

CLAIMS

1. A key security management system, comprising:

a security host, configured to receive a first operation request, verify the first operation request, and generate a second operation request based on the first operation request when the verification is passed, wherein the first operation request and the second operation request both comprise an identification; ~~and~~

a hardware security device, configured to receive the second operation request from the security host, verify the second operation request, parse the second operation request to obtain a type of the second operation request when the verification is passed, and perform an operation related to a key pair associated with the identification based on the type of the second operation request, wherein the key pair comprises a public key and a private key specific to the identification, wherein the identification comprises an identification of a user and an identification of an organization associated with the user, and the key security management system stores a master root key pair of the organization, wherein performing an operation related to the key pair associated with the identification based on the type of the second operation request comprises:

in response to that the type of the second operation request is a request for acquiring a public key of the user, determining the master root key pair of the organization according to the identification of the organization;

determining a key pair generation path of the user based on the identification of the user and a hierarchical deterministic rule;

deriving a key pair of the user based on the key pair generation path of the user and the master root key pair of the organization; and

sending the public key in the key pair of the user to the security host.

~~2. The key security management system according to claim 1, wherein the identification comprises an identification of an organization;~~

wherein performing an operation related to a key pair associated with the identification based on the type of the second operation request comprises:

in response to that the type of the second operation request is a request for generating a master root key pair of the organization, generating a random key seed and using the key seed to generate the master root key pair of the organization.

3. The key security management system according to claim 2, wherein after using the key seed to generate the master root key pair of the organization, the hardware security device is further configured to:

store the master root key pair of the organization; and

destroy the key seed.

4. The key security management system according to claim 1, wherein the identification comprises an identification of a user and an identification of an organization associated with the user, and the key security management system stores a master root key pair of the organization,

wherein performing an operation related to a key pair associated with the identification based on the type of the second operation request comprises:

in response to that the type of the second operation request is a request for acquiring a public key of the user, determining the master root key pair of the organization according to the identification of the organization;

determining a key pair generation path of the user based on the identification of the user and a hierarchical deterministic rule;

deriving a key pair of the user based on the key pair generation path of the user and the master root key pair of the organization; and

sending the public key in the key pair of the user to the security host.

52. The key security management system, according to claim 1, comprising:

a security host, configured to receive a first operation request, verify the first operation request, and generate a second operation request based on the first operation request when the

verification is passed, wherein the first operation request and the second operation request both comprise an identification;

a hardware security device, configured to receive the second operation request from the security host, verify the second operation request, parse the second operation request to obtain a type of the second operation request when the verification is passed, and perform an operation related to a key pair associated with the identification based on the type of the second operation request, wherein the key pair comprises a public key and a private key specific to the identification,

wherein the identification comprises an identification of a user and an identification of an organization associated with the user, the hardware security device stores a master root key pair of the organization, and the second operation request further comprises to-be-signed data of the user,

wherein performing an operation related to ~~a~~ the key pair associated with the identification based on the type of the second operation request comprises:

in response to that the type of the second operation request is a request for signing the to-be-signed data, determining the master root key pair of the organization according to the identification of the organization;

determining a key pair generation path of the user based on the identification of the user and a hierarchical deterministic rule;

deriving a key pair of the user based on the key pair generation path of the user and the master root key pair of the organization;

signing the to-be-signed data using a private key in the key pair of the user to obtain signed data; and

sending the signed data to the security host.

63. The key security management system according to claim 41 or 52, wherein determining ~~at~~the key pair generation path of the user based on the identification of the user comprises:

performing a hash operation on a combination of the identification of the user and the identification of the organization to obtain a hash value; and

determining the key pair generation path of the user based on the hash value and the hierarchical deterministic rule.

7.4. The key security management system according to claim 25, wherein after signing the to-be-signed data using the private key in the key pair of the user, the hardware security device is further configured to:

destroy the private key in the key pair of the user.

8.5. The key security management system according to claim 1, wherein the key security management system further comprises:

an application server, configured to generate the first operation request according to a request of an external node, and send the first operation request to the security host,

wherein the hardware security device is located in the same security network domain as the security host, so that the security host serves as a gateway through which the application server accesses the hardware security device.

9.6. The key security management system according to claim 45, wherein verifying the first operation request comprises:

parsing the first operation request to acquire an application server certificate and an application server signature comprised therein, wherein the application server certificate comprises an identification of the application server, a list of allowed service types of the application server, and a validity period of the application server certificate;

decrypting the application server signature using a public key of the application server, so as to acquire a service type requested by the first operation request;

comparing the service type requested by the first operation request with the list of allowed service types comprised in the application server certificate to determine whether the service type requested by the first operation request is allowed;

verifying whether the application server certificate is within the validity period of the application server certificate; and

acquiring a state of the application server certificate from a blockchain to verify the state of the application server certificate.

10 7. The key security management system according to claim 1, wherein verifying the second operation request comprises:

5 parsing the second operation request to acquire a security host certificate and a security host signature comprised therein, wherein the security host certificate comprises an identification of the security host, a list of allowed service types of the security host, and a validity period of the security host certificate;

decrypted the security host signature using a public key of the security host to determine
10 whether the second operation request is signed by the security host; and

verifying whether the security host certificate is within the validity period of the security host certificate.

11 8. A key security management method, comprising:

receiving, by a security host, a first operation request;

15 verifying, by the security host, the first operation request, and generating, by the security host, a second operation request based on the first operation request when the verification is passed, wherein the first operation request and the second operation request both comprise an identification;

receiving, by ~~the~~ a hardware security device, the second operation request from the security
20 host, verifying, by the hardware security device, the second operation request, and parsing, by the hardware security device, the second operation request to obtain a type of the second operation request when the verification is passed; ~~and~~

performing, by the hardware security device, an operation related to a key pair associated with the identification based on the type of the second operation request, wherein the key pair comprises
25 a public key and a private key specific to the identification, wherein the identification comprises

an identification of a user and an identification of an organization associated with the user, and the hardware security device stores a master root key pair of the organization,

wherein performing an operation related to the key pair associated with the identification based on the type of the second operation request comprises:

5 in response to that the type of the second operation request is a request for acquiring a public key of the user, determining the master root key pair of the organization according to the identification of the organization;

determining a key pair generation path of the user based on the identification of the user and a hierarchical deterministic rule;

10 deriving a key pair of the user based on the key pair generation path of the user and the master root key pair of the organization; and

sending the public key in the key pair of the user to the security host.

12. ~~The method according to claim 11, wherein the identification comprises an identification of an organization,~~

~~wherein performing an operation related to a key pair associated with the identification based on the type of the second operation request comprises:~~

15 ~~in response to that the type of the second operation request is a request for generating a master root key pair of the organization, generating a random key seed and using the key seed to generate~~
20 ~~the master root key pair of the organization.~~

13. ~~The method according to claim 12, wherein after using the key seed to generate the master root key pair of the organization, the method further comprises:~~

~~storing the master root key pair of the organization; and~~

~~destroying the key seed.~~

14. ~~The method according to claim 11, wherein the identification comprises an identification of a user and an identification of an organization associated with the user, and the hardware security device stores a master root key pair of the organization;~~

~~wherein performing an operation related to a key pair associated with the identification based on the type of the second operation request comprises:~~

~~in response to that the type of the second operation request is a request for acquiring a public key of the user, determining the master root key pair of the organization according to the identification of the organization;~~

~~determining a key pair generation path of the user based on the identification of the user and a hierarchical deterministic rule;~~

~~deriving a key pair of the user based on the key pair generation path of the user and the master root key pair of the organization; and~~

~~sending the public key in the key pair of the user to the security host.~~

159. The A key security management method according to claim 11, comprising:

receiving, by a security host, a first operation request;

verifying, by the security host, the first operation request, and generating, by the security host, a second operation request based on the first operation request when the verification is passed, wherein the first operation request and the second operation request both comprise an identification;

receiving, by the hardware security device, the second operation request from the security host, verifying, by the hardware security device, the second operation request, and parsing, by the hardware security device, the second operation request to obtain a type of the second operation request when the verification is passed; and

performing, by the hardware security device, an operation related to a key pair associated with the identification based on the type of the second operation request, wherein the key pair comprises a public key and a private key specific to the identification, wherein the identification comprises

an identification of a user and an identification of an organization associated with the user, the hardware security device stores a master root key pair of the organization, and the second operation request further comprises to-be-signed data of the user,

wherein performing an operation related to ~~a~~ the key pair associated with the identification based on the type of the second operation request comprises:

in response to that the type of the second operation request is a request for signing the to-be-signed data, determining the master root key pair of the organization according to the identification of the organization;

determining a key pair generation path of the user based on the identification of the user and a hierarchical deterministic rule;

deriving a key pair of the user based on the key pair generation path of the user and the master root key pair of the organization;

signing the to-be-signed data using a private key in the key pair of the user to obtain signed data; and

sending the signed data to the security host.

~~16~~10. The method according to claim ~~14~~8 or ~~15~~9, wherein determining ~~a~~ the key pair generation path of the user based on the identification of the user comprises:

performing a hash operation on a combination of the identification of the user and the identification of the organization to obtain a hash value; and

determining the key pair generation path of the user based on the hash value and the hierarchical deterministic rule.

~~17~~11. The method according to claim ~~15~~9, wherein after signing the to-be-signed data using the private key in the key pair of the user, the method comprises:

destroying the private key in the key pair of the user.

~~18~~12. The method according to claim ~~14~~8, wherein receiving ~~a~~ the first operation request comprises:

receiving, by the security host, the first operation request from an application server, wherein the hardware security device is located in the same security network domain as the security host, so that the security host serves as a gateway through which the application server accesses the hardware security device.

5 ~~19~~13. The method according to claim ~~11~~12, wherein verifying the first operation request comprises:

 parsing the first operation request to acquire an application server certificate and an application server signature comprised therein, wherein the application server certificate comprises an identification of the application server, a list of allowed service types of the application server,
10 and a validity period of the application server certificate;

 decrypting the application server signature using a public key of the application server, so as to acquire a service type requested by the first operation request;

 comparing the service type requested by the first operation request with the list of allowed service types comprised in the application server certificate to determine whether the service type
15 requested by the first operation request is allowed;

 verifying whether the application server certificate is within the validity period of the application server certificate; and

 acquiring a state of the application server certificate from a blockchain to verify the state of the application server certificate.

20 ~~20~~14. The method according to claim ~~11~~8, wherein verifying the second operation request comprises:

 parsing the second operation request to acquire a security host certificate and a security host signature comprised therein, wherein the security host certificate comprises an identification of the security host, a list of allowed service types of the security host, and a validity period of the security
25 host certificate;

decrypting the security host signature using a public key of the security host to determine whether the second operation request is signed by the security host; and

verifying whether the security host certificate is within the validity period of the security host certificate.

5 ~~21~~15. A non-volatile computer-readable storage medium having machine-executable instructions stored thereon, wherein the machine-executable instructions, when executed by a computer, perform the method according to any one of claims ~~11~~8 to ~~14~~20.

~~22~~16. A computer program comprising machine-executable instructions that, when executed, perform the method according to any one of claims ~~11~~8 to ~~14~~20.