

KEY MANAGEMENT METHOD, DEVICE AND READABLE STORAGE MEDIUM

This application claims priority for Chinese Patent Application submitted to the National
5 Intellectual Property Administration, PRC on August 24, 2017, Application No. 201710741118.3,
and titled “Key Management Method and Device, and Readable Storage Medium”, with all its
contents hereby incorporated by reference.

TECHNICAL FIELD

This application belongs to the field of keys, in particular to a key management method and
10 device, and a readable storage medium.

BACKGROUND

At present, in order to guarantee the security during network information transmission of service
systems, to-be-transmitted information of the service systems needs to be encrypted by keys.
However, when to-be-transmitted information is encrypted in the prior art, keys are manually
15 imported into local configuration files of the service systems by means of traditional media such as
USB flash disks, which cannot guarantee the security of the keys and may lead to complex operations
and low efficiency; and leakage of the keys may be caused by the loss of the local configuration files.

SUMMARY

The main objective of this application is to provide a key management method and device, and a
20 readable storage medium to solve the technical problems that during network information
transmission of existing service systems, keys are prone to leak and the security performance is low.

To fulfill the above objective, this application provides a key management method. The key
management method comprises:

Acquiring, when a key request of a service system is detected, an attribute of the service system,
25 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.

Optionally, 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:

5 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.

10 Optionally, 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.

15 Optionally, the method further comprises the following step to be performed after the step of 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:

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.

20 Optionally, 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.

25 Optionally, 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.

Optionally, 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
5 system is detected; and

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

Optionally, 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:

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

Furthermore, in order to fulfill the above objective, this application further provides a key management device. The key management device comprises a memory, a processor, a communication bus, and a key management program stored in the memory.

15 The communication bus is used for establishing a communication connection between the processor and the memory.

The processor is used for executing a backlight adjustment program to implement the following steps:

Acquiring, when a key request of a service system is detected, an attribute of the service system,
20 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.

Optionally, the step of acquiring an attribute of the service system and acquiring a key rule
25 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.

Optionally, 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:

5 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.

10 Optionally, the method further comprises following step to be performed after the step of 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:

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.

15 Optionally, 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.

Optionally, the key management method further comprises:

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

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

25 Optionally, 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.

Optionally, 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.

Furthermore, in order to fulfill the above objective, this application further provides a readable storage medium. One or more programs are stored in the readable storage medium and are executed by one or more processors to implement the following steps:

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 secret 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.

According to this application, when a key request of a service system is detected, an attribute of the service system is acquired, and a key rule corresponding to the service system is acquired on the basis of the attribute; a key is dynamically acquired on the basis of the key rule; and the key is sent to the corresponding service system to allow the service system to encrypt to-be-transmitted information of the service system according to the key. In this application, when a key request of a service system is detected, the key management system acquires a key on the basis of the request and sends the key to different service systems to allow the service systems to encrypt to-be-transmitted information of the service systems according to the key, so that key leakage at the service systems is effectively avoided; and the calling party (the service systems) does not sense or decrypt the key in this process, so that the technical problem that during the network information transmission of existing service systems, the key is prone to leak and the security performance is low is solved.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a flow diagram of a first embodiment of a key management method of this application;

FIG. 2 is a flow diagram of a second embodiment of the key management method of this application;

FIG. 3 is a device structural diagram of a hardware operating environment involved in the method of this application;

FIG. 4 is a scene diagram involved in the method of this application.

The realization of the objectives of this application, and the functional characteristics and advantages of this application are further explained below with reference to the accompanying drawings.

DESCRIPTION OF EMBODIMENTS

It should be understood that the embodiments described herein are only used for explaining this application, and are not intended to limit this application.

This application provides a key management method. Referring to FIG. 1, in a first embodiment of the key management method of this application, the key management method comprises:

S10: when a key request of a service system is detected, an attribute of the service system is acquired, and a key rule corresponding to the service system is acquired on the basis of the attribute.

In this application, a key management system is used for unified management of keys of all systems, such as centralized generation of different keys, secure storage of keys, and distribution of keys to corresponding service systems. As shown in FIG. 4, the key management system communicates with the service systems via a key service interface. In addition, the key management system realizes full-life-cycle management such as updating, storage, cancelling and usage of the generated keys and has a monitoring function to generate anomaly notification or early warning when the keys are abnormal.

Keys have key attributes which include preset validity information, length information and the like of the keys. In addition, the keys are presented in pairs, that is to say, the keys include symmetric keys and asymmetric keys, wherein each pair of asymmetric keys includes a public key used for encryption and a private key used for decryption. For example, as for the asymmetric keys, to-be-transmitted information sent from a transmitting terminal of a service system is encrypted by means of the public key and is then sent to a receiving terminal, the receiving terminal decrypts the transmitted information received on the basis of the private key. Namely, in this application, after acquiring asymmetric keys sent from the key management system, the service system acquires a

receiving terminal and a transmitting terminal of a to-be-handled service, sends the public key in the asymmetric keys to the transmitting terminal to allow the transmitting terminal to encrypt to-be-transmitted information on the basis of the public key, and sends the private key to the receiving terminal to allow the receiving terminal to decrypt the transmitted information received on the basis of the private key.

In the case where the keys are symmetric keys, the asymmetric keys are private keys. Namely, after acquiring the private keys sent from the key management system, the service system sends the identical private keys to a corresponding transmitting terminal and a corresponding receiving terminal respectively, so that the transmitting terminal encrypts to-be-transmitted information by means of one private key, and the receiving terminal decrypts the transmitted information received by means of the other private key. In addition, if the service system has multiple to-be-handled services before sending the private keys to the corresponding transmitting terminal and the corresponding receiving terminal, different keys are sent according to key requests corresponding to the to-be-handled services.

When the key request of the service system is detected, the attribute of the service system is acquired, wherein the service system sends the key request regularly or when there is a service to be handled, and the key management system receives the key request via a key service interface; keys are generated on the basis of a key generation strategy or algorithm and are then sent to the service system regularly, or keys are generated in real time and are then sent to the service system; and as shown in FIG. 4, before the keys are sent to the service system, the key management system acquires the attribute of the service system and then acquires a key rule corresponding to the service system on the basis of the attribute.

Wherein, as shown in FIG. 2, the step of acquiring the attribute of the service system and acquiring the key rule corresponding to the service system on the basis of the attribute comprises:

S11: a type of the service system is acquired, and configuration information corresponding to the to-be-transmitted information is acquired on the basis of the type of the service system.

The attribute of the service system includes the type of the service system. Different types of service systems require different key attributes. The key attribute include the key type, for instance,

public keys and private keys are different types of keys. Particularly, when public keys are used for encryption, a larger key space (the range of possible values of keys) can be realized; however, when the public keys are used for encrypting a mass of data, the time of an encryption process will be excessively long. On the contrary, the range of possible values of the private keys is narrow, and encryption can be completed within a short time; however, the private keys may be cracked due to exhaustion. In view of this, the to-be-transmitted information is encrypted by means of a public key or a private key according to the type of a to-be-handled service of the service system. Generally, when the to-be-handled service of the service system involves to-be-transmitted information containing a mass of data, a private key is used for encrypting the to-be-transmitted information to prevent a time delay of the transmission process; and when the to-be-handled service of the service system involves to-be-transmitted information containing a small amount of data, a public key is used for encrypting the to-be-transmitted information.

In addition, different types of service systems are used for handling different to-be-handled services which correspond to different types of to-be-transmitted information, and accordingly, different types of key rule information are required, wherein the key rule information required by the to-be-handled service is read from the configuration information of the to-be-handled service, that is to say, after the type of the service system is acquired, the configuration information of the corresponding to-be-transmitted information of this type of service system is acquired so as to acquire a corresponding key rule.

S12: the key rule corresponding to the service system is acquired on the basis of the configuration information of the to-be-transmitted information.

In this application, the configuration information includes key length demand information, key validity demand information, key encryption rule information, and the like. Acquisition of the key rule corresponding to the service system on the basis of the configuration information of the to-be-transmitted information refers to reading the key rule corresponding to the service system from the configuration information of the this type of to-be-transmitted information, wherein the key rule includes a key length rule, a key algorithm rule, and the like.

S20: a key is dynamically acquired on the basis of the key rule.

After the key rule corresponding to the service system is acquired, a key is dynamically acquired or generated on the basis of the key rule. In this acquisition process, one key is randomly selected from multiple keys conforming to the key rule. That is, keys are generated by the key management system in advance and are respectively stored in different key storage sub-libraries according to different attributes of the keys, and in the case where multiple keys conform to the key rule, the corresponding key is randomly selected from the multiple keys. In addition, in the process of dynamically generating the key on the basis of the key rule, binary codes 0 and 1 are combined in order according to the key rule to obtain the key conforming to the key rule; or the key is generated in real time according to the key rule.

S30: the key is sent to the corresponding service system to allow the service system to encrypt the to-be-transmitted information of the service system according to the key.

Particularly, in one embodiment, the step of sending the key to the corresponding service system to allow the service system to encrypt the to-be-transmitted information of the service system according to the key is explained as follows: when the service system is an A mail service system, the key management system acquires an attribute of the A mail service system and correspondingly generates an A-type key corresponding to this service system, then address information of the A mail service system is acquired, the A-type key is sent to the corresponding A mail service system on the basis of the address information, the A mail service system randomly distributes the A-type key to a to-be-sent mail and encrypts the to-be-sent mail, and in this process, the A mail service system does not sense or decrypt the key. In addition, there may be a key conforming to the attribute or demand of the A mail service system in a key storage library of the key management system; and if there is an A-type key in the key storage library, the A-type key is selected and sent to the service system.

According to this application, when a key request of a service system is detected, an attribute of the service system is acquired, and a key rule corresponding to the service system is acquired on the basis of the attribute; a key is dynamically acquired on the basis of the key rule; and the key is sent to the corresponding service system to allow the service system to encrypt to-be-transmitted information of the service system according to the key. In this application, when a key request of a service system is detected, the key management system acquires a key on the basis of the request and

sends the key to different service systems to allow the service systems to encrypt to-be-transmitted information of the service systems according to the key, so that key leakage at the service systems is effectively avoided; and the calling party (the service systems) does not sense or decrypt the key in this process, so that the technical problem that during the network information transmission of existing service systems, the key is prone to leak and the security performance is low is solved.

Furthermore, on the basis of the first embodiment of the key management method of this application, a second embodiment of the key management method is provided. In the second embodiment, the key rule includes a key algorithm. The key management method is applied to a key storage library. In this case, the step of dynamically acquiring a key on the basis of the key rule comprises:

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

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

Whether there is, in the key storage library, a key storage sub-library matching the key rule is detected on the basis of the key rule, wherein key rules such as length information, composition information and algorithm information of keys stored in key storage sub-libraries are pre-stored in the corresponding interface configuration of the key storage sub-libraries, or key rules corresponding to the key storage sub-libraries are stored in a configuration file set of the key management system; the key rule corresponding to the service system is compared with the key rules corresponding to the key storage sub-libraries in the key management system; when the key rule corresponding to the service system is inconstant with the key rules corresponding to the key storage sub-libraries in the key management system, matching fails, and a key needs to be generated in real time, that is, the key algorithm is called to generate a key with a preset validity and a preset key length on the basis of the key rule, wherein the key algorithm is an algorithm for public keys or an algorithm for private keys and is input to the key management system in advance; and after the key is generated in real time, a key storage sub-library matching the key is established, and the corresponding key is stored in the key storage sub-library. In addition, when the key management system detects that the key rule

corresponding to the service system is updated, a key is generated on the basis of the updated key rule and is sent to the service system.

In this embodiment, whether there is, in the key storage library, a key storage sub-library matching the key rule is detected on the basis of the key rule; and when there is no matching key storage sub-library, the key algorithm is called to generate a key with a preset validity and a preset key length on the basis of the key rule. The key management system is able to generate the key corresponding to the service system in real time, and the service system does not sense or decrypt the key in this process, so that user experience is further improved.

Furthermore, on the basis of the second embodiment of the key management method of this application, a third embodiment of the key management method is provided. In the third embodiment, the method further comprises the following step to be performed after the step of detecting whether there is, in the key storage library, a key storage sub-library matching the key rule:

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

The step of dynamically acquiring a key corresponding to the key rule from the key storage sub-library comprises:

Validity information of all keys in the key storage sub-library is acquired; and

Keys with a preset validity are acquired on the basis of the validity information, and a key corresponding to the key rule is dynamically selected from the keys with the preset validity.

When there is a matching key storage sub-library, a corresponding key is dynamically acquired from the key storage sub-library. Particularly, due to the validity of keys, validity information of all keys in the key storage sub-library is acquired, wherein the keys in the key storage sub-library are stored in batches in advance according to the validities of the keys; and keys with a preset validity are acquired on the basis of the validity information, and the corresponding key is dynamically selected from the keys with the preset validity, wherein dynamical selection may refer to random extraction of a preset number of keys, and then the preset number of extracted keys are sent to the service system.

In this embodiment, when there is a matching key storage sub-library, the corresponding key is dynamically acquired from the key storage sub-library. Wherein, the step of dynamically acquiring

the corresponding key from the key storage sub-library comprises: validity information of all keys in the key storage sub-library is acquired; and keys with a preset validity are acquired on the basis of the validity information, and the corresponding key is dynamically selected from the keys with the preset validity. In this application, the keys with the preset validity are acquired, so that delayed
5 transmission of the to-be-transmitted information of the service system caused by key invalidity are effectively avoided, and user experience is further improved.

Furthermore, on the basis of the first embodiment of the key management method, a fourth embodiment of the key management method is provided. In the fourth embodiment, the key management method further comprises:

10 Validity information of all keys in the key storage sub-library is acquired every a preset period of time; and

When any key without the preset validity is detected, the key without the preset validity is deleted or disabled.

The key management system acquires validity information of all keys in the key storage
15 sub-library every a preset period of time, wherein the keys in the key storage sub-library are stored in batches in advance according to the validities of the keys; and when any key without the preset validity is detected, the key without the preset validity is deleted or disabled. For instance, if B-type keys in the key storage sub-library have a preset validity of one month and are generated in April, 2017, the B-type keys will become invalid after May, 2017; and when it is detected that the B-type
20 keys are invalid, the B-type keys are deleted or disabled.

In this embodiment, the validity information of all the keys in the key storage sub-library are acquired every a preset period of time; and when any key without the preset validity is detected, the key without the preset validity is deleted or disabled. Keys without the preset validity are detected every a preset period of time and are then deleted or disabled, so that delayed transmission of the
25 to-be-transmitted information of the service system caused by key invalidity is effectively avoided, and user experience is further improved.

Furthermore, on the basis of the fourth embodiment of the key management method of this application, a fifth embodiment of the key management method is provided. In the fifth embodiment,

when a time interval exceeds the preset time, the type of an adjustment operation is detected.

The step of acquiring, when a key request of a service system is detected, an attribute of the service system comprises:

Identity authentication is carried out on the service system when the key request of the service
5 system is detected; and

The attribute of the service system is acquired when the identity authentication succeeds.

Identity authentication is carried out on the service system when the key request of the service
system is detected, wherein the identity authentication includes permission validation, role validation
and the like; and the attribute of the service system is acquired when the identity authentication
10 succeeds; or, when the identity authentications, prompt information is generated to remind the service
system of the identity authentication failure.

In this embodiment, identity authentication is carried out on the service system when the key
request of the service system is detected, and the attribute of the service system is acquired when the
identity authentication succeeds. By means of the identity authentication carried out on the service
15 system by the key management system, the security of the key management system is effectively
improved, thus further improving user experience.

Furthermore, on the basis of the first embodiment of the key management method of this
application, a sixth embodiment of the key management method is provided. In the sixth embodiment,
the method further comprises the following step to be performed after sending the key to the
20 corresponding service system, thus allowing the service system to encrypt to-be-transmitted
information of the service system according to the key:

An associated record of the key sent to the corresponding service system and the service system
is saved for subsequent queries.

In this embodiment, an associated record of the key sent to the corresponding service system and
25 the service system is saved for subsequent queries, for example, after the key management system
sends an A-type key to an M service system, a mapping relationship between the A-type key and the
M service system is saved in the key management system.

In this embodiment, the associated record of the key sent to the corresponding service system

and the service system is saved for subsequent queries, so that user experience is further improved.

Please refer to FIG. 3 which is a device structural diagram of a hardware operating environment involved in the embodiments of the method of this application.

A key management device in the embodiment of this application is terminal device such as a PC,
5 a smartphone, a tablet computer, an e-book reader, a moving picture experts group audio player III (MP3), a moving picture experts group audio layer IV (MP4), or a portable computer.

As shown in FIG. 3, the key management device comprises a processor 1001 such as a CPU, a memory 1005, and a communication bus 1002. Wherein, the communication bus 1002 is used for establishing a communication connection between the processor 1001 and the memory 1005; the
10 memory 1005 is a high-speed RAM or a stable non-volatile memory such as a disk memory; or, the memory 1005 is a memory device independent of the processor 1001.

Optionally, the key management device further comprises a user interface, a network interface, a camera, a radio frequency (RF) circuit, a sensor, an audio circuit, a WiFi module, and the like. The user interface comprises a display and an input unit such as a keyboard. Optionally, the user interface
15 further comprises a standard wired interface or a standard wireless interface. Optionally, the network interface comprises a standard wired interface or a standard wireless interface (such as a WI-FI interface).

Those skilled in the art would appreciate that the structure of the key management device shown in FIG. 3 is not intended to limit the key management device, and the key management device may
20 comprise more or less components than the structure shown in FIG. 3, or certain components are combined, or these components are configured in different manners.

As shown in FIG. 3, an operating system, a network communication module and a key management program are stored in the memory 1005 serving as a computer storage medium. The operating system is a program used for managing and controlling hardware and software resources of
25 the key management device and supports the operation of other software and/or programs. The network communication module is used for establishing communication between all modules in the memory 1005 and communication between the key management device and other hardware and software.

In the key management device shown in FIG. 3, the processor 1001 is used for executing the key management program in the memory 1005 to implement the following steps:

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;

5 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.

Furthermore, 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:

10 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.

Furthermore, 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

20 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.

Furthermore, the method further comprises the following step to be performed after the step of 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:

25 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.

Furthermore, 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.

Furthermore, the key management method further comprises:

5 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.

Furthermore, the step of acquiring, when a key request of a service system is detected, an attribute of the service system comprises:

10 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.

15 Furthermore, 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.

20 The specific implementation of the key management device of this application is basically the same as that of the embodiments of the key management method and will not be detailed anymore herein.

This application provides a readable storage medium. One or more programs are stored in the readable storage medium and are executed by one or more processors to implement the following steps:

25 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.

Furthermore, 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

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

Furthermore, 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:

10 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.

15 Furthermore, the method further comprises the following step to be performed after the step of 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:

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.

20 Furthermore, 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.

Furthermore, the key management method further comprises:

25 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.

Furthermore, 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

5 Acquiring the attribute of the service system when the identity authentication succeeds.

Furthermore, 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:

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

The specific implementation of the readable storage medium of this application is basically the same as that of the embodiments of the key management method and will not be detailed anymore herein.

15 The above embodiments are only preferred ones of this application, and are not intended to limit the patent scope of this application. All equivalent structures or equivalent process transformations made on the basis of the contents of this specification and drawings, or direct or indirect applications to other related technical fields should also fall within the patient scope of this application.

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;

5 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.

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
10 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.

15 3. The key management method according to Claim 1, 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

20 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.

4. The key management method according to Claim 3, wherein the method further comprises
the following step to be performed after the step of 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:

25 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.

5. The key management method according to Claim 4, 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.

5 6. The key management method according to Claim 5, 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

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

7. 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

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

8. 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:

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

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

25 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.

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 2.

11. 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.

12. 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.

13. 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 5.

14. 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 6.

15. 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.

5 16. 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 2.

10 17. 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.

18. 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.

15 19. 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 5.

20. 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 6.