

CLAIMS

1. A key management method, comprising:

acquiring, when a key request of a service system is detected, an attribute of the service system, and acquiring a key rule corresponding to the service system on the basis of the attribute;

dynamically acquiring a key on the basis of the key rule; and

sending the key to the corresponding service system, thus allowing the service system to encrypt to-be-transmitted information of the service system according to the key;

wherein the key rule includes a key algorithm, the key management method is applied to a key storage library, and the step of dynamically acquiring a key on the basis of the key rule comprises:

detecting whether there is, in the key storage library, a key storage sub-library matching the key rule on the basis of the key rule; and

when there is no key storage sub-library matching the key rule, calling the key algorithm to generate a key with a preset validity and a preset key length on the basis of the key rule; and

when there is a key storage sub-library matching the key rule, dynamically acquiring a key corresponding to the key rule from the key storage sub-library.

2. The key management method according to Claim 1, wherein the step of acquiring an attribute of the service system and acquiring a key rule corresponding to the service system on the basis of the attribute comprises:

acquiring a type of the service system, and acquiring configuration information corresponding to the to-be-transmitted information on the basis of the type of the service system; and

acquiring the key rule corresponding to the service system on the basis of the configuration information of the to-be-transmitted information.

3. The key management method according to Claim 1, wherein the step of dynamically acquiring a key corresponding to the key rule from the key storage sub-library comprises:

acquiring validity information of all keys in the key storage sub-library; and

acquiring keys with a preset validity on the basis of the validity information, and dynamically selecting the key corresponding to the key rule from the keys with the preset validity.

4. The key management method according to Claim 3, wherein the key management method further comprises:

acquiring validity information of all keys in the key storage sub-library every a preset period of time; and

when any key without the preset validity is detected, deleting or disabling the key without the preset validity.

5. The key management method according to Claim 1, wherein the step of acquiring, when a key request of a service system is detected, an attribute of the service system comprises:

carrying out identity authentication on the service system when the key request of the service system is detected; and

acquiring the attribute of the service system when the identity authentication succeeds.

6. The key management method according to Claim 1, wherein the method further comprises the following step to be performed after the step of sending the key to the corresponding service system, thus allowing the service system to encrypt to-be-transmitted information of the service system according to the key:

saving an associated record of the key sent to the corresponding service system and the service system for subsequent queries.

7. A key management device, comprising a memory, a processor, a communication bus, and a key management program stored in the memory, wherein:

the communication bus is used for establishing a communication connection between the processor and the memory; and

the processor is used for executing the key management program to implement the steps of the key management method according to Claim 1.

8. A key management device, comprising a memory, a processor, a communication bus, and a key management program stored in the memory, wherein:

the communication bus is used for establishing a communication connection between the processor and the memory; and

the processor is used for executing the key management program to implement the steps of the key management method according to Claim 2.

9. A key management device, comprising a memory, a processor, a communication bus, and a key management program stored in the memory, wherein:

the communication bus is used for establishing a communication connection between the processor and the memory; and

the processor is used for executing the key management program to implement the steps of the key management method according to Claim 3.

10. A key management device, comprising a memory, a processor, a communication bus, and a key management program stored in the memory, wherein:

the communication bus is used for establishing a communication connection between the processor and the memory; and the processor is used for executing the key management program to implement the steps of the key management method according to Claim 4.

11. A readable storage medium, having a key management program stored therein, wherein the key management program is executed by a processor to implement the steps of the key management method according to Claim 1.

12. A readable storage medium, having a key management program stored 5 therein, wherein the key management program is executed by a processor to implement the steps of the key management method according to Claim 2.

13. A readable storage medium, having a key management program stored therein, wherein the key management program is executed by a processor to implement the steps of the key management method according to Claim 3.

14. A readable storage medium, having a key management program stored therein, wherein the key management program is executed by a processor to implement the steps of the key management method according to Claim 4.