The objectives, technical solutions, and beneficial effects of the embodiments of this specification have been described in more detail with reference to the above-mentioned specific implementations. It should be understood that the above-mentioned descriptions are merely specific implementations of the embodiments of this specification and are not intended to limit the protection scope of this specification. Any modification, equivalent replacement, improvement, etc. made based on the technical solutions of this specification shall fall within the protection scope of this specification.

CLAIMS

What is claimed is:

1. An account opening method, applied to a terminal device, wherein the terminal device comprises a trusted execution environment (TEE) and an encryption hardware-based secure element, and the method comprises:
 - obtaining a user public key of a current user in the TEE;
 - signing the user public key in the TEE by using a predetermined manufacturer private key, to obtain a user certificate;
 - signing opening information in the secure element by using a user private key corresponding to the user public key, wherein the opening information is generated based on device information of the terminal device;
 - generating an opening request in the TEE based on at least the user certificate and signed opening information; and
 - in the TEE, generating an opening request packet based on the opening request, and sending the opening request packet to a server that opens an account, so that the server opens an account for the current user based on the opening request packet.
2. The method according to claim 1, wherein the obtaining a user public key of a current user comprises:
 - generating a corresponding user public/private key pair in the TEE by using a device public/private key pair generated in advance and a user identifier of the current user, wherein the user public/private key pair comprises the user public key and the user private key corresponding to the user public key.
3. The method according to claim 1, wherein the generating an opening request comprises:
 - obtaining a manufacturer digital certificate, wherein the manufacturer digital certificate comprises a manufacturer public key corresponding to the manufacturer private key; and
 - generating the opening request based on the user certificate, the manufacturer digital certificate, and the signed opening information.
4. The method according to any one of claims 1 to 3, wherein the generating an opening request packet based on the opening request comprises:
 - encrypting the opening request in the TEE by using a symmetric key, to obtain an encrypted opening request;
 - encrypting the symmetric key by using a server public key of the server, to obtain a first encrypted key after encryption; and
 - generating the opening request packet based on the encrypted opening request and the

first encrypted key.

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

randomly generating the symmetric key by using a predetermined random key generation method.

5 6. The method according to claim 4, further comprising:

obtaining a predetermined server public key agreed upon with the server from the TEE; or

obtaining the server public key from the server by using a predetermined key negotiation algorithm.

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

10 obtaining an opening reply packet that is fed back by the server based on the opening request packet; and

opening an account based on the opening reply packet.

8. The method according to claim 7, wherein the opening reply packet comprises an opening reply ciphertext encrypted by using the symmetric key and a second encrypted key obtained by
15 encrypting the symmetric key by using a server private key corresponding to the server public key; and

the opening an account based on the opening reply packet comprises:

decrypting the second encrypted key by using the server public key, to obtain a symmetric
key;

20 when it is determined that the symmetric key obtained through decryption is the same as the symmetric key generated in advance in the TEE, decrypting the opening reply ciphertext by using the symmetric key, to obtain an opening reply plaintext; and

opening an account based on the opening reply plaintext.

9. An account opening method, applied to a server, and comprising:

25 receiving an opening request packet sent by a terminal device based on a current user, wherein the opening request packet comprises an opening request, the opening request comprises a user certificate and signed opening information, the user certificate is obtained by signing a user public key of the current user by using a manufacturer private key predetermined in the terminal device, the signed opening information is obtained by signing opening information by using a user private
30 key corresponding to the current user, and the opening information is generated based on device information of the terminal device;

performing first verification on the user certificate by using a manufacturer public key corresponding to the manufacturer private key;

35 if the first verification is passed, performing second verification on the signed opening information by using the user public key in the user certificate; and

if the second verification is passed, determining an opening reply packet by using the device information in the opening information, and sending the opening reply packet to the terminal device, so that the terminal device opens an account based on the opening reply packet.

10. The method according to claim 9, wherein the opening request further comprises a
5 manufacturer digital certificate, and the manufacturer digital certificate comprises the manufacturer public key corresponding to the manufacturer private key; and

the performing first verification on the user certificate comprises:

performing third verification on the manufacturer digital certificate by using an obtained
manufacturer root public key; and

10 if the third verification is passed, performing first verification on the user certificate by using the manufacturer public key.

11. The method according to claim 9 or 10, wherein the opening request is an encrypted opening request obtained through encryption by using a symmetric key, and the opening request packet further comprises a first encrypted key obtained by encrypting the symmetric key by using
15 a server public key; and

before the performing first verification on the user certificate, the method further comprises:

decrypting the first encrypted key by using a server private key corresponding to the server public key, to obtain the symmetric key; and

20 decrypting the encrypted opening request by using the symmetric key, to obtain an opening request plaintext.

12. The method according to claim 11, wherein the determining an opening reply packet by using the device information in the opening information comprises:

determining an opening reply by using the device information;

25 encrypting the opening reply by using the symmetric key, to obtain an opening reply ciphertext;

encrypting the symmetric key by using the server private key, to obtain a second encrypted key after encryption; and

forming the opening reply packet based on the opening reply ciphertext and the second encrypted key.

30 13. An account opening system, wherein the account opening system comprises a terminal device and a server;

the terminal device is configured to perform the method according to any one of claims 1 to 8; and

the server is configured to perform the method according to any one of claims 9 to 12.

35 14. An account opening apparatus, applied to a terminal device, wherein the terminal device

comprises a trusted execution environment (TEE) and an encryption hardware-based secure element, and the apparatus comprises:

a first acquisition module, configured to obtain a user public key of a current user in the TEE;

5 a first signature module, configured to sign the user public key in the TEE by using a predetermined manufacturer private key, to obtain a user certificate;

a second signature module, configured to sign opening information in the secure element by using a user private key corresponding to the user public key, wherein the opening information is generated based on device information of the terminal device;

10 a request generation module, configured to generate an opening request in the TEE based on at least the user certificate and signed opening information; and

a generating and sending module, configured to: in the TEE, generate an opening request packet based on the opening request, and send the opening request packet to a server that opens an account, so that the server opens an account for the current user based on the opening request packet.

15 15. An account opening apparatus, applied to a server, and comprising:

a packet receiving module, configured to receive an opening request packet sent by a terminal device based on a current user, wherein the opening request packet comprises an opening request, the opening request comprises a user certificate and signed opening information, the user certificate is obtained by signing a user public key of the current user by using a manufacturer private key predetermined in the terminal device, the signed opening information is obtained by signing opening information by using a user private key corresponding to the current user, and the opening information is generated based on device information of the terminal device;

20 a first verification module, configured to perform first verification on the user certificate by using a manufacturer public key corresponding to the manufacturer private key;

25 a second verification module, configured to: if the first verification is passed, perform second verification on the signed opening information by using the user public key in the user certificate; and

30 a determining and sending module, configured to: if the second verification is passed, determine an opening reply packet by using the device information in the opening information, and send the opening reply packet to the terminal device, so that the terminal device opens an account based on the opening reply packet.

16. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and when executing the executable code, the processor implements the method according to any one of claims 1 to 8.

35 17. A computing device, comprising a memory and a processor, wherein the memory stores

executable code, and when executing the executable code, the processor implements the method according to any one of claims 9 to 12.